www.mruni.eu

Renata MARCINAUSKAITĖ

DAKTARO DISERTACIJA

Nusikalstamos veikos elektroninių duomenų ir informacinių sistemų konfidencialumui

(Lietuvos Respublikos baudžiamojo kodekso 198 ir 198[1] straipsniai)

SOCIALINIAI MOKSLAI,
TEISĖ (01 S)
VILNIUS, 2013

MYKOLO ROMERIO UNIVERSITETAS

MYKOLO ROMERIO UNIVERSITETAS

Renata Marcinauskaitė

NUSIKALSTAMOS VEIKOS ELEKTRONINIŲ DUOMENŲ IR INFORMACINIŲ SISTEMŲ KONFIDENCIALUMUI (LIETUVOS RESPUBLIKOS BAUDŽIAMOJO KODEKSO 198 IR 198^1 STRAIPSNIAI)

Daktaro disertacija
Socialiniai mokslai, teisė (01 S)

Vilnius, 2013

Disertacija rengta 2009–2013 metais Mykolo Romerio universiteto Teisės fakulteto Baudžiamosios teisės ir proceso institute.

Moksliniai vadovai:

prof. dr. Olegas Fedosiukas (Mykolo Romerio universitetas, socialiniai mokslai, teisė – 01 S), 2012–2013 metai,

doc. dr. Agnė Baranskaitė (Mykolo Romerio universitetas, socialiniai mokslai, teisė – 01 S), 2009–2012 metai.

ISBN 978-9955-19-599-3

© Mykolo Romerio universitetas, 2013

TURINYS

ĮVADAS 5

TYRIMŲ APŽVAGA 9

DARBO METODOLOGIJA 10

I. ESMINIAI NUSIKALSTAMŲ VEIKŲ, PADAROMŲ ELEKTRONINĖJE ERDVĖJE, BAUDŽIAMIEJI TEISINIAI ASPEKTAI 12
1. Terminologijos problema 12
2. Esminiai nusikalstamų veikų elektroninėje erdvėje kriminalizavimo ir aiškinimo aspektai 16
2.1. Nusikalstamų veikų elektroninėje erdvėje kriminalizavimas ir ekvivalentinio vertinimo principas 17
2.1.1. Ekvivalentinio vertinimo principo samprata ir įgyvendinimo būdai 18
2.1.2. Ekvivalentinio vertinimo principo taikymas kriminalizuojant nusikalstamas veikas elektroninėje erdvėje 20
2.2. Nusikalstamų veikų elektroninėje erdvėje požymių aiškinimas ir technologinio neutralumo principas 26
2.2.1. Technologinio neutralumo principo samprata 26
2.2.2. Technologinio neutralumo principo taikymo problemos ir galimi jų sprendimo būdai 29

II. ELEKTRONINIŲ DUOMENŲ IR INFORMACINIŲ SISTEMŲ KONFIDENCIALUMAS KAIP BAUDŽIAMOJO ĮSTATYMO SAUGOMA VERTYBĖ 36
1. Baudžiamojo įstatymo saugomos vertybės istorinė raida, jos įvardijimo įvairovė 36
2. Elektroninių duomenų ir informacinių sistemų saugumas: konfidencialumas, vientisumas ir prieinamumas 41
2.1. Elektroninių duomenų ir informacinių sistemų konfidencialumas 44

III. NETEISĖTAS PRISIJUNGIMAS PRIE INFORMACINĖS SISTEMOS (BK 198[1] straipsnis) 51
1. Neteisėto prisijungimo prie informacinės sistemos kriminalizavimo pagrindimas ir šios veikos inkriminavimo ypatumai 51
2. Objektyvieji neteisėto prisijungimo prie informacinės sistemos sudėties požymiai 57
2.1. Informacinė sistema kaip nusikalstamos veikos dalykas 58
2.2. Neteisėtas prisijungimas kaip pavojinga veika 63
2.2.1. Prisijungimo samprata 63
2.2.2. Prisijungimo neteisėtumo vertinimas 72
2.3. Informacinės sistemos apsaugos priemonių pažeidimas kaip nusikalstamos veikos padarymo būdas 84
2.4. Nusikalstamą veiką kvalifikuojančios aplinkybės 89
3. Subjektyvieji neteisėto prisijungimo prie informacinės sistemos sudėties požymiai 95

IV. NETEISĖTAS ELEKTRONINIŲ DUOMENŲ PERĖMIMAS IR PANAUDOJIMAS (BK 198 straipsnis) 99
1. Neteisėto elektroninių duomenų perėmimo ir panaudojimo kriminalizavimo pagrindimas ir inkriminavimo ypatumai 99

2. Objektyvieji neteisėto elektroninių duomenų perėmimo ir panaudojimo sudėties požymiai ... 104
2.1. Nevieši elektroniniai duomenys kaip nusikalstamos veikos dalykas ... 106
2.1.1. Elektroninių duomenų samprata ... 106
2.1.2. Elektroninių duomenų formos kitimo įtaka duomenis pripažįstant BK 198 straipsnyje esančios nusikalstamos veikos dalyku ... 113
2.1.3. Elektroninių duomenų ir informacinės sistemos ryšys ... 116
2.1.4. Neviešų elektroninių duomenų samprata ... 119
2.2. Pavojingos veikos ... 123
2.2.1. Perėmimas ... 125
2.2.2. Stebėjimas, fiksavimas ... 130
2.2.3. Įgijimas ... 135
2.2.4. Laikymas ... 138
2.2.5. Pasisavinimas ... 140
2.2.6. Paskleidimas ... 143
2.2.7. Kitoks panaudojimas ... 145
2.2.8. Pavojingų veikų neteisėtumo vertinimas ... 147
2.3. Nusikalstamą veiką kvalifikuojantys požymiai ... 150
3. Subjektyvieji neteisėto elektroninių duomenų perėmimo ir panaudojimo sudėties požymiai ... 153
V. NUSIKALSTAMŲ VEIKŲ ELEKTRONINIŲ DUOMENŲ IR INFORMACINIŲ SISTEMŲ KONFIDENCIALUMUI ATSKYRIMAS NUO PANAŠIŲ NUSIKALSTAMŲ VEIKŲ ... 156
1. Nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui tarpusavio santykis (BK 196, 198, 198[1] straipsniai) ... 157
2. Nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui (BK 198 ir 198[2] straipsniai) bei nusikalstamų veikų finansų sistemai (BK 214, 215 straipsniai) santykis ... 159
3. Neteisėto elektroninių duomenų perėmimo ir panaudojimo bei nusikaltimų privataus gyvenimo neliečiamumui santykis ... 163
IŠVADOS ... 168
PASIŪLYMAI ... 172
LITERATŪRA ... 173
PRIEDAS ... 187
SANTRAUKA ... 189
SUMMARY ... 204

ĮVADAS

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

Luciano Floridi[1]

Tiriamoji problema. Kompiuterinių informacinių technologijų ir elektroninių ryšių raida sudarė prielaidas didelės apimties įvairaus pobūdžio informacijos sklaidai, naujoms prieigos prie informacijos, taip pat jos apsikeitimo galimybėms atsirasti nacionaliniu ir tarptautiniu lygiu. Šis vienas iš globalinės transformacijos[2] aspektų atskleidė ne tik elektroninėje terpėje vykstančius teigiamus pokyčius, lemiančius ir skatinančius elektroninės erdvės naudotojų sąsają ir sąveiką, bet taip pat parodė informacinės visuomenės pažeidžiamumo problemą – viena iš elektroninėje erdvėje atsiradusių grėsmių yra joje padaromos nusikalstamos veikos. Į tokių veikų sąrašą patenka ne tik dėl naujųjų technologijų panaudojimo pakitusios tradicinės veikos, bet ir tos, kurios atsirado išimtinai kaip šių technologijų vystymosi rezultatas. Prie pastarųjų priskirtinos Lietuvos Respublikos baudžiamojo kodekso (toliau – BK) XXX skyriuje aprašytos nusikalstamos veikos elektroninių duomenų ir informacinių sistemų saugumui. Šiame darbe tiriama vienos iš jų rūšies – nusikalstamų veikų elektroninių duomenų ir informacinių sistemų konfidencialumui, numatytų BK 198 ir 198[1] straipsniuose, problematika. Ši rūšis išskirta struktūrizavus BK XXX skyriuje esančias nusikalstamas veikas: pasitelkus *CIA triadą*[3] į jas pažvelgta kaip į konfidencialumo, integralumo ir prieinamumo pažeidimus.

Technologijų pažangos ir nusikalstamų veikų padarymo galimybių sintezė rodo kiekybiškai daug ir kokybiškai naujas[4] baudžiamosios teisės problemas saugant visuomenės, kurioje pagrindinis galios ir produktyvumo šaltinis yra susijęs su sparčiu technologijomis pagrįstu informacijos apdorojimu[5], interesus elektroninėje erdvėje. Naujų pagal savo pobūdį diskusinių klausimų gausa lėmė, kad tiriant pasirinktų nusikalstamų veikų problematiką neapsiribota vien jų sudėties požymių turinio analize – į elektroninių duomenų ir informacinių sistemų konfidencialumo pažeidimus iš baudžiamosios teisės pozicijų pažvelgta plačiau. Darbe ieškota tokio pobūdžio nusikalstamų veikų ištakų, kriminalizavimo pateisinimo, galimo jų ryšio su tradicinėmis veikomis, atskyrimo nuo kitų panašių nusikalstamų veikų kriterijų. Taip pat formuluojant principines šių veikų aiškinimo pozicijas ne kartą kelti technologijų ir joms baudžiamajame įstatyme įvardyti vartojamos

---

1 Floridi, L. Open Problems in the Philosophy of Information. *Metaphilosophy*. 2004, 35(4): 554–555.

2 Kaip teigia B. Melnikas, „pasaulio, kaip nedalomos jame egzistuojančių gyvybės formų visumos, raida reiškiasi ciklišk ai vykstančiomis transformacijomis, pastarąsias suvokiant kaip esminius gyvenimo būdo pokyčius. <...> bet koks vystymąsis tegali reikštis tik vykstant kiekybiniams ir kokybiniams pokyčiams ar būti jų pasekmė, kai tam tikras gyvenimo reiškinys ar objektas įgyja *naują* jo būseną ar kokybę atspindinčių požymių“. (Melnikas, B. *Transformacijos: visuomenės pokyčiai, naujas tūkstantmetis, valdymas ir savireguliacija, Rytų ir Vidurio Europa*. Vilnius: Vaga, 2002, p. 19).

3 Plačiau apie *CIA triados* saugumo modelį ir jo taikymo galimybes, aiškinant baudžiamojo įstatymo saugomos vertybės turinį bei skirstant BK XXX skyriuje numatytas veikas, žiūrėti II dalyje.

4 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.

5 Castells, M. *Tinklaveikos visuomenės raida*. Kaunas: Poligrafija ir informatika, 2005, p. 34.

terminologijos suderinimo bei principų, suformuluotų ne baudžiamosios teisės srityje, pritaikomumo klausimai.

Darbo aktualumas, naujumas ir tyrimų rezultatų reikšmė. Sąlygos analizuoti nusikalstamas veikas elektroninių duomenų ir informacinių sistemų konfidencialumui nacionaliniu lygiu buvo sudarytos įsigaliojus 2000 metų BK[6], kai dėl technologijų pokyčių atsiradusios naujos veikos kriminalizuotos *sui generis* ir nebelaikomos kitų veikų sudedamąja dalimi. Tokių nusikalstamų veikų atsiradimas sukėlė fundamentalias teisėkūros bei baudžiamojo įstatymo normų taikymo (atitinkamai jų aiškinimo) problemas, į kurias jau atkreiptas dėmesys priėmus, bet dar neįsigaliojus 2000 metų BK. „Nors užsienio valstybių mokslininkai jau keletą metų diskutuoja apie <...> teisines problemas, susijusias su elektroninės erdvės panaudojimu, Lietuvoje pastebimos tik pradinių diskusijų apraiškos. Veikų elektroninėje erdvėje teisinio reglamentavimo ir atsakomybės pagrindų už neteisėtas veikas nustatymo (Lietuvos kontekste) klausimais nebuvo gilesnių studijų"[7] teigta tuometinėje mokslinėje literatūroje. Reikėtų pripažinti, kad praėjus bene dešimčiai metų šis teiginys tam tikra prasme išlieka vis dar aktualus – net ir sukūrus teisinius pagrindus baudžiamajai atsakomybei už tokias veikas kilti, gilesnių diskusijų dėl šių pagrindų tinkamumo praktiškai nėra. Be to, po 2000 metų baudžiamojo įstatymo įsigaliojimo praėjęs laiko tarpas 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 pakankamos, suprantamos, ar jomis buvo pasiekti norimi tikslai, koks realus jų taikymo rezultatas. Juo labiau kad teismų praktika šios kategorijos baudžiamosiose bylose yra gana chaotiška, dažni atvejai, kai konfidencialumą pažeidžiančios veikos yra neatpažįstamos, šių veikų sudėties požymiai inkriminuojami intuityviai be tvirtesnio teorinio pagrindimo. Be abejo, tokiai situacijai formuotis sąlygas sudaro *inter alia* ir nepakankama nusikalstamų veikų elektroninių duomenų ir informacinių sistemų konfidencialumui analizė doktrinos lygmeniu, diskusijų trūkumas.

Šio darbo mokslinis naujumas yra tai, kad pirmą kartą Lietuvoje disertacijos lygiu išsamiai išnagrinėtos nusikalstamos veikos elektroninių duomenų ir informacinių sistemų konfidencialumui. Darbe atskleisti Lietuvos baudžiamosios teisės doktrinoje dar nenagrinėti šių veikų sudėties požymių aspektai, pasisakyta dėl technologinių – teisinių problemų įtakos veikų aiškinimui ir inkriminavimui, sistemiškai analizuotos tarptautiniu ir Europos Sąjungos lygiu priimtų teisės aktų, užsienio valstybių bei Lietuvos baudžiamojo įstatymo normos. Vadovaujantis šių nusikalstamų veikų sudėties požymių analize suformuluoti nusikalstamų veikų elektroninių duomenų ir informacinių sistemų konfidencialumui atskyrimo nuo panašių nusikalstamų veikų kriterijai. Atkreiptas dėmesys į technologinio neutralumo ir ekvivalentinio vertinimo principų taikymo galimybes ir problemas baudžiamosios teisės kontekste. Tyrimas neapribotas tik teoriniu lygmeniu – pirmą kartą šių nusikalstamų veikų analizei pasitelkta teismų praktika, ją apibendrinus iškeltos konkre-

[6] Tikslumo dėlei reikėtų atkreipti dėmesį į tai, kad, skirtingai nei neteisėto elektroninių duomenų perėmimo ir panaudojimo nusikastama veika, neteisėtas prisijungimas prie informacinės sistemos kriminalizuotas vėliau – 2004 metais.

[7] Štitilis, D. Teisinės atsakomybės pagrindų nustatymo už neteisėtas veikas elektroninėje erdvėje problemos: daktaro disertacija: socialiniai mokslai, teisė (01 S). – Vilnius: LTU, 2002, p. 7.

čios kvalifikavimo problemos ir pateikti galimi jų sprendimo variantai. Be to, darbe atrinkta ir reikšminga užsienio valstybių teismų praktika – nagrinėtos bylos padėjo nustatyti Lietuvoje dar nepasitaikiusius probleminius nusikalstamų veikų elektroninių duomenų ir informacinių sistemų konfidencialumui aspektus.

Atsižvelgiant į tai, kad darbe pateikti moksliškai pagrįsti nusikalstamų veikų elektroninių duomenų ir informacinių sistemų konfidencialumui aiškinimo ir inkriminavimo problemų sprendimo variantai, ši medžiaga galės būti naudinga besiformuojančiai elektroninių nusikalstamų veikų doktrinai, taip pat naudojama praktiniu baudžiamojo įstatymo taikymo lygmeniu sprendžiant kylančius tokių nusikalstamų veikų kvalifikavimo klausimus.

Disertacijos tyrimo objektas. Šio disertacinio tyrimo objektas yra viena iš nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui rūšių – nusikalstamos veikos elektroninių duomenų ir informacinių sistemų konfidencialumui, numatytos BK 198 ir 198[1] straipsniuose, ir jų baudžiamojo teisinio vertinimo problemos.

Darbo tikslas ir uždaviniai. *Disertacinio darbo tikslas* – nustatyti nusikalstamų veikų, kuriomis pažeidžiamas elektroninių duomenų ir informacinių sistemų konfidencialumas, aiškinimui svarbias principines nuostatas, kuo išsamiau paaiškinti šių veikų sudėties požymius, identifikuoti jų baudžiamojo teisinio vertinimo problemas, taip pat nustačius esamo teisinio reguliavimo trūkumus, pateikti galimas jo tobulinimo ar šių veikų požymių aiškinimo kryptis.

Disertacinio darbo uždaviniai:

1. Analizuojant ekvivalentinio vertinimo ir technologinio neutralumo principus baudžiamosios teisės kontekste, atskleisti esminius nusikalstamų veikų, padaromų elektroninėje erdvėje, kriminalizavimo ir šių veikų požymių aiškinimo probleminius aspektus.

2. Baudžiamojo įstatymo saugomos vertybės pagrindu struktūrizavus BK XXX skyriuje esančias nusikalstamas veikas, identifikuoti tas, kurios pažeidžia elektroninių duomenų ir informacinių sistemų konfidencialumą, atskleisti, kaip ši vertybė interpretuotina elektroninių duomenų ir informacinių sistemų saugumo kontekste.

3. Kuo išsamiau atskleisti neteisėto prisijungimo prie informacinės sistemos nusikalstamos veikos (BK 198[1] straipsnis) sudėties požymius, nustatyti esamo teisinio reguliavimo ar sudėties požymių aiškinimo trūkumus, pateikti galimas teisinio reguliavimo tobulinimo ar šios veikos požymių aiškinimo kryptis.

4. Kuo išsamiau atskleisti neteisėto elektroninių duomenų perėmimo ir panaudojimo nusikalstamos veikos (BK 198 straipsnis) sudėties požymius, nustatyti esamo teisinio reguliavimo ar sudėties požymių aiškinimo trūkumus, pateikti galimas teisinio reguliavimo tobulinimo ar šios veikos požymių aiškinimo kryptis.

5. Išanalizuoti nusikalstamų veikų elektroninių duomenų ir informacinių sistemų konfidencialumui santykį su panašiomis nusikalstamomis veikomis, suformuluoti šių nusikalstamų veikų atskyrimo kriterijus.

Ginamieji disertacijos teiginiai:

1. Nusikalstamų veikų elektroninėje erdvėje kriminalizavimui ir sudėties požymių aiškinimui yra aktualūs ekvivalentinio vertinimo ir technologinio neutralumo principai.

2. Elektroninių duomenų ir informacinių sistemų saugumo interpretavimui pasitelkus *CIA triados* saugumo modelį, BK XXX skyriuje esančios veikos struktūrizuojamos į elektroninių duomenų ir informacinių sistemų konfidencialumo, integralumo bei prieinamumo pažeidimus.

3. Pasirinkta neteisėto prisijungimo prie informacinės sistemos nusikalstamos veikos koncepcija BK kelia šios veikos požymių aiškinimo, taigi ir šios veikos inkriminavimo problemų.

4. Neteisėto elektroninių duomenų perėmimo ir panaudojimo nusikalstamos veikos aprašymas BK kelia šios veikos sudėties požymių aiškinimo, jų tarpusavio santykio nustatymo, taigi ir šios veikos inkriminavimo sunkumų.

5. Nusikalstamų veikų elektroninių duomenų ir informacinių sistemų konfidencialumui atskyrimas nuo kitų veikų elektroninių duomenų ir informacinių sistemų saugumui, nusikalstamų veikų finansų sistemai ir nusikalstamų veikų privataus gyvenimo neliečiamumui yra probleminis.

TYRIMŲ APŽVAGA

Lietuvoje nusikalstamos veikos elektroninių duomenų ir informacinių sistemų konfidencialumui nebuvo plačiai nagrinėtos, praktiškai neanalizuoti ir šių nusikalstamų veikų sudėties požymiai. Bendrai veikų elektroninėje erdvėje tematika tiek galiojant 1961 m., tiek 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 skirta bendriems tokių veikų aiškinimo klausimams. Atskirais aspektais jas nagrinėjo ir R. Petrauskas, tiesa, dar galiojant 1961 m. baudžiamajam įstatymui. Jau įsigaliojus 2000 m. BK, pavieniai veikų elektroninėje erdvėje aiškinimo atvejai paprastai sutinkami mokomuosiuose leidiniuose, pavyzdžiui, 2006 metų vadovėlyje „Teisės informatika ir informatikos teisė“[8] ir 2004 metų leidinyje „Informacinių technologijų teisė“[9]. Dėl baudžiamojo įstatymo ir tarptautinių teisės aktų suderinamumo elektroninių nusikalstamų veikų reglamentavimo srityje yra pasisakęs D. Sauliūnas. Kai kurie šių veikų aspektai jų tyrimo metodikos kontekste aptariami ir N. Goranin bei D. Mažeikos. Paminėtinas ir baudžiamojo įstatymo komentaras, kuriame matyti glaustas teorinis elektroninių duomenų ir informacinių sistemų konfidencialumą pažeidžiančių veikų aiškinimas. Pastaruoju metu mokslinėje literatūroje daugiau dėmesio pradėta skirti tapatybės vagystės (angl. *identity theft*) elektroninėje erdvėje kriminalizavimo klausimams, kuriais domisi D. Štitilis, P. Pakutinskas, M. Laurinaitis ir I. Dauparaitė.

Kiek kitokia situacija yra užsienio valstybių baudžiamosios teisės moksle, kuriame įvairiems nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui bei apskritai nusikalstamų veikų elektroninėje erdvėje aspektams teikiamas didesnis dėmesys. Bendro pobūdžio elektroninių veikų kriminalizavimo ir aiškinimo, elgesio elektroninėje erdvėje vertinimo problemas savo darbuose nagrinėjo J. Clough, I. Walden, C. Reed, U. Kohl, S. W. Brenner, M. Schellekens, R. Ali, I. M. van der Haar, J.–B. Koops, R. W. Downing, P. Ohm, C. A. Kirby ir kt. Neteisėtos prieigos prie informacinės sistemos ar elektroninių duomenų kriminalizavimo, inkriminavimo *inter alia* ir tokių nusikalstamų veikų požymių aiškinimo klausimais yra pasisakę O. S. Kerr, M. W. S. Wong, M. J. Madison, I. Walden, D. Bainbridge, J. Angel, G. Thornton, J. Clough, B. A. Howell, A. S. Blunn, D. Rowland, E. Macdonald. Taip pat paminėtini ir Rusijos baudžiamosios teisės mokslininkai N. I. Vetrov, V. A. Mazurov, A. V. Naumov, A. G. Volevodz, V. E. Kozlov, O. Ja. Baev ir V. A. Meshherkov, S. A. Pashin ir kt.

---

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

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

DARBO METODOLOGIJA

Plačiausiai disertaciniame tyrime, aiškinant nusikalstamas veikas elektroninių duomenų ir informacinių sistemų konfidencialumui, naudoti metodai – *analizė* ir *sintezė*. *Analizės metodas* taikytas šių veikų struktūrą skaidant dalimis ir aiškinant atskirus objektyviuosius bei subjektyviuosius požymius. Be to, šis metodas leido atskleisti ir atskirų požymių, tiesiogiai susijusių su informacinėmis ir komunikacijos technologijomis, turinį – atskyrus teisinę ir technologinę požymių pusę spręstas jų suderinimo klausimas. Siekiant visapusio veikų pažinimo, neapsieita ir be *sintezės metodo*, kuris naudotas analizės metu dėl atskirų požymių gautas įžvalgas jungiant į vieną visumą. Būtent ši visuma sudarė sąlygas nustatyti, kokia šių veikų koncepcija vadovautasi jas apibrėžiant baudžiamajame įstatyme, kokios yra šių nusikalstamų veikų ribos.

Disertaciniame tyrime taip pat dažnai naudotas ir *sisteminės analizės metodas*, kurio parinkimą lėmė pačių nusikalstamų veikų elektroninių duomenų ir informacinių sistemų konfidencialumui specifika: įvairūs šių veikų aspektai sutinkami tarptautiniu ir Europos Sąjungos lygiu priimtuose teisės aktuose, aiškinant šias veikas būtina sieti skirtingose mokslo šakose suformuluotas teorijas. Šis metodas leido nustatyti nagrinėjamų nusikalstamų veikų vietą elektroninių nusikalstamų veikų ir nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui visete. Taikant jį spręstos kompleksinės technologinį aspektą turinčios problemos, tiesiogiai susijusios su disertaciniame tyrime keltu technologijų ir terminologijos klausimu. Sisteminės analizės metodas sudarė galimybes analizuoti veikų sudėties požymių tarpusavio ryšį, atskleisti šių veikų santykį su panašiomis baudžiamajame įstatyme numatytomis veikomis, ieškoti jų atskyrimo kriterijų.

Nagrinėjamų problemų kompleksiškumas lėmė, kad disertaciniame tyrime buvo būtina susieti baudžiamosios teisės ir informacinių bei komunikacijos technologijų sritis. Siekiant atskleisti technologinį – teisinį nusikalstamų veikų aspektą, taikytas *apibendrinimo metodas.* Išskyrus bendriausius, esminius technologijų srityje analizuojamų objektų požymius, jie derinti su sudėties požymių baudžiamaisiais teisiniais aspektais. Taip tyrime buvo sprendžiama technologijų ir joms įvardyti naudojamos terminologijos pritaikomumo baudžiamosios teisės srityje problema, pateiktas 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 Europos Sąjungos teisės aktais, skirtais kovai su veikomis elektroninėje erdvėje. Jų įtaka matyti ne tik Lietuvos, bet ir užsienio valstybių baudžiamojo įstatymo nuostatoms. Pasirinktas skirtingas minėtų teisės aktų reikalavimų įgyvendinimo būdas sudaro sąlygas formuotis ir skirtingoms tokio pobūdžio veikų koncepcijoms. Šių skirtumų identifikavimui ir analizei pasitelktas *lyginamasis metodas* leido sugretinti skirtingas veikų koncepcijas, įvairių mokslininkų nuomones, nustatyti veikų inkriminavimo problemas, suformuluoti galimus jų sprendimo variantus ir pan.

Atskleidžiant nusikalstamų veikų elektroninių duomenų ir informacinių sistemų konfidencialumui požymių turinį naudotas ir *lingvistinis metodas.* Atliekant disertacinį tyrimą buvo nustatytas įvairių sąvokų interpretavimo trūkumas, todėl šis metodas tapo aktualus bandant suformuluoti galimas jų aiškinimo kryptis. Tačiau taikant lingvistinį metodą pastebėta, kad baudžiamosios teisės srityje vartojamoms sąvokoms yra būdingas specifinis

nuo kasdieninės kalbos besiskiriantis turinys, kuris dar daugiau savitumo įgyja informacinių ir komunikacijos technologijų kontekste.

Disertaciniame tyrime pasitelktas taip pat empirinis *dokumentų analizės metodas.* Jis taikytas apibendrinant besiklostančią teismų praktiką nusikalstamų veikų elektroninių duomenų ir informacinių sistemų konfidencialumui bylose, naudojant teismų sprendimus išryškinant kylančias veikų inkriminavimo problemas, pagrindžiant galimus jų sprendimo variantus. Tyrime analizuoti ir užsienio valstybių teismų reikšmingiausi sprendimai, leidę kelti naujas, Lietuvoje kol kas dar nežinomas problemas, pateikiant jų sprendimo siūlymus.

I. ESMINIAI NUSIKALSTAMŲ VEIKŲ, PADAROMŲ ELEKTRONINĖJE ERDVĖJE, BAUDŽIAMIEJI TEISINIAI ASPEKTAI

1. Terminologijos problema

Siekiant šiame darbe vartojamų terminų aiškumo aptartina keletas elektroninių nusikalstamų veikų doktrinoje keliamų bendresnių, bet tarpusavyje glaudžiai susijusių tokių veikų įvardijimo ir jų visumos vidinės struktūros nustatymo problemų. Šių problemų sąsaja pasireiškia tuo, kad vartojami skirtingi terminai nurodo skirtingas nusikalstamas veikas, padaromas elektroninėje erdvėje. Todėl pasirinktas vienas ar kitas šias veikas žymintis terminas suponuoja, kad, jį vartojant, yra kalbama apie visas elektronines nusikalstamas veikas arba tik apie jų dalį. Toliau didesnis dėmesys bus skiriamas būtent šio santykio analizei[10].

Terminų parinkimo problema Lietuvos baudžiamojoje teisėje atsirado dėl to, kad BK savarankiška elektroninių nusikalstamų veikų rūšis nenumatyta. Atitinkamai jame nėra pateiktas oficialus tokio pobūdžio veikų pavadinimas (pagal rūšinę baudžiamojo įstatymo saugomą vertybę). Todėl įvairūs terminai formuluoti *de fakto,* siekiant kuo tiksliau apibūdinti tas elektroninėje erdvėje padaromas nusikalstamas veikas, kurias jie žymi. Beje, ši terminijos problema kelta tiek Lietuvos, tiek užsienio mokslinėje literatūroje (D. Štitilis, S. Toliušis, G. Urbas, R. G. Smith, P. Grabosky, S. W. Brenner, ir kt.)[11]. Joje pastebėta, kad kalbant apie tokio pobūdžio veikas dažnai vartojami kompiuterinių (angl. *computer crime*), aukštųjų technologijų (angl. *high – tech crime*), elektroninių (angl. *cybercrime*), virtualių (angl. *virtual crime*), skaitmeninių (angl. *digital crime*), su kompiuteriais susijusių (angl. *computer–related crime*), e–nusikalstamų veikų (angl., *e–crime*), nusikalstamų veikų elektroninėje erdvėje (angl. *cybercrime*)[12] ir kiti pavadinimai. Kaip minėta, kiekvienas jų turi specifinę reikšmę, kuri priklauso nuo to, kurios veikos, įtrauktos į elektroninių nusikalstamų veikų visumą, turimos mintyje. Atitinkamai vieni jų gali būti laikomi sinonimais, kiti – ne.

Taigi prieš pasirenkant toliau darbe vartosimus terminus aptartini du klausimai: 1) kokios nusikalstamos veikos pripažįstamos padarytomis elektroninėje erdvėje ir 2) kaip tokias nusikalstamas veikas tikslinga šiame darbe suskirstyti. Iškeltiems klausimams atsakyti svarbūs teisėkūrai įtakos turintys įvairūs tarptautiniu ir Europos Sąjungos lygiu priimti teisiniai instrumentai, tiesiogiai susiję su nusikalstamų veikų elektroninėje erdvėje reglamentavimu[13].

---

[10] Autorė norėtų atkreipti dėmesį į tai, kad šioje dalyje nesiekiama išsamiai išanalizuoti elektroninių nusikalstamų veikų doktrinoje keliamas terminijos ir šių veikų skirstymo problemas. Šios dalies tikslas – nurodyti darbe vartosimus terminus ir juos susieti su konkrečiomis nusikalstamomis veikomis elektroninėje erdvėje.

[11] Civilka, M., *et al.*, *supra* note 9, p. 508; Smith, R. G.; Grabosky, P.; Urbas, G. *Cyber Criminals on Trial.* Cambridge: Cambridge University Press, 2004, p. 5; *Crime Online*. Jewkes, Y. (ed.). Willan Publishing, 2007, p. 13.

[12] Smith, R. G.; Grabosky, P.; Urbas, G., *op. cit.*, p. 5; Štitilis, D. *Elektroniniai nusikaltimai*. Vilnius: Mykolo Romerio universitetas, 2011, p. 5.

[13] Toks elektroninių nusikalstamų veikų reglamentavimas buvo būtinas dėl jų transnacionalinio aspekto, į kurį atkreiptas dėmesys jau 1989 m. rugsėjo 13 d. Europos Tarybos Ministrų kabineto rekomendacijose valstybėms narėms Nr. R(89)9 dėl su kompiuteriais susijusių nusikaltimų. Teisėkūros veiksmų tarptautiniu ir Europos Sąjungos lygiu imtasi pripažinus, kad galimi pavienių valstybių veiksmai, reaguojant į atsiradusias grėsmes elektroninėje erdvėje, tiek savo apimtimi, tiek ir poveikiu nėra pakankamai efektyvūs.

Council of Europe Committee of Ministers Recommendation No. R (89) 9 Of the Committee of Ministers to Member States on Computer – related Crimes (Adopted by the Committee of Ministers on 13 September 1989 at the 428th meeting of the Ministers' Deputies) [interaktyvus], [žiūrėta 2012-01-24]. <https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=610660&SecMode=1&DocId=702280&Usage=2>.

Minėtų nusikalstamų veikų vidinei struktūrai atskleisti aktuali 2001 m. lapkričio 23 d. Europos Tarybos konvencija dėl elektroninių nusikaltimų (toliau – Konvencija dėl elektroninių nusikaltimų)[14], 2005 m. vasario 24 d. Tarybos pamatinis sprendimas 2005/222/TVR dėl atakų prieš informacines sistemas[15] (toliau – Pamatinis sprendimas 2005/222/TVR) ir 2013 m. rugpjūčio 12 d. Europos Parlamento bei Tarybos direktyva 2013/40/ES dėl atakų prieš informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR (toliau – Direktyva 2013/40/ES)[16]. Tiesa, pastarosios direktyvos nuostatos kol kas dar nėra perkeltos į Lietuvos nacionalinę teisę. Taip pat paminėtinas ir 2007 m. gegužės 22 d. Europos Komisijos Komunikatas Europos Parlamentui, Tarybai ir Europos Regionų komitetui Bendrosios politikos, skirtos kovai su elektroniniais nusikaltimais, linkme KOM/2007/0267 galutinis[17] (toliau – Komunikatas KOM/2007/0267).

Konvencijoje dėl elektroninių nusikaltimų numatyta plačiausia elektroninės erdvės saugumą pažeidžiančių ar jam grėsmę sukeliančių nusikaltimų (nusikalstamų veikų) apibrėžtis. Joje minimos šios grupės nusikaltimų: 1) nusikaltimai kompiuterinių duomenų ir sistemų konfidencialumui, vientisumui ir prieinamumui[18]; 2) kompiuteriniai nusikaltimai[19]; 3) turinio nusikaltimai[20]; 4) nusikaltimai, susiję su autorių teisių ir gretutinių teisių pažeidimais[21]. Todėl šis konvencinis elektroninių nusikalstamų veikų skirstymas iš esmės leidžia kalbėti apie kompiuterinius nusikaltimus, suvokiamus plačiąja prasme[22]. Pamatiniame sprendime 2005/222/TVR ir Direktyvoje 2013/40/ES teisinis reguliavimas šiuo aspektu siauresnis. Juose numatytos tik elektroninių duomenų ir informacinių sistemų saugumą tiesiogiai pažeidžiančios nusikalstamos veikos, kurios gali būti tapatinamos su kompiuterinėmis nusikalstamomis veikomis, suvokiamomis siaurąja prasme[23]. Toks elektroninės erdvės saugumą pažeidžiančių nusikalstamų veikų apibrėžčių skirtumas rodo, kad Pamatinio sprendimo 2005/222/TVR ir Direktyvos 2013/40/ES nusikalstamos veikos sudaro tik dalį minėtos Konvencijos nuostatų, t. y. atitinka kompiuterinės informacijos ir kompiuterinių sistemų konfidencialumą, vientisumą bei prieinamumą (1 skirsnio 1 dalis) pažeidžiančius nusikaltimus (nusikalstamas veikas).

---

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

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

[16] 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.

[17] 2007 m. gegužės 22 d. Europos Komisijos Komunikatas Europos Parlamentui, Tarybai ir Europos Regionų komitetui Bendrosios politikos, skirtos kovai su elektroniniais nusikaltimais, linkme KOM/2007/0267 galutinis. [interaktyvus], [žiūrėta 2012-01-24]. <http://eur-lex.europa.eu>.

[18] Konvencijos dėl elektroninių nusikaltimų II skyriaus 1 skirsnio 1 dalis: neteisėta prieiga (2 straipsnis), neteisėta perimtis (3 straipsnis), poveikis duomenims (4 straipsnis), poveikis sistemai (5 straipsnis), netinkamas įtaisų naudojimas (6 straipsnis).

[19] Konvencijos dėl elektroninių nusikaltimų II skyriaus 1 skirsnio 2 dalis: kompiuterinės klastotės (7 straipsnis), kompiuterinis sukčiavimas (8 straipsnis).

[20] Konvencijos dėl elektroninių nusikaltimų II skyriaus 1 skirsnio 3 dalis: nusikaltimai, susiję su vaikų pornografija (9 straipsnis).

[21] Konvencijos dėl elektroninių nusikaltimų II skyriaus 1 skirsnio 4 dalis: nusikaltimai, susiję su autorių teisių ir gretutinių teisių pažeidimais (10 straipsnis).

[22] Tai nusikalstamos veikos, kurių dalykas yra elektroniniai duomenys, arba informacinė sistema panaudojama kaip nusikalstamos veikos priemonė. Šių nusikalstamų veikų baudžiamojo įstatymo saugoma vertybė skiriasi (plačiau žr. Štitilis, D., *supra* note 12, p. 6).

[23] Tai nusikalstamos veikos, kurios paprastai nurodytos atskirose baudžiamųjų įstatymų skyriuose (pavyzdžiui, BK XXX skyriuje). Šioms nusikalstamoms veikoms būdinga ta pati baudžiamojo įstatymo saugoma vertybė (plačiau žr. Štitilis, D., *op. cit.*, p. 6).

Konvenciniam elektroninės erdvės saugumą pažeidžiančių nusikalstamų veikų skirstymui neprieštarauja ir rūšinius tokių veikų požymius leidžia išskirti taip pat Komunikate KOM/2007/0267 pateiktas elektroninių nusikaltimų (nusikalstamų veikų) klasifikavimas. Jame terminas elektroniniai nusikaltimai siejamas su trimis veikų rūšimis: 1) tradicinės veikos, padarytos naudojant informacines ir komunikacijos technologijas (pavyzdžiui, sukčiavimas elektroninėje erdvėje); 2) veikos, susijusios su neteisėto turinio medžiagos platinimu elektroninėje erdvėje (pavyzdžiui, rasinės neapykantos kurstymas, pornografinio turinio medžiagos platinimas); 3) tiesiogiai elektroninių duomenų ir informacinių sistemų saugumą pažeidžiančias veikas (pavyzdžiui, neteisėtas prisijungimas prie informacinės sistemos). Šis skirstymas taip pat kaip Konvencijos dėl elektroninių nusikaltimų atveju susijęs su kompiuteriniais nusikaltimais, suvokiamais plačiąja prasme.

Atsižvelgiant į minėtus skirstymus, galima pateikti keletą pastebėjimų dėl toliau darbe vartosimos terminijos. Pirmiausia, *nusikalstamos veikos elektroninių duomenų ir informacinių sistemų saugumui* yra viena iš *nusikalstamų veikų elektroninėje erdvėje* rūšių, todėl šie terminai tarpusavyje sąveikauja kaip dalis ir visuma. Atitinkamai jie negali būti ir darbe nėra vartojami kaip sinonimai. Antra, *nusikalstamoms veikoms elektroninių duomenų ir informacinių sistemų saugumui* įvardyti gali būti taikomas ir *kompiuterinių nusikalstamų veikų, suvokiamų siaurąja prasme,* terminas. Tačiau, atsižvelgiant į tai, kad šios veikos Konvencijoje dėl elektroninių nusikaltimų susietos su konfidencialumo (angl. *confidentiality*), integralumo (angl. *integrity*) ir prieinamumo (angl. *availability*) triada, tai šiame darbe tokioms veikoms įvardyti bus vartojamas *CIA nusikalstamų veikų* trumpinys. Trečia, kadangi *nusikalstamų veikų elektroninėje erdvėje*, *elektroninių nusikalstamų veikų* ir *kompiuterinių nusikalstamų veikų, suvokiamų plačiąja prasme*, terminai apima tas pačias nusikalstamas veikas, tai jie gali būti laikomi sinonimais. *Elektroninių nusikalstamų veikų* sąvokos atsiradimas siejamas su Konvencijos dėl elektroninių nusikaltimų oficialiu vertimu į lietuvių kalbą. Tačiau mokslinėje literatūroje ne kartą išsakyti pastebėjimai, kad tikslesniu laikytinas *nusikalstamų veikų elektroninėje erdvėje*, o ne *elektroninių nusikalstamų veikų* terminas, nes *Cybercrime* vertinys turėjo būti kildinamas iš termino *Cyberspace*, kuris verčiamas kaip elektroninė erdvė[24]. Toliau darbe šioms nusikalstamoms veikoms įvardyti vieną kitu pakeičiant bus vartojami du – *elektroninių nusikalstamų veikų* ir *nusikalstamų veikų, padaromų elektroninėje erdvėje*, terminai.

Taip pat reikėtų pateikti keletą pastabų dėl nusikalstamų veikų, padaromų elektroninėje erdvėje, vidinės struktūros. Tiek iš Konvencijos dėl elektroninių nusikaltimų, tiek iš Komunikate KOM/2007/0267 pateiktų skirstymų matyti, kad šiuose aktuose bendriausia prasme yra nurodomos: 1) *CIA nusikalstamos veikos*; 2) tradicinės nusikalstamos veikos, kurios pakito tiek, kiek informacinės ir komunikacijos technologijos turėjo įtakos jų padarymo būdams ir vietai. Antrajai grupei, autorės nuomone, gali būti priskirti Konvencijoje dėl elektroninių nusikaltimų minimi kompiuteriniai nusikaltimai, turinio nusikaltimai ir nusikaltimai, susiję su autorių teisių ir gretutinių teisių pažeidimais. Atitinkamai – Komunikate KOM/2007/0267 nurodytos tradicinės nusikalstamos veikos, padarytos naudojant informacines ir komunikacijos technologijas, ir nusikalstamos veikos, susijusios su neteisėto turinio medžiagos platinimu elektroninėje erdvėje[25]. Ši autorės pozicija neneigia

[24] Civilka, M., *et al.*, *supra* note 9, p. 511.

[25] Toks bendro pobūdžio skirstymas pasirinktas dėl to, kad Lietuvos BK tradicinių, tačiau dėl technologijų panaudojimo pakitusių nusikalstamų veikų kriminalizavimo būdas yra vienodas (tiek neteisėto turinio, tiek kitų tradicinių veikų atveju). Todėl jis galimas aptariant įvairius teisėkūros aspektus, susijusius su technologinio neutralumo ir ekvivalentinio vertinimo principais.

galimybės dėl naujųjų technologijų panaudojimo pakitusias tradicines veikas skaidyti smulkiau, siekiant tarp jų atrasti ir kitus ne tik šių technologijų panaudojimu grįstus bendrumus. Toks detalesnis skirstymas gali būti aktualus dėl to, kad pačios tradicinės nusikalstamos veikos yra įvairios ir yra priskiriamos skirtingoms jų rūšims (pagal BK specialiosios dalies skirstymą). Kadangi šiame darbe toks smulkesnis skaidymas nėra svarbus, tai bendriausia prasme jame bus analizuojamos *CIA nusikalstamos veikos* ir tradicinės veikos, pakitusios dėl informacinių ir komunikacijos technologijų panaudojimo. Pastarajai grupei autorė priskiria visas tradicines nusikalstamos veikos, kurios pagal savo pobūdį gali būti padaromos ne tik fizinėje, bet ir elektroninėje erdvėje. Taigi dėl naujųjų technologijų pakitusių tradicinių veikų sąrašas nėra ribojamas Konvencijoje dėl elektroninių nusikaltimų bei Komunikate KOM/2007/0267 nurodytomis veikomis. Darbe laikomasi nuomonės, kad nėra tikslinga sudaryti baigtinį tokių veikų sąrašą, nes dėl informacinių ir komunikacijos technologijų vystymosi vis daugiau anksčiau tradicinėmis laikomų nusikalstamų veikų bus „perkeliama“ į elektroninę erdvę. Pakitus technologijų panaudojimo galimybėms šis sąrašas itin greitai prarastų savo aktualumą.

Tradicines nusikalstamas veikas, padarytas elektroninėje erdvėje, šiuo atveju leidžia identifikuoti informacinių ir komunikacijos technologijų panaudojimo požymis. Nors jis, atsižvelgiant į Lietuvoje pasirinktą tokių nusikalstamų veikų kriminalizavimo būdą, nėra numatytas tradicinių nusikalstamų veikų sudėtyse, tačiau visuomet bus nustatomas ir turės įtakos įrodinėjant elektroninių nusikalstamų veikų padarymo faktą[26]. Šis požymis, atsižvelgiant į tai, kokia veika padaryta, gali būti apibūdintas: 1) per elektroninių duomenų ir informacinių sistemų saugumo pažeidimus (pavyzdžiui, elektroninio dokumento suklastojimo atveju)[27] ir (arba) 2) per pačios informacinės sistemos panaudojimą (pavyzdžiui, neteisėto turinio medžiagos platinimo elektroninėje erdvėje atveju)[28]. Be abejo, priklausomai nuo padarytos nusikalstamos veikos, gali būti nustatyti ir abu šie požymiai.

---

[26] Pavyzdžiui, baudžiamosios teisės teorijoje ir teismų praktikoje pripažįstama, kad sukčiavimo esmę geriausiai atskleidžia dviejų elementų – apgaulės ir turtinės naudos gavimo – tarpusavio sąsaja. Tačiau analizuojant sukčiavimą elektroninėje erdvėje reikėtų pripažinti, kad šie tradiciniai ir sukčiavimo esmę geriausiai apibūdinantys elementai yra būtini, tačiau nepakankami, kad kaltininko padaryta nusikalstama veika būtų priskirta dėl naujųjų technologijų panaudojimo pakitusių tradicinių nusikalstamų veikų grupei. Konvencijoje dėl elektroninių nusikaltimų numatyta kompiuterinio sukčiavimo apibrėžtis (8 straipsnis) leidžia išskirtą trečiąjį – kompiuterinės sistemos panaudojimo požymį, kuris apibūdinamas per elektroninių duomenų ir informacinių sistemų saugumo pažeidimus. Baudžiamojoje byloje nustačius šį elementą, atitinkamai bus sprendžiamos dėl jo kylančios įvairios šios veikos kvalifikavimo problemos (pavyzdžiui, koks turėtų būti nustatomas apgaulės turinys, jei ji buvo panaudota informacinei sistemai suklaidinti. Plačiau žr. Pranka, D. Apgaulės samprata ir reikšmė atribojant sukčiavimą ir civilinės teisės pažeidimą. *Socialinių mokslų studijos*, 2012, 4(2): 666–667; Sinkevičius, E. *Neteisėtas banko kredito gavimas arba panaudojimas ir jų kvalifikavimas*. Vilnius: Lietuvos teisės universiteto Leidybos centras, 2002, p. 51).

[27] Pavyzdžiui, Konvencijoje dėl elektroninių nusikaltimų apibrėžiant kompiuterinės klastotės nusikaltimą (7 straipsnis) šis požymis apibūdintas per elektroninių duomenų saugumo pažeidimus, t. y. baudžiamoji atsakomybė kyla už „sąmoningą ir neteisėtą kompiuterių duomenų įvedimą, pakeitimą, sunaikinimą arba galimybės naudotis tokia informacija panaikinimą“.

[28] Pavyzdžiui, Konvencijoje dėl elektroninių nusikaltimų toks kompiuterinės sistemos panaudojimo atvejis, nekalbant apie įvairius jos ar elektroninių duomenų saugumo pažeidimus, numatytas 9 straipsnyje aprašant nusikaltimus, susijusius su vaikų pornografija (pavyzdžiui, pornografinio turinio produkcijos, kurioje atvaizduotas vaikas, siūlymą arba pateikimą per kompiuterinę sistemą).

2. Esminiai nusikalstamų veikų elektroninėje erdvėje kriminalizavimo ir aiškinimo aspektai

Informacinių ir komunikacijos technologijų raida sudarė prielaidas didelės apimties ir įvairaus pobūdžio informacijos sklaidai, naujoms prieigos prie informacijos, taip pat jos apsikeitimo galimybėms atsirasti (globali komunikacija). Tačiau šis vienas iš globalizacijos aspektų leidžia pastebėti ir informacinės visuomenės pažeidžiamumo problemą (turint mintyje tiek vidinius, tiek ir išorinius informacinius ryšius). Viena iš elektroninėje erdvėje kylančių grėsmių yra joje padaromos nusikalstamos veikos. Į šių veikų sąrašą patenka ne tik dėl naujųjų technologijų panaudojimo pakitusios tradicinės, bet, kaip galima buvo pastebėti, ir specifinės elektroninėje erdvėje padaromos *CIA nusikalstamos veikos*. Tokie pakankamai radikalūs šių veikų padarymo galimybių pokyčiai kelia fundamentalias teisėkūros ir baudžiamojo įstatymo normų taikymo (atitinkamai jų aiškinimo) problemas.

Minėtų problemų kilmę aiškiau padeda suvokti ir jas spręsti teisėkūros lygmeniu plačiai taikomi elgesio fizinėje ir elektroninėje erdvėje ekvivalentinio vertinimo (angl. *principle of equivalence, principle of online and offline equivalence*) bei technologinio neutralumo (angl. *principle of technological neutrality*) principai. Kadangi šie principai leidžia nuspėti įstatymo leidėjo valią, nustatant atitinkamus elgesio elektroninėje erdvėje reikalavimus, tai jie aktualūs ir teismų praktikoje. Čia, pereinant nuo teisės normos imperatyvų prie jų įgyvendinimo, ekvivalentinio vertinimo ir technologinio neutralumo pozicijos padeda atskleisti su technologijomis susijusios teisės normos turinį ir ją tiksliai bei vienodai taikyti.

Baudžiamosios teisės kontekste analizuojant įvairius minėtų principų aspektus vis dėlto reikėtų pastebėti, kad jų ištakos nėra tiesiogiai siejamos su šia teisės šaka. Tačiau kaip vieną iš galimų pavojingų veikų reguliavimo elektroninėje erdvėje priemonių[29] pasirinkus baudžiamąjį teisinį reguliavimą, jie tampa aktualūs ir šioje srityje. Į pakankamai plačią minėtų principų taikymo sferą patenka ne tik tos Lietuvos BK normos, kuriose aiškiai matoma nusikalstamų veikų sudėties požymių sąsaja su informacinėmis ir komunikacijos technologijomis, bet ir tos, kuriose tiesioginių nuorodų į naująsias technologijas nėra. Pastarieji atvejai tai baudžiamojo įstatymo normos, numatančios atsakomybę už tradicines nusikalstamas veikas, pakitusias dėl informacinių ir komunikacijos technologijų panaudojimo[30].

---

[29] Plačiau apie kitas elektroninės erdvės reguliavimo (savireguliacijos) priemones, pavyzdžiui, socialines normas (elektroninės erdvės etikos taisykles, papročius), rinką, *kodą* (architektūrą) žr.: Spinello, R. A. *Cyberethics: Morality and Law in Cyberspace*. Jones and Bartlett Publishers, Inc. 2000, p. 2–6; Strawbridge, M. *Netiquette: Internet Etiquette in the Age of the Blog*. Software Reference Ltd. 2006; Reidenberg, J. R. Lex Informatica: The Formulation of Information Policy Rules through Technology. *Texas Law Review*. 1998, 76 (3); Valauskas, E. J. Lex Networkia: Understanding the Internet Community. *First Monday*. 1996, 1 (4-7); *The Internet Encyclopedia*. Bidgoli H. (ed.). John Wiley and Sons, Inc. 2004, p. 274–285.

[30] Technologinio neutralumo principas taip pat aktualus analizuojant kitus, tiesiogiai su elektroninių veikų padarymu sąsają turinčius baudžiamosios teisės institutus. Pavyzdžiui, turto konfiskavimas (BK 72 straipsnis) neturėtų būti siejamas tik su materialią išraišką turinčiu turtu. Toks platesnis aiškinimas svarbus, kai konfiskuotinas turtas, kuris buvo elektroninėje erdvėje padaromų veikų priemonė, įrankis ar rezultatas. Šiam turtui ne visais atvejais bus būdingas materialumo požymis (pavyzdžiui, kenkėjiškos programos, elektroniniai dokumentai ir kt.). Platesnis aiškinimas atitiktų Tarybos 2005 m. vasario 24 d. pamatinio sprendimo 2005/212/TVR dėl nusikalstamu būdu įgytų lėšų, nusikaltimo priemonių ir turto konfiskavimo [2005] OL L 68/49 (kurio nuostatos perkeltos į Lietuvos nacionalinę teisės sistemą) reikalavimus. Pagal minėto Pamatinio sprendimo nuostatas, konfiskuotino turto sąvoka turėtų apimti „bet kaip apibrėžtą turtą,

Prieš analizuojant ekvivalentinio vertinimo ir technologinio neutralumo principus atkreiptinas dėmesys ir į baudžiamojoje teisėje svarbų jų taikymo aspektą. Kadangi jie, kaip minėta, buvo apibrėžti ne šioje teisės šakoje, tai kaip tokie neturi šios teisės šakos specifikos nulemtų jų taikymo apribojimų. Technologinio neutralumo principas gali būti kildinamas iš informacinių ir komunikacijos technologijų reguliavimo srities[31], o ekvivalentinio vertinimo principas pradėtas taikyti visose srityse[32], kuriose būtina spręsti kilusias kokybiškai naujas elektroninės erdvės teisinio reguliavimo problemas. Todėl nusikalstamų veikų elektroninėje erdvėje kriminalizavimo ir kvalifikavimo sunkumų sprendimas yra neatsiejamas ir nuo šių principų taikymo baudžiamojoje teisėje ribų nustatymo.

2.1. Nusikalstamų veikų elektroninėje erdvėje kriminalizavimas ir ekvivalentinio vertinimo principas

Tradicines nusikalstamas veikas „perkėlus“ į elektroninę erdvę pakito jų padarymo galimybės, taip pat elektroninėje erdvėje atsirado seniau nežinomos veikos, kurias galima laikyti išimtinai naujųjų technologijų vystymosi rezultatu. Todėl elektroninių nusikalstamų veikų kriminalizavimo problemų sprendimas nėra siejamas tik su esamų baudžiamosios teisės normų pritaikomumo jas kvalifikuojant įvertinimu. Tam, kad tokia analizė nebūtų fragmentiška, ekvivalentinio vertinimo principas su doktrinoje išplėtotais jo praktinio įgyvendinimo būdais leidžia apsispręsti: 1) kaip turėtų būti kriminalizuojamos nusikalstamos veikos elektroninėje erdvėje; 2) kaip praktiškai įgyvendinti šio principo reikalaujamą lygiavertį vertinimą. Ekvivalentinio vertinimo principo aktualumas ypač išryškėja tais atvejais, kai, sprendžiant baudžiamosios atsakomybės nustatymo problemas, pastebimi esminiai veikų, padaromų fizinėje ir elektroninėje erdvėje, skirtumai.

---

ir materialų arba nematerialų, kilnojamąjį ir nekilnojamąjį turtą ir teisinius dokumentus, patvirtinančius nuosavybės teisę arba interesą į tokį turtą“. Nors toks aiškinimas įsitvirtinęs teismų praktikoje (Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2010 m. vasario 18 d. Teismų praktikos taikant turto konfiskavimą (BK 72 straipsnis) apžvalgos išvadų 4 punktas. *Teismų praktika*. 2010, Nr. 32.), tačiau pavieniais atvejais konfiskuotinas turtas vis dėlto siejamas su jo materialumu. Pavyzdžiui, Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2010 m. lapkričio 16 d. nutartyje baudžiamojoje byloje (bylos Nr. 2K-500/2010) nurodoma, kad „teismų praktikoje nusikalstamos veikos padarymo priemonėmis pripažįstami įtaisai, įrengimai, mechanizmai, prietaisai ir kiti materialūs daiktai, kurie sudaro sąlygas ar palengvina tokios veikos padarymą, nors jų panaudojimas pats savaime tiesiogiai nedaro žalos atitinkamos veikos objektui ar dalykui“.

[31] Technologinio neutralumo principas minimas įvairiuose Europos Sąjungos lygiu priimtuose dokumentuose, susijusiuose su informacinių ir komunikacijos technologijų reguliavimų sritimi. Pavyzdžiui, kaip vienas iš penkių reguliavimo principų jis minimas Komisijos komunikate Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui 1999 metų Ryšių apžvalgoje „Dėl naujųjų elektroninės komunikacijos infrastruktūros ir susijusių paslaugų pagrindų“ COM(1999)539 (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 2013-06-02]. <www.ictregulationtoolkit.org/en/Document.1501.pdf>). Tai buvo vienas iš principų, kuriais tuo metu vadovautasi Europos Sąjungos lygiu priimant elektroninių ryšių reguliavimo pagrindus.

[32] Pavyzdžiui, autorių teisių ir gretutinių teisių apsauga elektroninėje erdvėje (civilinėmis teisinėmis priemonėmis), elektroninių pinigų, elektroninio parašo pripažinimo ir naudojimo galimybės bei kitos su elektroninės erdvės panaudojimu susijusios sritys.

2.1.1. Ekvivalentinio vertinimo principo samprata ir įgyvendinimo būdai

Vystantis informacinėms ir komunikacijos technologijoms, tinkamo teisinio reguliavimo sukūrimo (derinant esamą prie elektroninės erdvės ypatumų ar kuriant naują) problemų atsirado visose su jomis vienu ar kitu aspektu susijusiose srityse (ne išimtis ir baudžiamoji teisė). Kadangi dauguma veiklų, iki tol egzistavusių fiziniame pasaulyje, „persikėlė“ į elektroninę erdvę, tai jos „įgijo tam tikrą specifiką, atsižvelgiant į jų elektroninę formą, komunikavimo internete būdus bei interneto globalumą ir kitus specifinius elektroninės komunikacinės erdvės požymius“[33]. Dėl informacinių ir komunikacijos technologijų atsiradę nauji tarpusavio sąveikos būdai[34] leido pastebėti elektroninės erdvės ypatumus, dažnai išreiškiamus „dematerializavimo“ (angl. *dematerialisation*), „skaitmeninimo“ (angl. *digitisation*)[35], „automatizacijos“[36] požymiais, atitinkamai ir esminius fizinės bei elektroninės erdvės (kuriai netaikytini fizinės erdvės mato kriterijai)[37] skirtumus. Būtent tai sudarė sąlygas kelti kokybiškai naujas ir kiekybiškai daug teisinių problemų[38]. Išryškėjus minėtiems skirtumams, tinkamo elektroninės erdvės reguliavimo[39] problemas dar labiau aštrino elektroninės erdvės kaip nepriklausomos ir nereguliuojamos (J. P. Barlow ir kt.)[40] ar kaip savarankiškos erdvės su savo teisine baze ir institucijomis (D. R. Johnson, D. G. Post ir kt.)[41] požiūrių šalininkai. Vis dėlto šie gana radikalūs siūlymai neįsitvirtino – negalėjo kilti abejonių, kad, pirma, įmanoma atrasti teisinius šios erdvės reguliavimo būdus ir, antra, kad šie būdai nebūtinai turi būti tokie kraštutiniai kaip siūlyti.

Dėl to kaip pradinė pozicija, bandant sukurti (ar pritaikyti) teisinį reguliavimą elektroninei erdvei, teisėkūroje pradėtas plačiai naudoti elgesio elektroninėje ir fizinėje erdvėje ekvivalentinio vertinimo principas. Jis mokslinėje literatūroje taip pat įvardijamas „technologinio abejingumo“ (angl. *technology indifference*) terminu[42]. Šis principas susijęs su

---

[33] Štitilis, D., *supra* note 7, p. 19.

[34] Sąveika elektroninėje erdvėje dažniausiai vyksta tarp asmens ir informacinių sistemų sudedamųjų dalių (pavyzdžiui, ryšių tinklais asmens su kompiuteriu) arba tarp pačių informacinių sistemų komponentų (pavyzdžiui, sąveika ryšių tinklais tarp keleto kompiuterių). Taip pat patys informaciniai procesai dažnai būna automatizuoti arba automatiniai.

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

[36] Civilka, M., *et al.*, *supra* note 9, p. 511.

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

[38] Kohl, U., *supra* note 4, p. 126–128.
Tokia teisinio reguliavimo įvairovė gali būti siejama su retai minimu, bet būtinu vienu iš teisinio reguliavimo kūrimo aspektų, kad „teisės normos ir principai paprastai atspindi ne vien norminius nustatymus, kas turėtų arba neturėtų įvykti esant tam tikroms aplinkybėms, bet taip pat ir pamatinį pasaulio prigimties suvokimą. Toks priklausomumas nuo empirinio suvokimo yra pagrindas teisėkūros įvairovei“. (Schauer, F. Free Speech and the Demise of the Soapbox. *Columbia Law Review*, 1984, 84 (2): 558).

[39] Reikėtų pritarti nuomonei, kad elektroninė erdvė pati savaime nėra teisinio reguliavimo objektas, nes juo laikytini teisiniai santykiai, kuriems daromas poveikis teisės normomis (Štitilis, D., *op. cit.*, p. 21). Todėl šiame darbe vartojamas bendras elektroninės erdvės reguliavimo terminas reiškia ne pačios elektroninės erdvės kaip objekto reguliavimą, bet poveikį teisiniams santykiams, susijusiems su šia erdve.

[40] Barlow, J. P. A Declaration of Independence of Cyberspace. [interaktyvus], [žiūrėta 2012-09-29]. <https://projects.eff.org/~barlow/Declaration-Final.html>.

[41] Johnson, D. R.; Post, D. G. Law and Borders–The Rise of Law in Cyberspace. *Stanford Law Review.* 1996, 48: 1367.

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

įvairiais technologijų ir teisės derinimo aspektais – jis gali būti laikomas teisėkūros atspirties tašku („kas galioja fizinėje, tas galioja ir elektroninėje erdvėje“), teisėkūros metodu, gairėmis ar teisėkūros pozicija[43]. Tačiau visais šiais atvejais ekvivalentiškumo principas bendriausia prasme atspindi idėją, kad esamos ar kuriamos teisės normos turėtų nustatyti vienodus reikalavimus tiek fizinėje, tiek elektroninėje erdvėje atliekamiems veiksmams. Baudžiamosios teisės srityje tai atitinkamai reikštų, kad baudžiamojo įstatymo normos vienodą vertybių apsaugos lygį šiose erdvėse galėtų užtikrinti būtent per lygiavertį nusikalstamų veikų, padaromų fizinėje ir elektroninėje erdvėse, vertinimą. Taip suvokiant ekvivalentinio vertinimo principą, jo aktualumas pasireiškia tuo, kad jis stabdo „natūralią žmogišką tendenciją elektroninę erdvę vertinti kaip kažką „kito“, kur leidžiami skirtingi ir dažnai žemesni elgesio standartai“[44].

Tačiau ši pažangi lygiaverčio veiksmų vertinimo idėja kelia ir nemažai praktinių jos įgyvendinimo klausimų. Ekvivalentiškumo principas, turintis užtikrinti nuoseklų teisinį reguliavimą, nieko nepasako, kokiomis priemonėmis šis vienodas vertinimas turėtų būti pasiektas. Anot M. Schellekens, teisės norma yra kaip „juoda dėžė“[45] – nors jos turinys turi atitikti minėtus reikalavimus, tačiau kaip tai padaryti paliekama spręsti teisėkūrai ir praktikai. Taigi lygiaverčio vertinimo pasiekimo klausimą šis principas palieka atvirą.

Siekiant išspręsti praktines minėto principo įgyvendinimo problemas, doktrinoje bandoma pagrįsti funkcinio, o ne formalaus ekvivalentiškumo (pagrįsto analogiškomis normomis ir formuluotėmis) svarbą. Pastarojo būdo nepakankamumas akivaizdus, kai kalbama apie situacijas, kurioms tiesiogiai negali būti pritaikyti fizinės erdvės atitikmenys. Analizuojant šiuos būdus, reikėtų pastebėti, kad jie abu vienodai numato tą patį nuoseklaus fizinės ir elektroninės erdvės teisinio reguliavimo (išvengiant spragų) užtikrinimo atspirties tašką. Veiksmams elektroninėje erdvėje vertinti siūloma pasitelkti tas teisės normas, kurios taikomos analogiškiems (ar panašiems) veiksmams fizinėje erdvėje vertinti[46]. Toks sprendimas kartu leidžia išvengti ir bereikalingos teisėkūros. Beje, šio požiūrio ištakas galima įžvelgti pačioje teisės normos prigimtyje, leidžiančioje jai išlikti net ir pasikeitus aplinkybėms – „jeigu be žvilgsnio atgal teisės norma kaip atsakas į nuolat besikeičiančią visuomenę būtų taip pat nuolat besikeičianti, jos iš viso nebūtų. <...> Jeigu taisyklė nuolat kistų <...> teisės norma negalėtų atlikti savo pagrindinių funkcijų, konkrečiai, užtikrinti tikrumo, numatomumo, tvarkos ir saugumo“[47]. Todėl pirmumas šiuo atveju yra teikiamas jau esančios teisės normos pakankamai plačiam interpretavimui, o ne naujų kūrimui. Atitinkamai tokia, anksčiau tik fizinėje erdvėje padaromiems veiksmams reguliuoti taikyta norma, bus kaskart „naujai atrandama“[48] ją taikant ir veiksmams elektroninėje erdvėje.

Tačiau toks teisėkūros atžvilgiu gana ekonomiškas požiūris turi ir trūkumų. Dėl fizinės ir elektroninės erdvės esminių skirtumų dažnai jose atliekamų veiksmų lyginimas ir analogiškas vertinimas gali tapti neįmanomu. Atitinkamai nebus įmanoma atrasti ar sukurti

---

[43] Schellekens, M. What holds Off-Line, also holds On-Line? [interaktyvus], [žiūrėta 2012-09-29]. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=952275>.

[44] Reed, C., *supra* note 35, p. 253.

[45] Schellekens, M., *op. cit.,* p. 6.

[46] *Ibid.*, p. 5.
Formalaus ekvivalentiškumo atveju neneigiama ir specialių teisės normų kūrimo galimybė. Tačiau jos formuluojamos bendrosios normos pagrindu ir jose naudojami analogiški bendrojoje normoje esantys terminai.

[47] Kohl, U., *supra* note 4, p. 133.

[48] Schellekens, M., *op. cit.*, p. 7.

tokioms situacijoms taikytiną tą pačią teisės normą. Į tokius ekvivalentiškumo principo įgyvendinimo sunkumus atkreipė dėmesį ir šio principo taikymo šalininkai (M. Schellekens, U. Kohl, C. Reed ir kt.)[49]. Anot C. Reed, veiksmai elektroninėje erdvėje ne visuomet turi atitikmenį fizinėje erdvėje, tai lemia, kad ekvivalentiškumo principo įgyvendinimas ne visuomet yra galimas[50], o tam tikrais atvejais veiksmų vertinimo lygiavertiškumas „gali pasirodyti neįvykdomas siekis“[51]. Panašios nuomonės yra ir M. Schellekens, kurios teigimu, teisės normos paieška gali baigtis tuo, kad nebus rasta tinkama elgsenos elektroninėje erdvėje vertinimui pritaikoma norma[52]. Šiuo atveju išryškėja ir anksčiau minėto formalaus ekvivalentiškumo požiūrio trūkumai.

Todėl kitas lankstesnis variantas galėtų būti siejamas su C. Reed siūlymu siekti funkcionalaus ekvivalentiškumo[53]. Šis būdas neatmesdamas ir tos pačios teisės normos taikymo galimybių leidžia taip pat sukurti ir naudoti specifines išimtinai elektroninei erdvei pritaikytas teisės normas[54]. Iš tiesų galimos situacijos, kai ta pati teisės norma be pakeitimų bus tinkama reguliuoti elgesį tiek fizinėje, tiek elektroninėje erdvėje. Tačiau tam tikrais atvejais, siekiant užtikrinti atitinkamą vertybių apsaugos lygį virtualioje erdvėje, neišvengiamai taps būtinos specialios tik elgsenai šioje erdvėje vertinti skirtos nuostatos. Tokia išvada aktuali svarstant ir įvairius nusikalstamo elgesio elektroninėje erdvėje kriminalizavimo variantus.

2.1.2. Ekvivalentinio vertinimo principo taikymas kriminalizuojant nusikalstamas veikas elektroninėje erdvėje

Ekvivalentinio vertinimo principo įgyvendinimas baudžiamojoje teisėje bendriausia prasme reikštų, kad tos baudžiamojo įstatymo normos, kurios taikomos nusikalstamoms veikoms, padarytoms fizinėje erdvėje kvalifikuoti, taip pat galėtų būti pritaikomos ir analogiškoms veikoms elektroninėje erdvėje. Toks jų platus interpretavimas (pasitelkiant tinkamą teisinę argumentaciją) užtikrintų baudžiamojo teisinio reguliavimo pakankamumą – praplėtus baudžiamojo įstatymo normų veikimo sritį, neliktų galimybės kalbėti apie BK paliktas spragas, leidžiančias išvengti baudžiamosios atsakomybės už elektroninių nusikalstamų veikų padarymą. Tačiau vertinant, ar toks būdas padėtų išspręsti visų elektroninių nusikalstamų veikų kriminalizavimo problemas, neturėtų būti pamirštama, kad į jų visumą yra įtrauktos ne tik veikos, turinčios aiškų ir be didesnių problemų atrandamą bei pritaikomą atitikmenį fizinėje erdvėje, bet ir tos, kurios tokių tiesiogiai pritaikomų atitikmenų neturi. Tokia nusikalstamų veikų elektroninėje erdvėje įvairovė verčia kalbėti apie minėto funkcinio ekvivalentiškumo požiūrio privalumus ir specialių normų kūrimo poreikį.

Prieš išsamiau aptariant įstatymo leidėjo naudotus ekvivalentinio vertinimo principo įgyvendinimo būdus Lietuvos BK, reikėtų atkreipti dėmesį į nuoseklaus vieno ar kito

[49] Schellekens, M., *supra* note 43, p. 5; Kohl, U., *supra* note 4, p. 150; Reed, C., *supra* note 35, p. 257.

[50] Reed, C., *op. cit.*, p. 264.

[51] Reed, C., *supra* note 42, p. 277.

[52] Schellekens, M., *op. cit.*, p. 5.

[53] Reed, C., *op. cit.*, p. 251.

[54] Tokios išimtys baudžiamosios teisės kontekste būtinos, nes ne visos veikos, kurios padaromos fizinėje erdvėje, gali būti perkeliami į elektroninę erdvę (pavyzdžiui, iššaginimas (BK 149 straipsnis), vagystė (BK 178 straipsnis), turto sunaikinimas arba sugadinimas (BK 187 straipsnis) ir kt.). Ir atvirkščiai – ne visi veiksmai elektroninėje erdvėje gali turėti tiesiogiai pritaikomų analogų fizinėje erdvėje.

pasirinkto būdo taikymo svarbą. Nuoseklumas šiuo atveju užtikrina vienodą požiūrį į konkrečios rūšies elektronines nusikalstamas veikas, o tai leidžia įgyvendinti vienodo vertinimo ir vienodo vertybių apsaugos lygio reikalavimus. Atvirkštinis variantas, kai pirmumas buvo teikiamas pavienių baudžiamosios teisės normų keitimui, neturint bendros elektroninių nusikalstamų veikų (arba bent vienos iš jų rūšių) vertinimo pozicijos, matyti 1961 m. BK. Galiojant šiam BK, įvairūs su elektroninių duomenų ir informacinių sistemų saugumo pažeidimais susiję požymiai: 1) buvo numatyti tik kai kuriose kvalifikuotose tradicinių nusikalstamų veikų sudėtyse (274 straipsnio 2 dalis (Sukčiavimas), 277 straipsnio 2 dalis (Turtinės žalos padarymas apgaule arba piktnaudžiaujant pasitikėjimu)); 2) leido išskirti vienintelę savarankišką, tačiau tik su rinkimų ir referendumo sritimi susijusią nusikalstamą veiką (135[2] straipsnis (Tyčinis poveikis kompiuterinei informacijai ar jos apdorojimui). Šio BK straipsnio pavadinimas mokslinėje literatūroje ne veltui vadintas pribloškiančiai klaidinančiu[55] – tik iš straipsnio turinio galima buvo nustatyti, kad veika yra susijusi su rinkimų ir referendumų tvarkos pažeidimais, o ne su *CIA nusikalstamomis veikomis. CIA nusikalstamos veikos*, galiojant 1961 m., BK kriminalizuotos nebuvo. Dėmesys į tokią ydingą situaciją, kad baudžiamosios teisės normos dėl esamų spragų nepritaikomos naujo pobūdžio pavojingoms veikoms elektroninėje erdvėje kvalifikuoti, buvo atkreiptas ir Lietuvos mokslininkų darbuose. Pasisakant apie 1961 m. BK buvusią nusikaltimų sistemą, pabrėžta, kad „<...> labai daug veikų, kurios galėjo būti priskirtos kompiuteriniams nusikaltimams, kriminalizuotos nebuvo“[56], todėl „įstatymų leidėjas turi labai kruopščiai pasiruošti šiai neišvengiamai kompiuterinei velniavai, numatydamas už tai atsakomybę“[57].

Būtent toks pakankamai chaotiškas su elektroninių duomenų ir informacinių sistemų saugumo pažeidimais susijusio požymio numatymas tik kai kuriose tradicinių nusikalstamų veikų sudėtyse rodė pakankamai fragmentišką įstatymo leidėjo požiūrį į elektronines nusikalstamas veikas. Todėl pagrįstai buvo galima kelti klausimus, kodėl minėtas požymis nebuvo numatytas kitose veikose, kurios taip pat galėjo būti padaromos elektroninėje erdvėje (pavyzdžiui, neteisėtas autorių teisių ar gretutinių teisių techninių apsaugos priemonių pašalinimas (142 (3) straipsnis), šmeižimas (132 straipsnis), oficialaus dokumento suklastojimas ar suklastoto oficialaus dokumento realizavimas ar panaudojimas (207 straipsnis) ir daugelis kitų). Atitinkamai, kodėl elektroninių duomenų ir informacinių sistemų saugumo pažeidimai didino tik jau minėtų 1961 m. BK 274 straipsnio 2 dalyje, 277 straipsnio 2 dalyje numatytų veikų pavojingumą. Tiesa, tuometinėje baudžiamosios teisės teorijoje buvo bandoma pagrįsti didesnį šių veikų pavojingumą, nurodant, kad kompiuterinės technikos panaudojimas sudaro galimybes pasisavinti daugiau turto[58], padaryti daug didesnę žalą valstybei, atskiriems asmenims arba įstaigoms[59]. Tačiau vis dėlto reikėtų pripažinti, kad įvairios elektroninės erdvės suteikiamos galimybės[60] galėjo būti panaudojamos ne tik minėtoms, bet ir kitoms veikoms, pavyzdžiui, šmeižimui, įžeidimui, įvairiems autorių teisių ar gretutinių teisių pažeidimams ir pan., padaryti. Todėl, kaip matyti,

---

[55] Civilka, M., *et al., supra* note 9, p. 526.

[56] *Ibid*., p. 528.

[57] *Ibid*.

[58] Pavilonis, V.; Abramavičius, A. Lietuvos Respublikos baudžiamojo kodekso novelos. *Teisė*, 1994, 1:112.

[59] Abramavičius, A., *et al. Baudžiamoji teisė*. Specialioji dalis. Vilnius: Eugrimas, 2000, p. 397, 421.

[60] Nusikalstamos veikos padarymo greitis, jos mastai, mažos nusikalstamos veikos padarymo sąnaudos, tapatybės nuslėpimo, veikos padarymo įvairiose valstybėse galimybės ir kt.

tuometinis nusikalstamų veikų elektroninėje erdvėje reguliavimas sunkiai galėjo atitikti ekvivalentinio vertinimo principo reikalavimus.

Įsigaliojus 2000 m. BK, situacija iš esmės pasikeitė. Baudžiamoji atsakomybė už nusikalstamų veikų elektroninėje erdvėje padarymą nustatyta dviem skirtingais būdais: 1) specifinėms dėl informacinių ir komunikacijos technologijų vystymosi atsiradusioms veikoms kvalifikuoti BK įtvirtintos savarankiškos normos (BK 196–198[2] straipsniai); 2) tradicinių nusikalstamų veikų, padarytų fizinėje ir virtualioje erdvėje, ekvivalentus vertinimas užtikrintas jų kvalifikavimui taikant tą patį BK straipsnį (pavyzdžiui, baudžiamoji atsakomybė pagal BK 309 straipsnį turėtų kilti nepriklausomai nuo to, ar pornografinio turinio dalykai platinami fizinėje ar elektroninėje erdvėje).

Analizuojant pirmąjį atvejį primintina, kad tokios *sui generis* teisėkūros pagrindimas galėtų būti siejamas su jau minėtais formalaus ekvivalentiškumo trūkumus. Tai situacijos, kai nustatoma, kad elektroninėje erdvėje padaryti veiksmai nepatenka, o iš tikrųjų dėl savo pobūdžio ir negalėtų patekti į jau esamo teisinio reguliavimo sritį. Nuomonė, kad tokiais atvejais teisės normų, numatančių baudžiamąją atsakomybę už tradicinių veikų padarymą, taikymas būtų keliantis abejonių arba visiškai netinkamas, ne kartą išsakyta ir mokslinėje literatūroje (S. W. Brenner, I. Walden)[61]. Pavyzdžiui, S. W. Brenner atkreipė dėmesį į tai, kad *DDos ataka* (angl. *Distributed Denial of Service attack*) neatitinka jokios tradicinių nusikalstamų veikų kategorijos – „tai nėra vagystė, turo prievartavimas ar vandališki veiksmai. Todėl teisė turi pateikti definicijas, naudotinas šioms naujos rūšies nusikalstamoms veikoms apibrėžti“[62]. Beje, tą patį galima būtų pasakyti ir apie kenkėjiškos programinės įrangos (pavyzdžiui, kompiuterinių virusų, *Trojos arklių*) platinimo ir daugelį kitų neteisėtų veikų, kurioms vertinti nėra tiesiogiai pritaikomų atitikmenų fizinėje erdvėje. Pritarus šiai mokslininkų išsakytai pozicijai, vis dėlto reikėtų pastebėti, kad, kuriant naująjį BK (viename iš 2000 m. BK projektų), toks kriminalizavimo nepakankamumo problemos sprendimas (formuluojant savarankiškas baudžiamojo įstatymo normas) buvo siūlomas tik kaip vienas iš galimų variantų. Pagal kitą būdą, kvalifikuojant *CIA nusikalstamas veikas*, siūlyta taikyti bendrojo pobūdžio taisykles bei naudoti tradicines veikas numatančius baudžiamojo įstatymo straipsnius[63]. Toks būdas yra orientuotas į praktinį baudžiamojo įstatymo taikymo lygmenį ir susijęs su pakankamai plačiu tradicinių nusikalstamos veikos sudėties požymių interpretavimu (taip juos pritaikant pagal savo pobūdį naujoms veikoms). Nors toks variantas galėtų atrodyti lankstesnis, tačiau jis neturėtų būti suvokiamas kaip paneigiantis teisės normų apibrėžties ir jų praktinio taikymo ryšį – teismo sprendimas, būdamas racionalus baudžiamojo įstatymo priderinimas prie tikrovės ir konkrečios situacijos, negali iškreipti šių teisės normų esmės[64]. Tokie tradicinių nusikalstamų veikų inkriminavimo apribojimai gali būti kildinami, be kita ko, ir iš baudžiamosios teisės doktrinos ir teismų praktikos nustatytų konkrečių nusikalstamų veikų sudėties

[61] *Computer Law: The Law and Regulation of Information Technology*. Reed, C.; Angel, J. (eds). 6-asis leidimas. Oxford: Oxford University Press, 2007, p. 564; *The History of Information Security: A Comprehensive Handbook*. Leeuw, D. K.; Bergstra, J. (eds). Amsterdam, *et al.*: Elsevier, 2007, p. 706.

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

[63] Petrauskas, R.; Štitilis, D. *Kompiuteriniai nusikaltimai ir jų prevencija*. Vilnius: Lietuvos teisės akademijos Leidybos centras, 2000, p. 46.

[64] Pikelis, A. *Baudžiamosios teisėkūros labirintai: Lietuvos Aukščiausiojo Teismo senato nutarimas ir teismų praktika taikant Baudžiamojo kodekso 178 ir 180 straipsnius*. Vilnius: Petro ofsetas, p. 150.

požymių turinio ribų. Jų nepaisymas ir pakankamai platus sudėties požymių aiškinimas sukeltų nemažai esminių kvalifikavimo problemų, *inter alia* panaikintų nusikalstamų veikų atribojimo kriterijus, todėl daugumos baudžiamojo įstatymo teisės normų, turinčių teorinį ir praktinį pagrindimą, taikymas taptų sudėtingas[65]. Būtent tokia situacija ir leidžia kalbėti apie esminius veikų, padarytų fizinėje ir elektroninėje erdvėje, skirtumus, atitinkamai ir savarankiškų *CIA nusikalstamoms veikoms* taikytinų baudžiamojo įstatymo normų poreikį. Tačiau į šiuos skirtumus neturėtų būti pažvelgta pernelyg supaprastintai – net jei *CIA nusikalstamos veikos* iš pirmo žvilgsnio gali pasirodyti neturinčios analogų fizinėje erdvėje, naujos ir sunkiai paaiškinamos, tačiau vis dėlto kai kurie jų aspektai paprastai leis pamatyti tam tikrų panašumų su tradicinėmis nusikalstamomis veikomis. Todėl, pavyzdžiui, apie neteisėto įsibrovimo doktrinos vystymąsi „skaitmeniniame kontekste“ liudija neteisėto prisijungimo prie informacinės sistemos veika (BK 198[1] straipsnis), taip pat į neteisėto disponavimo neviešais elektroniniais duomenimis (BK 198 straipsnis) dalyką metaforiškai bandoma pažvelgti kaip į asmens „kvazi – fizinius daiktus“ elektroninėje erdvėje, kurie kaip ir materialūs daiktai gali būti slepiami, laikomi arba perkeliami, perduodami[66]. Funkcinis ekvivalentiškumas tokiais atvejais pasireikštų tuo, kad neradus pritaikomos normos elektroninėje erdvėje padarytiems veiksmams vertinti būtų koncentruojamasi į „panašumus nepaisant skirtumų“[67] ir naujos normos kuriamos atsižvelgiant į esamą artimiausio tokių veiksmų atitikmens fizinėje erdvėje reguliavimą. Beje, toks požiūris nėra svetimas – be metaforiško abstrakcijų vertimo daiktais (sudaiktinimo) neapsieinama ir kitose teisės šakose, pavyzdžiui, civilinėje teisėje kalbant apie turtines teises[68] *inter alia* autorines teises[69] ir pan.

Antruoju atveju (analizuojant tradicines dėl technologijų panaudojimo pakitusias veikas), kriminalizavimo būdo pasirinkimą lemia įstatymų leidėjo pozicija, ar naujųjų technologijų panaudojimas turėjo lemiamos įtakos tradicinių nusikalstamų veikų sudėties požymių turinio aiškinimui[70], taip pat ar esamos tradicinių nusikalstamų veikų sudėtis

---

[65] Pavyzdžiui, siekiant, kad neteisėtam elektroninių duomenų įgijimui kvalifikuoti galėtų būti taikomas BK 178 straipsnis, turėtų būti atsisakoma vagystės dalyką apibūdinančio turto materialumo požymio. Tačiau tokie pakeitimai, be kitų, sukeltų ir BK 178 bei 179 straipsniuose numatytų veikų atribojimo problemų.

[66] Apie tai plačiau žiūrėti III ir IV dalyse.

[67] Reed, C., *supra* note 35, p. 265.

[68] Pobedonoccev, K. Kurs grazhdanskago prava. Pervaja chast. [The course of civil law. First part]. Sanktpeterburg, 1896, s. 1–7; Fedosiuk, O. Nuosavybė ir turtas Civiliniame ir Baudžiamajame kodeksuose. *Jurisprudencija*. 2002, 28(20).

[69] Arlauskas, S. Metaforos ir normos: autorinių teisių samprata skaitmeninėje visuomenėje/Knygos recenzija. *Socialinių mokslų studijos*. 2013, 5(1).

[70] Mokslinėje literatūroje nėra vieningos nuomonės, ar naujųjų technologijų panaudojimas turėtų būti vertintinas kaip aplinkybė pakeitusi tradicinių nusikalstamų veikų prigimtį ir leidžianti kalbėti apie atsiradusią naują nusikalstamų veikų rūšį. Ši problema vaizdžiai pateikiama frazėmis *new wine, no bottles* ir *old wine in new bottles.* Frazė *new wine, no bottles* vartojama kai norima pabrėžti išskirtines elektroninės erdvės savybes ir pasakyti, kad joje atsiranda visiškai naujos nusikalstamo elgesio apraiškos (plačiau žr. Walden, I. *Computer Crimes and Digital Investigations*. Oxford: Oxford 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 pateikti vartojama frazė *old wine in new bottles*, reiškianti, kad naujųjų technologijų panaudojimas esminės įtakos tradicinėms nusikalstamoms veikoms neturėjo. Jų pasitelkimas reiškia ne ką kitą kaip 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).

numatančios normos yra pakankamos analogiškoms veikoms padarytoms elektroninėje erdvėje kvalifikuoti[71].

Pritarus požiūriui, kad elektroninės erdvės panaudojimas yra aplinkybė, leidžianti kalbėti apie iš esmės naują nusikalstamų veikų rūšį, kurių vertinimui nepakankamas nustatytas teisinis reguliavimas (tiek nusikalstamumo, tiek ir baudžiamumo prasme), pasirenkamas specialių normų kūrimo būdas. Pavyzdžiui, kompiuterinis sukčiavimas kaip speciali sukčiavimo norma numatyta Latvijos (177 (1) skyrius), Estijos (213 paragrafas), Lenkijos (287 straipsnis) ir Vokietijos (263a skyrius) baudžiamuosiuose įstatymuose.

Kitas galimas teisėkūros variantas teikia prioritetą lankstumui prieš kazuistinį reguliavimą – jis leidžia baudžiamajame įstatyme atsisakyti tiesioginių nuorodų į informacines ir komunikacijos technologijas. Tokiais atvejais esamų tradicinių nusikalstamų veikų sudėčių požymiai teisės taikymo lygmeniu interpretuojami plačiai, technologijų panaudojimo aplinkybę vertinant tik tiek, kiek ji praplėtė šių tradicinių veikų padarymo būdus. Šiuo atveju informacinių ir komunikacijos technologijų panaudojimo požymis, leidžiantis padarytą veiką priskirti tradicinių dėl technologijų panaudojimo pakitusių veikų grupei, galės būti nustatomas ne iš straipsnio dispozicijos, o iš praktiniame šios normos taikymo lygmenyje pateikto išaiškinimo. Aišku reikėtų sutikti, kad toks į tradicinių nusikalstamų veikų sudėties požymių pakankamai platų aiškinimą orientuotas baudžiamosios atsakomybės nustatymo būdas vertinimo prasme yra sudėtingesnis. Todėl išvadai, kad baudžiamajame įstatyme nustatyta atsakomybė už tokio pobūdžio veikas, yra būtina baudžiamosios teisės teorijos ir teismų praktikos analizė. Specialių normų trūkumas šiuo atveju negali nieko pasakyti apie tinkamą ar priešingai – netinkamų dėl naujųjų technologijų pakitusių tradicinių nusikalstamų veikų kriminalizavimą.

Šiuo aspektu vertinant Lietuvos BK specialiosios dalies nuostatas, matyti, kad įstatymų leidėjas pasirinko antrąjį lankstesnį šių nusikalstamų veikų įtvirtinimo būdą. Tokią išvadą leidžia daryti tai, kad po Konvencijos dėl elektroninių nusikaltimų ratifikavimo (2004 m. sausio 22 d.) BK 182, 192, 300 ir 309 straipsniai nebuvo papildyti požymiais, vienu ar kitu aspektu susijusiais su informacinėmis ar komunikacijos technologijomis. Taip pat baudžiamajame įstatyme nebuvo numatytos ir specialios tokias elektronines nusikalstamas veikas numatančios normos. Beje, tokių požymių nenumato ir kitos tradicinių nusikalstamų veikų sudėtys, nors šios veikos pagal savo pobūdį taip pat gali būti padaromos elektroninėje erdvėje (pavyzdžiui, šmeižimas, įžeidimas, terorizmo kurstymas ir kt.). Todėl minėtų tradicinių veikų pritaikymas naujoms su elektroninės erdvės specifika susijusioms situacijoms, paliktas baudžiamosios teisės doktrinai ir teismų praktikai[72].

---

[71] Baudžiamojo įstatymo normos, taikytinos kvalifikuojant tradicines nusikalstamas veikas, gali būti pritaikomos analogiškoms veikoms elektroninėje erdvėje, jei: 1) tradicinių nusikalstamų veikų sudėtyse nėra numatyta požymių, turinčių tiesioginės sąsajos su fizine erdve, arba į sudėtį įtraukti alternatyvūs materialios išraiškos nežymintys požymiai (tai aktualu kalbant ne tik apie nusikalstamos veikos dalyką, bet ir apie pačią pavojingą veiką, padarinius ir kt.); 2) subjektyviesiems požymiams nustatyti netrukdo ta aplinkybė, kad informacinių ir komunikacijos technologijos neturi fiziniam asmeniui būdingos sąmonės (pavyzdžiui, vertinant apgaulės kaip kito asmens suklaidinimo būdo panaudojimo faktą).

[72] Kaip pavyzdį galima paminėti BK 300 straipsnį, kuriame kriminalizuotas dokumento suklastojimas ar disponavimas suklastotu dokumentu. Po Konvencijos dėl elektroninių nusikaltimų ratifikavimo 2004 m. sausio 22 d., BK 300 straipsnis buvo keistas, tačiau šie pakeitimai nebuvo susiję su konvencinių nuostatų įgyvendinimu (Konvencijos 7 straipsnis). Platesnio šios nusikalstamos veikos sudėties požymių interpretavimo tendencijos matyti teismų praktikoje. Pavyzdžiui, Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų

Tačiau reikėtų paminėti, kad mokslinėje literatūroje vis dėlto galima sutikti ir kitokių, pirmumą pažodiniam konvencinių nuostatų perkėlimui į nacionalinę teisę teikiančių, nuomonių. Anot D. Sauliūno, Konvencijos dėl elektroninių nusikaltimų 8 straipsnis numato aiškią pareigą Lietuvai kriminalizuoti *expressis verbis* kompiuterinį sukčiavimą, kaip specifinę sukčiavimo rūšį[73]. Vis dėlto su tokia išvada neleidžia sutikti pačios Konvencijos aiškinamojoje ataskaitoje[74] nurodytos jos nuostatų įgyvendinimo nacionalinėje teisėje galimybės. Šios aiškinamosios ataskaitos 79 punkte nurodoma, kad Konvencijos 7–10 straipsniai yra susiję su tradicinėmis nusikalstamomis veikomis (nusikaltimais), kurios padaromos naudojant kompiuterinę sistemą. Kadangi dauguma valstybių yra kriminalizavusios analogiškas tradicines veikas, tai jau esamos sudėtys gali būti arba nėra pakankamai plačios, kad būtų pritaikomos naujoms situacijoms. Todėl valstybės, įgyvendindamos konvencines nuostatas, turi įvertinti esamas teisės normas ir nustatyti, ar įrodžius kompiuterinės sistemos ar kompiuterių tinklo panaudojimo faktą, šios normos galės būti taikomos. Jei esančios teisės normos apima tokio pobūdžio pavojingas veikas, Konvencija nenustato reikalavimo keisti tradicinių nusikalstamų veikų sudėtis arba baudžiamajame įstatyme numatyti naujas nusikalstamas veikas (nusikaltimus). Kaip matyti, Konvencijos aiškinamojoje ataskaitoje pateiktas pakankamai lankstus ir į valstybių nacionalinės teisės tradicijas atkreipiantis dėmesį požiūris. Be to, elektroninių nusikalstamų veikų doktrinoje, dar net neįsigaliojus 2000 m. BK, buvo manoma, kad bendroji naujojo BK 182 straipsnyje numatyta sukčiavimo norma galės būti taikoma ir elektroniniam sukčiavimui kvalifikuoti[75].

Taigi apibendrinus galima būtų teigti, kad pasirinktų elektroninių nusikalstamų veikų kriminalizavimo būdų įvairovę lemia pakankamai skirtingos į jų visumą įtrauktos veikos. Kai yra kalbama apie tradicines veikas, pakitusias dėl naujųjų technologijų panaudojimo, jų lygiavertį vertinimą įmanoma užtikrinti pasitelkus BK normas, numatančias atsakomy-

---

skyriaus teisėjų kolegijos 2010 m. rugsėjo 28 d. nutartyje baudžiamojoje byloje (bylos Nr. 2K-426/2010) atkreiptas dėmesys ne į dokumento formos (materialus ar elektroninis dokumentas), o į jo turinio svarbą: *Kolegija pažymi, kad <...> 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)*.

Panaši situacija ir sukčiavimo (BK 182 straipsnis) atveju. Apgaulės, būtinos konstatuoti, kad buvo padarytas sukčiavimas, ribos praplėstos teismų praktikoje. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2001 m. spalio 9 d. nutartyje baudžiamojoje byloje (bylos Nr. 2K-682/2001) pripažinta, kad melagingomis žiniomis gali būti suklaidinamas ne tik žmogus, bet ir elektroninė sistema: *<...> 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, ir taip suklaidina elektroninę sistemą ir kartu banką.* Taip pat bendrosios BK 182 straipsnyje numatytos sukčiavimo normos taikymas elektroninio sukčiavimo atvejais matyti žemesnių instancijų teismuose (pavyzdžiui, Klaipėdos miesto apylinkės teismo 2010 m. rugsėjo 16 d. teismo baudžiamasis įsakymas baudžiamojoje byloje (bylos Nr. 1-1039-659/2010), Šilalės rajono apylinkės teismo 2010 m. lapkričio 4 d. teismo baudžiamasis įsakymas baudžiamojoje byloje (bylos Nr. 1-121-799/2010), Vilniaus miesto 1 apylinkės teismo 2009 m. rugsėjo 14 d. nuosprendyje baudžiamojoje byloje (bylos Nr. N1-1470-88/2009) ir kt.).

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

[74] Convention on Cybercrime Explanatory Report [interaktyvus], [žiūrėta 2012-01-24]. <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>.

[75] Štitilis, D., *supra* note 7, p. 149.

bę už analogiškas fizinėje erdvėje padaromas veikas. Tačiau toks ekvivalentinio vertinimo įgyvendinimas yra probleminis, kai bandomos kvalifikuoti *CIA nusikalstamos veikos*, – pastarosioms „atrasti" galinčios tikti baudžiamojo įstatymo normos nėra įmanoma. Todėl akivaizdu, kad siekiant funkcinio ekvivalentiškumo būtinos savarankiškos tik už jų padarymą atsakomybę numatančios normos.

2.2. Nusikalstamų veikų elektroninėje erdvėje požymių aiškinimas ir technologinio neutralumo principas

Nusikalstamų veikų elektroninėje erdvėje sudėties požymių aiškinimui įtakos turi sparti informacinių ir komunikacijos technologijų raida. Kadangi šios technologijos nuolat kinta, tai akivaizdus ir greitas tokio pobūdžio nusikalstamų veikų vystymasis. Atsižvelgiant į tai, įvairūs nusikalstamų veikų elektroninėje erdvėje kriminalizavimo aspektai kaskart turėtų būti vertinami jų pakankamumo požiūriu, nustatant, ar esamas *status quo* atitinka besikeičiančias aplinkybes. Nors tokia peržiūra aktuali vertinant visų elektroninių nusikalstamų veikų požymių pakankamumą, tačiau jos svarba bene aiškiausiai matyti tais atvejais, kai nuorodos į informacines ir komunikacijos technologijas įtvirtintos tiesiogiai straipsnio dispozicijoje. Todėl toliau darbe didesnis dėmesys bus skiriamas technologinio neutralumo principo taikymui aprašant ir aiškinant *CIA nusikalstamų veikų* sudėties požymius. Šio principo aktualumas bendriausia prasme pasireiškia tuo, kad jis: 1) leidžia išvengti daugelio dėl naujųjų technologijų pasikeitimo galinčių kilti *CIA nusikalstamų veikų* sudėties požymių nepritaikomumo problemų (ypač nustačius reikšmingus technologijų pokyčius); 2) padeda nuspręsti, kokia prasmė turėtų būti suteikiama įvairiems nusikalstamų veikų sudėtyse naudojamiems ir su informacinėmis bei komunikacijos technologijomis susijusiems terminams (pavyzdžiui, informacinė sistema, šios sistemos apsaugos priemonės, kompiuteris, elektroniniai duomenys ir kt.). Juo labiau kad BK nėra pateiktas autentiškas šių sąvokų išaiškinimas.

2.2.1. Technologinio neutralumo principo samprata

Su naujosiomis technologijomis turinčių ryšį nusikalstamų veikų sudėties požymių turinys yra pakankamai dinamiškas, o tai kelia sudėties požymių apibrėžtumo bei tinkamos terminijos parinkimo problemas. Bendriausia prasme tokie gana keblūs technologiniai – baudžiamieji teisiniai sudėties požymių aiškinimo sunkumai gali būti įvardyti arba kompiuterinėje etikoje suformuluotu „konceptualios painiavos"[76] terminu arba baudžiamosios teisės moksle minimu „technologijų ir terminologijos klausimu". Šis klausimas profesoriaus I. Walden susietas su „ribų, šviesiosios linijos (angl. *bright line*)"[77] nustatymu ir iš to logiškai išvedamu baudžiamojoje sferoje itin svarbiu teisinio tikrumo (angl. *legal certainty*)

[76] Moor, J. H. What is Computer Ethics. [interaktyvus], p. 18, [žiūrėta 2012-09-09]. <http://www.blackwellpublishing.com/content/BPL_Images/Content_store/Sample_chapter/9781855548442/CEAC01.pdf>.

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

principu“[78]. Minėtą technologijų ir terminologijos problemą bene aiškiausiai leidžia suvokti technologinio neutralumo principas, kuris teisėkūros lygmeniu pasitelkiamas informacinių ir komunikacijos technologijų kitimo problemoms spręsti (atsižvelgus į įstatymo leidėjo valią, gali būti taikomas ir baudžiamosios teisės normų aiškinimo ir taikymo atveju).

Išvada, kas BK yra suprantama ties vienu ar kitu technologinį aspektą turinčiu sudėties požymiu (atitinkamai, kokios yra jo turinio ribos), priklauso nuo pasirinkto vieno iš galimų jų interpretavimui taikytinų principų – technologinio neutralumo (angl. *technological neutrality*) arba technologinio tikslumo (angl. *technological specific*). Nors abu šie principai naudojami su technologijomis susijusios teisėkūros srityje[79], tačiau mokslinėje literatūroje (J.–B. Koops, R. W. Downing, C. A. Kirby ir kt.)[80] vis dėlto dominuojančiu, nors ir su tam tikromis išimtimis ir kritika (P. Ohm, C. Reed ir kt.)[81], laikomas lygiavertį technologijų vertinimą užtikrinantis technologinio neutralumo principas. Į technologiškai neutralų teisinį reguliavimą, pagrįstą pripažinimu, kad informacinėje terpėje vykstantys pokyčiai, lemiantys „vartotojų unikalią sąsają elektroninėje erdvėje“[82], yra pernelyg spartūs, kad prie jų galima būtų bandyti priderinti teisės normas, atkreiptas dėmesys ir tarptautiniu lygmeniu priimtose deklaracijose[83].

Technologinio neutralumo kaip *gerojo* reguliavimo principas pirmą kartą Europos Sąjungos lygiu daugiausiai dėmesio sulaukė telekomunikacijų reguliavimo peržiūrėjimo metu (vėliau minimas ir kitose srityse). Kaip vienas iš penkių reguliavimo principų jis apibūdintas per technologijų diskriminavimo draudimą, t. y. teisinis reguliavimas „neturi nei nustatyti, nei diskriminuoti, teikdamas pirmenybę konkrečios rūšies technologijoms, o turi užtikrinti, kad ta pati paslauga būtų reguliuojama lygiaverčiu būdu, neatsižvelgiant į būdus, kuriais ji yra suteikta“[84]. Panašiai technologinio neutralumo principas, atkreipiant dėmesį į teisės normos tikslus, o ne konkrečias technologijas (technologinį tikslumą), suformuluotas ir Lietuvos Respublikos elektroninių ryšių įstatymo (toliau – Elektroninių ryšių įstatymas) 2 straipsnio 2 dalyje. Čia, 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 kad teisės normos būtų taikomos kiek

[78] Walden, I., *supra* note 70, p. 13.

[79] Atsižvelgus į įstatymo leidėjo valią, pasitelkiami ir baudžiamosios teisės normų aiškinimo bei taikymo atveju.

[80] Koops, B.–J. *Should ICT regulation be Technology-Neutral?* [interaktyvus], [žiūrėta 2013-04-24]. <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.

[81] Ohm, P. The Arguments against Technology–Neutral Surveillance Laws. *Texas Law Review*, 2010, 88(7); Reed, C. *supra* note 42.

[82] Štitilis, D., *supra* note 7, p. 7.

[83] Pasaulinio aukščiausio lygio susitikimo informacinės visuomenės klausimais, vykusio Ženevoje 2003 m. gruodžio 10–12 d., metu priimta principų deklaracija „Informacinės visuomenės sukūrimas – globalus naujojo tūkstantmečio uždavinys“. [interaktyvus], [žiūrėta 2012-04-20]. <http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1161%7C1160>.

[84] 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 2013-06-02]. <www.ictregulationtoolkit.org/en/Document.1501.pdf>.

įmanoma neatsižvelgiant į technologijas, kurios naudojamos su konkrečiu teisiniu santykiu susijusiems elektroninių ryšių tinklams ar elektroninių ryšių paslaugoms teikti".

Į technologinio neutralumo principo galimybes užtikrinti lygiavertį technologijų vertinimą atkreiptas dėmesys ir įvairiuose šį principą tyrinėjusių mokslininkų darbuose (P. Ohm, R. Ali, I/ M. van den Haar, B.-J. Koops ir kt.)[85]. Be to, juose technologijoms neutralus teisinis reguliavimas susietas ir su tokio reguliavimo pastovumu bei efektyvumu, nes jis šių savybių nepraras ir pakitus technologijoms. Kadangi akivaizdu, kad technologijos vystosi daug greičiau nei su jomis susijusios teisės normos, tai galima būtų pritarti R. Ali pastebėjimui, kad „reguliavimas turi būti lankstus, nekintantis ilgesnį laiką ir atviras technologijų pokyčiams"[86]. Panašios nuomonės yra ir I. M. van der Haar, kuri teisinio reguliavimo pastovumą susiejo su reikalavimu, kad „vietoj nekintamų specifines technologijas mininčių normų turėtų būti kuriamos dinamiškos kartu su technologijomis galinčios vystytis normos"[87]. Tuo tarpu technologinio tikslumo principas tokio lankstumo užtikrinti negali – nuolat vystantis technologijoms teisinis reguliavimas savo efektyvumą gali prarasti bet kuriuo momentu. Todėl ne veltui P. Ohm darbuose šio tipo reguliavimas susietas su „technologijų saulėlydžio"[88] terminu.

Žiūrint iš baudžiamosios teisės pozicijų ir įvertinus teisės bei technologijų sąveikos perspektyvas, šis principas leidžia išvengti teisės normų taikymo apribojimų, galinčių kilti dėl jose naudojamų su technologijomis susijusių požymių. Kaip teigia R.W. Downing, „jei įstatymų leidėjas nusprendė uždrausti konkrečios rūšies veiksmus su prijungtu prie Interneto namų kompiuteriu, tai *technologiškai neutrali* strategija įpareigotų tokią pat veiką laikyti nusikalstama, jei ji padaryta naudojant asmeninį delninį kompiuterį, mobilų telefoną ar kitos kartos skaitmeninius prietaisus"[89]. Taigi technologinio neutralumo principą grindžiant technologijų diskriminavimo draudimu, jis iš esmės reiškia ne ką kitą kaip draudimą teikti prioritetą vienai technologijai prieš kitą. Todėl pagal jį nusikalstamos veikos sudėties požymiai turėtų būti apibrėžiami taip, kad netaptų priklausomi nuo informacinių ir komunikacijos technologijų pokyčių, specifinių jų savybių, jei toks priklausomumas nėra įstatymo leidėjo valia. Taip pat baudžiamajame įstatyme turėtų būti vengiama nuorodų į konkrečius nusikalstamų veikų padarymo būdus elektroninėje erdvėje (pavyzdžiui, kaip buvo prisijungta ar kokiu būdu buvo padarytas neteisėtas poveikis informacinei sistemai ir pan.), o dėmesys kreipiamas į rezultatą, kuris atsiranda dėl tokių neteisėtų veikų (pavyzdžiui, veika buvo pažeistas informacinės sistemos konfidencialumas arba sistema tapo neprieinama teisėtiems vartotojams ir pan.).

Kaip technologiškai specifinių terminų vartojimo atvejį, sukėlusį nepakankamo kriminalizavimo problemą, galima būtų paminėti kaimyninių valstybių (Latvija, Estija ir kt.) ankstesnius bandymus nustatyti baudžiamąją atsakomybę už disponavimą kenkėjiškomis programomis. Šių valstybių kodeksuose nurodžius kompiuterinio viruso terminą liko nekriminalizuotas *Trojos arklių* ir kitų kenkimo programų kūrimas bei platinimas[90]. Tam tikrų

[85] Ohm, P., *supra* note 81; Ali, R. Technological Neutrality. *Lex Electronica*, 2009, 14(2); Van der Haar, I. M. Technological Neutrality: What Does It Entail? [interaktyvus], [žiūrėta 2013-06-01]. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=985260>; Koops, B.–J., *supra* note 80.

[86] Ali, R., *op. cit.*, p. 12.

[87] Van der Haar, I. M., *op. cit.,* p. 24.

[88] Ohm, P., *op. cit.*, p. 1686.

[89] Downing, R. W., *supra* note 80, p. 716.

[90] Štitilis, D., *supra* note 7, p. 145.

nesklandumų neišvengta ir Lietuvos BK nustatant baudžiamąją atsakomybę už *CIA nusikalstamas veikas*. 2003 m. įsigaliojus naujajam BK, jo XXX skyriuje aprašytose nusikalstamose veikose vartotas terminas „kompiuterinė informacija", taip paliekant neaiškumų, ar terminai informacija ir duomenys turėtų būti, anot įstatymo leidėjo, laikomi sinonimais, ar iš tikrųjų tarp jų yra padarytas sąmoningas skirtumas. Kadangi šis terminų atskyrimas yra pakankamai svarbus[91], tai mokslinėje literatūroje vis dėlto daryta prielaida, kad šių terminų skirtumo įstatymo leidėjas neįžvelgė, atitinkamai jie vartoti kaip sinonimai[92].

Taip pat galimybę baudžiamosios teisės kontekste minėti technologinio neutralumo principą, jo privalumus ir trūkumus suteikia Konvencijos dėl elektroninių nusikaltimų aiškinamojoje ataskaitoje nurodytas nacionalinėje teisėje įgyvendintinų ir su materialine baudžiamąja teise susijusių nuostatų interpretavimo būdas. Konvencijoje, nustačius minimalius nusikalstamų veikų elektroninėje erdvėje sudėties požymiams keliamus reikalavimus, neišvengta su informacinėmis ir komunikacijos technologijomis susijusios terminijos. Atsižvelgiant į tai, Konvencijos aiškinamojo rašto 36 punkte pateiktas jos įgyvendinimui nacionalinėje teisėje svarbus išaiškinimas, kad „nors materialinės baudžiamosios teisės nuostatos yra susietos su nusikaltimais, padaromais naudojant informacines technologijas, Konvencija vartoja technologiškai neutralią kalbą, kad teisės pažeidimai, už kuriuos baudžiama pagal baudžiamuosius įstatymus, galėtų būti taikomos abejoms – naudojamoms dabartinėms ir būsimosioms technologijoms" (36 punktas)[93].

2.2.2. Technologinio neutralumo principo taikymo problemos ir galimi jų sprendimo būdai

Nors technologinio neutralumo principas atrodytų galintis išspręsti pakankamai daug tiek teisėkūros, tiek ir baudžiamosios teisės normų aiškinimo problemų, tačiau jis kelia ir nemažai jo praktinio taikymo klausimų. Iš jų bene svarbiausi būtų: 1) kaip užtikrinti technologijoms neutralų nusikalstamos veikos sudėties požymių interpretavimą; 2) kaip pasiekti, kad toks požymių aiškinimas būtų suderintas su baudžiamojoje teisėje svarbiais legalumo (lot. *nullum crimen, nulla poene sine lege*) ir teisinio tikrumo principais.

Pagal technologinio neutralumo principą *CIA nusikalstamų veikų* inkriminavimui neturėtų sudaryti kliūčių technologijų, tiek naudojamų kaip nusikalstamos veikos priemonė ar įrankis, tiek ir galinčių būti nusikalstamos veikos dalyku, įvairovė. Požiūris, kad pačios technologijos savaime yra „neutralios"[94], todėl dėl jų panaudojimo kilus neigia-

---

[91] Informacinių sistemų naudotojui elektroniniai duomenys gali būti nematomi ir nesuprantami (pavyzdžiui, duomenų apdorojimo ar jų perdavimo procese), todėl jie informacija tampa tuomet, kai įgyja prasmę. Pakeitus duomenis, informacija, kurią suvokia naudotojas, gali ir nekisti. Pavyzdžiui, neteisėtai padarius pakeitimus kompiuterio *host rinkmenoje (*angl. *host file)*, naudotojas gali būti nukreipiamas, į suklastotus elektroninės bankininkystės puslapius. Atrodytų, kad pakeitus elektroninius duomenis, vaizdo informacija, kurią suvoks naudotojas, patekęs į suklastotą puslapį, taip pat turėtų keistis. Tačiau padaryti pakeitimai *host rinkmenoje* naudotojui dažniausiai nebus suvokiami dėl suklastoto puslapio itin didelio panašumo į tikrąjį. Be to, jis nesupras ir užslėptos šio tinklalapio funkcijos (surinkti asmens tapatybės patvirtinimo priemonių duomenis, persiųsti juos į kaltininko sukurtas elektroninio pašto dėžutes ir pan.).

[92] Civilka, M., *et al*., *supra* note 9, p. 529.

[93] The Explanatory Report to the Convention on Cybercrime. [interaktyvus], [žiūrėta 2012-08-26]. <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>.

[94] Ali, R., *supra* note 85, p. 6.

moms pasekmėms (pavyzdžiui, naudojantis jomis padaroma nusikalstama veika) turėtų būti koncentruojamasi ne į pačias technologijas, o į netinkamą jų naudojimą, yra artimas instrumentalinei teorijai[95]. Ji pagrįsta idėja, kad bet kokia technologija yra tik priemonė, skirta jos naudotojo tikslams siekti. Ne veltui C. Reed pabrėžė, kad „informacinės ir komunikacijos technologijos jų pačių labui niekada nebuvo išsamiai reguliuojamos, tačiau buvo siekta kontroliuoti tokių technologijų naudotojus ir naudą, kuri yra gaunama iš jų“[96]. Tai leidžia daryti išvadą, kad nusikalstamos veikos inkriminavimui neturėtų trukdyti technologijų pokyčiai, nes pavojingumą paprastai rodo ne jos pačios, bet jomis padaroma žala ar sukeliama žalos grėsmė saugomoms vertybėms ir kiti požymiai.

Dėl to baudžiamojo įstatymo normų pritaikomumas įvairiems atvejams gali būti užtikrinamas dviem glaudžiai vienas su kitu susijusiais būdais: 1) per technologijoms neutralų tokių požymių aprašymą BK straipsnio dispozicijose (prioritetą teikiant bendriems terminams, o ne konkrečioms technologijoms); 2) per technologijoms neutralų jų interpretavimą (atsižvelgiant į plečiamojo aiškinimo draudimą).

Daugelis minėto principo įvairius aspektus nagrinėjusių mokslininkų (I. M. van der Haar, P. Ohm, B.–J. Koops ir kt.)[97], neutralumo technologijų atžvilgiu įgyvendinimą pirmiausia siejo su tinkamu jų apibrėžimų konstravimu. Kuriant teisinį reguliavimą, anot I. M. van der Haar, „turėtų būti pasirenkamos į funkcijas nukreiptos definicijos, kurios, į jas neįtraukus užuominų apie pačias technologijas, būtų priklausomos tik nuo funkcijas žyminčių sąvokų“[98]. Į poveikio, funkcijų ir bendriausių požymių, o ne konkrečios rūšies technologijų svarbą atkreipė dėmesį ir P. Ohm, kuris technologinio neutralumo užtikrinimą susiejo su „plačios, atviros tekstūros terminais, kurie nusako tikslus, poveikį, funkcijas ir kitas bendras savybes“[99]. Tokius siūlymus vertinant iš baudžiamosios teisės pozicijų, jie reikštų, kad prioritetas formuluojant ir aiškinant su technologijomis susijusius požymius turėtų būti teikiamas bendriausią reikšmę turintiems terminams, technologijų funkcijas, o ne pačias technologijas numatančioms sąvokoms. Būtent tai leistų išvengti galimų baudžiamosios teisės spragų pakitus vienai ar kitai technologijai.

Vienas iš tokios definicijos pavyzdžių – Konvencijos dėl elektroninių nusikaltimų 1 straipsnyje pateiktas kompiuterinės sistemos apibrėžimas. Pagal jį „kompiuterinė sistema – tai įtaisas arba tarpusavyje sujungtų ar susijusių įtaisų grupė, iš kurių vienas ar daugiau pagal programą automatiškai apdoroja duomenis“[100]. Konvencijos aiškinamosios ataskaitos 23 punkte šis apibrėžimas detalizuotas, kad „Konvencijoje kompiuterinė sistema yra prietaisas, sudarytas iš aparatinės įrangos ir programinės įrangos, sukurtos apdoroti skaitmeninius duomenis. Jis gali apimti įvesties, išvesties ir saugojimo priemones. Jis gali būti vienas arba gali būti sujungtas tinklu su kitais panašiais prietaisais“[101]. Kaip matyti, Konvencijoje pateiktu kompiuterinės sistemos sąvokos apibrėžimu nebuvo siekta tiksliai išspręsti šios sąvokos apibrėžties problemą – kompiuterinės sistemos terminas aprašytas gana abstrakčiomis sąvokomis ir sistemos atliekamomis funkcijomis. Be kita

[95] Ali, R., *supra* note 85, p. 6.

[96] Reed, C., *supra* note 42, p. 282.

[97] Van der Haar, I. M., *supra* note 85; Ohm, P., *supra* note 81, p. 1687; Koops, B.–J., *supra* note 80.

[98] Van der Haar, I. M., *op. cit*., p. 23.

[99] Ohm, P., *op. cit.*, p. 1687.

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

[101] The Explanatory Report to the Convention on Cybercrime. [interaktyvus], [žiūrėta 2012-08-26]. <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>.

ko, Konvencijos dalyvėms taip pat suteikta diskrecija atsisakyti pažodinio šių nuostatų įgyvendinimo (22 punktas)[102].

Vis dėlto iš pirmo žvilgsnio atrodanti gana pažangi daugelio autorių keliama į technologijų funkcijas orientuoto apibrėžimo idėja baudžiamosios teisės kontekste galėtų susilaukti ir kritikos. Pirmiausia, pakankamai abstrakčios sąvokos neleidžia nustatyti baudžiamosios teisės veikimo ribų, antra, aiškiai neapibrėžto turinio požymiai gali neatitikti legalumo ir teisinio tikrumo principų reikalavimų.

Todėl, pereinant prie antrojo klausimo, kaip tokį požymių aiškinimą suderinti su baudžiamosios teisės principais, analizės, galima būtų paminėti jau aptartą Konvencijoje dėl elektroninių nusikaltimų pateiktą gana abstraktų ir į sistemos funkciją (automatinį duomenų apdorojimą) orientuotą kompiuterinės sistemos apibrėžimą. Sukonstruotas tokiu būdu jis turi itin daug bendrumų su visomis informacijos apdorojimo technologijomis, nes jos visos yra skirtos apdoroti duomenis ar informaciją – „kelyje nuo pradinių duomenų iki reikiamų rezultatų gavimo visos atliekamos procedūros vienaip ar kitaip apdoroja jiems pateiktus duomenis“[103]. Būtent šis dviprasmiškumas gali lemti, kad *CIA nusikalstamų veikų* požymių apimtys ir apskritai jų suvokimas, neatsižvelgus į įstatymo leidėjo tikslus formuluojant vieną ar kitą nusikalstamų veikų sudėtį, gali kaskart skirtis.

Šis vienas iš technologijų ir terminologijos problemos aspektų neliko nepastebėtas ir mokslinėje literatūroje – technologijoms neutralios nuostatos „padeda išvengti pernelyg siauro reguliavimo leisdamos pernelyg platų“ teigė P. Ohm[104]. Į technologinio neutralumo principo savybę išplėsti teisinį reguliavimą, nors ir artimoms, bet skirtingoms sritims, atkreipė dėmesį ir I. M. van der Haar[105].

Baudžiamosios teisės kontekste pernelyg plataus baudžiamojo teisinio reguliavimo problemą šiuo atveju geriausiai atspindi *perkriminalizavimo* (angl. *over–criminalization*) terminas. Apie *perkriminalizavimą* iš esmės galima kalbėti, kai „baudžiamoji teisė pradeda veikti už savo teisėtų funkcijų ribų“[106], kas dažniausiai reiškia ir piktnaudžiavimą baudžiamąja teise. Šios ribų problemos analizė yra neatsiejama nuo baudžiamosios teisės principų sistemoje esančių legalumo (lot. *nullum crimen, nulla poene sine lege*) ir kaltės (lot. *nullum crimen, nullum poena sine culpa*) principų. Būtent per jų reikalavimų įgyvendinimą „užtikrinama baudžiamųjų įstatymų leidybos ir jų taikymo atitiktis Konstitucijai ir joje įtvirtintiems bendriesiems teisės principams (teisinės valstybės, humanizmo, teisingumo, lygiateisiškumo, proporcingumo, protingumo ir kt.)“[107].

Kalbant apie *perkriminalizavimo* pavojų, *CIA nusikalstamų veikų* doktrinoje atkreiptas dėmesys į pakankamai įdomią situaciją – didėjant skaičiui asmenų, naudojančių informacines ir komunikacijos technologijas, taip pat įvairovei prietaisų, kurie gali atlikti įvesties, išvesties ir duomenų apdorojimo funkcijas, kyla sunkumų nustatant, kas iš tikro gali būti laikoma kompiuteriu. Pavyzdžiui, mobiliųjų technologijų, galinčių atlikti minėtas funkci-

[102] The Explanatory Report to the Convention on Cybercrime. [interaktyvus], [žiūrėta 2012-08-26]. <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>.

[103] Skyrius, R.; Mikalauskienė, A.; Zalieckaitė, L. *Informacijos ir komunikacijos technologijos*. Vilnius: UAB „Vilniaus spauda“, 2008, p. 166.

[104] Ohm, P., *supra* note 81, p. 1686.

[105] Van der Haar, I. M., *supra* note 85.

[106] Ashworth, A. Conceptions of Overcriminalization. *Ohio State Journal Of Criminal Law*. 2008, 5:407.

[107] Fedosiuk, O. Baudžiamoji atsakomybė kaip kraštutinė priemonė (*ultima ratio*): teorija ir realybė. *Jurisprudencija*, 2012. Nr. 19 (2):716.

jas ir būti tinklo dalimi (sujungus dvi – mobiliojo ryšio ir tinklo technologijas), prilyginimas kompiuteriams jau neturėtų kelti abejonių. Tačiau mokslinėje literatūroje taikliai pastebima, kad rankiniai bevieliai prietaisai, tokie kaip, pavyzdžiui, išmanieji telefonai, gali neatitikti daugumos žmonių suvokimo, kas yra kompiuteris[108].

Dėl to pritarus pakankamai lanksčioms ir besivystančioms technologijoms pritaikomoms sąvokoms, mokslinėje literatūroje vis dėlto pastebėta ir neigiama tokio aiškinimo pusė. Pernelyg lanksčios sąvokos veda prie pernelyg plačios ir dažnai nenuspėjamos jų apimties (angl. *over-inclusiveness*). Todėl nors ir klasikinėmis funkcijomis apibūdinama kompiuterio sąvoka[109] gali apimti „įvairius namų apyvokos ar kitus prietaisus, dėl kurių paprastai nebūtų taikomos kompiuterinių nusikaltimų nuostatos. Pavyzdžiui, veiksmai, kuriais paleidžiama saugos signalizacija, <...> gali būti priežastis kompiuteriui atlikti funkciją“[110]. Taip pat kompiuteriu gali būti laikomas nešiojamas skaičiuotuvas, kompiuterinė sistema automobilyje, Mp3 ar DVD grotuvas, net ir dauguma namų apyvokos daiktų, nes jie visi pajėgūs atlikti duomenų apdorojimo funkciją[111]. Taigi, atsižvelgdamas į įvairių prietaisų kompiuterizavimo tendenciją, I. Walden iškėlė idėją, kad „ateitis pranašauja galimybę sukurti namų apyvokos prietaisus su įmontuojamomis sistemomis ir prieiga prie interneto, suteikiančia išplėstas jų nuotolinio valdymo galimybes, o tai neišvengiamai leis atsirasti visiškai naujoms nusikalstamo elgesio formoms“[112].

Kitas svarbus aspektas tas, kad teisinis reguliavimas, laikantis technologinio neutralumo principo, yra ne tik abstraktus teisėkūros metu naudojamų technologijų atžvilgiu, bet taip pat siejamas su galimomis jų ateities perspektyvomis. Kadangi jis apima ir tas technologijas, kurių išradimas ar vystymasis iš anksto negali būti numatytas, tai ribiniais technologijų panaudojimo atvejais gali kilti abejonių dėl jo atitikimo legalumo ir teisinio tikrumo principams. Europos Žmogaus Teisių Teismas (toliau – Teismas) savo praktikoje, apibrėždamas žmogaus teisių ir laisvių apsaugos standartus, ne kartą akcentavo ir reikalavimus, keliamus valstybės vidaus teisės kokybei. Teismas, primindamas Europos Žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos (toliau – Konvencija) 7 straipsnyje įtvirtinto principo (nėra bausmės be įstatymo) esmę, pabrėžė ir įstatymo[113] prieinamumo (angl. *accessability*) ir numatomumo (angl. *foreseebility*) reikalavimus. Todėl, nesant minimalaus prieinamumo ir pakankamai nuspėjamo išaiškinimo, negalėtų būti laikoma, jog nuteisiant kaltininką yra įvykdyti Konvencijos 7 straipsnio reikalavimai[114]. Taip pat išsamaus, tikslaus ir aiškaus nusikalstamos veikos teisinio apibūdinimo reikalavimai kyla iš teisinės valstybės principo[115], kurio įvairūs turinio aspektai ir iš jo išvedamo teisinio saugumo imperatyvai suformuluoti Lietuvos Respublikos Konstitucinio Teismo jurisprudencijoje[116]. Į tai, kad vienas iš legalumo principo aspektų

[108] Walden, I., *supra* note 70, p. 16.
[109] Blundell, B. G. *Computer Systems and Networks*. London: Thomson: Middesex University Press, 2007, p. 2–3.
[110] Clough, J. *Principles of Cybercrime*. Cambridge: Cambridge University Press, 2010, p. 55.
[111] *Ibid*., p. 56.
[112] Walden, I., *supra* note 70, p. 16.
[113] Teismo praktikoje sąvoka įstatymas, minima Konvencijoje, apima rašytinę teisę (angl. *statute law*) ir teismų praktiką (angl. *case-law*).
[114] *Custers, Deveaux and Turk v. Denmark*, no. 11843/03, 11847/03, 11849/03, ECHR 2007; *Dragotoniu and Militaru-Pidhorni v. Romania*, no. 77193/01, 77196/01, ECHR 2007.
[115] Švedas, G. Veikos kriminalizavimo kriterijai: teorija ir praktika. *Teisė*. 2012, 82: 21.
[116] Konstitucinio Teismo 2001 m. liepos 12 d., 2003 m. gegužės 30 d., 2006 m. sausio 16 d. ir kiti nutarimai.

yra siejamas su maksimaliu nusikalstamos veikos požymių aprašymo tikslumu ir aiškumu, atkreiptas dėmesys ir mokslinėje literatūroje[117].

Beje, ši galinti kilti problema aktuali ne tik tais atvejais, kai įstatymų leidėjas nenumatė autentiško su technologijomis susijusių sąvokų išaiškinimo (kaip tai padaryta Lietuvos BK), bet ir tada, kai toks aiškinimas yra pateikiamas įstatymų (statutų) lygmeniu. Sąvokos, numatytos įstatymuose (statutuose), dėl technologinio neutralumo principo taikymo vis tiek išlieka pakankamai abstrakčios ir tiksliai neleidžia apibrėžti jų ribų. Kaip tokios problemos kilimo ir jos sprendimo pavyzdį galima būtų paminėti JAV apeliacinio teismo (7-osios apygardos) 2005 m. balandžio 18 d. sprendimą byloje *Jungtinės Amerikos Valstijos prieš Mitrą (US v. Mitra)*[118], 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))[119] 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 (angl. hardware) ir programinę (angl. software) 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 miesto ryšių bokštus „perdengusio“ signalo. Vėliau vietoje sistemos blokavimo kaltininkas kiekvieną pasibaigusį jos naudotojų pokalbį papildydavo erotine moters dejone.

Nesutikdamas su prokuroro nuomone, jog Smartnet II yra kompiuteris[120], 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 turi būti laikoma kompiuteriu. Toks aiškinimas būtų pernelyg platus, taip pat jo tokio nebuvo įmanoma numatyti priimant minėtas 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 bendro 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. Be to, teismo neįtikino

---

[117] Fedosiuk, O., *supra* note 107, p. 726.

[118] *United States v. Mitra*, no. 04-2328, April 18, 2005-US 7th Cir. [interaktyvus], [žiūrėta 2012-09-04]. <http://caselaw.findlaw.com/us-7th-circuit/1031818.html>.

[119] The Code of the United States. [interaktyvus], [žiūrėta 2012-09-04]. <http://www.law.cornell.edu/uscode/text/18/1030>.

[120] 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. Tačiau šis terminas neįtraukia automatinių rašomųjų mašinėlių arba rinkimo mašinų (angl. *typesetter*), nešiojamų rankinių skaičiuotuvų ar kitų panašių prietaisų“. Pagal prokuroro išsakytus argumentus, *Smartnet II* sistema turėtų būti pripažįstama kompiuteriu, nes ją, be kitų dalių, sudaro lustas (angl. *chip*), kuris, valdymo kanalu gavęs signalą, atlieka didelės spartos duomenų apdorojimo funkciją.

kaltininko teiginiai, kad baudžiamosios normos buvo išaiškintos tokiu būdu, kurio nebuvo įmanoma tikėtis. Teismas nesutiko su tuo, kad buvo pažeistas protingo žmogaus (angl. reasonable man) kriterijus, nes iš tikro nuostatos buvo išaiškintos taip, kaip jos suformuluotos, o ne taip, kaip norėjo kaltininkas.

Šioje situacijoje komunikavimui naudota sistema (*Smartnet II*) dėl savo sandaros ir atliekamų funkcijų[121] atitiko kompiuterį leidžiančius identifikuoti požymius. Tačiau vis dėlto toks atvejis rodo ateityje galinčias kilti pakankamai rimtas abejones dėl informacinių ir komunikacijos technologijas žyminčių abstrakčių sąvokų išaiškinimo tikslumo ir tinkamo teisės normų taikymo. Kadangi technologijoms neutralūs terminai, kaip minėta, dažniausiai yra bendrojo pobūdžio, tai ribiniais neteisėtų technologijų panaudojimo atvejais abejonė dėl neaiškios normos tinkamo interpretavimo gali kilti visuomet. Atitinkamai ši abejonė bus siejama su legalumo ir teisinio tikrumo principų reikalavimų pažeidimais.

Kadangi iš tikrųjų nėra paprasta pateikti apibrėžimą, kuris, pavyzdžiui, leistų kalbėti ne apie kišeninį skaičiuotuvą, o apie skreitinį kompiuterį (angl. *laptop computer*)[122], tai šios problemos sprendimo variantai galėtų būti siejami ne tik su bandymais, kaip įmanoma tinkamiau apibrėžti technologijas žyminčias sąvokas (pavyzdžiui, abstrakčiai pateikiant nuorodas į aparatinę ir programinę įrangą). Šiuo aspektu ne mažiau svarbus yra praktinis baudžiamojo įstatymo taikymo lygmuo, t. y. teismų praktika.

Įstatymo leidėjui baudžiamajame įstatyme nepateikus autentiško 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 <...>“[123]. Tačiau kalbant apie precedentus negalima užmiršti ir teismo, sprendžiančio teisės aiškinimo klausimus, diskrecijos ribų, t. y. kokį turinį teismas gali suteikti su informacinėmis ir komunikacijos technologijomis susijusiems požymiams, kokiais kriterijais vadovaudamasis turi spręsti, ar padaryta veika turi būti pripažįstama nusikalstama.

Todėl, sprendžiant baudžiamosios atsakomybės kilimo klausimą, vienas iš kriterijų galėtų būti tos aplinkybės, kurios vertinamos kriminalizuojant nusikalstamas veikas. Jei veikos pavojingumas, baudžiamosios teisės funkcionavimo sritis ir ribos, baudžiamosios teisės kaip paskutinės priemonės (lot. *ultima ratio*) ir kiti[124] pagrindai leidžia spręsti kriminalizavimo pagrįstumą, tai jie galėtų apibrėžti ir neaiškios baudžiamojo įstatymo normos taikymo ribas. Pavyzdžiui, analizuojant *ultima ratio* principo praktines taikymo galimybes, mokslinėje literatūroje atkreiptas dėmesys į tai, kad šis principas reikalauja nustatyti tinkamą veikos pavojingumą, nes abstrakčios definicijos kartu su tikrai pavojingu elgesiu gali apimti ir abejotino pavojingumo veikas[125].

---

[121] 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.

[122] Clough, J., *supra* note 110, p. 54.

[123] Pikelis, A., *supra* note 64, p. 46.

[124] Švedas, G., *supra* note 115, p. 12–24.

[125] Fedosiuk, O., *supra* note 107, p. 733.

Kitas galimas variantas – baudžiamosiose bylose, nustačius neteisėtą informacinių ir komunikacijos technologijų panaudojimo faktą, jų pažinimui pasitelkti specialias žinias turintį ekspertą arba specialistą. Eksperto (specialisto) technikos žinios gali padėti nustatyti ne tik vieno ar kito su informacinėmis ir komunikacijos technologijomis susijusio termino turinį, bet ir turėti įtakos nusikalstamos veikos kvalifikavimui[126]. Tačiau, vertinant ekspertizės akte (specialisto išvadoje) pateikiamas išvadas, turėtų būti atsižvelgta į tai, kad jos yra tik prielaida teisinei išvadai, nes nusikalstamos veikos sudėties požymių nustatymas yra teismo, o ne ekspertų (specialistų) kompetencija. Tai kad „ekspertai sprendžia tik techninius klausimus, o teismas – tik teisinius", ir tai, kad „tik teismo kompetencija yra vertinti ekspertų išvadas ir sutikti su jomis pilnai ar iš dalies"[127], nes „įrodymų vertinimas ir jais pagrįstų išvadų byloje sprendžiamais klausimais darymas yra teismo, priimančio baigiamąjį aktą, prerogatyva"[128], ne kartą atkreipė dėmesį ir Lietuvos Aukščiausiasis Teismas. Tokia pozicija svarbi ta prasme, kad pagal eksperto (specialisto) išvadą panaudotą prietaisą priskyrus informacinėms ir komunikacijos technologijoms, to neturėtų pakakti sprendimui, kad padaryta *CIA nusikalstama veika*. Šis saugiklis siejamas 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 anksčiau minėti *ultima ratio* ir kiti tinkamam baudžiamojo įstatymo taikymui svarbūs kriterijai.

CIA nusikalstamų veikų kvalifikavimo atveju ne mažiau svarbus ir šių nuostatų priėmimo kontekstas, t. y. pagrindinės priežastys, lėmusios normoje įtvirtintos sąvokos ar požymio nustatymą, pagrindinius tikslus, ko siekta numačius 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"[129].

Todėl praktikoje galimos situacijos, kai panaudota priemonė pagal atliekamas funkcijas bus priskiriama informacinėms ir komunikacijos technologijoms, tačiau pati padaryta veika nebus laikoma nusikalstama (nes baudžiamojo įstatymo taikymas neatitiks pagrindinių baudžiamosios teisės principų). Ir atvirkščiai – 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"[130].

Taigi galima būtų teigti, kad, technologinio neutralumo principą taikant baudžiamojoje teisėje, jo apimtis neišvengiamai siaurina baudžiamosios teisės principai, leidžiantys išvengti pernelyg plataus ir nepagrįsto veikų kriminalizavimo, atitinkamai ir baudžiamosios teisės ribų išplėtimo. Todėl tinkamas technologinio neutralumo principo taikymas galimas tik tuo atveju, jei yra randamas kompromisas tarp šio ir baudžiamojoje teisėje svarbių legalumo ir teisinio tikrumo principų.

---

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

[127] Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2005 m. vasario 22 d. nutartis baudžiamojoje byloje (bylos Nr. 2K-187/2005).

[128] Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2010 m. spalio 12 d. nutartis baudžiamojoje byloje (bylos Nr. 2K-448/2010).

[129] Pikelis, A., *supra* note 64, p. 45.

[130] Clough, J., *supra* note 110, p. 57.

II. ELEKTRONINIŲ DUOMENŲ IR INFORMACINIŲ SISTEMŲ KONFIDENCIALUMAS KAIP BAUDŽIAMOJO ĮSTATYMO SAUGOMA VERTYBĖ

Baudžiamojo įstatymo saugomos vertybės (objekto) kaip vieno iš pagrindinių objektyviųjų požymių[131] funkcijos skirtingai reiškiasi įvairiuose baudžiamojo teisinio reguliavimo etapuose. Todėl vertybė svarbi ne tik praktiniu baudžiamojo įstatymo taikymo lygmeniu, bet taip pat teisėkūros procese – ypač analizuojant įvairius pavojingų asmens padaromų veikų kriminalizavimo aspektus, kai gimininges nusikalstamos veikos baudžiamojo įstatymo saugomo teisinio gėrio pagrindu sisteminamos į atskiras rūšis (grupes). Beje, rūšinė BK XXX skyriuje esanti vertybė yra ir vienas iš kriterijų, naudojamų elektroninių nusikalstamų veikų struktūrizavimui. Ji tai tas pagrindas, kuris iš nusikalstamų veikų elektroninėje erdvėje visumos leidžia išskirti savarankišką jų rūšį – tiesiogiai elektroninių duomenų ir informacinių sistemų saugumą pažeidžiančias ar grėsmę jam sukeliančias nusikalstamas veikas, kuriomis tiesiogiai daromas neigiamas poveikis elektroninių duomenų ir informacinių sistemų konfidencialumui, integralumui ir (ar) prieinamumui (*CIA nusikalstamos veikos*).

1. Baudžiamojo įstatymo saugomos vertybės istorinė raida, jos įvardijimo įvairovė

Baudžiamojo įstatymo saugomo teisinio gėrio nustatymo ir tinkamo jo išaiškinimo svarbos akcentavimas tiek visų *CIA nusikalstamų veikų*, tiek nusikalstamų veikų elektroninių duomenų ir informacinių sistemų konfidencialumui atveju yra neatsitiktinis. Šios veikos galiojant 1961 m. BK, kaip *delicta sui generis*, nebuvo kriminalizuotos, todėl teisinio gėrio, kuriam jomis būtų padaroma žala arba sukeliama tokios žalos atsiradimo grėsmė, įvairūs įvardijimo aspektai Lietuvos baudžiamosios teisės doktrinoje nenagrinėti.

Galiojant 1961 m. BK, įvairūs elektroninių duomenų ir informacinių sistemų saugumo pažeidimus nurodantys požymiai buvo numatyti tik kai kuriose kvalifikuotose tradicinių nusikalstamų veikų sudėtyse (1961 m. BK 274 straipsnio 2 dalis, 277 straipsnio 2 dalis), taip pat su rinkimų ir referendumo tvarkos pažeidimais susijusiame 1961 m. BK 135^2 straipsnyje. Tokia nusikalstamų veikų konstrukcija ir kvalifikuojančių požymių turinys sudarė prielaidas kalbėti ne tik apie veikų pavojingumą didinančias aplinkybes, bet taip pat apie keletą baudžiamojo įstatymo saugomų vertybių (pavyzdžiui, veikos padarymo būdas[132]

[131] Objektas kaip vienas iš pagrindinių nusikalstamos veikos sudėties požymių apibūdinamas per tai, į ką kėsinamasi nusikalstama veika ir kam, ją padarius, yra sukeliama arba gali būti sukelta žala (žalos grėsė). Nors baudžiamosios teisės teorijoje iš esmės sutarta dėl tokio bendro objekto apibūdinimo, tačiau, konkretizuojant, kas juo turėtų būti laikoma, mokslininkų nuomonės išsiskiria. Todėl baudžiamosios teisės teorijoje galima sutikti nuomonių, kad jis tai visuomeniniai santykiai, visuomeniniai santykiai ir teisės normos, reguliuojančios šiuos santykius, teisiniai gėriai, interesai, dalykas ir kt. Kadangi šio darbo tikslas nėra išanalizuoti ir pagrįsti, kuri iš pozicijų tiksliausiai atskleidžia šio objektyviojo požymio esmę, tai detaliau mokslininkų ginčas dėl objekto nebus analizuojamas. Atsižvelgiant į šiuolaikinės Lietuvos baudžiamosios teisės tradicijas, juo šiame darbe bus laikomos baudžiamojo įstatymo saugomos vertybės.

[132] 1961 m. BK 277 straipsnio 2 dalies ir 274 straipsnio 2 dalies dispozicijose nusikalstamų veikų padarymo būdas, susijęs su neteisėtu informacinių sistemų panaudojimu, suformuluotas analogiškai. Tiek BK 277 straipsnio 2 dalyje, tiek ir BK 274 straipsnio 2 dalyje numatyta, kad šios nusikalstamos veikos padaromos „sudarant žinomai neteisingą kompiuterinę programą, įrašant į kompiuterio atmintį klaidingus duomenis, taip pat kitaip paveikiant kompiuterinę informaciją ar jos apdorojimą“.

arba pati pavojinga veika[133]). Tačiau tuometinėje baudžiamosios teisės teorijoje nagrinėjamu aspektu daugiausia dėmesio skirta pagrindinės vertybės analizei, sudėties požymių, tiesiogiai susijusių su neteisėtu naujųjų technologijų panaudojimu, išaiškinimui ir tokių veikų didesnio pavojingumo pagrindimui[134].

Todėl pirmosios rūšinio teisinio gėrio nustatymo nacionaliniu lygiu problemos kilo *CIA nusikalstamas veikas* tiesiogiai kriminalizavus 2000 m. BK ir jas laikant nebe sudėtine kitų veikų dalimi, o savarankišką baudžiamąją teisinę reikšmę turinčiomis veikomis. Būtent šiuo laikotarpiu atsirado galimybės kalbėti apie *CIA nusikalstamų veikų* vidinę struktūrą, atitinkamai ir apie nusikalstamas veikas, pažeidžiančias elektroninių duomenų ir informacinių sistemų konfidencialumą. Tačiau tinkamos baudžiamojo įstatymo saugomos vertybės, leidžiančios atskleisti tokių nusikalstamų veikų esmę ir sujungti jas į savarankišką rūšį, parinkimas 2000 m. BK sukėlė ir nemažai sunkumų – bet kokie vertybės formulavimo bandymai neturėjo tvirto teorinio pagrindimo. Taip pat ne tik pritarimo, bet ir nemažai kritikos sulaukė *CIA nusikalstamų veikų* aprašymas BK tiek dėl per siauro šių nusikalstamų veikų sąrašo, numatytų nusikalstamų veikų sudėties požymių neišsamumo, tiek ir dėl pačios baudžiamojo įstatymo saugomos vertybės formuluotės.

Pirminis 2000 m. BK XXX skyriaus pavadinimas, pateikęs oficialų vertybės variantą, buvo *Nusikaltimai informatikai.* Toks pasirinkimas mokslinėje literatūroje ne veltui buvo kritikuojamas[135]. Informatika gali būti apibūdinama įvairiai[136], tačiau ji bendriausia prasme visuomet bus laikoma mokslo šaka, nagrinėjančia informaciją, jos kūrimą ir apdorojimą bei šiuos procesus vykdančias sistemas. Kadangi akivaizdu, jog dėl naujųjų technologijų vystymosi atsiradusiomis nusikalstamomis veikomis negali būti kėsinamasi į informatiką kaip mokslą, tai šiuos BK numatytos vertybės netikslumus siūlyta spręsti *informatikos* terminą aiškinant plačiąja prasme. Taip šis terminas 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“[137]. Nors sprendimas vertybę aiškinti plačiau iš dalies galėjo padėti spręsti šio objektyviojo požymio netikslumus, bet nepaslėpė jo trūkumų. Šiuo laikotarpiu šalia bandymų aiškinimu koreguoti vertybės požymį taip pat siūlyta, išvengiant dviprasmybių, teisinį gėrį įvardyti kaip *kompiuterinės informacijos saugumą*[138].

[133] 135 (2) straipsnyje veika apibūdinta kaip „žinomai neteisingos kompiuterinės programos sudarymas, klaidingų duomenų įrašymas į kompiuterio atmintį, taip pat kitoks tyčinis poveikis kompiuterinei informacijai ar jos apdorojimui“. Tokie veiksmai laikyti nusikalstamais, jeigu jie turėjo ar galėjo turėti įtakos rinkimų ar referendumo rezultatams.

[134] Abramavičius, A., *et al*., *supra* note 59, p. 397, 421.

[135] Civilka, M., *et al., supra* note 9, p. 528. Goranin, N.; Mažeika, D. *Nusikaltimai elektroninėje erdvėje ir jų tyrimo metodikos*. Mokomoji knyga. Kaunas: TEV [i.e. Technologija], 2011, p.23.

[136] 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: „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 priemonė“. (Žilinskas, A.; Leonavičius, G.; Valavičius, E. *Informatika*. Vilnius: „Aldorija“, 2000, p. 5.) ir kt.

[137] Civilka, M., *et al., supra* note 9, p. 529.

[138] *Ibid*.

Vėlesni BK XXX skyriaus nusikalstamų veikų sudėčių keitimai buvo susiję su tarptautiniais Lietuvos įsipareigojimais ratifikavus Konvenciją dėl elektroninių nusikaltimų bei Europos Sąjungos lygiu priėmus Tarybos pamatinį sprendimą 2005/222/TVR. Konvencijos dėl elektroninių nusikaltimų preambulėje bei 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*), tačiau šiuo aspektu baudžiamojo įstatymo nuostatos 2004 metų pakeitimais koreguotos nebuvo[139]. Netinkama teisinio gėrio formuluotė pakeista tik 2007 metais[140] į nacionalinę teisės sistemą perkėlus Tarybos pamatinio sprendimo 2005/222/TVR nuostatas ir taip su jomis suderinus įvairius baudžiamosios atsakomybės už *CIA nusikalstamų veikų* padarymą aspektus. Pertvarkius BK XXX skyriuje įtvirtintas nusikalstamų veikų apibrėžtis, kartu pakeistas ir šias veikas į savarankišką rūšį jungiančios vertybės pavadinimas, suformuluojant daug tikslesnį jos pavadinimą – *elektroninių duomenų ir informacinių sistemų saugumas*. Šis teisinio gėrio pavadinimas leidžia aiškiau suvokti BK XXX skyriuje esančių nusikalstamų veikų prigimtį, jų vidinę struktūrą ir kalbėti apie įvairius elektroninių duomenų ir informacinių sistemų saugumo, *inter alia* ir konfidencialumo, pažeidimo aspektus.

Pakankamai įvairų požiūrį, kokias vertybes pažeidžia *CIA nusikalstamos veikos*, galima pastebėti analizuojant užsienio šalių baudžiamuosius įstatymus. Daugumos valstybių kaip ir Lietuvos baudžiamųjų įstatymų pokyčius lėmė Konvencijos dėl elektroninių nusikaltimų nuostatos, kurios, valstybėms tapus šios Konvencijos dalyvėmis[141], turėjo būti įgyvendintos jų nacionalinėje teisėje. *CIA nusikalstamų veikų* kriminalizavimas atskleidė pakankamai skirtingą požiūrį į teisinius gėrius. Galima būtų teigti, kad tam nemažai įtakos turėjo šiose valstybėse galiojančių baudžiamųjų įstatymų esama struktūra. Būtent jos įtaka akivaizdžiausiai matyti tais atvejais, kai *CIA nusikalstamų veikų* požymiai aprašomi jau esamuose skyriuose – taip, atsižvelgiant į vertybes, šioms veikoms baudžiamajame įstatyme yra parenkama tinkamiausia vieta. Tuo atveju, jei baudžiamajame įstatyme šioms

[139] 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.

Siekiant suderinti BK su Konvencija dėl elektroninių nusikaltimų nuostatomis, 2004 m. sausio 29 d. BK XXX skyrius papildytas dviem naujais 198^1 ir 198^2 straipsniais, kuriais kriminalizuotas neteisėtas prisijungimas prie kompiuterio ar kompiuterių tinklo (BK 198^1 straipsnis) ir neteisėtas disponavimas įrenginiais, kompiuterinėmis programomis, slaptažodžiais, prisijungimo kodais ir kitokiais duomenimis, skirtais nusikaltimams daryti (BK 198^2 straipsnis). Šie pakeitimai buvo susiję tik su baudžiamojo įstatymo spragų šalinimu, kriminalizuojant naujas nusikalstamas veikas, vienu ar kitu būdu pažeidžiančias elektroninių duomenų ar informacinių sistemų saugumą, tačiau ne su esamų nusikalstamų veikų sudėčių požymių (atitinkamai baudžiamojo įstatymo saugomos vertybės) koregavimu.

[140] 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.

[141] Toliau darbe, siekiant atskleisti teisinio reguliavimo įvairovę, pateikiami įvairių užsienio valstybių baudžiamųjų įstatymų pavyzdžiai, neatsižvelgiant į tai, ar šios valstybės yra ratifikavusios Konvenciją dėl elektroninių nusikaltimų. Pasirinkti nagrinėti Vokietijos, Prancūzijos, Estijos, Latvijos, Lenkijos ir Rusijos baudžiamieji įstatymai. Paminėtina, kad Lenkija Konvenciją dėl elektroninių nusikaltimų yra pasirašiusi, tačiau neratifikavusi, Rusija prie šios Konvencijos nėra prisijungusi. Todėl šių valstybių baudžiamiesiems įstatymams Konvencija dėl elektroninių nusikaltimų tiesiogiai neturi įtakos.

veikoms neatrandama tinkama vieta, kuriami atskiri baudžiamojo įstatymo struktūriniai vienetai (skyriai, paragrafai ar pan.)

Pavyzdžiui, Vokietijos baudžiamajame įstatyme[142] dalis *CIA nusikalstamų veikų*, kurios siejamos su elektroninių duomenų ir informacinių sistemų konfidencialumo pažeidimais, įtrauktos į baudžiamojo įstatymo skyrių, numatantį įvairias su privatumo pažeidimais susijusias veikas (vok. *Verletzung des persönlichen Lebens – und Geheimbereichs*)[143]. Kitos, reiškiančios neteisėtą poveikį elektroniniams duomenims ir informacinei sistemai, priskirtos žalą turtui sukeliančioms veikoms (vok. *Sachbeschädigung*)[144]. Panašų požiūrį į *CIA nusikalstamas veikas* galima pastebėti ir Prancūzijos[145] bei Estijos[146] baudžiamuosiuose įstatymuose. Prancūzijoje dalis konfidencialumą pažeidžiančių veikų yra įtrauktos į sekciją, numatančią slaptumo pažeidimus (pranc. *De l'atteinte au secret*), o tiksliau į šios sekcijos paragrafą, numatantį susirašinėjimo slaptumo pažeidimus (pranc. *De l'atteinte au secret des correspondances*)[147]. Tos veikos, kuriomis yra daromas neteisėtas poveikis elektroniniams duomenims ar informacinei sistemai, priskirtos prie kitų nusikaltimų nuosavybei (pranc. *Des autres atteintes aux biens*), t. y. nusikalstamoms veikoms, susijusioms su neteisėta prieiga prie automatizuotos duomenų apdorojimo sistemos (pranc. *Des atteintes aux systèmes de traitement automatisé de données*)[148]. Estijos baudžiamajame įstatyme[149] pastarosios veikos priskirtos nusikaltimams nuosavybei, t. y. žalą turtui sukeliančioms veikoms[150] ir veikoms, susijusioms su neteisėtu naudojimu[151]. Tuo tarpu konfidencialumo pažeidimai įtraukti į nusikaltimų prieš asmenį dalį, t. y. jos skyrių – nusikaltimus laisvei[152].

---

[142] Criminal Code of the Federal Republic of Germany. [interaktyvus], [žiūrėta 2013-06-01]. <http://www.gesetze-im-internet.de/englisch_stgb/index.html>.

[143] Vokietijos baudžiamojo įstatymo penkioliktame skyriuje numatytos šios veikos: duomenų šnipinėjimas (202a straipsnis), duomenų perėmimas (202b straipsnis) ir duomenų šnipinėjimo ir perėmimo parengiamieji veiksmai (202c straipsnis).

[144] Vokietijos baudžiamojo įstatymo dvidešimt septintame skyriuje numatytos šios veikos: duomenų pakeitimas (303a straipsnis) ir kompiuterio sabotažas (303b straipsnis).

[145] Penal Code of the French Republic. [interaktyvus], [žiūrėta 2013-06-01]. <http://www.legifrance.gouv.fr/Traductions/en-English/Legifrance-translations>.

[146] Penal Code of the Republic of Latvia. [interaktyvus], [žiūrėta 2013-06-01]. <http://www.legislationline.org/download/action/download/id/1280/file/4d16963509db70c09d23e52cb8df.htm/preview>.

[147] 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).

[148] 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.

[149] Criminal Code of the Republic of Estonia. [interaktyvus], [žiūrėta 2013-06-01]. <http://www.legislationline.org/download/action/download/id/1280/file/4d16963509db70c09d23e52cb8df.htm/preview>.

[150] Estijos baudžiamojo įstatymo 13 dalies (Nusikaltimai nuosavybei) 1 skyriaus (Nusikaltimai nuosavybei) 2 poskyryje (Žalą turtui) numatytos šios veikos: kompiuterio sabotažas (206 paragrafas), prisijungimo prie kompiuterių tinklo pažeidimai (207 paragrafas), kompiuterinių virusų platinimas (208 paragrafas).

[151] Estijos baudžiamojo įstatymo 13 dalies (Nusikaltimai nuosavybei) 2 skyriaus (Nusikaltimai visų rūšių turtui) 3 poskyryje (Neteisėtas naudojimasis) numatytos šios veikos: neteisėtas kompiuterio, kompiuterio sistemos ar kompiuterio tinklo naudojimas (217 paragrafas) ir parengiamieji veiksmai, įvykdyti su kompiuteriniais susijusiems nusikaltimams (216 (1) paragrafas).

[152] Estijos baudžiamojo įstatymo 9 dalies (Nusikalstymams prieš asmenį) 6 skyriuje (Nusikaltimai laisvei) numatyta veika neteisėtas stebėjimas (137 straipsnis).

Kitose valstybėse *CIA nusikalstamos veikos* nėra skaidomos dalimis – jos numatytos tame pačiame baudžiamojo įstatymo skyriuje. Pavyzdžiui, Lenkijos baudžiamajame įstatyme[153] šios veikos kriminalizuotos XXXIII skyriuje *Nusikaltimai informacijos apsaugai*. Rusijos baudžiamajame įstatyme[154] jos numatytos IX dalies *Nusikaltimai visuomenės saugumui ir tvarkai* 28 skyriuje *Nusikaltimai kompiuterinės informacijos srityje*. Latvijos baudžiamojo įstatymo[155] XX skyriuje *Nusikalstamos veikos bendrajam saugumui ir viešajai tvarkai*. Šiai valstybių grupei galima būtų priskirti ir Lietuvą, kurios baudžiamajame įstatyme *CIA nusikalstamos veikos* numatytos tame pačiame BK XXX skyriuje *Nusikalstamos veikos elektroninių duomenų ir informacinių sistemų saugumui*.

Toks užsienio valstybių sulyginimas aktualus dviem aspektais: 1) jis leidžia pastebėti į *CIA nusikalstamų veikų* visumą įtrauktų veikų smulkesnio grupavimo galimybes. Tai ypač matyti analizuojant tų valstybių baudžiamuosius įstatymus, kuriuose šios veikos kriminalizuotos skirtinguose skyriuose. Be abejo, toks skirstymas nebus aiškus, jeigu baudžiamuosiuose įstatymuose visos *CIA nusikalstamos veikos* įtrauktos į tą patį jų skyrių, o pati vertybė suformuluota pakankamai bendrai. Tokiu pavyzdiu gali būti laikomas ir Lietuvos BK, kurio XXX skyriuje rūšinė vertybė aprašyta pakankamai abstrakčiai ir iš pirmo žvilgsnio tarsi nesuteikia tokio pobūdžio veikų smulkesnio skirstymo galimybių; 2) jis parodo skirtingus valstybių požiūrius į tai, kokios vertybės pažeidžiamos *CIA nusikalstamomis veikomis*. Tai nubrėžia ir atitinkamas kitų valstybių doktrinoje susiformavusių požiūrių taikymo ribas atskleidžiant Lietuvos BK XXX skyriuje esančios rūšinės vertybės turinį. Todėl užsienio mokslininkų išsakytos pozicijos, kas apskritai gali būti laikoma baudžiamojo įstatymo saugoma vertybe ir kokia vertybė pažeidžiama *CIA nusikalstamomis veikomis*, turėtų būti vertinamos atsižvelgiant į tos valstybės baudžiamojo įstatymo nuostatas. Bet kokios idėjos tokiu atveju atspindės konkrečios valstybės baudžiamojo įstatymo struktūrą ir kriterijus, kuriais ji buvo sudaryta. Todėl neturėtų kelti nuostabos, kad tam tiktais atvejais vertybių aiškinimai, priklausomai nuo to, kokios valstybės atstovai juos pateikia, gali būti tik iš dalies pritaikomi atskleidžiant Lietuvos BK XXX skyriuje numatytos vertybės turinį.

Tačiau Lietuvoje besiformuojančioje elektroninių nusikalstamų veikų doktrinoje vis dėlto galima pastebėti bandymų atsižvelgti ir į užsienio valstybių patirtį aiškinant teisinio gėrio turinį. Pavyzdžiui, D. Štitilio teigimu, tokio pobūdžio veikoms yra būdingas bendras objektas – visuomeniniai santykiai informacijos apdorojimo procese[156]. Ši nuomonė artima Rusijos mokslininkų (V. A. Mazurov, A. G. Volevodz ir kt.)[157] siūlomoms teisinio gėrio interpretacijoms, kad nusikaltimo objektu turėtų būti laikomas saugumas subjektų veikloje, susijusioje su informacijos sukūrimu, apdorojimu ir naudojimu. V. A. Mazurovo teigimu, nusikaltimų kompiuterinės informacijos srityje objektas yra visuma teisinių santykių, saugomų baudžiamosios teisės priemonėmis. Kadangi šie nusikaltimai numatyti

[153] Criminal Code of the Republic of Poland. [interaktyvus], [žiūrėta 2013-06-01]. <http://www.legislationline.org/documents/section/criminal-codes/country/10>.

[154] Criminal Code of the Russian Federation. [interaktyvus], [žiūrėta 2013-06-01]. <http://www.russian-criminal-code.com>.

[155] Criminal Code of the Republic of Latvia. [interaktyvus], [žiūrėta 2013-06-01]. <http://legislationline.org/documents/section/criminal-codes>.

[156] Štitilis, D., *supra* note 12, p. 6.

[157] Mazurov, V. A. *Kompiuternye prestuplenija: klasifikacija i sposoby protivodeistvija* [Computer crime: classification and ways of countraction]. Moskva: Paletip, 2002, s. 19; Volevodz A. G. *Protivodeistvie kompiuternym prestuplenijam* [Counteraction to computer crime]. Moskva: Izdatelstvo «Jurlitinform», 2002, s. 61.

Rusijos baudžiamojo įstatymo IX dalyje *Nusikaltimai visuomenės saugumui ir tvarkai*, tai jų objektas yra visuomeniniai santykiai, susiję su visuomenės saugumu. Tačiau kartu jis pabrėžia, kad nusikaltimais kompiuterinės informacijos srityje kėsinasi ne į visus visuomenės saugumo teisinius santykius, o tik į jų dalį – santykius, susijusius su informaciniu saugumu[158]. Tokią išvadą autorius daro atsižvelgdamas į tai, kad šie nusikaltimai yra numatyti Rusijos baudžiamojo įstatymo IX dalies 28 skyriuje *Nusikaltimai kompiuterinės informacijos srityje*. Patį informacinį saugumą V. A. Mazurovas apibūdina kaip svarbių asmens, visuomenės ir valstybės interesų apsaugą informacinėje srityje nuo išorinių ir vidinių grėsmių. Informacinė sritis, anot autoriaus, yra „subjektų veiklos sritis, susijusi su informacijos sukūrimu, apdorojimu ir naudojimu“[159].

Negalima būtų teigti, kad minėto Lietuvos atstovo požiūris į baudžiamojo įstatymo saugomą vertybę yra klaidinantis. Iš tiesų bendriausia prasme nusikalstamos veikos, numatytos BK XXX skyriuje, kelia grėsmę elektroninėje erdvėje ir yra susijusios su įvairiais saugumo pažeidimais – jomis kėsinamasi į saugų duomenų apdorojimą ir saugią informacinių sistemų veiklą. Tačiau vis dėlto tokia baudžiamojo įstatymo saugomos vertybės aiškinimo pozicija, yra pakankamai abstrakti ir nutolusi nuo to teisinio gėrio, kuris tiesiogiai įvardytas BK XXX skyriuje. Todėl šiame skyriuje numatytų veikų rūšinės vertybės, aprašytos kaip elektroninių duomenų ir informacinių sistemų saugumas, turinio aiškinimui būtų artimesnė Konvencijoje dėl elektroninių nusikaltimų minima kompiuterinių duomenų ir sistemų konfidencialumo, vientisumo ir prieinamumo triada (II skyriaus 1 skirsnio 1 dalies pavadinimas). Tokia vertybės sandara nebūtų svetima elektroninių nusikalstamų veikų doktrinai – autoriai, komentavę BK 196–198[2] straipsnius (R. Mockevičius, D. Valatkevičius)[160], elektroninių duomenų ir informacinių sistemų saugumo pažeidimų nevengia apibūdinti per neteisėtą poveikį jų konfidencialumui, vientisumui, prieinamumui ir autentiškumui (tapatumui).

2. Elektroninių duomenų ir informacinių sistemų saugumas: konfidencialumas, vientisumas ir prieinamumas

Elektroninių duomenų ir informacinių sistemų bei platesne prasme suvokiamo elektroninės erdvės saugumo koncepcijos ištakos siejamos su viena iš etikos sričių – kompiuterine etika[161], susiformavusia, kaip atsakas į įvairius informacinėje visuomenėje vykstančius ir daugialypės globalizacijos sąlygotus procesus. Tiesa, analizuojant kompiuterinėje

[158] Mazurov, V. A., *supra* note 157, p. 19.

[159] *Ibid*., p. 21.

[160] Abramavičius, A., *et al. Lietuvos baudžiamojo kodekso komentaras. Specialioji dalis (99-212 straipsniai)*. Vilnius: Registrų centras, 2009, p. 416–443.

[161] Kompiuterinės etikos kaip savarankiškos etikos srities raida reiškiasi per nuolatinį jos tyrimų srities plėtimą ir tikslinimą. Nors kompiuterinė etika kaip tyrimų sritis pradėjo formuotis palyginti neseniai (jos pradžia siejama su profesoriaus N. Wiener darbais ir siekia XX a. vidurį), tačiau jau dabar galima pastebėti skirtingų jai įvardyti vartojamų ir prie įvairių jos tyrimo sričių derinamų pavadinimų – *kompiuterinė etika*, *kibernetinė etika*, *globalios komunikacijos* ar *interneto etika*, *informacijos etika ir kt.* Šią etikos sritį, autorės nuomone, tiksliausia vadinti *informacinių ir komunikacijos technologijų* arba *elektroninės erdvės etika*, kadangi tai leistų aprėpti visą elektroninės erdvės sritį. Tačiau atsižvelgiant į tai, kad visų šių bandymų apibrėžti šios etikos srities nagrinėjimo ribas ir parinkti jas atitinkantį etikos pavadinimą ištakos yra siejamos su *kompiuterine etika*, todėl tekste bus vartojamas klasikiniu laikytinas būtent šis terminas.

etikoje iškeltas idėjas, kurios leidžia aiškiau suvokti baudžiamosios teisės moksle atsiradusias naujas informacinių sistemų neteisėto panaudojimo vertinimo problemas, reikėtų atkreipti dėmesį į pakankamai bendrą jų pobūdį ir tinkamumą įvairioms, ne tik baudžiamajai teisei, sritims. Nors iš vienos pusės šis abstraktumas gali būti kritikuojamas, kaip apribojantis galimybę pritaikyti vieną ar kitą požiūrį sudėtingoms problemoms spręsti, tačiau vis dėlto negalima būtų paneigti šių požiūrių aktualumo renkantis galimą baudžiamojoje teisėje kilusių problemų sprendimo variantą. Be to, esminių etinių vertybių įtaka teisės normų formulavimui neginčijama kompiuterinės etikos šalininkų (R. A. Spinello ir kt.)[162], į jas kaip į pagrindą teisiniam gėriui, teisės normai ir nusikalstamos veikos sudėčiai atsirasti nurodoma ir baudžiamosios teisės teorijoje[163].

Būtent kompiuterinėje etikoje minimas informacinių sistemų sąlygotas vertybių peržiūrėjimo poreikis[164] baudžiamosios teisės kontekste gali būti konkretizuojamas iki baudžiamojo įstatymo saugomos vertybės įvardijimo ir jos išgryninimo klausimų. O įvairūs tinkamo teisinio gėrio nustatymo ir turinio atskleidimo aspektai tiesiogiai susiję su informacinių sistemų pažangos sukeltomis ir kompiuterinėje etikoje minimomis „nuostatų trūkumo“[165], (angl. *policy vacuum*) „konceptualios painiavos“[166] (angl. *conceptual muddle*) ir informacinių sistemų „loginio lankstumo“[167] (angl. *logically malleable*) problemomis.

Analizuojant pačios BK XXX skyriaus pavadinime numatytos vertybės išaiškinimo problemas, vienas svarbesnių aspektų būtų susijęs su elektroninių duomenų ir informacinių sistemų saugumo turinį sudarančių elementų nustatymu. Būtent šios vertybės vidinės struktūros suvokimas sudaro sąlygas *CIA nusikalstamas veikas* skaidyti į smulkesnes grupes, iš jų išskirti elektroninių duomenų ir informacinių sistemų konfidencialumą pažeidžiančias veikas.

---

[162] Spinello, R. A., *supra* note 29, p. 6.

[163] Wessel, J. *Baudžiamoji teisė. Bendroji dalis: baudžiamoji veikla ir jos struktūra*. Vilnius: Eugrimas, 2003, p. 28.

[164] Moor, J. H. *Reason, Relativity and Responsability in Computer Ethics*. [interaktyvus]. p. 17, [žiūrėta 2012-08-04]. <http://www.site.uottawa.ca/~stan/csi2911/moor1.pdf>.

[165] Su *nuostatų trūkumo* problema yra susiduriama kaskart, kai nustatomas informacinių ir komunikacijos technologijų reguliavimo nepakankamumas. Baudžiamosios teisės kontekste ši problema galėjo būti matoma analizuojant ekvivalentaus vertinimo principo taikymo problemas. Nustačius, kad ne visos baudžiamojo įstatymo normos yra pritaikomos veikoms elektroninėje erdvėje kvalifikuoti, baudžiamajame įstatyme įtvirtintos naujos – išimtinai *CIA nusikalstamas veikas* numatančios normos. Atitinkamai tokia teisėkūra, sprendžiant *nuostatų trūkumo* problemą, buvo susijusi su teisinio gėrio nustatymo ir apibrėžimo problemomis (Moor, J. H., *supra* note 76, p. 18–19).

[166] *Konceptualios painiavos* problemos išsprendimas leidžia pasirinkti tinkamą veiksmų vertinimo poziciją ir nustatyti tam tikrus bendrus elgesio, įtakojamo informacinių ir komunikacijos technologijų, standartus (Moor, J. H., *supra* note 164, p. 27).

Kadangi *konceptualios painiavos* problema yra pakankamai bendro pobūdžio, tai ji apima ir sąvokų konstravimo sunkumus. Jie taip pat siejami su anksčiau minėtomis technologinio neutralumo principo taikymo ir technologijų bei terminologijos problemomis. Jos be abejo turi įtakos ir *CIA nusikalstamomis veikomis* pažeidžiamos baudžiamojo įstatymo saugomos vertybės turinio atskleidimui.

[167] *Loginio lankstumo* problema kyla dėl informacinių ir komunikacijos technologijų beribių galimybių, t. y. jos gali būti sukurtos atlikti bet kokioms funkcijoms, kurios apibūdinamos įvesties, išvesties ir duomenų apdorojimo veiksmais. (Moor, J. H., *supra* note 76, p. 18–19). Tokia naujųjų technologijų savybė lemia, kad anksčiau minėtos *nuostatų trūkumo* ir *konceptualios painiavos* problemos iškils kaskart vystantis technologijoms. Atitinkamai baudžiamojo įstatymo saugomos vertybės tikslinimas bus būtinas dėl technologijų vystymosi pakitus CIA veikoms.

Pirmiausia reikėtų pastebėti, kad vertybės pavadinime tiesiogiai minimas saugumas gali būti atskleidžiamas pasitelkiant lingvistinį aiškinimą. Tokiu atveju užtektų nurodyti, kad elektroniniai duomenys ir informacinės sistemos yra saugios tuomet, kai joms nekeliamas pavojus arba jos apsaugotos nuo pavojų[168]. Tačiau tokia bendro pobūdžio saugumo samprata yra neinformatyvi – iš jos nėra aišku apie kokias grėsmes ir kokias elektroninių duomenų ir informacinių sistemų savybes, kurios turėtų būti apsaugotos, yra kalbama. Todėl elektroninių nusikalstamų veikų doktrinoje, aiškinant įvairius saugumo aspektus, krypstama kita linkme – vietoj bendros saugumo koncepcijos dažniausiai pateikiama pakankamai detali, saugumo modelius atspindinti jos samprata. Tikslumo dėlei reikėtų atkreipti dėmesį į tai, kad mokslinėje literatūroje suformuluotos dvi pagrindinės saugumo koncepcijos: *elektroninės erdvės saugumas* (angl. *Cybersecurity*) ir *techninis kompiuterių saugumas* (angl. *Technical computer security*)[169].

Plačiausią prasmę saugumui suteikia *elektroninės erdvės saugumo* koncepcija, tačiau būtent siauresnė *techninio kompiuterių saugumo* samprata padeda aiškiau suvokti BK XXX skyriuje aprašytas veikas ir jų struktūrą. Šios saugumo koncepcijos ištakų turėtų būti ieškoma saugumo politikos, o konkrečiau saugumo modelių srityje kalbant apie *CIA triados* saugumo modelį. Analogiškos šį modelį sudarančios informacijos saugotinos savybės taip pat minimos viename iš pagrindinių saugumo srityje priimtų standartų *LST ISO/IEC 27001:2006 lt – Informacijos technologija – Saugumo metodai – Informacijos saugumo valdymo sistemos – Reikalavimai (toliau – ISO/IEC 27001)*. Šis standartas parengtas siekiant pateikti informacijos saugumo valdymo sistemos parengimo, įgyvendinimo, naudojimo, stebėsenos, analizės, priežiūros ir tobulinimo modelį. Jame informacijos saugumas apibūdintas kaip informacijos konfidencialumo, vientisumo ir prieinamumo išsaugojimas. Taip pat nurodyta, kad informacijos saugumas apima ir tokias informacijos savybes kaip autentiškumas, atskaitingumas, negalėjimas išsižadėti ir patikimumas. Tačiau analizuojant mokslinėje literatūroje pateikiamus saugumo aiškinimo variantus, be klasikinio požiūrio (E. W. Michael, M. E. Whitman, M. Bishop, G. Skersys, A. Venčkauskas, J. Toldinas ir kt.)[170], galima matyti ir siekius savaip interpretuoti *CIA triadą*

---

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

[169] Mokslinėje literatūroje suformuluotos dvi – platesnė *elektroninės erdvės saugumo* ir siauresnė bei *CIA triadą* atspindinti *techninio kompiuterių saugumo* sampratos. Šių skirtingų savo apimtimi sampratų susiformavimui tiesioginės įtakos turėjo pakankamai plati nusikalstamų veikų elektroninėje erdvėje apibrėžtis: į jų visumą yra įtrauktos ne tik veikos, darančios žalą elektroninių duomenų ir IS saugumui, bet ir tradicinės veikos, kurios pakito dėl informacinių ir komunikacijos technologijų panaudojimo galimybių. *Elektroninės erdvės saugumo* samprata minima, kai norima pabrėžti elektroninės erdvės apsaugą nuo grėsmių, kylančių dėl įvairių elektroninėje erdvėje padaromų veikų. Tuo tarpu *techninio kompiuterių saugumo* koncepcija paprastai siejama tik su *CIA nusikalstamomis veikomis* ir apsaugos nuo jų poreikiu. (Plačiau žr.: 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.* (edit.). New York (N.Y.): New York University Press, 2007, p. 63).

[170] Whitman, M. E., *et al. Principles of information security*. 3-ioji laida. Boston: Thomson: Course Technology, 2009, p. 10; *Computer and Information security handbook*/ sudarytojas Vacca, J. R., 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.

sudarančius elementus[171], taip pat bandymus praplėsti jos turinį, įtraukiant daugiau saugumą apibūdinančių požymių[172]. Be to, dažnai minėti saugumo elementai mokslinėje literatūroje vadinami įvairiai: saugumo pagrindiniais principais[173], siekiais[174] ar koncepcijomis[175]. Tačiau nepriklausomai nuo jų interpretacijų įvairovės reikėtų pripažinti, kad *techninio kompiuterių saugumo* šerdimi išlieka *CIA triada* – elektroninių duomenų ir informacinių sistemų konfidencialumas, integralumas ir prieinamumas. Šie klasikiniais pripažįstami elektroninių duomenų ir informacinių sistemų saugumo aspektai minimi ir Konvencijos dėl elektroninių nusikaltimų 1 skirsnio 1 dalyje, kurioje pateiktos „nusikaltimų kompiuterinių duomenų ir sistemų konfidencialumui, vientisumui ir prieinamumui" apibrėžtys. Būtent ši elektroninių duomenų ir informacinių sistemų trijų savybių visuma sudaro galimybes išskirti atskiras BK XXX skyriuje esančių nusikalstamų veikų grupes ir nustatyti tas, kurios pažeidžia elektroninių duomenų ir informacinių sistemų konfidencialumą.

2.1. Elektroninių duomenų ir informacinių sistemų konfidencialumas

Minėta, kad klasikiniu požiūriu grįstam elektroninių duomenų ir IS saugumo reikalavimui įgyvendinti būtina išlaikyti tris pagrindines jų savybes – konfidencialumą, integralumą[176]

---

[171] Pavyzdžiui, dalis autorių vietoj elektroninių duomenų ir informacinių sistemų prieinamumo į *CIA triados* sudėtį įtraukia kitą elementą – jų autentiškumą (angl. *authentication*). Susiejęs elektroninių duomenų autentiškumą su duomenų šaltinio tikrumo garantu, šie autoriai akcentuoja, kad autentiškumas tampa neatsiejamu nuo elektroninių duomenų integralumo, todėl abu sujungiami į vieną elektroninių duomenų autentiškumo elementą (Sumit, K.; Nishit, N.; Sumita, N. *Communication networks: principles and practice*. New York: McGraw-Hill, 2007, p. 336.).

[172] Bene radikaliausiu požiūriu į *CIA triados* elementų visumą gali būti laikoma D. Parkerio suformuluota šešių elementų sistema, kuri dažnai vadinama *D. Parkerio heksada.* Šioje naujoje techninio kompiuterių saugumo struktūroje išskiriami tokie pamatiniai elementai kaip konfidencialumas, integralumas, prieinamumas, autentiškumas, naudingumas ir nuosavybės teisių išsaugojimas, kurie 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. (eds). New York, *et al*.: Wiley, 2002).

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

[174] Stoneburner, G. *Underlying Technical Models for Information Technology Security: recomendations of the National Institute of Standards and Technology* [interaktyvus], [žiūrėta 2010-09-27]. <http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf>.

[175] Sumit, K.; Nishit, N.; Sumita, N., *supra* note 171, p. 336.

[176] Į *CIA triados* sudėtį įeinantis elektroninių duomenų ir informacinių sistemų integralumas patvirtina elektroninių duomenų ir informacinių sistemų vidinės struktūros užbaigtumą bei vientisumą. Taigi elektroninių duomenų integralumas laikytinas duomenų savybe, liudijančia, kad jų apdorojimo metu duomenys be atitinkamų teisėtų įgaliojimų nebuvo pakeisti. Į integralumo sąvoką kai kurie autoriai (pavyzdžiui, M. Bishop ir kt.) įtraukia ne tik duomenų integralumą (turinio aspektą), bet taip pat ir kilmės integralumą (duomenų šaltinio aspektą, kuris dar vadinamas autentiškumo nustatymu (angl. *authentication*). IS integralumas reikštų, kad duomenų apdorojimo funkcijas atliekančiose IS nebuvo atlikti neteisėti pakeitimai, modifikacijos. Pavyzdžiui, viena iš alternatyvių BK 196 straipsnio 1 dalyje kriminalizuotų veikų – neteisėtas elektroninių duomenų pakeitimas, kaltininkui gali būti inkriminuojamas ir tais atvejais, kai jis tyčiniais veiksmais padaro pakeitimų elektroninių duomenų struktūroje taip pažeisdamas ir šių duomenų integralumą. Kitas pavyzdys būtų susijęs su BK 197 straipsnio taikymu. Kaltininko veika gali būti vertinama kaip neteisėtas poveikis IS ir tais atvejais, kai neteisėtais pakeitimais IS buvo sutrikdytas jos darbas. (Plačiau žr. Marcinauskaitė, R., *supra* note 169; Bishop, M., *supra* note 170, p. 5; Venčkauskas, A.; Toldinas, J., *supra* note 170, p. 9 ir kt.).

ir prieinamumą[177]. Kaip vieną iš konfidencialumo elektroninėje erdvėje apsaugos variantų pasirinkus baudžiamosios teisės priemones, tokios vertybės pažeidimai tiesiogiai kriminalizuoti BK 198 ir 198[1] straipsniuose. Pirmajame aprašyti neviešų elektroninių duomenų konfidencialumo pažeidimai neteisėtai jais disponuojant – stebint, fiksuojant, perimant, įgyjant, laikant, pasisavinant, paskleidžiant ar kitaip panaudojant. Antrajame atskirai kriminalizuoti IS konfidencialumo pažeidimai neteisėtai prisijungiant prie IS (jei buvo pažeistos IS apsaugos priemonės). Baudžiamosios atsakomybės už šias veikas nustatymo BK XXX skyriuje ypatumas *inter alia* yra tas, kad jos kriminalizuotos kaip savarankiškos veikos. Tai verčia atskirti elektroninių duomenų bei IS konfidencialumą ir šią vertybę analizuoti atskirai neviešų elektroninių duomenų ir apribotą (ar atsietą) prieigą turinčių IS kontekste.

Analizuojant rūšinio teisinio gėrio formuluotę matyti, kad ji savyje jungia ne tik teisinį (konfidencialumas), bet ir technologinį aspektą (elektroniniai duomenys ir IS). Žvelgiant į konfidencialumą pačia bendriausia lingvistine prasme, jis gali būti susiejamas su slaptumu ir pasitikėjimu. Pavyzdžiui, *konfidencialus* žodynuose apibrėžiamas kaip viešai neskelbtinas, slaptas[178], skirtas būti laikomu paslaptyje[179], taip pat pasakytas arba parašytas slaptai ir ketinamas laikyti paslaptyje[180] arba perduotas pasitikint, slaptai[181]. Toks požiūris, be abejo, nurodo galimą vertybės aiškinimo kryptį, tačiau kartu tiksliam jos interpretavimui yra būtinas minėtų teisinio ir technologinio aspektų suderinimas. Apžvelgus literatūroje pateikiamus elektroninių duomenų ir IS konfidencialumo apibrėžimus, galima pastebėti, kad apie šį *CIA triados* elementą paprastai kalbama konkrečių analizuojamų problemų kontekste, kurios bene dažniausiai verčia akcentuoti būtent elektroninių duomenų konfidencialumo poreikį.

Daugelio autorių (E. W. Michael, M. E. Whitman, M. Bishop, G. Skersys, A. Venčkauskas, J. Toldinas ir kt.)[182] darbuose elektroninių duomenų konfidencialumas suvokiamas panašiai ir bendriausia prasme siejamas su draudimu atskleisti duomenis tiems asmenims ar sistemoms, kurie neturi prieigos prie šių duomenų teisės. Pagal E. W. Michael ir M. E. Whitman „informacija išsaugo konfidencialumą kai ji apsaugota nuo atskleidimo

---

[177] Prieinamumas užtikrina, kad turintiems atitinkamus įgaliojimus vartotojams – asmenims ar IS, elektroniniai duomenys yra prieinami be trukdžių ar kliūčių ir gaunami reikiamu formatu arba informacija turi būti prieinama bet kuriuo užklausos pateikimo metu (Plačiau žr.: *Computer and Information security handbook.* Vacca, J. R. (ed.). Amsterdam: Elsevier: Morgan Kaufmann, 2009, p. 256; Whitman, M. E., *et al*., *supra* note 170, p. 9). Vis dėlto reikėtų pastebėti, kad nors dalis autorių aptardami šį elementą akcentuoja tik elektroninių duomenų prieinamumą, šios savybės nereikėtų pamiršti atskirai kalbant ir apie IS. Juo labiau kad tokio pobūdžio pavojingos asmens elgsenos elektroninėje erdvėje pasireiškimo formos, nukreiptos prieš IS prieinamumą, kriminalizuotos BK 197 straipsnyje. Pagal jį atsakomybė kyla, jeigu neteisėtai sutrikdomas ar nutraukiamas informacinės sistemos darbas padarant atitinkamo masto žalą (pavyzdžiui, *DDos atakos* atveju).

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

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

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

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

[182] Whitman, M. E., *et al*., *supra* note 170, p. 10; *Computer and Information security handbook.* Vacca, J. R. (red), Amsterdam: Elsevier: Morgan Kaufmann, 2009, p. 256.; Bishop, M., *supra* note 170, p. 4; Skersys, G., *supra* note 170, p. 11; Venčkauskas, A.; Toldinas, J., *supra* note 170, p. 9.

neautorizuotiems asmenims ar sistemoms“[183]. Panašų apibrėžimą pateikė ir A. Venčkauskas bei J. Toldinas, pagal kuriuos konfidencialumas tai „užtikrinimas, kad slapti duomenys bus prieinami tik tiems vartotojams, kuriems ši prieiga leista (tokie vartotojai vadinami autorizuotaisiais)“[184]. Kai kuriais atvejais autorių darbuose bandoma atskirai akcentuoti ne tik IS laikomų, bet ir joje perduodamų duomenų neatskleidimo svarbą – anot S. Kašėtos ir T. Adomkaus, „konfidencialumas sistemoje arba tinkle reiškia tai, kad dedant, keičiant ar siunčiant informaciją sistemoje ar tinkle, ji nebus nuskaityta ar pasisavinta kitų asmenų“[185]. Taigi teigtina, kad bendriausia prasme konfidencialumas reikštų, jog „informacija turi būti pateikta tik tam, kam priklauso, ir niekam kitam“[186]. Beje, šie požiūriai artimi ISO/IEC 27001 suformuotam informacijos konfidencialumo suvokimui, kad tai savybė, nusakanti, jog informacija „nebus prieinama ar pateikiama neįgaliotiems fiziniams ar juridiniams asmenims arba procesams“. Panašiai šis *CIA triados* elementas aiškintas ir Informacinių sistemų bei technologijų žodyne – jame duomenų konfidencialumas apibūdintas per galėjimą užtikrinti, „kad duomenys yra neprieinami neįgaliotiems vartotojams“[187].

BK 198[1] straipsnyje numačius atsakomybę už neteisėto prisijungimo prie IS veiką aktualu nustatyti, kaip slaptumo, perdavimo pasitikint aspektai reiškiasi IS apsaugos srityje. Tiesa, apie IS konfidencialumą literatūroje užsimenama rečiau, dažniausiai tokį poreikį susiejant su IS esančios informacijos (duomenų) saugumo svarba. Vienų autorių teigimu, siekiant apsaugoti informacinio saugumo interesus, be kitų, 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“[188]. Kiti autoriai, apibūdindami informacijos apsaugos tikslus trimis – konfidencialumo, prieinamumo ir integralumo išsaugojimo poreikiais, nurodo, kad informacijos konfidencialumo apsauga galima priemonėmis, kuriomis „nustatomos informacinių sistemų vartotojų prieigos teisės, t. y. prie kokių informacinių išteklių (duomenų, katalogų ar sistemų) konkretus vartotojas turi prieigos teisę“[189]. Taigi, kaip matyti, apie IS konfidencialumą kalbama tada, kai ši sistema turi užtikrinti joje esančių duomenų slaptumą paprastai neleidžiant prieigos prie jų, jei tam nėra suteikta teisė. Be abejo, vienas iš IS konfidencialumo užtikrinimo tikslų yra jose laikomų elektroninių duomenų apsauga, nes neteisėta prieiga prie sistemos dažnai gali būti tik tarpinis etapas kaltininkui siekiant atlikti tolesnius veiksmus joje. Tačiau žiūrint iš baudžiamosios teisės pozicijų reikėtų pažymėti, kad BK 198[1] straipsnyje neteisėtas prisijungimas prie IS kriminalizuotas *per se* be ryšio su tolesniais kaltininko veiksmais sistemoje, todėl apibrėžiant IS konfidencialumą vis dėlto siūlytina jį aiškinti be nuorodų į elektroninių duomenų neviešumo apsaugą. Tokiu atveju IS konfidencialumas reikštų, kad sistemos, atliekančios duomenų apdorojimo funkcijas,

[183] Whitman, M. E., *et al*., *supra* note 170, p. 10.
[184] Venčkauskas, A.; Toldinas, J., *supra* note 170, p. 9.
[185] Kašėta, S.; Adomkus, T. *Telefonijos informacijos ir VoIP sauga*. Kaunas: Vitae Litera, 2008, p. 12.
[186] Plėštys, R., *et al*. *Tinklų sauga*. Kaunas: Vitae Litera, 2008, p. 17.
[187] *Dictionary of Information Science and Technology*. I tomas. Khosrow – Pour, M. (ed.). Hershey, Pa., *et al*: Idea Group Reference, 2007, p. 152.
[188] Kazanavičius, E., *et al*. *Informacijos saugos vadyba*. Kaunas: Vitae Litera, 2008, p. 10.
[189] Budnikas, A., *et al*. *Elektroninės valdžios sauga*. Kaunas: Vitae Litera, 2008, p. 51.

yra prieinamos tik prieigos teisę prie šių sistemų turintiems vartotojams ir tik ta apimtimi, kuria jiems ši teisė buvo suteikta.

Kadangi aptartų elektroninių duomenų ir IS konfidencialumo sąvokų ištakos nėra siejamos su baudžiamąja teise, tai, analizuojant šį *CIA triados* elementą kaip baudžiamojo įstatymo saugomą vertybę, akcentuotina keletas svarbių aspektų: 1) kaip jau minėta, konfidencialumas laikytinas ne tik vienu iš elektroninių duomenų, bet taip pat ir IS saugumo elementu. Apie tokį atskyrimą sudaro sąlygas kalbėti BK XXX skyriuje nurodyto teisinio gėrio konstrukcija – jo su technologijomis susijusioje dalyje savarankiškai šalia elektroninių duomenų minima ir IS. Atsižvelgiant į tai, saugumo elementai atskirai analizuotini tiek IS, tiek ir elektroninių duomenų kontekste; 2) neviešų elektroninių duomenų konfidencialumo išsaugojimas svarbus viso duomenų apdorojimo proceso metu[190], todėl, apibrėžiant šią duomenų savybę, neturėtų būti išskiriamas duomenų neviešumo užtikrinimas atliekant tik kažkurį elektroninių duomenų tvarkymo veiksmą; 3) atsižvelgiama į tai, kad informacinių procesų dalyviai yra ne tik žmonės, bet ir IS, konfidencialumo apibrėžimuose šalia asmenų neleistinos prieigos minimi ir neįgalioti procesai (pavyzdžiui, ISO/IEC 27001) arba neautorizuota sistemų prieiga (pavyzdžiui, E. W. Michael ir M. E. Whitman pateiktame konfidencialumo apibrėžime). Nors toks skirstymas leidžia aiškiau suvokti nusikalstamos veikos padarymo mechanizmą, tačiau iš baudžiamosios teisės pozicijų sprendžiant, kas gali pažeisti elektroninių duomenų ir IS konfidencialumą, jis kol kas aktualus tik nustatant asmens kaltę[191]. Konstatavus, kad kaltininkas veikė tyčia, IS ir jos komponentai, kurie buvo panaudoti konfidencialumo pažeidimams padaryti, būtų pripažinti tik padarytos veikos priemonėmis ar įrankiais; 4) sprendžiant, kokios yra konfidencialumo apsaugos ribos, esminę reikšmę turi tokių terminų kaip *informacija* ir *duomenys* skirtumai. Nors jie, priklausomai nuo konteksto, dažnai vartojami kaip sinonimai, tačiau baudžiamojoje teisėje aiškinant tiek vertybės, tiek ir dalyko požymius tikslumo dėlei siūlytina vartoti *duomenų* terminą. Taip būtų išvengta neaiškumų, ar baudžiamosios teisės priemonėmis pakankamai užtikrinamas duomenų, esančių *iki informaciniame etape*[192], konfidencialumas.

Kitas probleminis BK XXX skyriuje numatytos rūšinės vertybės aiškinimo aspektas susijęs su konfidencialumo ir privatumo ryšiu. *CIA triada*, leidžianti į saugumą pažvelgti kaip į konfidencialumo, integralumo ir prieinamumo visumą, atskleidžia ir BK 198 straipsnyje bei 166 – 168 straipsniuose esančių nusikalstamų veikų tarpusavio santykio problemą. Kai neteisėtas disponavimas neviešais elektroniniais duomenimis rodo elektroninių duomenų konfidencialumo pažeidimus, tai BK XXIV skyriuje esančios veikos – neteisėtą intervenciją į asmens privatų gyvenimą. Analizuojant minėtuose BK straipsniuose numatytų nusikalstamų veikų sudėties požymius matyti, kad būtent teisinių gėrių, o tiksliau konfidencialumo ir asmens privataus gyvenimo neliečiamumo atskyrimo kriterijai galėtų padėti nustatyti BK 198 straipsnyje ir BK XXIV skyriuje esančių veikų skirtumus.

Taigi aiškinantis privataus gyvenimo neliečiamumo sampratą, bendrinė privatumo reikšmė jį susieja su nuošalumu, slaptumo būsena ir leidžia vartoti tokius jo sinonimus kaip vienuma, atsiskyrimas[193]. Todėl termino privatus gyvenimas išaiškinimui pasitelkus paties

[190] Apie tai plačiau žiūrėti IV dalies 2.2 poskyryje.

[191] Apie tai plačiau žiūrėti IV dalies 3 skyriuje.

[192] Apie tai plačiau žiūrėti IV dalies 2.1 poskyryje.

[193] *Funk & Wagnalls standard dictionary of the English language: combined with Britannica world language dictionary*. I tomas. Chicago (Ill.): Encyclopaedia Britannica, 1960, p. 1003.

termino privatus lingvistinį aiškinimą, apie šią sritį galima būtų kalbėti kaip apie atskirtą nuo viešumos, pasitraukusią[194], neviešą[195], asmeninę, slaptą, neskirtą dalintis su kitais[196]. Tačiau tokios pakankamai bendros interpretacijos tik iš dalies paaiškina privataus gyvenimo turinį – jos nepadeda išspręsti bene svarbiausios privataus gyvenimo sričių ir atitinkamai privataus gyvenimo ribų problemos. Prieš detaliau aptariant šį aspektą paminėtina, kad teisė į privataus gyvenimo neliečiamumą, o tiksliau asmens teisės į privatumą, numatyta įvairiuose tarptautiniuose teisės aktuose[197], ne tik Lietuvos, bet ir kitų valstybių nacionalinėse konstitucijose. Lietuvos Respublikos Konstitucijos 22 straipsnyje įtvirtintas bendras principas, kad žmogaus privatus gyvenimas yra neliečiamas. Šios Konstitucijoje numatytos principinės nuostatos turinys išplėtotas Lietuvos Respublikos Konstitucinio Teismo jurisprudencijoje kartu joje suformuluojant ir privataus žmogaus gyvenimo koncepciją. Ne kartą pasisakydamas dėl Konstitucijos 22 straipsnyje numatytos asmens teisės į privatų gyvenimą ir jos ribojimų Konstitucinis Teismas pažymėjo, kad pagal Konstituciją „privatus žmogaus gyvenimas – tai individo asmeninis gyvenimas: gyvenimo būdas, šeimyninė padėtis, gyvenamoji aplinka, santykiai su kitais asmenimis, individo pažiūros, įsitikinimai, įpročiai, jo fizinė bei psichinė būklė, sveikata, garbė, orumas ir kt. Konstitucijos 22 straipsnio normose įtvirtintas žmogaus privataus gyvenimo neliečiamumas suponuoja asmens teisę į privatumą. Žmogaus teisė į privatumą apima asmeninio, šeimos ir namų gyvenimo, garbės ir reputacijos neliečiamumą, asmens fizinę ir psichinę neliečiamybę, asmeninių faktų slaptumą, draudimą skelbti gautą ar surinktą konfidencialią 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). Beje, plati ir įvairias asmeninės nepriklausomybės sritis apimanti privataus gyvenimo sąvoka formuluojama ne tik konstitucinėje jurisprudencijoje, bet bandyta apibrėžti ir nacionaliniuose įstatymuose. Pavyzdžiui, pagal Lietuvos Respublikos visuomenės informavimo įstatymo (*Valstybės žinios*. 1996, Nr. 71-1706) 2 straipsnio 45 punktą 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“.

[194] *Funk & Wagnalls standard dictionary of the English language: combined with Britannica world language dictionary.* I tomas. Chicago (Ill.): Encyclopaedia Britannica, 1960, p. 1003.

[195] *Tarptautinių žodžių žodynas*. Sudarytojai Bendorienė, A., *et al.* Atsakomasis redaktorius Kinderys A. Vilnius: Alma litera, 2001, p. 602.

[196] *Longman dictionary of Contemporary English*. Summers, D. (edit. director). Berlin; München: Langenscheidt. Longman, 1987, p. 823.

[197] Visuotinės žmogaus teisių deklaracijos 12 straipsnyje nurodoma, kad „niekas neturi patirti savavališko kišimosi į jo privatumą, šeimos gyvenimą, buitį ar susirašinėjimą arba kėsinimosi į jo garbę ir reputaciją. Kiekvienas turi teisę į įstatymo apsaugą nuo tokio kišimosi arba kėsinimosi“; Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos 8 straipsnyje teigiama, kad „kiekvienas turi teisę į tai, kad būtų gerbiamas jo asmeninis ir jo šeimos gyvenimas, buto neliečiamybė ir susirašinėjimo slaptumas“; Tarptautinio pilietinių ir politinių teisių pakto 17 straipsnyje įtvirtinta, kad „niekas neturi patirti savavališko ar neteisėto kišimosi į jo asmeninį ir šeimyninį gyvenimą, jo būsto neliečiamybę, susirašinėjimo slaptumą, neteisėto kėsinimosi į jo garbę ir orumą“ taip pat, kad „kiekvienas asmuo turi teisę į įstatymo apsaugą nuo tokio kišimosi arba tokių pasikėsinimų“.

Kartu šios definicijos parodo, kad neįmanoma pateikti išsamios privataus gyvenimo apibrėžties ir nustatyti griežtas jo ribas, todėl tam tikrų duomenų statusas priklausys nuo daugelio vertintinų aplinkybių, konteksto. Anot Lankausko M., „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“[198]. Tiesa, reikėtų pastebėti, kad tokios būtinybės iš tiesų nėra – į tai atkreipė dėmesį Europos Žmogaus Teisių Teismas byloje *Niemietz prieš Vokietiją* (Niemietz v. Germany). Savo sprendime Teismas nurodė, kad „nėra įmanoma ar būtina bandyti pateikti galutinę „privataus gyvenimo“ sąvokos apibrėžtį. Tačiau būtų pernelyg ribota šią sąvoką susiaurinat iki „vidinės srities“, kurioje individas gali gyventi savo asmeninį gyvenimą taip, kaip pasirenka, ir dėl to pašalinti išorinį pasaulį, nepatenkantį į šią sritį. Pagarba privačiam gyvenimui tam tikru mastu turi apimti teisę sukurti ir plėtoti santykius su kitais žmonėmis“[199].

Kaip matyti, išsamiai apibrėžti asmens privatumo sritį praktiškai neįmanoma, tačiau tam tikrus jos kontūrus, privatumo vidinę struktūrą nors ir abstrakčiai, bet vis dėlto leidžia nustatyti pačios teisės į privatumą aprašymas tarptautiniuose ir nacionaliniuose teisės aktuose. Todėl tarpusavyje susijusios asmeninės nepriklausomybės sritys gali būti laikomos, pavyzdžiui, privatus, šeimos gyvenimas, būstas ar asmens susirašinėjimas[200], taip pat literatūroje galima sutikti kiek kitokių, tačiau panašių skirstymų, pavyzdžiui, joje kalbama apie informacinį, fizinį, komunikacinį ar teritorinį privatumą[201] ir pan. Nors šie kategorizavimai yra daugiau teorinio, metodologinio pobūdžio, tačiau jie padeda aiškiau suvokti BK XXIV skyriaus vidinę struktūrą. Štai, pavyzdžiui, teritorinio privatumo pažeidimai kriminalizuoti BK 165 straipsnyje, numatančiame atsakomybę už neteisėtą asmens būsto neliečiamumo pažeidimą; atsakomybė už komunikacinio privatumo pažeidimus nustatyta BK 166 straipsnyje, kuriame aprašyti asmens susižinojimo neliečiamumo pažeidimo požymiai ir pan. Todėl, pavyzdžiui, apsikeitimu asmeninio pobūdžio informacija nelaikomas tarnybinis, oficialus, dalykinis susirašinėjimas[202]. Tai akcentuota ir teismų praktikoje. Kauno apylinkės teismo 2013 m. birželio 7 d. nuosprendyje baudžiamojoje byloje (bylos Nr. 1-680-530/2013) konstatuota, kad: *Asmens susižinojimo neliečiamumo objektas – privataus žmonių bendravimo viešojo ryšio priemonėmis tvarka ir slaptumas. Tai pasikeitimas privataus pobūdžio informacija tarp privačių asmenų. Ne privačių asmenų, tame tarpe – įmonių vadovų tarpusavio profesinis susirašinėjimas, tarnybinis bendravimas – nėra šio straipsnio [BK 166 straipsnis – aut. pastaba] saugoma socialinių santykių sritis.*

Žiūrint iš baudžiamosios teisės pozicijų tokia situacija probleminė todėl, kad abstrakčios privatumo ribos neleidžia aiškiai atskirti BK 198 ir BK 166–168 straipsniuose numatytų nusikalstamų veikų – priklausomai nuo to, ar duomenys bus susieti su asmens privačiu gyvenimu, ar vis dėlto jie bus laikomi konfidencialiais duomenimis *CIA triados* prasme, skirsis ir kaltininko veikai kvalifikuoti taikytinas straipsnis. Tačiau privatumo ana-

[198] 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.

[199] *Niemietz v. Germany*, no. 13710/88, ECHR 1992.

[200] Pagal Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos 8 straipsnį.

[201] Panomariovas, A. Asmens privataus gyvenimo paslaptis ir su ja susijusios problemos baudžiamajame procese. *Jurisprudencija*, 2001, 23(15): 99.; Kiškis, M., *et al*., *supra* note 8, p. 115–116.

[202] *Lietuvos Respublikos konstitucijos komentaras*. K. Jovaišas (atsakingas redaktorius). Vilnius: Teisės institutas, 2000, p. 165.

lizė sudaro sąlygas suformuluoti nors ir bendro pobūdžio, tačiau orientacinį ir tiesiogiai su baudžiamojo įstatymo vertybe susijusį minėtų nusikalstamų veikų atskyrimo kriterijų. Tais atvejais, kai nusikalstama veika elektroninėje erdvėje pažeidžiamas asmens privataus gyvenimo neliečiamumas, veikos teisiniam vertinimui išreikšti taikytini BK XXIV skyriuje esantys BK straipsniai, kitais atvejais, nustačius neviešų elektroninių duomenų disponavimo pažeidimus, inkriminuotina kita – BK 198 straipsnyje esanti nusikalstama veika (jei nenustatyta šiame straipsnyje esančios normos atžvilgiu speciali norma).

Tačiau pažymėtina, kad mokslinėje literatūroje sutinkami ne visai tikslūs baudžiamojo įstatymo saugomų vertybių aiškinimai, o tai gali formuoti ir diskutuotiną BK 198 straipsnio taikymo praktiką. Pavyzdžiui, kaip teigia N. Goranin ir D. Mažeika, 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“[203]. Autoriai kaip neviešų elektroninių duomenų pavyzdį pateikia ir privataus asmens elektroninius laiškus, o tai apie neteisėtus veiksmus su jais leidžia kalbėti kaip apie neteisėtą disponavimą neviešais elektroniniais duomenimis ir tokios veikos kvalifikavimui taikyti BK 198 straipsnį. Iš tiesų tokio pobūdžio laiškai atitinka elektroninių duomenų požymius[204], tačiau, kaip galima buvo pastebėti, asmens komunikacinis privatumas pirmiausia siejamas su asmens privatumu, taigi neteisėtos intervencijos į susižinojimo neliečiamumo sritį laikytinos asmens privataus gyvenimo neliečiamumo pažeidimais. Todėl įvairiems neteisėtiems veiksmams, kuriais, pavyzdžiui, perimami, fiksuojami ar stebimi asmens elektroninių ryšių tinklais siunčiami pranešimai ar kitaip pažeidžiamas asmens susižinojimo neliečiamumas, kvalifikuoti taikytinas ne BK 198, o 166 straipsnis. Tokios BK 166 straipsnio taikymo tendencijos matyti ir teismų praktikoje, pavyzdžiui, Vilniaus miesto 2 apylinkės teismo 2008 m. liepos 2 d. nuosprendyje baudžiamojoje byloje (bylos Nr. 1-5-655/2008), Šiaulių rajono apylinkės teismo 2010 m. liepos 19 d. teismo baudžiamajame įsakyme baudžiamojoje byloje (bylos Nr. 1-199-776/2010), Šilutės rajono apylinkės teismo 2006 m. birželio 28 d. nuosprendyje baudžiamojoje byloje (bylos N1- 249-299/2005) ir kt.[205]

Taigi galima būtų teigti, kad elektroninių duomenų ir informacinių sistemų saugumo turinį atskleidžia ir BK XXX skyriaus nusikalstamas veikas struktūrizuoja *CIA triados* modelis. Pasitelkus jį veikos elektroninių duomenų ir informacinių sistemų saugumui gali būti suskirstytos į elektroninių duomenų ir IS konfidencialumo, integralumo ir prieinamumo pažeidimus. Su elektroninių duomenų konfidencialumo pažeidimais tiesiogiai siejama BK 198 straipsnyje numatyta veika, o IS konfidencialumą pažeidžia BK 198[1] straipsnyje esanti veika.

[203] Goranin, N.; Mažeika, D., *supra* note 135, p. 25–26.

[204] Plačiau apie tai žiūrėti V dalies 3 skyriuje.

[205] Plačiau apie BK 198 straipsnyje ir BK XXIV skyriuje numatytų nusikalstamų veikų atskyrimo problemas žiūrėti V dalies 1 skyriuje.

III. NETEISĖTAS PRISIJUNGIMAS PRIE INFORMACINĖS SISTEMOS (BK 198[1] straipsnis)

1. Neteisėto prisijungimo prie informacinės sistemos kriminalizavimo pagrindimas ir šios veikos inkriminavimo ypatumai

Neteisėto prisijungimo prie IS kaip nusikalstamos veikos įtvirtinimas Lietuvos BK sietinas su anksčiau aptartu ekvivalentaus elgesio fizinėje ir elektroninėje erdvėje vertinimo principo, o tiksliau su funkcinio ekvivalentiškumo įgyvendinimu. Minėta, kad sprendžiant *CIA nusikalstamų veikų* baudžiamojo teisinio vertinimo problemas, jos 2000 m. BK buvo kriminalizuotos kaip *delicta sui generis*. Tačiau įsigaliojus 2000 m. BK, neteisėto prisijungimo veika iš pradžių jame nebuvo numatyta. Tai, be abejo, galėjo kelti tam tikrų abejonių, ar baudžiamosios teisės priemonėmis užtikrinama pakankama konfidencialumo apsauga elektroninėje erdvėje.

Ši kriminalizavimo nepakankamumo problema išspręsta 2004 m. Lietuvai ratifikavus Konvenciją dėl elektroninių nusikaltimų ir įgyvendinus jos reikalavimus nacionalinėje teisėje. Todėl nebūtų suklysta teigiant, kad neteisėto prisijungimo prie IS ištakų pirmiausia reikėtų ieškoti būtent tarptautiniuose teisės aktuose – atsižvelgiant į juos tokia veika jau po 2000 m. BK įsigaliojimo buvo kriminalizuota pirmą kartą. Kaip pastebi G. Švedas, įstatymų leidėjui pasirinkus įstatyminį tarptautinių sutarčių ir nacionalinės teisės suderinimo būdą, 2004 m. ratifikavus Konvenciją dėl elektroninių nusikaltimų buvo pakeistos arba papildytos beveik visų BK XXX skyriuje numatytų nusikalstamų veikų sudėtys[206]. BK 198[1] straipsnyje neteisėto prisijungimo prie kompiuterio ar kompiuterinio tinklo veika (kaip tuomet ji vadinta) įtvirtinta kaip Konvencijos dėl elektroninių nusikaltimų 2 straipsnyje aprašytos neteisėtos prieigos atitikmuo. Vėlesnius jos pakeitimus lėmė Pamatinio sprendimo 2005/222/TVR nuostatos, kurios į nacionalinę teisę buvo perkeltos 2007 metais[207]. Atsižvelgiant į šio Europos Sąjungos teisės akto 2 straipsnį, BK 198[1] straipsnyje vietoj kompiuterio ar kompiuterinio tinklo įvestas daug abstraktesnis IS terminas ir išskirta šią veiką kvalifikuojanti aplinkybė, susijusi su padidinta IS svarba – jos strategine reikšme nacionaliniam saugumui, didele reikšme valstybės valdymui, ūkiui ar finansų sistemai. Nors ši aplinkybė Pamatinio sprendimo 2005/222/TVR 2 straipsnyje tiesiogiai nėra minima, tačiau ji gali būti kildinama iš Pamatinio sprendimo 7 straipsnio 2 dalies, numatančios, kad atsakomybė gali būti griežtinama ir tais atvejais, kai nusikalstama veika „padarė didelių nuostolių ar padarė poveikio esminiams interesams“. Tokia BK 198[1] straipsnio redakcija galioja ir šiuo metu.

Toks minėtų tarptautinių, Europos Sąjungos teisės aktų ir nacionalinės baudžiamosios teisės ryšys rodo, kad neteisėtam prisijungimui prie IS apibūdinti pasirinkti požymiai BK 198[1] straipsnyje buvo aprašyti atsižvelgiant į šiuose teisės aktuose numatytus minimalius tokios veikos sudėčiai keliamus reikalavimus. Todėl tiek objektyvūs, tiek subjektyvūs

---

[206] *Nepriklausomos Lietuvos teisė: praeitis, dabartis ir ateitis: recenzuotų mokslinių straipsnių rinkinys: liber amicorum profesoriui Jonui Prapiesčiui*. Švedas, G. (vyr. mokslinis redaktorius). Vilnius: Vilniaus universiteto Teisės fakulteto Alumni draugija, 2012, p. 108.

[207] 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.

jos požymiai turėtų būti aiškinami turint mintyje Konvencijos dėl elektroninių nusikaltimų ir Pamatinio sprendimo 2005/222/TVR nuostatas.

Tačiau analizuojant įvairius tarptautinių ir Europos Sąjungos teisės aktų reikalavimų įgyvendinimo aspektus pirmiausia pažymėtina, kad ne visos valstybės yra ratifikavusios Konvenciją dėl elektroninių nusikaltimų[208] ir tik Europos Sąjungos valstybėms narėms privalomas Pamatinis sprendimas 2005/222/TVR. Antra, atkreiptinas dėmesys ir į šių teisės aktų suteiktas diskrecijos ribas, t. y. galimybes valstybėms, atsižvelgiant į nacionalinės teisės tradicijas, pasirinkti vieną iš galimų veikos nusikalstamumo nustatymo variantų – atitinkamą sudėties konstrukciją, į ją įtrauktinus požymius ir kita. Taigi, minėtuose teisės aktuose nustačius „potencialų veikos plotį“[209] buvo sudarytos galimybės formuotis įvairioms neteisėtos prieigos koncepcijoms, liudijančioms apie skirtingą valstybių požiūrį į šią nusikalstamą veiką. Pakankamai įvairūs tokios nusikalstamos veikos kriminalizavimo būdai taip pat lėmė ne tik skirtingą mokslininkų požiūrį į ją, bet ir skirtingas neteisėtos prieigos analizės kryptis. Į tai turėtų būti atsižvelgiama analizuojant įvairias mokslininkų išsakomas idėjas ir bandant spręsti nacionalinėje baudžiamojoje teisėje kylančias šios veikos inkriminavimo problemas.

Konvencijos dėl elektroninių nusikaltimų 2 straipsnis įpareigoja nustatyti baudžiamąją atsakomybę už sąmoningą ir neteisėtą prieigą prie visos kompiuterinės sistemos arba jos dalies. Šiame straipsnyje numatyta galimybė susiaurinti pakankamai 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, taip pat veika nukreipta prieš kompiuterinę sistemą, sujungtą su kita kompiuterine sistema. Panašius reikalavimus šios nusikalstamos veikos sudėčiai kelia ir Pamatinis sprendimas 2005/222/TVR. Jo 2 straipsnyje neteisėta prieiga prie IS laikoma tyčinė prieiga prie visos arba dalies IS neturint tam teisės. Sprendime tiesiogiai nurodoma, kad baudžiamosios teisės priemonės taikytinos bent tais atvejais, kurie nėra nereikšmingi. Taip pat šio straipsnio 2 dalyje numatyta galimybė neteisėtą prieigą susieti su kurios nors saugumo priemonės pažeidimu (kaip, beje, ir Direktyvos 2013/40/ES 3 straipsnyje) .

Baudžiamosios atsakomybės numatymas už neteisėtą prisijungimą kaip savarankišką veiką gali būti siejamas su Konvencijos dėl elektroninių nusikaltimų aiškinamojoje ataskaitoje minimomis priemonėmis, kurių turėtų būti imtasi „ankstyvajame etape“, kol nėra įvykdytos kitos nusikalstamos veikos sistemoje (45 punktas). Kaip teigia J. Clough, ši veika tai „baudimo už „nutolusią“ žalą, kurios kilimas priklauso nuo kaltinamojo ar kito asmens būsimo sprendimo padaryti nusikaltimą, pavyzdys“[210]. Iš tiesų neteisėtas įsibrovimas gali suteikti prieigą „prie konfidencialių duomenų (įskaitant slaptažodžius, informaciją apie sistemą) ir paslapčių, sudaryti galimybę nemokamai naudotis sistema arba paskatinti programišius (angl. *hacker*) padaryti daug pavojingesnius su kompiuteriais susijusius nusikaltimus, tokius kaip sukčiavimas ar klastojimas“ (44 punktas). Tačiau minėtoje ataskaitoje atkreipiamas dėmesys į kitą – tokios veikos *perkriminalizavimo* problemą. Joje nurodoma, kad bau-

[208] Valstybių, ratifikavusių Konvenciją dėl elektroninių nusikaltimų, sąrašas yra pasiekiamas internetiniu adresu <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG>.

[209] Clough, J., *supra* note 110, p. 48.

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

džiamosios atsakomybės poreikis už neteisėtą prieigą nėra ginčijamas, tačiau tam tikri prieštaravimai gali kilti tais atvejais, kai paprasčiausiu įsibrovimu nebuvo sukeltas pavojus arba net ir tada, kai tokiais neteisėtais veiksmais buvo nustatytos saugumo spragos (49 punktas). Todėl siekiant išvengti nepagrįsto baudžiamosios atsakomybės taikymo, užsienio valstybėse, konstruojant šios nusikalstamos veikos sudėtį, prieigos, jos neteisėtumo, tyčios požymiai pripažįstami būtinais, tačiau nepakankamais baudžiamajai atsakomybei kilti. Pasirinkus kiek siauresnį požiūrį, reikalaujama nustatyti papildomas jos pavojingumą didinančias aplinkybes. Šios įvairios aplinkybės numatytos tiek Konvencijos dėl elektroninių nusikaltimų 2 straipsnyje, tiek ir Pamatinio sprendimo 2005/222/TVR 2 straipsnyje bei Direktyvos 2013/40/ES 3 straipsnyje (tai, pavyzdžiui, anksčiau minėtos apsaugos priemonių pažeidimo, ketinimo gauti elektroninius duomenis, kitus nesąžiningus ketinimus liudijančios aplinkybės ir pan.). Jos valstybėms leidžia nusistatyti neteisėtos prieigos kriminalizavimo ribas ir gali būti laikomos racionaliais reikalavimais pripažįstant veikas nusikalstamomis.

Priklausomai nuo pasirinktos neteisėtos prieigos prie IS koncepcijos, užsienio valstybėse galima pastebėti įvairius šios nusikalstamos veikos požymių kombinacijos būdus, atitinkamai ir skirtingus tokios veikos *perkriminalizavimo* problemos sprendimo variantus. Dalyje valstybių baudžiamoji atsakomybė numatyta už neteisėtą prieigą ne prie IS, o prie duomenų, jeigu buvo padarytas neteisėtas poveikis apsaugos priemonėms arba sistemai. Tokiais atvejais neteisėtos prieigos prie IS veika tampa kitos – neteisėtos prieigos prie duomenų – veikos sudedamąja dalimi.

Pavyzdžiui, Vokietijos[211] baudžiamajame įstatyme su neteisėta prieiga yra susijęs 202a straipsnis, kuriame kriminalizuotas duomenų šnipinėjimas. Ši veika pasireiškia duomenų, apsaugotų nuo neteisėtos prieigos, įgijimu, įveikiant apsaugą. Jungtinėje Karalystėje neteisėtos prieigos veika numatyta Netinkamo naudojimosi kompiuteriais akto[212] 1 straipsnyje. Ši veika aprašyta kaip privertimas kompiuterį atlikti bet kokią funkciją siekiant gauti prieigą prie programos arba duomenų, laikomų kompiuteryje, arba sudarant galimybes tokią prieigą gauti. Baudžiamajai atsakomybei kilti būtina nustatyti tiek prieigos neteisėtumą, tiek ir asmens žinojimą, kad, priversdamas kompiuterį atlikti funkciją, jis elgiasi neteisėtai. Panašų požiūrį į neteisėtą prieigą galima pastebėti Konvencijos dėl elektroninių nusikaltimų neratifikavusios Rusijos Federacijos baudžiamajame įstatyme. Jame neteisėtos prieigos prie kompiuterinės informacijos veika kriminalizuota 272 straipsnyje, pagal kurį baudžiamoji atsakomybė kyla, jei neteisėta prieiga prie apsaugotos kompiuterinės informacijos (esančios automatiniu būdu nuskaitomose laikmenose, kompiuteryje, kompiuterinėje sistemoje, jų tinkle) buvo susijusi su informacijos sunaikinimu, apribojimu, pakeitimu ar kopijavimu arba sistemos veiklos sutrikdymu.

Kitose valstybėse atsakomybė tiesiogiai numatyta už neteisėtą prieigą prie IS, šalia neteisėtumo ir prieigos gavimo požymių taip pat minint kitas šios veikos pavojingumą rodančias aplinkybes.

Pavyzdžiui, Prancūzijos[213] baudžiamajame įstatyme neteisėtos prieigos veika kriminalizuota 323-1 straipsnyje. Ji aprašyta kaip apgaulingas priėjimas arba pasilikimas visoje ar

---

[211] Vokietijos Federacinė Respublika Konvenciją dėl elektroninių nusikaltimų ratifikavo 2009 m. kovo 9 d.

[212] Computer Misuse Act. [interaktyvus], [žiūrėta 2013-06-01]. <http://www.legislation.gov.uk/ukpga/1990/18/section/1>.
Jungtinė Karalystė Konvenciją dėl elektroninių nusikaltimų ratifikavo 2011 m. gegužės 20 d.

[213] Prancūzijos Respublika Konvenciją dėl elektroninių nusikaltimų ratifikavo 2006 m. sausio 10 d.

dalyje automatinėje duomenų apdorojimo sistemoje. Poveikis sistemoje esantiems duomenims arba pačios sistemos funkcionavimui laikomi šią veiką kvalifikuojančiomis aplinkybėmis. Jungtinių Amerikos Valstijų įstatymų sąvado[214] 18 U.S.C. § 1030 (a) (1)–(5) punktuose kriminalizuoti įvairūs neteisėtos ar teisėtumo ribas peržengiančios prieigos prie kompiuterio variantai. Juos apibendrinus galima teigti, kad 1030 paragrafe baudžiamoji atsakomybė numatyta už neteisėtą ar teisėtumo ribas peržengiančią prieigą, jei po jos sekė informacijos, turtinės naudos įgijimo ir kiti panašūs neteisėti veiksmai[215]. Estijos[216] baudžiamajame įstatyme neteisėtas kompiuterinės sistemos panaudojimas kriminalizuotas 217 straipsnyje. Pagal šį straipsnį baudžiamoji atsakomybė kyla, jei nustatoma neteisėta prieiga prie kompiuterinės sistemos pašalinant arba apeinant jos apsaugos priemones. Taip pat šio straipsnio 2 dalyje numatyta nemažai kvalifikuojančių aplinkybių, pavyzdžiui, didelės žalos sukėlimas, prieiga prie svarbaus sektoriaus kompiuterinės sistemos ir pan. Šiai grupei valstybių taip pat galėtų būti priskirta Lietuva, kurios BK 198[1] straipsnyje baudžiamoji atsakomybė numatyta už neteisėtą prieigą prie IS, pažeidžiant jos apsaugos priemones.

Įvairus požiūris į neteisėtos prieigos nusikalstamą veiką rodo ne tik jos sulyginimo sunkumus, bet taip pat ir kvalifikavimo problemas, kurios, priklausomai nuo šios veikos požymių aprašymo, gali kilti ne visose, o tik kai kuriose valstybėse. Vienas iš tokių akivaizdesnių atvejų siejamas su anksčiau aptartais bendresniais neteisėtos prieigos kriminalizavimo skirtumais. Būtent jie leidžia spręsti, kieno – IS ar duomenų – konfidencialumo pažeidimai yra šios nusikalstamos veikos ašis. Šis atskyrimas, anot J. Clough, yra ypač svarbus, nes pirmuoju atveju „pabrėžiama kaltininko sąveika su kompiuteriu, o ne su konkrečiais duomenimis“[217]. Antruoju priešingai – dėmesio centre yra prieigos prie duomenų neteisėtumo nustatymas.

Analizuojant Lietuvos BK 198[1] straipsnyje numatytą neteisėto prisijungimo prie IS veiką matyti, kad jos apibrėžtis susiaurinta vienu iš Konvencijos dėl elektroninių nusikaltimų ir Pamatinio sprendimo 2005/222/TVR numatytų būdų. Tai yra, siekiant išvengti akivaizdžiai nežalingų veikų kriminalizavimo, šiame straipsnyje numatytai pareigai inkriminuoti būtina įrodyti ne tik prisijungimo prie IS neteisėtumą, bet ir tai, kad toks prisijungimas buvo padarytas pažeidžiant IS apsaugos priemones. Kvalifikuotoje šios veikos sudėtyje prisijungimas prie strateginę reikšmę nacionaliniam saugumui arba didelę reikšmę valstybės valdymui, ūkiui, ar finansų sistemai turinčios IS laikomas aplinkybe, didinančia neteisėto prisijungimo pavojingumo laipsnį (BK 198[1] straipsnio 2 dalis). Toks nusikalstamos veikos požymių aprašymas BK 198[1] straipsnyje reiškia, kad neteisėtas prisijungimas prie IS baudžiamajame įstatyme kriminalizuotas *per se* be sąsajos su tolesnėmis kaltininko veikomis jau pačioje sistemoje. Šis aspektas taip pat parodo nusikalstamų veikų daugeto nustatymo problemas.

Iš *CIA nusikalstamų veikų* padarymo mechanizmo matyti, kad kaltininko veiksmai paprastai neapsiriboja tik neteisėta prieiga prie IS – įsibrovus į ją padaromos ir kitos nusi-

[214] The Code of the United States. [interaktyvus], [žiūrėta 2012-09-04]. <http://www.law.cornell.edu/uscode/text/18/1030>.
Jungtinės Amerikos Valstijos Konvenciją dėl elektroninių nusikaltimų ratifikavo 2006 m. rugsėjo 29 d.

[215] Kaip išimtį galima būtų paminėti tik 18 U.S.C. § 1030 (a) 3 punkte kriminalizuotą neteisėtą prieigą prie Jungtinių Amerikos Valstijų Vyriausybės kompiuterio, jei tokia veika padarė poveikį tokio kompiuterio naudojimuisi.

[216] Estijos Respublika Konvenciją dėl elektroninių nusikaltimų ratifikavo 2003 m. gegužės 12 d.

[217] Clough, J., *supra* note 110, p. 72.

kalstamos veikos, pažeidžiančios IS ar elektroninių duomenų konfidencialumą, integralumą, prieinamumą ar kitas vertybes. Kadangi neteisėtas prisijungimas BK kriminalizuotas kaip pavojingas pats savaime ir nėra įtrauktas į kitų nusikalstamų veikų sudėtį, tai ši veika turėtų būti inkriminuojama kiekvieną kartą nustačius visus BK 198[1] straipsnyje aprašytus jos sudėties požymius. Iš tiesų įstatymo leidėjo pasirinktas toks šios veikos kriminalizavimo būdas sukuria gana įdomią visų kaltininko padarytų veikų kvalifikavimo situaciją. Jai aiškiau pavaizduoti gali būti pasitelkiamas A. Česnio ir J. Jukniaus minimas atakų prieš IS skirstymas į dvi – atsisakymo aptarnauti (DoS) ir prieigos gavimo – grupes. Antrosios atveju, nepriklausomai nuo to, koks būtų asmens tikslas, kenkimo veiksmai yra visuomet „atliekami gavus prieigą prie informacinės sistemos ir įsilaužus į vidų“[218]. Todėl akivaizdu, kad galimybes atlikti paskesnes nusikalstamas veikas jau pačioje sistemoje kaltininkui suteikia jo pirminiai neteisėto prisijungimo veiksmai. Taigi iš baudžiamosios teisės pozicijų vertinant padarytas nusikalstamas veikas, neturėtų stebinti itin dažni neteisėto prisijungimo inkriminavimo atvejai. Tačiau teismų praktikoje ši veika vis dėlto ne visuomet įžvelgiama tarp visų kaltininko padarytų nusikalstamų veikų elektroninėje erdvėje.

Pavyzdžiui, vienas iš sukčiavimo elektroninėje erdvėje etapų[219] susijęs su IS konfidencialumo pažeidimais neteisėtai panaudojant svetimus naudotojui IS atpažinti suteiktus autentifikavimo duomenis, kuriais jis prisijungia prie sistemos[220]. Nors šis etapas sukčiavimo atveju dažnai yra tarpinis, tačiau jis paprastai neišvengiamas, kaltininkui paskesniais veiksmais siekiant atlikti neteisėtas mokėjimo operacijas sistemoje. Apie galimybes tokį prisijungimą pažeidus IS apsaugos priemones[221] kvalifikuoti pagal BK 198[1] straipsnį užsiminta ir Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2012 m. birželio 26 d. nutartyje baudžiamojoje byloje (bylos Nr. 2K-375/2012). Joje sprendžiant nusikalstamų veikų, numatytų BK 198 ir 215 straipsniuose, atskyrimo problemą pažymėta, kad kaltininko veiksmai *neteisėtai prisijungus prie internetinės bankininkystės sistemos, panaudojant svetimus vartotoją identifikuojančius duomenis, galėtų būti kvalifikuojami ir pagal 198[1] straipsnį kaip neteisėtas prisijungimas prie informacinės sistemos pažeidžiant apsaugos duomenis. T. S. tokių kaltinimų pareikšta nebuvo <...>.*

Tačiau iš žemesnės instancijos teismų sprendimų, priimtų šios kategorijos baudžiamosiose bylose, matyti, kad BK 198[1] straipsnyje esančios nusikalstamos veikos inkriminavi-

---

[218] Česnys, A.; Juknius, J. *Saugumo patikros ir etiško įsilaužimo technologijos*. Kaunas: KTU leidykla „Technologija“ 2011, p. 21.

[219] Sukčiavimo elektroninėje erdvėje etapų visapusiam baudžiamajam teisiniam vertinimui nepakankama tik BK 182 straipsnyje numatyta sukčiavimo norma. Kadangi ši nusikalstama veika yra susieta su įvairiais elektroninių duomenų ir IS saugumo pažeidimais, tai be BK 182 straipsnio, kaltininkui taip pat turėtų būti inkriminuojamos BK XXX skyriuje ir (ar) BK 215 bei 214 straipsniuose numatytos nusikalstamos veikos. Be to, būtent nuorodos į BK 214, 215, 196–198[2] straipsnius liudija, kad sukčiavimui padaryti neteisėtai panaudota IS ir (ar) elektroniniai duomenys. Atitinkamai toks sukčiavimas gali būti priskiriamas anksčiau aptartai dėl informacinių technologijų panaudojimo pakitusių tradicinių nusikalstamų veikų grupei.

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

[221] Naudotoją elektroninių paslaugų sistemoje leidžianti atpažinti autentiškumo patvirtinimo procedūra gali būti laikoma viena iš šios sistemos saugumo užtikrinimo priemonių. Todėl kaltininko veiksmai, kuriais neteisėtai panaudojami kito asmens autentifikavimo duomenys ir taip prisijungiama prie šios sistemos, kvalifikuotini pagal BK 198[1] straipsnį (plačiau žr.: Kalpokas, V.; Marcinauskaitė, R. Tapatybės vagystė elektroninėje erdvėje: technologiniai aspektai ir baudžiamasis teisinis vertinimas. *Teisės problemos*. 2012, Nr. 3(77): 46).

mo praktika, nustačius neteisėtus kaltininko prisijungimo prie elektroninės bankininkystės sistemos veiksmus, nėra nuosekli. Vienais atvejais šis etapas išskiriamas ir neteisėtas prisijungimas prie IS laikomas savarankiška pagal BK 198[1] straipsnį kvalifikuotina nusikalstama veika. Kitais – neteisėtas prisijungimas prie IS, panaudojus kito asmens autentifikavimo šioje sistemoje duomenis, kaltininkui neinkriminuotas.

Neteisėtas prisijungimas prie elektroninės bankininkystės sistemos, pažeidžiant jos apsaugos priemones, atskirai pagal BK 198[1] straipsnį kvalifikuotas, pavyzdžiui, Vilniaus miesto 1 apylinkės teismo 2010 m. kovo 5 d. teismo baudžiamajame įsakyme, priimtame baudžiamojoje byloje (bylos Nr. N1-724-276/2010). Teismas nustatė, kad R. B. keletą kartų neteisėtai prisijungė prie bankų klientų (nukentėjusiųjų) paskirų elektroninės bankininkystės sistemose. Šiame baudžiamajame įsakyme konstatuota, kad, be kitų nusikalstamų veiksmų, R. B. taip pat *naudodamas asmeninį kompiuterį, jame įdiegtą interneto naršyklės kompiuterinę programą ir neteisėtai įgytus elektroninės bankininkystės sistemos (duomenys neskelbtini) naudotojo autentifikavimo vardus ir slaptažodžius, <...> buvo prisijungęs prie elektroninės bankininkystės sistemos (duomenys neskelbtini) ir šios sistemos naudotojų autentifikavimo langelyje įvesdavo AB (duomenys neskelbtini) kliento T. P. vartotojo vardą, nuolatinį slaptažodį bei kintamą T. P. išduotos slaptažodžių kortelės slaptažodį. AB (duomenys neskelbtini) tarnybinėje stotyje įdiegta sistema automatiniu režimu šiuos vardus ir slaptažodžius įvedusį asmenį autentifikavo kaip teisėtą elektroninės bankininkystės sistemos vartotoją T. P. ir <...> peradresavo jį į T. P. paskyrą elektroninės bankininkystės sistemoje (duomenys neskelbtini).*

Tokiu būdu R. B. neteisėtai, pažeisdamas <...> AB (duomenys neskelbtini) elektroninės bankininkystės sistemos <...> apsaugos priemones, numatančias, kad teisę prisijungti prie šių sistemų paskyrų turi tik šio banko klientai, sudarę su AB (duomenys neskelbtini) <...> elektroninės bankininkystės sutartis, autentifikuojami pagal jiems suteiktus kodus, vardus ir slaptažodžius, prisijungė prie <...> paskirų [tarp jų ir T. P paskyros – aut. pastaba] elektroninės bankininkystės sistemose (duomenys neskelbtini). Šios aplinkybės teismui leido pripažinti, kad R. B., be BK 214 straipsnio 1 dalies, 215 straipsnio 1 dalies, 182 straipsnio 1 dalies, turėtų būti inkriminuojama ir BK 198[1] straipsnio 1 dalis, numatanti atsakomybę už neteisėtą prisijungimą prie IS. Šis atvejis teismų praktikoje nėra vienintelis – neteisėti kaltininko prisijungimo prie elektroninės bankininkystės veiksmai pagal BK 198[1] straipsnį taip pat kvalifikuoti Vilniaus miesto 1 apylinkės teismo 2009 m. rugsėjo 14 d. teismo baudžiamajame įsakyme baudžiamojoje byloje (bylos Nr. N1-1470-88/2009), Kupiškio rajono apylinkės teismo 2009 m. rugsėjo 2 d. nuosprendyje baudžiamojoje byloje (bylos Nr. 1-53-100/2009) ir kt. Tiesa, reikėtų paminėti, kad šios kategorijos baudžiamosiose bylose galima sutikti ir tokių atvejų, kai minėti kaltininko veiksmai atskirai pagal BK 198[1] straipsnį kaip neteisėtas prisijungimas prie IS nekvalifikuoti (pavyzdžiui, Vilniaus miesto 4 apylinkės teismo 2010 m. gegužės 17 d. nuosprendis baudžiamojoje byloje (bylos Nr. 1-106-816/2010), Vilniaus miesto 1 apylinkės teismo nuosprendis baudžiamojoje byloje (bylos Nr. 1-68-203/2011) ir kt.).

Autentifikavimo procedūra, kaip viena iš IS apsaugos priemonių, būdinga ne tik elektroninei bankininkystei, bet ir kitom įvairias elektronines paslaugas (elektroninės parduotuvės, elektroninis paštas, socialiniai tinklai ir kt.) teikiančioms sistemoms. Todėl nustačius neteisėto prisijungimo prie šių sistemų faktą, kaltininkui taip pat inkriminuotina BK 198[1] straipsnyje numatyta nusikalstama veika. Pavyzdžiui, Klaipėdos miesto apylinkės

teismo 2009 m. birželio 29 d. teismo baudžiamuoju įsakymu baudžiamojoje byloje (bylos Nr. 1-740-93/2009) V. B., be kitų nusikalstamų veikų, nuteistas ir už neteisėtą prisijungimą prie internetinės prekybos ir aukcionų sistemos. Teismas pripažino V. B. kaltu padarius nusikalstamą veiką, numatytą BK 198[1] straipsnio 1 dalyje, t. y. *2007 m. balandžio 9 d. pastate, (duomenys neskelbtini), per šiam pastatui suteiktą interneto prieigą, naudojant nešiojamąjį kompiuterį <...>, jame įdiegtą internete naršyklės programą bei neteisėtai įgytus internetinės prekybos ir aukcionų sistemos (duomenys neskelbtini) vartotojo C. C. autentifikavimo kodą ir slaptažodį, kaip teisėtas C. C. paskyros internetinės prekybos ir aukcionų sistemoje (duomenys neskelbtini) vartotojas prisijungus prie šios sistemos (kompiuterinio tinklo), pažeidžiant jos apsaugos priemones.*

Apibendrinus galima teigti, kad viena pagrindinių problemų, su kuriomis susiduriama elektroninių nusikalstamų veikų bylose yra ta, kad neteisėtas prisijungimas prie IS ne visuomet pastebimas tarp visų kaltininko padarytų veikų elektroninėje erdvėje. Tokia praktika neatitinka Konvencijos dėl elektroninių nusikaltimų ir Pamatinio sprendimo 2005/222/TVR tikslų, kai juose apibrėžus neteisėtos prieigos veiką, siekta kriminalizuoti jau pirminius kaltininko veiksmus, sudarančius sąlygas kitoms nusikalstamoms veikoms sistemoje padaryti. Todėl neteisėtą prisijungimą kriminalizavus *per se,* ši veika visuomet inkriminuotina šalia kitų kaltininko jau sistemoje padarytų nusikalstamų veikų, jei nustatyti visi BK 198[1] straipsnyje numatyti jos sudėties požymiai.

2. Objektyvieji neteisėto prisijungimo prie informacinės sistemos sudėties požymiai

Sprendžiant kokia – ar pakankamai plačia, ar priešingai – siauresne – neteisėtos prieigos koncepcija buvo vadovautasi BK įtvirtinant neteisėto prisijungimo prie IS veiką, svarbu aptarti šios nusikalstamos veikos sudėties požymius. Būtent jų visuma padeda nustatyti neteisėto prisijungimo veikos „plotį", o tarpusavio sąsaja – apibrėžti atskirų šios veikos požymių turinį (dažnai interpretuojant vieną jų tenka atsižvelgti į tai, kaip suprantami kiti). Taip, pavyzdžiui, neteisėtumo aiškinimui turi įtakos IS apsaugos priemonių suvokimas, prisijungimo analizei – apsaugos priemonių nustatyti prieigos prie IS apribojimo būdai ir pan.

Ši veika iš pirmo žvilgsnio gali pasirodyti kaip nauja, iš baudžiamosios teisės pozicijų sunkiai paaiškinama ir neturinti ryšio su tradicinėmis baudžiamosios teisės doktrinomis. Tačiau, kai tik tokia veika ir jos požymiai suvokiami, jie akivaizdžiai leidžia pastebėti šių doktrinų vystymąsi, tačiau, be abejo, ne fizinėje erdvėje, o „skaitmeniniame kontekste" (pavyzdžiui, kalbant apie neteisėto įsibrovimo doktriną). Todėl galima būtų pritarti Kerr O. S. nuomonei, kad bene „naudingiausias orientyras interpretuojant naujausius aktus gali būti randamas praeityje"[222]. Apie tokį ryšį su jau esančiomis nusikalstamomis veikomis ir jų aiškinimo bendriausiomis pozicijomis iš dalies galima spręsti ir iš anksčiau minėto ekvivalentinio vertinimo principo.

Vis dėlto neteisėto prisijungimo prie IS aiškinimas susiduria su specifinėmis elektroninėms nusikalstamoms veikoms būdingomis problemomis. Šios veikos sudėtyje tiesiogiai numačius technologijas žyminčius terminus ir požymius, susijusius su įvairiais technologijų panaudojimo aspektais, kaskart tenka spręsti jų apibrėžties problemas. Juo labiau kad BK XXX skyriuje nėra pateiktas autentiškas jame vartojamų sąvokų išaiškinimas. Be to, šių

[222] Kerr, O. S. Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes. *NYU Law Review.* 2003, 78(5): 1668.

problemų sprendimą dažnai komplikuoja ir kriminalizuojant šią veiką įgyvendinti technologinio neutralumo principo reikalavimai. Todėl akivaizdu, kad anksčiau aptartas technologijų ir terminologijos klausimas iškyla nuolat – aiškinantis neteisėto prisijungimo sudėties požymius, atrenkant terminus toms pačioms sąvokoms pavadinti, formuluojant apibrėžtis ir kt.

2.1. Informacinė sistema kaip nusikalstamos veikos dalykas

Neteisėto prisijungimo prie IS dalykas BK 198[1] straipsnio dispozicijoje įvardytas kaip IS. Kadangi BK XXX skyriuje nėra pateiktas autentiškas jame vartojamų terminų išaiškinimas, tai, analizuojant šį objektyvųjį požymį, aktualu išspręsti jau ne kartą minėtą technologijų ir terminologijos klausimą.

Analizuojant užsienio valstybių neteisėtos prieigos kriminalizavimo praktiką matyti, kad technologijų sąvokų problemos bandomos spręsti dviem būdais: 1) technologijas žymintys terminai paliekami neapibrėžtais (pavyzdžiui, Prancūzija, Estija, Rusija, Čekija, Lietuva ir kt.). Nors toks požiūris, atsižvelgiant į technologinio neutralumo principo reikalavimus, turi akivaizdžių privalumų, tačiau teisės taikymo lygmeniui nepalieka aiškių kriterijų, kas gali būti ir kas nėra IS ar jos komponentai; 2) teisės aktuose nurodomos įvairių su technologijomis susijusių terminų reikšmės (pavyzdžiui, Jungtinės Amerikos Valstijos, Kipras, Austrija ir kt.). Nors šis būdas iš pirmo žvilgsnio galėtų atrodyti kaip galintis užtikrinti sudėties požymių aiškumą, tačiau dėl įtvirtinto pakankamai bendro sąvokų turinio tokie apibrėžimai kelia analogiškas problemas kaip ir tuomet, kai jie nėra suformuluoti[223].

Lietuvą priskyrus pirmajai valstybių grupei, teigtina, kad tinkamas IS interpretavimas paliekamas BK 198[1] straipsnio taikytojo nuožiūrai. Tačiau toks požiūris, leidžiantis pakankamai lanksčiai pažvelgti į IS sąvokos turinį, sukelia ir jos apibrėžties problemų. Neteisėto prisijungimo dalyko aiškinimas komplikuojasi dėl toms pačioms sąvokoms pavadinti vartojamų terminų per didelės įvairovės ir pačių sąvokų abstraktumo. Šiuos IS aiškinimo sunkumus iš dalies padeda spręsti Konvencijos dėl elektroninių nusikaltimų ir Pamatinio sprendimo 2005/222/TVR nuostatos bei jose suformuluotas požiūris į naująsias technologijas. Taip pat IS turiniui atskleisti gali būti aktualūs ir Tarptautinės standartizacijos organizacijos (ISO) ir Tarptautinės elektrotechnikos komisijos (IEC) sudaryti tarptautiniai standartai. Kadangi informacinės technologijos skatina intensyvius informacijos mainus tarptautiniu mastu, tai šie standartai padeda spręsti terminų, vartojamų įvairiose srityse, įvairovės, sąvokų apibrėžčių nebuvimo ar jų netikslumų problemas. Nagrinėjamu aspektu vienas aktualesnių yra ISO/IEC 2382-1:1996 *Informacijos technologijos. Terminai ir apibrėžimai. 1-oji laida. Pagrindiniai terminai* (toliau – ISO/IEC 2382-1:1996). Jis priklauso tarptautinių standartų ISO (ISO/IEC) 2382 grupei, kuri jungia duomenų apdorojimo, informacijos technologijų ir informacijos apdorojimo sistemų terminų bei apibrėžimų standartus. Jais siekiama pateikti tikslias, nesudėtingas, visiems suprantamas ir bendrai vartosenai priimtinas apibrėžtis.

Taigi prieš analizuojant neteisėtos prieigos prie IS dalyko požymį, reikėtų paminėti, kad universalaus IS suvokimo nėra, nes kiekvienas autorius ją traktuoja kažkiek skirtingai. Be to, dažnai greta IS taip pat minimi kompiuterinės sistemos, informacinių technologijų (toliau –

[223] Plačiau apie technologijoms neutralių sąvokų problemas ir jų sprendimo variantus žiūrėti I dalies 2.2 poskyryje.

IT)[224] ir komunikacijos technologijų terminai. Todėl aktualus ir šių terminų, vartojant juos baudžiamosios teisės kontekste, tarpusavio ryšys. Taip pat atkreiptinas dėmesys į tai, kad įvairioms IS apibrėžti vartojamoms sąvokoms gana didelės įtakos turėjo minėtas technologinio neutralumo principas, todėl jos dažniausiai konstruojamos nurodant bendras sistemos funkcijas ir tikslus bei vengiant specifinių, konkrečias technologijas žyminčių terminų.

Anot K. C. Laudon ir J. P. Laudon, IS gali būti 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“[225]. Panašios nuomonės yra ir Lietuvos mokslininkai (D. Dzemydienė, R. Naujikienė, A. Saulis, O. Vasilecas ir kt.). A. Saulio ir O. Vasileco teigimu, IS – tai „sistema, paverčianti išorinius ir vidinius duomenis informacija, užtikrinanti informacijos kaupimą, saugojimą, apdorojimą ir perdavimą naudotojui reikiamu pavidalu, sudaranti galimybę priimti optimalius sprendimus“[226]. Apibrėždamos IS, į įvairias jos funkcijas atkreipė dėmesį ir D. Dzemydienė bei R. Naujikienė. Jų manymu, IS galima apibūdinti kaip „kompleksą komponentų, skirtų įvairių rūšių duomenims ir informacijai rinkti, saugoti, apdoroti, laikyti bei skleisti, siekiant tam tikrų organizacijos tikslų ir taikant kompiuterines technologijas“[227]. Analizuojant šias sąvokas akivaizdu, kad jos atitinka bendrosios sistemų teorijos teiginius, jog sistema yra vienetas, kuris funkcionuoja aplinkoje, padeda siekti bendrų tikslų ir yra sudarytas iš daugelio tarpusavyje sąveikaujančių dalių.

Nors šios IS sistemų apibrėžtys pakankamai nuosekliai atskleidžia IS esmę, tačiau, vertinant iš baudžiamosios teisės pozicijų, jose yra keletas aspektų, kurie, kvalifikuojant neteisėto prisijungimo prie IS veiką, gali kelti ir sumaišties. Pagrindiniai minėtų sąvokų perėmimo ir taikymo baudžiamosios teisės kontekste sunkumai gali kilti dėl jose nurodomų IS sudedamųjų dalių (vadinamų IS komponentais arba posistemėmis)[228]. Kartu šis klausimas tiesiogiai siejamas ir su kita – IS, IT ir komunikacijos technologijų tarpusavio ryšio nustatymo problema.

Daugelis mokslininkų (T. Bilevičienė, R. Skyrius, A. Mikalauskienė, O. Vasilecas, J. R. Gordon, S. R. Gordon ir kt.), nagrinėjusių IS kūrimo ir pritaikomumo įvairiose veiklos srityse galimybes, IS sudedamųjų dalių neapriboja tik informacinėmis ir komunikacijos technologijomis. Vieni jų teigia, kad IS komponentai yra techninė įranga, programinė įranga, duomenys ir žmonės[229]. Panaši šiai ir ta nuomonė, kad „IS jungia informacines technologijas su duomenimis, duomenų apdorojimo procedūras ir žmones, kurie renka ir naudoja duomenis <...>“[230] arba kad sistemos komponentai yra „kompiuterinė sistema,

[224] Rekomenduojama vartoti informacinių, o ne informacijos technologijų terminą, nes pati informacija nėra nei procesas, nei veikla, nei darbas. (Jonušauskas, S.; Naujikienė, R.; Petrauskas, R. *Kompiuterinio raštingumo pagrindai, reikalingi Europos kompiuterių vartotojo pažymėjimui gauti*. Vilnius: Lietuvos teisės universiteto Leidybos centras, 2004, p. 12–13.).

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

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

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

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

[229] Saulis, A.; Vasilecas, O., *op. cit.*, p. 9.

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

žmonės, procedūros, duomenys ir informacija, ryšio priemonės (kai kompiuteris dirba tinkle)“[231]. Taip pat galima sutikti pakankamai platų požiūrį į IS išreiškiančių pozicijų, kai greta informacinių technologijų minimos ir taikomosios programos, uždaviniai ir kompleksai, duomenys, duomenų bazės, žmonės – IS vartotojai, žmonės – IS specialistai, naudojimosi IS taisyklės ir reglamentai, ryšio su kitomis IS priemonės[232]. Tačiau nepriklausomai nuo to, ar IS apibrėžiama pakankamai abstrakčiai ar detalizuojant ją sudarančius komponentus, vis dėlto bendriausia prasme turimas mintyje technologijų, funkcijų ir šias technologijas naudojančių žmonių tarpusavio ryšys. Tai yra, IS pagal šiuos požiūrius, be informacinių ir komunikacijos technologijų, apima ir savo funkcionavimo kontekstą, siejamą su šios sistemos paskirtimi ir jos vartotojais. Beje, toks požiūris į IS komponentus matyti ir ISO/IEC 2382-1:1996 standarte, kur IS apibūdinta 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“. Todėl analizuojant IS ir IT ryšį reikėtų paminėti U. Gupta pastebėjimą, kad „kompiuteris ir kitos informacinės technologijos yra priemonės, naudojamos sukurti informacinėms sistemoms. <...> Informacinės sistemos sujungia informacines technologijos, kad užtikrintų skirtingų naudotojų informacijos poreikius“[233]. Šie požiūriai, nagrinėjant juos neteisėto prisijungimo prie IS kvalifikavimo kontekste, natūraliai kelia klausimą, ar nustatant neteisėtos prieigos prie IS dalyką turėtų būti vertinami ne tik technologiniai aspektai, bet ir visi anksčiau minėti IS sistemą sudarantys komponentai. Sprendžiant šią problemą pažymėtina, kad BK 198[1] straipsnyje minimos IS ištakų pirmiausia reikėtų ieškoti tiesiogiai ne komunikacijos ir informacijos mokslų srityje, o tarptautiniuose ir Europos Sąjungos dokumentuose, kuriuose ji numatyta. Todėl šiuo aspektu aktualu nustatyti, kokia reikšmė BK 198[1] straipsnyje esančiam IS terminui galėjo būti suteikta, įgyvendinant Konvencijos dėl elektroninių nusikaltimų 2 straipsnio ir Pamatinio sprendimo 2005/222/TVR 2 straipsnio nuostatas Lietuvos nacionalinėje teisėje.

Pagal Pamatinio sprendimo 2005/222/TVR 1 straipsnio a punktą IS apibrėžta kaip „prietaisas arba tarpusavyje sujungtų ar susijusių prietaisų grupė, iš kurių vienas arba daugiau pagal programą vykdo automatinį kompiuterinių duomenų tvarkymą[234], taip pat juose saugomi, tvarkomi, iš jų išrenkami arba jais perduodami kompiuteriniai duomenys turint tikslą juos apdoroti, panaudoti, apsaugoti ir prižiūrėti“. Pamatinio sprendimo 2005/222/TVR aiškinamajame memorandume akcentuota, kad IS terminas sąmoningai vartojamas plačiausia prasme. Todėl, siekiant Pamatinio sprendimo 2005/222/TVR tikslų, IS apima patį savarankišką kompiuterį, personalinius delninukus (angl. *personal digital organiser*), mobiliuosius telefonus, intranetą, ekstranetą ir, žinoma, tinklus, serverius bei kitus Interneto infrastruktūros įrenginius.

Skirtingai nei Pamatiniame sprendime 2005/222/TVR, Konvencijoje dėl elektroninių nusikaltimų vartojamas nebe IS, o kompiuterinės sistemos terminas. Jis šios Konvencijos

[231] Jonušauskas, S.; Bilevičienė, T.; Kažemikaitis, V., *supra* note 136, p. 5.

[232] Skyrius, R.; Mikalauskienė, A.; Zaliackienė, L., *supra* note 103, p. 17–18.

[233] Gupta, U., *supra* note 228, p. 16–17.

[234] Pagal ISO/IEC 2382-1:1996 standartą „duomenų apdorojimas – sistemingas operacijų su duomenimis atlikimas (pavyzdžiui, aritmetinės ir loginės operacijos su duomenimis; duomenų rūšiavimas ir suliejimas; programų kompiliavimas ir surinkimas; operacijos su tekstu – redagavimas, rūšiavimas, suliejimas, įrašymas į atmintį, paieška, rodymas ekrane, spausdinimas)“.

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[235] ir programinės įrangos[236] ir sukurtus vykdyti elektroninių duomenų automatinį apdorojimą. Kompiuterinė sistema gali turėti įvesties, išvesties ir laikymo (saugojimo) įrangą. Tai gali būti savarankiška kompiuterinė sistema arba tinklu sujungta su kitomis panašiomis sistemomis. Kompiuterinę sistemą paprastai sudaro įvairūs įrenginiai, kurie gali būti suskirstyti į procesorių (angl. *processor*)[237] arba centrinį procesorinį įrenginį (CPĮ) ir išorinius įrenginius (angl. *peripherals*). Išoriniais įrenginiais[238] laikomi tokie įrenginiai, kurie atlieka tam tikras specifines funkcijas sąveikaudami su apdorojimą vykdančiu vienetu (angl. *processing unit*), pavyzdžiui, spausdintuvas, kompaktinių diskų skaitymo ar įrašymo įrenginiai (angl. *CD reader/writer*), taip pat kiti laikymo (saugojimo) funkcijas atliekantys įrenginiai.

Kaip matyti, tiek kalbant apie kompiuterinę sistemą Konvencijoje dėl elektroninių nusikaltimų, tiek apie IS Pamatiniame sprendime 2005/222/TVR, aptariami išimtinai bendriausi technologiniai sistemų aspektai – aparatinė ir programinė įranga, sistemos atliekamos funkcijos. Šiuose teisės aktuose pateikti apibrėžimai taip pat leidžia pastebėti daug Pamatiniame sprendime 2005/222/TVR minimos IS ir Konvencijoje dėl elektroninių nusikaltimų esančios kompiuterinės sistemos panašumų. Taigi teigtina, kad BK 198[1] straipsnyje vartojamas IS terminas suvokiamas siauriau – be IS taikomojo aspekto ir bendriausia prasme galėtų būti laikomas IT (apimančių ir komunikavimo technologijas) sinonimu[239]. Todėl nustatant neteisėto prisijungimo prie IS dalyko požymį kaltininko veikoje, jo vertinimui neturėtų turėti įtakos anksčiau minėti IS vartotojai ir aplinka, kurioje ji funkcionuoja. Toks požiūris į IS matyti ir nacionaliniuose teisės aktuose, kuriuose dėmesys apibūdinant sistemą teikiamas techninių ir programinių priemonių visumai, būtinai elektroniniams duomenims apdoroti. Pavyzdžiui, Lietuvos Respublikos informacinės visuomenės paslaugų įstatymo[240] 2 straipsnio 9 dalyje IS apibrėžta be jos taikymo konteksto kaip „techninių ir programinių priemonių visuma, naudojama informacijai kurti, siųsti, priimti, išsaugoti ar kitaip tvarkyti elektroniniu būdu“.

---

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

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

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

[238] 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)“.

[239] 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 yra pateikiamas taip pat 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., *supra* note 136, p. 24.).

[240] *Valstybės žinios*. 2006, Nr. 65-2380.

Tačiau baudžiamosios teisės kontekste išvedant tokį IS, IT ir komunikacijos technologijų ryšį būtinas tam tikras patikslinimas:

1) IS, numatyta BK 198[1] straipsnyje, turėtų būti siejama tik su kompiuterizuotomis IS. Būtent kompiuterizuotos IS taiko informacines technologijas[241] duomenų apdorojimo procesams realizuoti[242]. Kaip teigia Potter R., „kompiuteriu pagrįstos IS, tai IS, kurios naudoja kompiuterių technologijas, kad atliktų kai kurias arba visas numatytas užduotis. Nors ne visos informacinės sistemos yra kompiuterizuotos, bet dauguma yra. Dėl šių priežasčių terminas „informacinės sistemos" paprastai vartojamas kaip „kompiuteriais pagrįstų informacinių sistemų" sinonimas"[243]. Todėl tik kompiuterizuotos IS, kaip jos suvokiamos Pamatiniame sprendime 2005/222/TVR, gali būti tapatinamos su Konvencijoje dėl elektroninių nusikaltimų minimomis kompiuterinėmis sistemomis.

2) analizuojant IT (ar IS) ir komunikacijos technologijas, paminėtinas dvejopas požiūris į jų tarpusavio sąsają. Vienais atvejais komunikacijos technologijos laikomos IT (IS) sudedamąja dalimi[244]. Tačiau, norint akcentuoti įvairius ryšio įrenginius ir informacijos perdavimo būdus, komunikacinės technologijos gali būti minimos ir šalia IT (IS)[245]. Vertinant Konvencijos dėl elektroninių nusikaltimų ir Pamatinio sprendimo 2005/222/TVR nuostatas matyti, kad apibrėžiant tiek kompiuterinę sistemą, tiek IS laikytasi pirmosios pozicijos ir komunikacijos technologijos įtrauktos į IS ir kompiuterinės sistemos turinį. Pamatiniame sprendime, pateikiant IS apibrėžimą, tiesiogiai minimi prietaisai ar susijusių prietaisų grupės, kuriais „perduodami kompiuteriniai duomenys". Kaip pavyzdį galima pateikti to paties Pamatinio sprendimo aiškinamajame memorandume nurodytus intranetą, ekstranetą, tinklus, serverius ir kitus Interneto infrastruktūros įrenginius. Konvencinėse nuostatose numatytas kompiuterinės sistemos apibrėžimas yra pakankamai bendro pobūdžio, tačiau nuorodas į komunikacijos technologijas parodo jame bendriausia prasme minimos sąsajos tarp įtaisų. Taip pat šios Konvencijos aiškinamojoje ataskaitoje nemažas dėmesys skiriamas tinklų, sujungiančių kompiuterines sistemas arba sujungtų tarpusavyje, rūšių aprašymui (24 punktas).

Taigi, šiame kontekste analizuojant BK 198[1] straipsnyje nurodytą nusikalstamos veikos dalyką, galima būtų padaryti keletą svarbių išvadų: 1) 2004 m. įgyvendinus Konvencijos dėl elektroninių nusikaltimų nuostatas, kaip minėta, ši nusikalstama veika buvo įvardyta kaip neteisėtas prisijungimas prie kompiuterio ar kompiuterinio tinklo. Atitinkamai

---

[241] Informacinių technologijų terminas dažniausiai yra siejamas su kompiuterinėmis informacinėmis technologijomis, kurių materialų pagrindą sudaro kompiuterių technologijos. Tačiau vis dėlto reikėtų atkreipti dėmesį, kad informacinių technologijų samprata yra daug platesnė – joms priklauso viskas, kas skirta įrašyti, perduoti ar išreikšti informaciją (pavyzdžiui, net ir tradicinės popierinės technologijos – dokumentai, laiškai, spaudai ir t.t.) (plačiau žr.: Skyrius, R.; Mikalauskienė, A.; Zalieckaitė, L., *supra* note 103, p. 17).

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

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

[244] Pavyzdžiui, vienais atvejais 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). Kitais atvejais apie IT turinį galima atskleisti per jos sudedamųjų dalių raidą: kompiuterių, programinės įrangos, duomenų kaupimo įrangos ir ryšių įrangos (Skyrius, R.; Mikalauskienė, A.; Zalieckaitė, L., *supra* note 103, p. 22.).

[245] *Enciklopedinis kompiuterijos žodynas*. 2-asis papildytas leidimas. Vilnius: TEV, 2008, p. 160.

nusikalstamos veikos dalyku laikytas kompiuteris arba kompiuterinis tinklas, tai reiškė, kad, kvalifikuojant tokio pobūdžio veikas, turėjo būti nustatomi būtent jų konfidencialumo pažeidimai. Dėl vėlesnių 2007 metų pakeitimų šios veikos dalykas kito – jis BK 198[1] straipsnyje nurodytas kaip IS; 2) kadangi paskutinius minėto BK straipsnio pakeitimus lėmė Pamatinio sprendimo 2005/222/TVR nuostatų perkėlimas į nacionalinės teisės sistemą, tai neteisėto prisijungimo sudėtyje numatyto IS požymio ištakų reikėtų ieškoti būtent šiame Europos Sąjungos teisės akte; 3) nors įgyvendinant Pamatinį sprendimą BK nebuvo pateiktas autentiškas su technologijomis susijusių sąvokų išaiškinimas, vis dėlto šio sprendimo įtaka, interpretuojant neteisėto prisijungimo prie IS sudėties požymius, išlieka akivaizdi. Todėl nebūtų apsirikta, jei IS požymis būtų atskleidžiamas vadovaujantis minėto sprendimo 1 straipsnio a punkte pateikta IS apibrėžtimi[246]. Į tokį glaudų Pamatinio sprendimo 2005/222/TVR nuostatų ir įvairių technologijas žyminčių sąvokų ryšį atkreiptas dėmesys ir BK XXX skyriaus nusikalstamas veikas komentuojančių autorių[247]; 4) Į IS kaip neteisėto prisijungimo dalyko požymio turinį įtrauktos ne tik IT, bet ir komunikacijos technologijos. Tokia išvada darytina atsižvelgiant į tai, kad anksčiau BK 198[1] straipsnio dispozicijoje minimos kompiuterio ir kompiuterinio tinklo technologijos po 2007 metų pakeitimų buvo sujungtos ir šiame BK straipsnyje įvardytos vienu IS terminu.

Analizuojant neteisėto prisijungimo prie IS dalyko požymius, svarbu aptarti dar vieną baudžiamajai teisei aktualų jo aspektą. Tiek Konvencijoje dėl elektroninių nusikaltimų, tiek ir Pamatiniame sprendime 2005/222/TVR pateiktuose kompiuterinės sistemos ir IS apibrėžimuose nurodomi atskiri prietaisai ar tarpusavyje susijusių prietaisų grupės, kurie ir sudaro šias sistemas. Vadovaujantis minėtos bendrosios sistemų teorijos teiginiais pažymėtina, kad IS funkcionuoja kaip vienetas, sudarytas iš įvairių jos sudedamųjų dalių derinių. Todėl pats neteisėtas poveikis IS konfidencialumui gali būti padaromas tiesiogiai veikiant tik tam tikrus specifines funkcijas atliekančius jos komponentus. Kaip pastebi A. Venčkauskas ir J. Toldinas, „konfidencialumo, prieinamumo ir vientisumo sąvokos taikomos ne tik informacijai (duomenims), bet ir kitiems tinklo ištekliams, pavyzdžiui, išoriniams įrenginiams arba priedams. Yra daugybė sisteminių išteklių, kurių „neteisėto“ panaudojimo galimybė gali sudaryti sąlygas pažeisti sistemos saugumą“[248]. Kadangi IS komponentai funkcionuoja kaip viena visuma, tai neteisėtas prisijungimas prie IS turėtų būti konstatuojamas ir tais atvejais, kai, pažeidus IS ar jos dalių apsaugos priemones, prieiga buvo gauta prie atskirų sistemos elementų (pavyzdžiui, išorinių įrenginių, tinklo infrastruktūros įrenginių ir pan.).

2.2. Neteisėtas prisijungimas kaip pavojinga veika

2.2.1. Prisijungimo samprata

Galiojančiame BK 198[1] straipsnyje pavojinga veika įvardyta kaip neteisėtas prisijungimas. Atskleidžiant šio požymio turinį akcentuotina, kad tiek prisijungimas, tiek jo netei-

[246] Kaip minėta, Pamatinio sprendimo 2005/222/TVR 1 straipsnio a punkte informacinė sistema apibrėžta kaip „prietaisas arba tarpusavyje sujungtų ar susijusių prietaisų grupė, iš kurių vienas arba daugiau pagal programą vykdo automatinį kompiuterinių duomenų tvarkymą, taip pat juose saugomi, tvarkomi, iš jų išrenkami arba jais perduodami kompiuteriniai duomenys su tikslu juos apdoroti, panaudoti, apsaugoti ir prižiūrėti“.

[247] Abramavičius, A., *et al.*, *supra* note 160, p. 426.

[248] Venčkauskas, A.; Toldinas, J., *supra* note 170, p. 9.

sėtumas, atsižvelgiant į tarptautinius ir Europos Sąjungos teisės aktus, mokslinėje literatūroje išsakomas nuomones, užsienio valstybių tokios veikos kriminalizavimo patirtį, gali būti interpretuojamas labai įvairiai. Kadangi neteisėtam prisijungimui įmanoma suteikti pakankamai plačią arba ganėtinai siaurą reikšmę, tai aiškinant šį pavojingos veikos požymį turėtų būti nustatoma, kaip plačiai įstatymų leidėjas siekė kriminalizuoti neteisėto prisijungimo prie IS nusikalstamą veiką.

Analizuojant prisijungimo prie IS veiką atkreiptinas dėmesys į tai, kad tiek Konvencijoje dėl elektroninių nusikaltimų (2 straipsnis), tiek ir Pamatiniame sprendime 2005/222/TVR (2 straipsnis) toks terminas nėra minimas. Šiuose teisės aktuose kalbama ne apie neteisėtą prisijungimą, o apie neteisėtą prieigą (angl. *access*) prie IS. Nors iš pirmo žvilgsnio galėtų atrodyti, kad šie terminai žymi analogiškas sąvokas, tačiau vis dėlto prisijungimui prie IS būdinga tam tikra specifika. Tokį skirtumą lemia įvairūs prieigos prie IS interpretavimo variantai, kurie gali šiai sąvokai suteikti arba labai plačią reikšmę, arba priešingai – ją susiaurinti. Todėl priklausomai nuo požiūrio prieiga gali būti laikoma prisijungimo sinonimu, tačiau prieiga prie IS gali būti suprantama ir plačiau nei prisijungimas. Kadangi prisijungimo terminas Lietuvos BK nėra išaiškintas, tai bandant nustatyti prieigos ir prisijungimo santykį bei atskleisti jų turinį reikėtų atsižvelgti ne tik į bendrinę šių žodžių reikšmę, bet taip pat pasirinkti vieną iš galimų požiūrių į elektroninę erdvę – jos vertinimo perspektyvą.

Informacinių ir komunikacijos technologijų srityje prieiga prie IS suvokiama panašiai. Ji apibūdinama kaip įėjimo prie duomenų ar IS gavimas[249], galimybė įeiti ir naudotis sistema[250] arba galimybė prieiti prie sistemos išteklių[251]. Panašiai ji apibūdinama ir Konvencijos dėl elektroninių nusikaltimų aiškinamojoje ataskaitoje – joje prieiga tai „įėjimas į visą arba dalį kompiuterinės sistemos“ (46 punktas). Iš šių aiškinimų matyti, kad prieiga bendriausia prasme suvokiama kaip įėjimas ir priartėjimas prie IS išteklių. Tačiau tokia išvada leidžia pastebėti įdomų aspektą – aiškinant šią veiką nevengiama tų pasakymų, kurie vartojami veiksmams fizinėje erdvėje apibūdinti. Pavyzdžiui, kadangi prieiga laikoma įėjimu į IS, tai atitinkamai galimas ir išėjimas iš jos (tai laikytina analogu įėjimui ir išėjimui iš patalpos). Į tokią gana keblią situaciją, kai veiksmams elektroninėje erdvėje paaiškinti bandomi pritaikyti artimi fizinės erdvės kriterijai, atkreiptas dėmesys ir mokslinėje literatūroje (M. W. S. Wong, M. J. Madison, J. Clough, O. S. Kerr ir kt.)[252]. Įvairūs autoriai, nagrinėdami probleminius neteisėtos prieigos aspektus, pateikė pakankamai įdomius palyginimus ir bandymus paaiškinti, kodėl baudžiamojoje teisėje elektroninės erdvės vertinimas nenutolo nuo fizinės erdvės suvokimo. M. J. Madison teigimu, dažnai „Internetas yra apibūdinamas vietos ir erdvės terminais iš dalies dėl to, kad tokiu būdu mes jį suprantame ir apie jį įgauname patirties“[253]. Vienas iš J. Clough nagrinėjamų prieigos vertinimo variantų autoriui leido kompiuterį prilyginti „dėžei“, informacijos saugyklai, į kurią patekimas yra uždraustas. Taip pat, nagrinėdamas Konvencijos dėl elektroninių

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

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

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

[252] 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., *supra* note 110; Kerr, O. S., *supra* note 222.

[253] Madison, M. J., *op. cit.*, p. 442.

nusikaltimų nuostatas bei jų išaiškinimus, autorius pastebėjo, kad „įėjimo į visą ar dalį kompiuterinės sistemos“ pasakymas „sukelia būvimo kompiuterio „viduje“ arba „išorėje“ įsivaizdavimą“[254]. Akivaizdu, kad toks neteisėtas patekimas į IS vidų būtų siejamas ne su fizine, o su M. W. S. Wong įvardyta „virtualia prieiga“[255], kuri panaši į neteisėtą įėjimą į fizinėje erdvėje esančią vietą. Tokie samprotavimai leidžia ne tik suformuluoti elektroninės erdvės kaip vietos palyginimą, bet taip pat pastebėti tradicinės neteisėto įsibrovimo į svetimą valdą (angl. *trespass*) doktrinos raidą[256]. Būtent ši doktrina mokslinėje literatūroje (I. Walden, M. W. S. Wong, D. Reed ir kt.)[257] dažnai laikoma logišku atspirties tašku aiškinant neteisėto prisijungimo prie IS veiką ir vadinama elektroninio įsibrovimo į svetimą erdvę terminu (angl. *cybertrespass*). Nors ši doktrina yra bendrosios teisės sistemos valstybių „kūrinys“, tačiau vis dėlto apie įsibrovimo doktrinos vystymąsi galima kalbėti ir analizuojant Lietuvos BK nuostatas. Jame numatyta keletas nusikalstamų veikų, į kurių sudėtį įtrauktas įsibrovimo elementas. Tai BK 165 straipsnyje aprašyta neteisėto asmens būsto neliečiamumo pažeidimo veika, BK 178 straipsnio 2 dalyje esanti vagystė įsibraunant į patalpą, saugyklą ar saugomą teritoriją ir BK 180 straipsnio 2 dalyje kriminalizuotas plėšimas įsibraunant į patalpą. Kaip teigia A. Pikelis, „įstatymų leidėjas, pabrėždamas konstitucinį žmogaus būsto neliečiamumo principą, sąmoningai įtvirtino ir išimtinę teisinę jo apsaugą baudžiamosios teisės priemonėmis“[258]. Analizuojant „įsibrovimą“ elektroninėje erdvėje, galima būtų teigti, kad tam tikra privatumo apsauga, *mutatis mutandis* įgyvendinant žmogaus būsto neliečiamumo principą, yra užtikrinta BK 198[1] straipsnyje, numatančiame baudžiamąją atsakomybę už neteisėtą prisijungimą prie IS. Kadangi ši veika BK kriminalizuota *per se* be ryšio 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). Apie tokią vertinimo galimybę yra užsiminęs ir D. Štitilis, kurio manymu, „informacinių technologijų vystymasis leidžia neliečiamybę pažeisti kitomis formomis, taigi elektroninis įsiveržimas iš dalies gali būti prilyginamas fiziniam įsiveržimui į būstą“[259]. Todėl apibendrinus teigtina, kad šis prieigos prie IS aiškinimo variantas rodo „virtualią analogiją“[260], kuri reikštų ne ką kitą kaip tradicinio supratimo apie neteisėtą įsibrovimą perėmimą ir pritaikymą elektroninės erdvės kontekste.

Tačiau toks požiūris neskiria pakankamai dėmesio įvairiems IS technologiniams aspektams – nuolat besivystančioms įvesties, duomenų apdorojimo (tarp jų ir komunikavi-

[254] Clough, J., *supra* note 110, p. 59.

[255] Wong, M. W. S., *supra* note 252, p. 123.

[256] Bendrosios teisės tradicijos valstybėse suformuluota *trespass doktrina* yra pakankamai plati ir apima tris pagrindines formas: įsibrovimas į svetimą valdą (angl. *trespass to land*), kilnojamojo turto savininko teisės pažeidimas (angl. *trespass to goods*) ir kėsinimas į asmenį (angl. *trespass to person*). Sprendžiant, kuri iš jų yra tinkama kalbėti apie „virtualią 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, yra tiksliau kalbėti apie *trespass to goods* virtualią analogiją. Tuo tarpu, jei nusikalstama veika tiesiogiai kriminalizuota kaip neteisėta prieiga prie IS, tinkamesnė *trespass to land* virtuali analogija.

[257] Walden, I., *supra* note 70, p. 163; Wong, M. W. S, *op. cit*., p. 90–107; Reed, D. Should the English Legal System adopt the US Law of Cyber–Trespass? *SCRIPTed*. 2011, 8(1): 46–68.

[258] Pikelis, A., *supra* note 64, p. 99.

[259] Štitilis, D., *supra* note 7, p. 143.

[260] Kerr, O. S., *supra* note 222, p. 1620.

mo), išvesties galimybėms. IS veikia fizinėje erdvėje, turi tam tikrus fizinius parametrus, pasižymi atitinkamais ją sudarančių komponentų sąveikos būdais, tačiau kartu ji sukuria elektroninę erdvę. Ši erdvė pati savaime nėra analogiška fizinei erdvei – ji yra IS, veikiančios fizinėje erdvėje, veiklos rezultatas. Tokią gana keblią situaciją gerai atspindi Lessig L. pateiktas pastebėjimas, 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 abejose – realioje erdvėje ir elektroninėje erdvėje – tuo pačiu metu"[261]. Būtent pastebėjus šį dualumą, mokslinėje literatūroje pradėta kalbėti apie dvi skirtingas elektroninės erdvės vertinimo pozicijas – *išorinę* ir *vidinę perspektyvą*[262]. Šie O. S. Kerr pasiūlyti elektroninės erdvės vertinimo variantai turėjo pakankamai didelės praktinės reikšmės, todėl jie buvo perimti kitų mokslininkų (M. W. S. Wong, J. Clough ir kt.)[263], analizuojančių įvairius neteisėtos prieigos probleminius aspektus. Kadangi šios vertinimo pozicijos tarpusavyje konkuruoja, tai vienos iš jų pasirinkimas ir taikymas toms pačioms faktinėms aplinkybėms gali lemti visiškai skirtingą neteisėtos prieigos prie IS baudžiamąjį teisinį vertinimą.

Vidinė perspektyva leidžia į elektroninę erdvę pažvelgti kaip į „virtualią realybę"[264]. Tai sudaro galimybes elektroninės erdvės suvokimui ir veiksmų joje vertinimui taikyti fizinėje erdvėje nustatytus kriterijus arba kitaip tariant kalbėti apie jau minėtą „virtualią analogiją". Atitinkamai poreikis skirstyti elektroninę erdvę į dalis ir nustatyti jų ribas yra pagrįstas tradiciniu fizinės erdvės skaidymu į tam tikras teritorijas, o tai sudaro galimybes analizuoti ir vertinti įvairius konfidencialumo pažeidimus. Tai leido J. Clough kompiuterį prilyginti „dėžei" ir informacijos saugyklai, o prieigą prie IS laikyti metaforišku patekimu į kompiuterio „vidų" kaip įėjimu į pastatą[265]. Toks O. S. Kerr pasiūlytas vienas iš galimų požiūrių į elektroninę erdvę tiesiogiai atspinti IS naudotojo elektroninės erdvės įsivaizdavimą ir jos suvokimą. Beje, laikantis šio požiūrio elektroninės erdvės vertinimui ieškoma analogijų fizinėje erdvėje ir keliamos idėjos apie neteisėto įsibrovimo doktrinos vystymąsi ir jos taikymą elektroninės erdvės kontekste.

Kaip klasikinis *vidinės perspektyvos* taikymo pavyzdys mokslinėje literatūroje[266] 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 artimu durų užraktui, o „vartotojo vardo ir slaptažodžio įvedimas yra tarsi raktas, reikalingas užraktui atrakinti"[267]. Todėl, jei vartotojas įveda teisingus duomenis, jis gauna prieigą prie kompiuterio. Ir priešingai – jei kompiuteriui buvo pateikti klaidingi duomenys, vartotojui prieiga buvo nesuteikta. Priešingai iš *vidinės perspektyvos* pozicijų būtų vertinami neteisėti tinklų ar prievadų peržiūros veiksmai, kuriais, pavyzdžiui, renkama įvairi su IP adresais, sistemoje veikiančiais servisais, operacine sistema, įdiegtomis programomis susijusi ir panaši informacija (duomenų srauto „pasiklausymas" tinklo viduje[268]) Taip dažniausiai nustatomas IS pažeidžiamos

[261] Lessig, L. *Code and other Laws of Cyberspace*. New York (N.Y.): Basic books, 1999, p. 21.
[262] Kerr, O. S. The Problem of Perspective in Internet Law. *Georgetown Law Journal*. 2003, 91.
[263] Wong, M. W. S., *supra* note 252, p. 123; Clough, J., *supra* note 110, p. 59.
[264] Kerr, O. S., *supra* note 262.
[265] Clough, J., *supra* note 110, p.59.
[266] Kerr, O. S., *supra* note 222, p. 1620; Clough, J., *op. cit.*, p. 59.
[267] Kerr, O. S., *op. cit.*, p. 1620.
[268] Venčkauskas, A.; Toldinas, J., *supra* note 170, p. 10.

vietos, o esamos saugumo spragos išnaudojamos neteisėtai į ją įsibraunant. Kadangi šie veiksmai, žiūrint iš *vidinės perspektyvos* pozicijų, nėra laikomi „virtualiu įėjimu“ į IS, tai jiems apibūdinti yra naudojamas „durų rankenų klebenimo“[269] palyginimas.

Taikant *išorinės perspektyvos* variantą į elektroninę erdvę žiūrima ne kaip į „virtualią realybę“, bet tik kaip į IS veiklos rezultatą. Toks požiūris teikia pirmumą nebe šios erdvės naudotojo įsivaizdavimui, o kaip įvardijo J. Clough– atspindi „pašaliečio“[270] suvokimą. Būdamas fizinėje erdvėje, jis IS mato kaip tam tikrą mechanizmą, sudarytą iš komponentų, kurie tarpusavyje komunikuoja siųsdami, gaudami ar kitaip apdorodami duomenis. Būtent tokių funkcijų atlikimas ir lemia pokyčius virtualioje erdvėje. Todėl *išorinės perspektyvos* pasirinkimo atveju pagrindinis dėmesys skiriamas IS funkcijų, komunikavimo būdų nustatymui ir analizei, neatsižvelgiant į tai, kokius pokyčius jos sukelia elektroninėje erdvėje kaip „virtualioje realybėje“. Kaip pavyzdį galima būtų pateikti atvejį, kai vartotojas, naudodamasis naršyklės paslaugomis, siekia apsilankyti konkrečiame tinklalapyje. Sėkmingai įvykdytos užklausos atveju pagal *vidinės perspektyvos* teoriją vartotojas tiesiog matys atvertą jo pageidaujamą tinklalapį. Tačiau tokia „virtuali realybė“ tiesiogiai neatspindi tų IS 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[271], 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 t. t.). Taigi tai, ką vartotojas mato būdamas virtualioje erdvėje, ir tai, kokias funkcijas atlieka IS, sukurdama šią erdvę, iš esmės skiriasi. Todėl IS įvairių funkcijų apibūdinimui šiuo atveju gali būti pasitelkiamas taiklus O. S. Kerr pateiktas „veikimo už scenos“[272] palyginimas. Tačiau toks atskyrimas keičia ir patį požiūrį į prieigą prie IS, nes *išorinės perspektyvos* atveju pasitelkiamas nebe virtualaus įėjimo į IS (liudijančio virtualią prieigą), o sąveikos su ja kriterijus. Šis kriterijus daugelio prieigos problematiką nagrinėjusių autorių įvardijamas įvairiai: kaip „interakcija su kompiuteriu“[273], „susisiekimas su kompiuteriu“[274], „privertimas kompiuterį atsakyti“[275] ar pan. Visais šiais atvejais turimas mintyje IS funkcijos inicijavimas. Vertinant išimtinai tik tai, kaip veikia kompiuteris, O. S. Kerr nuomone, prieiga gali būti interpretuojama kaip bet koks susisiekimas su kompiuteriu. Todėl taikant *išorinės perspektyvos* teoriją prieigai konstatuoti užtektų, jei kompiuteriui buvo nusiųsta komanda vykdyti funkciją ir „kompiuteris atlieka reikalavimą kaip nustatyta“[276]. Panašią situaciją, apibūdindamas prieigos vertinimo variantus, mini ir M. W. S. Wong: vienas iš atvejų, leidžiančių kalbėti apie prieigą, anot jo, gali būti laikoma įrodyta vartotojo ir kompiuterio interakcija. Tačiau detalizuodamas šią situaciją jis svarsto, ar tokiais atvejais pakanka nustatyti užklausos

[269] Clough, J., *supra* note 210, p. 154.
[270] Kerr, O. S., *supra* note 222, p. 1620.
[271] DNS tai „domenų vardus skaitmeniniais Interneto adresais verčiantis serveris“. (Paulauskas, K. V. *Aiškinamasis kompiuterijos terminų santrumpų žodynas*. Kaunas: Technologija, 2000, p. 83).
[272] Kerr, O. S., *op. cit.*, p. 1620.
[273] Wong, M. W. S., *supra* note 252, p. 123.
[274] Kerr, O. S., *op. cit.*, p. 1620.
[275] Clough, J., *supra* note 110, p. 59.
[276] Kerr, O. S., *op. cit.*, p. 1620.

siuntimo faktą ar turėtų būti reikalaujama „iš to sekančio automatizuoto ar kitokio kompiuterio atsako“[277].

Kaip pavyzdys, padedantis aiškiau suvokti *išorinės* ir *vidinės perspektyvų* skirtumus, paminėtinas anksčiau aptartas atvejis asmeniui bandant prisijungti prie vartotojo vardu ir slaptažodžiu apsaugoto kompiuterio. Žvelgiant iš *vidinės perspektyvos*, prieiga prie kompiuterio būtų tapatinama su „virtualiu įėjimu“ ir konstatuota nustačius, kad asmuo įvedė teisingus sistemos reikalaujamus duomenis. Priešingu atveju, nepavykus autentifikavimui (pavyzdžiui, įvedus klaidingus duomenis), būtų laikoma, kad prieiga asmeniui nebuvo suteikta. Tačiau taikant *išorinės perspektyvos* teorijos kriterijus, tokios situacijos vertinimas yra kiek kitoks. Nors išvada dėl prieigos gavimo sutaptų tais atvejais, kai asmuo sėkmingai prisijungia prie kompiuterio, tačiau esant nesėkmingam bandymui vertinimas iš esmės skirtųsi. Net ir negavęs „virtualaus įėjimo“ jis, įvesdamas neteisingą vartotojo vardą arba slaptažodį, privertė kompiuterį atlikti funkciją ir pateikti rezultatą, nurodantį, kad yra įvesti neteisingi duomenys ir prieiga jam nesuteikiama. Pagal *išorinės perspektyvos* teoriją šie veiksmai gali būti prilyginami prieigai prie kompiuterio. Taip pat, skirtingai nei *vidinės perspektyvos* atveju, vertinami ir anksčiau aptarti prievadų ar tinklų peržiūros veiksmai. Reikėtų pastebėti, kad peržiūros proceso metu vyksta tam tikras pasikeitimas duomenimis (bendravimas) su sistema: į asmens siunčiamus duomenis (užklausas) gaunamas sistemos atsakymas, taip sistema atlieka jai priskirtą funkciją. Todėl tai, kas iš „virtualios realybės“ pozicijų būtų laikoma tik „durų rankenų klebenimu“, *išorinės perspektyvos* atveju yra vertinama kaip prieiga prie IS. Todėl, kaip teisingai pastebėjo O. S. Kerr ir J. Clough, tokio pobūdžio veiksmus fizinės erdvės kontekste vis dėlto tiksliau laikyti ne prieiga prie kompiuterio, o tiesiog naudojimąsi juo[278].

Analizuojant šiuos prieigos prie IS interpretavimo būdus gali kilti klausimas, kokios įtakos nusikalstamos veikos kvalifikavimui turės pasirinktas kažkuris vienas iš siūlomų variantų, t. y. prieigą tapatinant su „virtualiu įėjimu“ arba ją laikant bet kokia interakcija su IS. Kadangi šios *vidinė* ir *išorinė perspektyvos* atspindi siauresnį ir priešingai platesnį požiūrį į prieigos prie IS gavimą, tai pasirinktas jos interpretavimo būdas, kaip galima buvo pastebėti: 1) skirtingai nustato šios nusikalstamos veikos pradžios ir pabaigos momentą; 2) skirtingai apibrėžia nusikalstamos veikos ribas, atitinkamai ir jos inkriminavimo galimybes[279].

Ieškant minėtų perspektyvų ištakų matyti, kad joms susiformuoti sąlygas sudarė gana įvairus užsienio valstybių požiūris į šią IS konfidencialumą pažeidžiančią nusikalstamą veiką. Priklausomai nuo jo, baudžiamuosiuose įstatymuose (statutuose) pasirinkti skirtingi šios veikos aprašymo būdai ir prieigos aiškinimo variantai. Dažnai prieigos plačias interpretavimo (atitinkamai jos vertinimui iš *išorinės perspektyvos*) galimybes lemia pateikiamas oficialus vartojamų sąvokų išaiškinimas arba pačios neteisėtos prieigos sudėtyje numatyti jos požymiai. Pastarojo atvejo pavyzdžiu gali būti Jungtinės Karalystės 1990 m. Netinkamo naudojimosi kompiuteriais akto 1 straipsnyje esanti neteisėtos prieigos prie kompiuterinių

[277] Wong, M. W. S., *supra* note 252, p. 123.

[278] Kerr, O. S., *supra* note 222, p. 60.

[279] Kaip vienas iš mokslinėje literatūroje minimų tokios problemos pavyzdžių yra elektroninių laiškų siuntimo atvejis (Kerr, O. S., *op. cit.*, p. 1621). Į elektroninių laiškų siuntimo vertinimo problemą atkreiptas dėmesys ir Konvencijos dėl elektroninių nusikaltimų aiškinamojoje ataskaitoje (46 punktas). Joje, prieigą apibrėžus, kaip įėjimą į visą arba dalį kompiuterinės sistemos, išaiškinta, kad ji vis dėlto neapima paprasčiausio elektroninių laiškų ar rinkmenų siuntimo sistemai. Tačiau klausimas, kaip turėtų būti vertinami atvejai, kai elektroniniais laiškais yra siunčiama kenkėjiška programinė įranga, kuri vėliau, patekusi į sistemą, atlieka nepageidaujamas funkcijas, iš tiesų BK 198[1] straipsnio prasme yra diskutuotinas.

duomenų sudėtis. Baudžiamoji atsakomybė pagal šį straipsnį kyla, jeigu, be kitų požymių, yra nustatyta, kad kaltininkas privertė kompiuterį atlikti bet kokią funkciją ketindamas užtikrinti prieigą prie programos ar duomenų, laikomų kompiuteryje, arba sudarydamas sąlygas, kad tokia prieiga būtų užtikrinta[280]. Kadangi šios nusikalstamos veikos sudėtyje įtvirtintas platus ir aiškių apribojimų nenumatantis prieigos apibūdinimas, tai mokslinėje literatūroje pateikiami paprasčiausio kompiuterio įjungimo, kenkėjiškos programinės įrangos siuntimo ir kiti pavyzdžiai, kurie šiuo atveju galėtų prilygti tokiam veiksmui[281].

Tačiau išvada, kokia perspektyva vadovaujamasi užsienio valstybėse aiškinant neteisėtą prieigą prie IS, turėtų priklausyti ne tik nuo to, kaip yra aprašyti tokios nusikalstamos veikos požymiai, bet ir nuo to, kokia teismų praktika formuojama šios kategorijos bylose. Praktinis teisės aktų taikymo lygmuo aktualus tiek tais atvejais, kai prieigos išaiškinimas aktuose nėra pateikiamas (pavyzdžiui, Vokietijoje, Prancūzijoje, Estijoje, Lietuvoje ir kt.), tiek ir tada, kai teisės aktuose prieigos sąvoka atskleista (pavyzdžiui, įvairių Jungtinių Amerikos Valstijų statutai). Pavyzdžiui, O. S. Kerr ir J. Clough[282], analizuodami įvairiose Jungtinėse Amerikos Valstijose priimtus teismų sprendimus, pastebėjo, kad vienais atvejais teismai bando susiaurinti pakankamai plačius prieigos apibrėžimus, vadovaudamiesi *vidinės perspektyvos* kriterijais, 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)*[283].

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[284] esančią jos sąvoką. Toks sprendimas buvo pagrįstas ankstesniais precedentais, kuriuose preziumuota, jog Statute vartojamiems žodžiams yra suteikta įprastinė jų reikšmė, tai 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"

[280] Computer Misuse Act. [interaktyvus], [žiūrėta 2013-06-01]. <http://www.legislation.gov.uk/ukpga/1990/18/contents>.

[281] Clough, J., *supra* note 110, p. 63.

[282] Kerr, O. S., *supra* note 222, p. 1625; Clough, J., *supra* note 210, p. 155.

[283] *State of Kansas v. Anthony A. Allen*, no. 74,639, Soupreme Court of Kansas, 1996. [Interaktyvus], [žiūrėta 2013-06-02]. <http://files.grimmelmann.net/cases/Allen.pdf>.

[284] Kanzaso valstijos statute prieiga yra apibūdinta kaip „nurodymų davimas, komunikavimas, duomenų laikymas, duomenų sugrąžinimas ar kitoks pasinaudojimas kompiuterio, kompiuterinės sistemos, kompiuterio tinklo ištekliais". The Statutes of Kanzas. [Interaktyvus], [žiūrėta 2012-11-16]. <http://kansasstatutes.lesterama.org/Chapter_21/Article_37/21-3755.html>.

kompiuteriais ar iš to ką nors gauti. Byloje prieita prie išvados, kad kaltininkas nebuvo gavęs prieigos prie šios bendrovės kompiuterinės sistemos.

Taigi, taikant *vidinės* ar *išorinės perspektyvos* vertinimo kriterijus, prieiga prie IS gali būti suprantama siaurąja arba plačiąja prasme. Pakankamai platų požiūrį atspindi fizinės realybės pozicija, reiškianti, kad ja gali būtų pripažįstama bet kokia sąveika su IS. Tuo tarpu žvelgiant iš virtualios realybės pusės prieiga yra aiškinama siauriau – kaip „virtualus įėjimas" į sistemą. Šios perspektyvos aktualios aiškinantis ir kaip plačiai Lietuvos BK 198[1] straipsnyje kriminalizuotas neteisėtas prisijungimas prie IS. Būtent apie siauresnį pavojingos veikos variantą Lietuvos atveju leidžia kalbėti prieigai įvardyti pasirinktas prisijungimo terminas ir kiti sudėties požymiai, pavyzdžiui, šios nusikalstamos veikos padarymo būdas, reikalaujantis nustatyti apsaugos priemonių pažeidimo prisijungiant prie IS faktą.

Pagal įprastinę reikšmę prisijungimo veiksmas apibrėžiamas kaip „komanda, kuria prisijungiama prie tinklo arba sistemos ir pradedamas darbo seansas su ja"[285]. Pagal tokį aiškinimą prisijungimo momentą galima laikyti darbo seanso su sistema pradžia, nepriklausomai nuo priėjimo prie IS būdo (tiesiogiai arba naudojant elektroninių ryšių tinklus). Tačiau tai nėra vienintelis šios pavojingos veikos interpretavimo variantas – aiškinant prisijungimą gali būti pasitelkiamas ir galimybės prieiti prie sistemos išteklių (programinės, techninės įrangos, duomenų) kriterijus. Nors BK 198[1] straipsnio dispozicijoje jis nėra minimas, tačiau apie tokį *naudos kriterijų* tarsi leistų kalbėti pati prisijungimo prie IS sąvoka. Sėkmingas prisijungimas dažniausiai sudaro galimybes sistemoje padaryti vienokio ar kitokio pobūdžio veiksmus (pavyzdžiui, elektroninės bankininkystės sistemoje atlikti finansines operacijas[286], pakeisti tinklalapio turinį[287], socialinio tinklalapio lankytojams priskirtus autentifikavimo duomenis[288] ar kitokius elektroninius duomenis[289] ir pan.). Toks požiūris matyti ir BK 198[1] straipsnį komentavusių autorių pateiktame prisijungimo apibrėžime. Pagal juos, prisijungimas „tai informacinės sistemos vartotojo ar abonemento veiksmai, kuriais jis gali prieiti prie atitinkamos svetimos informacinės sistemos resursų (kompiuterio techninės įrangos, periferinių įrenginių, saugomos ar perduodamos kompiuterinės informacijos ir pan.)"[290]. Todėl prisijungimo baigtumo momentas siejamas su kaltininko realia galimybe „pamatyti informacinės sistemos laikomas duomenų bylas, susipažinti su duomenų turiniu, atlikti kitus veiksmus (juos keisti, trinti, kopijuoti ir t. t.)"[291]. Šis *naudos kriterijus* rodo daug prisijungimo ir iš *vidinės perspektyvos* pozicijų suvokiamos prieigos panašumų. Jau minėta, kad pagal įprastinį prieigos aiškinimą įvairiose jos apibrėžimuose šalia įėjimo į sistemą taip pat nurodoma ir galimybė naudotis ja[292], galimybė pri-

[285] Dagienė, V., *et al*., *supra* note 251, p. 375.

[286] Vilniaus miesto 1 apylinkės teismo 2009 m. rugsėjo 14 d. teismo baudžiamasis įsakymas baudžiamojoje byloje (bylos Nr. N1-1470-88/2009); Kupiškio rajono apylinkės teismo 2009 m. rugsėjo 2 d. nuosprendis baudžiamojoje byloje (bylos Nr. 1-53-100/2009) ir kt.

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

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

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

[290] Abramavičius, A., *et al*., *supra* note 160, p. 436.

[291] *Ibid*., p. 436–437.

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

eiti prie sistemos išteklių[293] ar įėjimo prie duomenų ar IS gavimas[294]. Būtent toks siauresnis prieigos kaip „įėjimo į visą arba dalį sistemos“ aiškinimas matyti ir Konvencijos dėl elektroninių nusikaltimų aiškinamojoje ataskaitoje (46 punktas). Taigi nepriklausomai nuo to, ar prisijungimas būtų laikomas komanda, kuria pradedamas darbo seanso su sistema, ar jam apibūdinti pasitelkiamas *naudos kriterijus*, abiem atvejais jis metaforiškai gali būti prilyginamas „virtualiam įėjimui“ į IS. Be to, išvadą, kad šiai nusikalstamai veikai konstatuoti nepakanka tik sąveikos su sistema, leidžia padaryti ir reikalavimas nustatyti jos apsaugos priemonių pažeidimą. Paprasčiausios sąveikos ir prisijungimo atskyrimas taip pat gali būti matomas analizuojant kokybinius „naudojimosi“ kompiuteriu skirtumus, t. y. kokiu mastu kaltininkas gali naudoti kompiuterį[295]. Todėl veiksmai, kuriais nepavyko prisijungti prie IS, galėtų būti vertinami tik kaip parengtinė nusikalstama veika, nes jais nėra pasiekiamas toks naudojimosi kompiuteriu lygis, kurį gauna asmuo, sėkmingai prisijungęs prie IS.

Tačiau toks prisijungimo prie IS aiškinimas reikalauja ir tam tikro patikslinimo. *Naudos kriterijus* iš tiesų padeda geriau suvokti prisijungimo prie IS esmę, tačiau šią veiką kriminalizavus *per se*, jos inkriminavimo neturėtų riboti tai, ar kaltininkas turėjo realią galimybę atlikti tolesnius veiksmus sistemoje[296], ar jis tokia galimybe pasinaudojo, taip pat ar prieš pažeisdamas IS konfidencialumą jis turėjo tyčią jau pačioje sistemoje atlikti kitas nusikalstamas veikas. Kadangi neteisėto prisijungimo prie IS nusikalstamos veikos sudėtis yra formali, tai jos baigtumo momentas turėtų būti siejamas su sėkmingo prisijungimo prie IS veiksmu, kuriam įtakos kaltininko galimybės atlikti tolesnius veiksmus sistemoje neturėtų turėti.

Analizuojant teismų praktiką, inkriminuojant BK 198[1] straipsnyje numatytą nusikalstamą veiką, matyti, kad joje dažniausiai prisijungimo sąvoka nėra aiškinama, taip pat nebuvo kilę problemų sprendžiant dėl šios veikos baigtumo momento, t. y. kada prisijungimas gali būti laikomas sėkmingu, o kada nepavykusiu. Tokia situacija susiklosčiusi dėl to, kad kaltininkas be IS konfidencialumo pažeidimo, būna padaręs ir kitas nusikalstamas veikas pačioje sistemoje, todėl neteisėto prisijungimo prie IS veika paprastai būna baigta. Todėl konstatuojant neteisėto prisijungimo faktą dažniausiai nurodomas konkretus būdas, kuriuo šie neteisėti veiksmai padaryti. Pavyzdžiui, tais atvejais, kai yra pažeidžiami autentifikavimo procedūros nustatyti reikalavimai, teismų sprendimuose konstatuojama, kad prisijungiant prie internetinės prekybos ir aukcionų sistemos panaudoti neteisėtai įgyti šios sistemos vartotojo autentifikavimo kodai ir slaptažodžiai[297] arba prisijungiant prie elektroninės bankininkystės sistemos neteisėtai panaudoti jos vartotojo tapatybės patvirtinimo priemonių duomenys[298] ir pan.

Taigi teigtina, kad prisijungimo veikos aiškinimui artimesnė *vidinės perspektyvos pozicija*, todėl šį veiksmą galima metaforiškai lyginti su „virtualiu įėjimu“ į IS. Patekimas vidun sudaro galimybes prieiti prie sistemos išteklių – techninės, programinės įrangos,

---

[293] Dagienė, V., *et al*., *supra* note 251, p. 369.

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

[295] Clough, J., *supra* note 110, p. 68.

[296] Pavyzdžiui, sistemoje nerandami norėti peržiūrėti duomenys ar jie apsaugoti slaptažodžiu, sistema veikia testuojamoje aplinkoje, kaltininkas prisijungia prie stebimos IS (angl. *honeypot*) ir kt.

[297] Klaipėdos miesto 2009 m. birželio 29 d. teismo baudžiamasis įsakymas baudžiamojoje byloje (bylos Nr. 1-740-93/2009).

[298] Vilniaus miesto 1 apylinkės teismo 2009 m. rugsėjo 14 d. teismo baudžiamasis įsakymas baudžiamojoje byloje (bylos Nr. N1-1470-88/2009).

duomenų ir pan. Tačiau toks *naudos kriterijus*, nors ir leidžia aiškiau suvokti prisijungimą, neturėtų turėti įtakos sprendžiant dėl šios nusikalstamos veikos baigtumo momento. Tai yra prisijungimo veiksmo vertinimui neturi būti svarbi kaltininko galimybė atlikti tolesnius veiksmus IS – šios galimybės turėtų atsispindėti kvalifikuojant jo padarytas kitas veikas jau pačioje sistemoje.

2.2.2. Prisijungimo neteisėtumo vertinimas

Pagrindinė teisėto ir neteisėto prisijungimo prie IS atribojimo problema labiausiai susijusi su privačių ir viešų erdvių, sukurtų elektroninėje erdvėje, atskyrimu ir jų ribų nustatymo galimybėmis. Akivaizdu, kad šiuo atveju privačios ir viešos sferos koncepcijų, kurios suformuluotos veiksmams fizinėje erdvėje vertinti, taikymas dėl unikalių elektroninės erdvės savybių susiduria su tam tikrais sunkumais. Anot I. Walden, itin paplitusi Interneto koncepcija, kad tai „tam tikras servisas, prieinamas per „tinklų tinklą", dažniausiai funkcionuojančiu kaip vieša vieta, reguliuojama numanomais leidimais, kuriais remiantis yra keičiamasi informacija"[299]. Tokia išvada pagrįsta pamatine komunikavimo elektroninėje erdvėje filosofijos, kad „ištekliai, kurių URL[300] yra žinomas, turėtų būti prieinami iš bet kurio sujungto kompiuterio, nebent buvo imtasi techninių žingsnių padaryti juos neprieinamais"[301]. Toks požiūris į viešų ir privačių erdvių atskyrimą rodo ne tik teisinius, bet ir tam tikrus techninius barjerus, iš dalies apibrėžiančius privačios elektroninės erdvės ribas. Šių ribų nustatymo būdas skiriasi nuo to, kurio imamasi fizinėje erdvėje: pagal L. Lessig, elektroninėje erdvėje galimų veiksmų apribojimus nustato šios erdvės architektūra, pagrįsta kompiuterio kodu. Autorius pastebi, kad „programinė ir techninė įranga, kuri sukuria elektroninę erdvę, nustato suvaržymų, kaip galima elgtis, rinkinį"[302]. Panašias technologijas, į kurias sąmoningai įmontuotas mechanizmas, galintis daryti įtakos asmens elgesiui, B.–J. Koops įvardijo „norminių technologijų"[303] terminu. Tokių technologijomis nustatytų suvaržymų turinys gali kaskart skirtis, bet būtent jie nustato prieigos prie elektroninės erdvės sąlygas. Pavyzdžiui, vienais atvejais IS konfidencialumas gali būti užtikrintas įdiegus prieigos kontrolės programinę įrangą, kitais atvejais prieigai prie IS nebus nustatyti apskritai jokie apribojimai.

Šis aspektas svarbus analizuojant vertybių (ne išimtis IS konfidencialumas), apsaugos galimybes elektroninėje erdvėje. Priklausomai nuo sukurto kodo, vertybėms gali būti nustatoma didesnė arba priešingai – mažesnė apsauga. Būtent tai leido L. Lessig kelti klausimą, kokios vertybės turėtų būti „įmontuotos į erdvę"[304], kad paskatintų įvairias gyvenimo formas joje? Kalbėdamas apie elgesio suvaržymus elektroninėje erdvėje, autorius atkreipė dėmesį į tai, kad „nėra pasirinkimo, kuris nebūtų susijęs su tam tikra *statyba*. Kodas nie-

[299] Walden, I., *supra* note 70, p. 163.

[300] 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., *supra* note 271, p. 301).

[301] Reed, C. *Internet: law text and materials*. Cambridge: Cambridge University Press, 2004, p. 66.

[302] Lessig, L., *supra* note 261, p. 89.

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

[304] Lessig, L., *op. cit*., p. 6.

kada nėra randamas; jis yra visuomet sukuriamas <...>“[305]. Tokie autoriaus pastebėjimai leidžia daryti išvadą, kad prieigai prie IS nustatyti įvairūs apribojimai rodo priemones, kurių buvo imtasi šios sistemos konfidencialumui užtikrinti, ir išreiškia jos savininko ar teisėto valdytojo požiūrį į prieigos prie sistemos galimybes ir sąlygas. Reikėtų paminėti, kad įvairių prieigos prie IS apribojimų taikymas dažniausiai yra nulemtas saugumo politikos apibrėžtų sistemos saugos reikalavimų (pavyzdžiui, kam ir kokiomis sąlygomis suteikta prisijungimo teisė prie IS). Atitinkamai tokių apribojimų nepaisymas liudija prieigos prie IS neteisėtumą, taigi ir šios sistemos konfidencialumo pažeidimus.

BK 198[1] straipsnyje numatytas prisijungimo neteisėtumo nustatymo reikalavimas siejamas su Konvencijos dėl elektroninių nusikaltimų ir Pamatinio sprendimo 2005/222/TVR nuostatomis, kuriose numatyta pareiga kriminalizuoti ne bet kokią, o neteisėtą prieigą prie IS. Būtent prieigos neteisėtumas parodo įvairius IS konfidencialumo pažeidimus. Tiek Konvencijos dėl elektroninių nusikaltimų 2 straipsnyje, tiek ir Pamatinio sprendimo 2005/222/TVR 2 straipsnyje minima „neteisėta prieiga“ arba kitaip „prieiga neturint tam teisės“ prie visos IS arba jos dalies. Todėl akivaizdu, kad šie teisės aktai nereikalauja kriminalizuoti tokių veikų, kai prieiga prie IS arba jos dalies gauta turint sistemos (arba jos dalies) savininko ar teisėto valdytojo leidimą[306]. Į tokio leidimo būvimą, sprendžiant prieigos prie IS teisėtumo klausimą, atkreiptas dėmesys ir Konvencijos dėl elektroninių nusikaltimų aiškinamosios ataskaitos 47 punkte. Todėl kaip neteisėta prieiga prie IS nevertintini jungimosi veiksmai prie atvirų ir viešai prieinamų sistemų (ar jų dalių).

Analizuojant teismų praktiką matyti, kad teismų sprendimuose pats prieigos neteisėtumo turinys atskleidžiamas retai. Šią tendenciją iš esmės lemia anksčiau minėta glaudi prisijungimo, jo neteisėtumo ir saugumo priemonių pažeidimų sąsaja, todėl neteisėtumas paprastai konstatuojamas nurodžius konkrečius IS saugumo priemonių pažeidimo veiksmus. Kaip pavyzdžius galima paminėti Kupiškio rajono apylinkės teismo 2009 m. rugsėjo 2 d. nuosprendį baudžiamojoje byloje (bylos Nr. 1-53-100/2009) ir Radviliškio rajono apylinkės teismo 2010 m. kovo 22 d. teismo baudžiamąjį įsakymą baudžiamojoje byloje (bylos Nr. 1-116-632/2010).

Kupiškio rajono apylinkės teismo nuosprendžiu J. V. nuteistas pagal BK 198[1] straipsnio 1 dalį, 214 straipsnio 1 dalį, 215 straipsnio 1 dalį ir 182 straipsnio 1 dalį. Teismas nustatė, kad *J. V. jo gyvenamojoje vietoje, <...> per šiam namui <...> suteiktą interneto <...> prieigą <...>, naudodamas iš internetinio tinklapio atsisiustą kompiuterinę programą „Fire Fox + Tamper data“, skirtą kompiuterinio tinklo stebėsenai atlikti, prisijungė prie AB (duomenys neskelbtini) banko internetinio tinklapio (duomenys neskelbtini) jam, kaip banko klientui, suteiktais internetinės bankininkystės rekvizitais, apėjo AB (duomenys neskelbtini) banko internetiniame tinklapyje įdiegtas apsaugos priemones, neteisėtai prisijungė prie banko informacinės sistemos, kaip asmuo, įgalintas ją administruoti, atsitiktinio parinkimo būdu nustatė 29 banko klientams: (duomenys neskelbtini) suteiktus internetinės bankininkystės neviešus naudotojo tapatybės patvirtinimo elektroninius duomenis ID (autentifikavimo ko-*

[305] Lessig, L., *supra* note 261, p. 6.

[306] Šis aspektas aktualus kalbant apie saugumo patikras bei etiško įsibrovimo technologijas. Jos dažnai tapatinamos su įsiskverbimo testavimu, kuris, jei laikomasi visų tokiems testavimams keliamų reikalavimų, neturėtų būti vertinamas kaip nusikalstama veika, numatyta BK 198[1] straipsnyje. Būtent neteisėto prisijungimo prie IS sudėtyje numatytas neteisėtumo bei tyčios požymiai susiaurina šios veikos taikymo galimybes ir leidžia minėtų etiškų įsibrovimo veiksmų nelaikyti nusikalstamais.

dus), t. y. neteisėtai juos įgijo ir laikė iki tol, kol neteisėtai jais pasinaudojęs inicijavo ir atliko 31 finansinę operaciją <...>. Šiuo atveju prisijungimo neteisėtumą leido nustatyti kaltininko veiksmai, kuriais buvo pasinaudota banko programoje buvusia spraga, sudariusia galimybes įeiti į kitų asmenų sąskaitas.

Tuo tarpu Radviliškio rajono apylinkės teismo baudžiamajame įsakyme prisijungimo neteisėtumas įžvelgtas dėl autentifikavimo procedūros pažeidimų, kai prieiga prie IS buvo gauta panaudojant iš anksto žinomus tinklalapio turinio valdymo sistemos prisijungimo duomenis. Šiuo baudžiamuoju įsakymu G. T. nuteistas pagal BK 198[1] straipsnio 1 dalį už tai, kad *jis panaudodamas prisijungimo duomenis, t. y. vardą (duomenys neskelbtini) ir slaptažodį (duomenys neskelbtini), neteisėtai prisijungė prie informacinės sistemos – VšĮ (duomenys neskelbtini) tinklalapio (duomenys neskelbtini) turinio valdymo sistemos ir šiame tinklalapyje, adresu (duomenys neskelbtini) sukūrė bylas „indexl.php“, „index.php“, taip savo veiksmais sukurdamas galimybę pakeisti tinklalapio (duomenys neskelbtini) turinį, tuo pasinaudodamas jis <...> iš internetinės prieigos, esančios adresu (duomenys neskelbtini), neteisėtai prisijungė prie tinklalapio (duomenys neskelbtini) ir jame patalpino tokio turinio pranešimą: „Nuo kada suprasit, kad negalima lamas samdyti prižiūrėti tokį didelį portalą. P. S.: Krizė dar nesibaigė, būkit ramūs.*

Tačiau, kai teismų sprendimuose detalizuotas neteisėtumo turinys, matyti, kad jo suvokimas yra analogiškas minėtuose tarptautiniuose bei Europos Sąjungos teisės pateiktam prisijungimo neteisėtumo išaiškinimui. Pavyzdžiui, Vilniaus miesto 1 apylinkės teismo 2011 m. gruodžio 6 d. nuosprendyje baudžiamojoje byloje (bylos Nr. 1-1430-276/2011) konstatuota, kad T. Č. padarė BK 198 straipsnio 1 dalyje, 198[1] straipsnio 1 dalyje ir 210 straipsnyje numatytas nusikalstamas veikas. Nuosprendyje nurodoma, kad jis neteisėtai, t. y. *neturėdamas šios informacinės sistemos savininko ar teisėto valdytojo leidimo jungtis prie šios informacinės sistemos [banko tarnybinėse stotyse administruojamos neviešos IS – aut. pastaba], tyčia, pažeisdamas šios sistemos apsaugos priemones, prisijungė prie šios banko informacinės sistemos kaip neribotą prieigos teisę turintis vartotojas.*

Analizuojant neteisėtumo požymį matyti, kad Konvencijos dėl elektroninių nusikaltimų ir Pamatinio sprendimo 2005/222/TVR nuostatos leidžia pastebėti tik vieną iš prieigos neteisėtumo interpretavimo variantų. Kiek plačiau į šią problemą pažvelgti sudaro sąlygas skirtinga užsienio valstybių praktika aprašant neteisėtos prieigos prie IS veiką. Taigi, apibendrinus įvairius požiūrius į IS konfidencialumo pažeidimus, išskirtinos šios problemos: 1) neteisėtumo turinio ir jo ribų nustatymo problemos; 2) prieigos prie IS neteisėtumo konstatavimo pagal prieigos apribojimų nustatymo ir jų pažeidimo būdus problemos.

Pirmasis klausimas atspindi vieną iš mokslinėje literatūroje kylančių diskusijų, susijusių su dviem prieigos teisėtumo pažeidimo aspektais, – neteisėta prieiga (angl. *unauthorized access*) ir teisėtumo ribas peržengiančia prieiga (angl. *exceeding authorized access*) bei jų tarpusavio santykiu. Nagrinėjant šiuos prieigos prie IS variantus, daugumos mokslininkų (D. Bainbridge, B. A. Howell, I. Walden, O. S. Kerr, C. Reed, J. Angel ir kt.)[307] darbuose

[307] *Computer and Information security handbook*. Vacca J. R. (red). 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*. (edit.). New York (N.Y.): New York University Press, 2007, p. 90–93; Walden, I., *supra* note 70, p. 164; Kerr, O. S., *supra* note 222, p. 1630. *Computer Law: The Law and Regulation of Information Technology*. 6-asis leidimas. Reed, C.; Angel, J. (eds.). Oxford: Oxford University Press, 2007.

keliamas klausimas, ar gali būti nustatyti nusikalstamos veikos požymiai, jei teisėta prieiga prie IS buvo panaudota neteisėtiems tikslams. Ši situacija, anot D. Bainbridge ir kitų autorių[308], susiklosto tada, kai vartotojas, turintis teisę prieiti prie IS ir jos išteklių, viršija vidaus arba kitais teisės aktais nustatytas tokio leidimo ribas. Todėl pagrindinė spręstina problema yra ta, ar „teisėta prieiga, panaudota neteisėtiems tikslams, išlieka teisėta prieiga?“[309] Atsakymo į šį klausimą paieškas komplikuoja įvairios neteisėtumo, prisijungiant prie IS, interpretavimo galimybės – nuo pakankamai plataus požiūrio į šį požymį, iki ganėtinai siauro. Aiškinimo įvairovę lemia ir minėti šios nusikalstamos veikos aprašymo skirtumai užsienio valstybių baudžiamuosiuose įstatymuose. Priklausomai nuo pasirinktos tokios nusikalstamos veikos konstrukcijos vienose valstybėse yra tiesiogiai kriminalizuota neteisėta ir teisėtumo ribas peržengianti prieiga prie IS[310], kitose – numačius tik neteisėtos prieigos požymį, paliekamas atviras klausimas dėl jo turinio[311].

Bandant aiškiau suvokti neteisėtos ir teisėtumo ribas peržengiančios prieigos santykį, galima būtų pasitelkti pašalinio asmens (angl. *outsider*) ir IS teisėto vartotojo (angl. *insider*) kriterijus ir atitinkamai kalbėti apie išorinius ir vidinius prisijungimus prie IS. Būtent pašalinio asmens (kartais įvardijamo „svetimšalio“ terminu)[312] ir teisėto vartotojo skirtumais yra pagrįstas neteisėtos ir teisėtumo ribas peržengiančios prieigos atskyrimas. Mokslinėje literatūroje (Ch. Day, G. Thornton, O. S. Kerr, B. A. Howell ir kt.)[313] pagrindinė aplinkybė, leidžianti nustatyti pašalinį asmenį, yra jo prieigos teisių prie IS nebūvimas, o tai rodo neteisėtą prisijungimą prie IS „iš išorės“. Apibūdindamas įsibrovimą iš išorės, G. Thornton teigė, kad tokio pobūdžio veiksmai atliekami asmens, kuris neturi prieigos teisės prie IS, tačiau neteisėtai (pavyzdžiui, pažeidžiant sistemos saugumo priemones) siekia tam tikro lygio prieigą prie jos gauti[314]. Todėl tokiai prieigai apibūdinti dažnai naudojama „įsilaužimo ir įėjimo“[315] analogija. Kiek kitaip prieigos prie IS situacija atrodo, kai vertinami vartotojo, nustatytomis sąlygomis turinčio teisėtą prieigą prie IS, veiksmai. Kaip pastebi Ch. Day, tai asmenys, „kurie priklausomai nuo jų vaidmens organizacijoje turi tam tikro lygio autorizuotą prieigą prie IS terpės ir sistemos. Prieigos lygis gali kisti nuo paprasto vartotojo iki sistemos administratoriaus su beveik neribotomis teisėmis“[316]. Šio asmens atsakomybės klausimas kyla tada, kai jis prisijungia prie IS turėdamas tikslą, kuriam įgyvendinti prieigos teisė nebuvo suteikta. Kadangi tai skirtingi nei įsibrovimo „iš išorės“ atvejai, tai jiems apibūdinti dažnai pasitelkiamas kitas – teisėtumo ribas peržengiančios

---

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

[309] Bainbridge, D., *supra* note 307, p. 385.

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

[311] Pavyzdžiui, Jungtinėje Karalystėje prieigos neteisėtumo požymio aiškinimas praplėstas teismų praktikoje.

[312] Štitilis, D., *supra* note 12, p. 21.

[313] Thornton, G. Unauthorised Access (hacking). [interaktyvus], [žiūrėta 2012-11-26]. < http://ebookbrowse.com/grant-thornton-unauthorised-access-pdf-d18884414>; Kerr, O. S., *supra* note 222, p. 1630; *Cybercrime: Digital Cops in a Networked Environment.* Balkin, J., *et al*. (ed.). New York (N.Y.): New York University Press, 2007, p. 90.

[314] Thornton, G., *op. cit*., p. 1.

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

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

prieigos – požymis. Jis leidžia pamatyti ir tokios veikos aiškinimų bei *ultra vires* doktrinos panašumų.

Taigi neteisėtos ir teisėtumo ribas peržengiančios prieigos požymiai atskleidžia dvi skirtingas prieigos prie IS puses. Juos abu numačius nusikalstamos veikos sudėtyje, veikos apibrėžtis neišvengiamai būtų išplėsta – baudžiamoji atsakomybė tuomet kiltų ne tik už prieigą prie IS neturint tam teisės, bet taip pat už leistinos prieigos apimčių viršijimą. Kaip pavyzdį galima paminėti Jungtinių Amerikos Valstijų įstatymų sąvado 18 U.S.C. § 1030 (a) (1)–(5) punktus[317], kuriuose *expressis verbis* numatyti neteisėtos ir teisėtumo ribas peržengiančios prieigos požymiai. Taip pat galimi atvejai, kai sudėtyje nurodomas tik vienas – neteisėtos prieigos požymis, tačiau jo turinys praplečiamas teismų praktikoje. Kaip teigia W. S. Wong, Jungtinėje Karalystėje neteisėtos prieigos požymis apima abu variantus, todėl tai, „kurį aspektą konkreti byla iškelia, yra fakto klausimas ir priklauso nuo kiekvienos bylos aplinkybių“[318]. Tačiau pažymėtina, 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 *perkriminalizavimo* pavojaus, yra šio patekimo į IS etapo susiejimas su tolesniais jau sistemoje atliekamais kaltininko veiksmais. Pasirinkus tokį veikos kriminalizavimo variantą, pats neteisėtumo požymis pasiduoda platesniam aiškinimui ir atitinkamai leidžia formuotis lankstesniam požiūriui į jį.

Kiek kitoks neteisėtumo aiškinimas, manytina, yra tais atvejais, kai neteisėta prieiga prie IS kriminalizuota *per se,* t. y. be sąsajos su tolesniais kaltininko veiksmais sistemoje ar jo nusikalstamais ketinimais. Tokia situacija sudaro ribotas galimybes kalbėti apie teisėtumo ribas peržengiančią prieigą – siekiant išvengti baudžiamajai atsakomybei kilti būtino pavojingumo lygio nesiekiančių veiksmų kriminalizavimo, turėtų būti pasitelkiamas daug siauresnis neteisėtos prieigos aiškinimo būdas. Priešingu atveju į baudžiamosios teisės reguliavimo sritį patektų įvairūs civiliniai ar drausminiai teisiniai santykiai[319]. 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 pažymima, kad palankesnes sąlygas nusikalstamoms veikoms elektroninėje erdvėje padaryti gali sudaryti tai, kad kaltininkas dėl einamų pareigų turi prieigą prie IS, kuriai gali kilti grėsmė, todėl nacionalinėje teisėje turėtų būti atsižvelgta į tokias aplinkybes (18 punktas). Svarstytina, ar į šią aplinkybę negalėtų būti atsižvelgiama kaltininkui individualizuojant bausmę už IS padarytas kitas nusikalstamas veikas (jų didesnį pavojingumą rodytų tai, kad kaltininkas turėjo teisėtą prieigą prie IS ir ja piktnaudžiavo), taip pat neatmestina galimybė padarytų veikų kvalifikavimui taikyti BK 228 straipsnį, jei nustatyti specialaus subjekto, didelės žalos ir kiti piktnaudžiavimo veikos inkriminavimui reikšmingi požymiai.

Kaip pavyzdys, kai buvo bandytos nustatyti neteisėtos prieigos turinio ribos ir pateiktas pakankamai siauras šio požymio aiškinimas, paminėtinas Merilendo apeliacinio teis-

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

[318] Wong, M. W. S., *supra* note 252, p. 126.

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

mo 1998 m. sprendimas baudžiamojoje byloje *Briggs prieš Merilendo valstiją* (*Briggs v. State of Maryland*)[320].

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 Merilendo kodekso §146 (c) (2) (i) 27 straipsnyje[321]. 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 minėtame straipsnyje, yra susijusi tik su veiksmais, kurie atliekami neturint prieigos teisės prie sistemos (pavyzdžiui, kalbant apie programišių (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 minėta norma siekta kriminalizuoti tik tuos netinkamo naudojimo kompiuteriu ar kompiuteriniais tinklais atvejus, kai pati prieiga yra neteisėta.

Prieigos neteisėtumo požymis taip pat numatytas Lietuvos BK 198[1] straipsnyje. Sprendžiant apie jo turinio ribas, turėtų būti atsižvelgiama ne tik į tai, kad ši nusikalstama veika, kaip jau minėta, kriminalizuota *per se*, bet taip pat į kitus neteisėtumą padedančius suvokti sudėties požymius. Pavyzdžiui, šios veikos padarymo būdas, kuris įtvirtintas BK 198[1] straipsnyje atsižvelgiant į Konvencijos dėl elektroninių nusikaltimų ir Pamatinio sprendimo 2005/222/TVR nuostatas, apibūdintas kaip IS apsaugos priemonių pažeidimas. Kadangi apsaugos priemonių tikslas yra užtikrinti, kad prie IS galėtų prisijungti tik prieigos teisę prie jos turintys vartotojai, tai manytina, kad šis požymis sudaro galimybę kalbėti apie siauresnį neteisėtos prieigos turinį į šią veiką neįtraukti teisėtumo ribas peržengiančios prieigos. Ši išvada neužkerta kelio kaltininkui inkriminuoti kitas jo padarytas nusikalstamas veikas, nes prisijungimas prie IS turint tam teisę savaime nedaro teisėtų kitų kaltininko veikų IS. Kadangi atskirai yra vertinami IS konfidencialumo pažeidimai, tai savarankiškai vertintini ir kiti, pavyzdžiui, elektroninių duomenų konfidencialumo, integralumo, prieinamumo ar kitų vertybių pažeidimai.

Tokį požiūrį galima pastebėti analizuojant nors ir negausią teismų praktiką. Pavyzdžiui, Vilniaus miesto 1 apylinkės teismo 2011 m. gruodžio 6 d. nuosprendžiu baudžiamojoje byloje (bylos Nr. 1-1430-276/2011) T. Č. 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. Šioje byloje teismas nustatė, kad T. Č. *laikotarpiu*

[320] *Briggs v. State of Maryland*, no. 24, Court of Appeals of Maryland, 1997. [interaktyvus], [žiūrėta 2013-06-02]. <http://law.justia.com/cases/maryland/court-of-appeals/1998/24a97-2.html>.

[321] Vėlesniais pakeitimais Merilendo kodekso 7-302 paragrafe numatyta ne tik neteisėta, bet ir teisėtumo ribas peržengianti prieiga prie kompiuterio ar duomenų (The Code of Maryland. [interaktyvus], [žiūrėta 2013-06-02]. <http://law.justia.com/codes/maryland/2010/criminal-law/title-7/subtitle-3/7-302>).

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 minėtus 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 nešiojamame 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 str. 1 d., 198[1] *str. 1 d., 210 str.* Šis nuosprendis aktualus tuo aspektu, kad jame spręstas buvusio darbuotojo prisijungimo prie IS teisėtumo klausimas. Nustačius, kad jis prie banko IS prisijungė po prieigos teisės prie visų banko IS panaikinimo, tokie veiksmai pripažinti neteisėtais ir kvalifikuoti pagal BK 198[1] straipsnio 1 dalį.

Nustačius, kad darbuotojas, turėdamas teisę prisijungti prie IS, ja pasinaudojo kitoms nusikalstamoms veikoms padaryti, BK 198[1] straipsnyje numatyta neteisėto prisijungimo veika paprastai neinkriminuota. Pavyzdžiui, Vilniaus rajono apylinkės teismo 2009 m. rugsėjo 8 d. nuosprendyje baudžiamojoje byloje (bylos Nr.1–278-298/2009) spręstas 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 reikmėm prisijunti prie Registro centro duomenų bazės negalima. Kai išėjo iš darbo, jis savo reikmėm prisijungdavo prie Registro centro duomenų bazės iš skirtingų kompiuterių, kurie priklausė jam, draugams, internetinėms kavinėms. Prisijungdavo tikslu gauti duomenis apie asmenų nekilnojamąjį turtą.* Esant tokioms aplinkybėms, Ž. Š., be kitų nusikalstamų veikų (BK 259 straipsnio 2 dalis), inkriminuota BK 198 straipsnio 1 dalis. Jo prisijungimo veiksmai prie IS pagal BK 198[1] straipsnį nevertinti. Panašią praktiką galima pastebėti ir Mažeikių rajono apylinkės teismo 2009 m. rugpjūčio 12 d. nuosprendyje baudžiamojoje byloje (bylos Nr. 1-188-785/2009), Šiaulių miesto apylinkės teismo 2011 m. liepos 18 d. teismo baudžiamajame įsakyme baudžiamojoje byloje (bylos Nr. 1-617-885/2011).

Antrasis prisijungimo neteisėtumo interpretavimui svarbus aspektas, kaip jau minėta, susijęs su mokslinėje literatūroje (Ch. Day, O. S. Kerr, J. Clough, M. W. S. Wong ir kt.) plačiai nagrinėjamais pagrindiniais prieigos prie IS apribojimo būdais ir atitinkamai pagal juos suskirstytais prieigos neteisėtumo pasireiškimo variantais. Šiai analizei svarbios IS savininko ar teisėto valdytojo pasitelktos priemonės, kurios padeda nustatyti prisijungimo prie IS sąlygas ir atitinkamą teisių lygį sistemos vartotojams. Kaip teigia O. S. Kerr, nors apie leidimą prieiti prie IS yra kalbama kaip apie „monolitinę sąvoką“[322], tačiau iš tiesų ji atspindi du pagrįstai vieną nuo kito atskirtus prieigos apribojimo būdus. Vienas jų yra pagrįstas *kompiuterio kodu*, kitas – sutartimi. Toks atskyrimas matyti ir kitų mokslininkų (J. Clough, M. W. S. Wong, Ch. Day ir kt.) darbuose analizuojant bene analogiškus „kodu“ ir sutartimi nustatytus apribojimus, apibrėžiančius prieigos prie kompiuterio sąlygas arba tokią prieigą draudžiančius[323]. Būtent šis skirstymas mokslinėje literatūroje leido išskirti du savarankiškus neteisėtos prieigos prie IS gavimo būdus – prieigą apeinant *kodu* nustatytas ribas ir prieigą pažeidžiant sutartimi[324] pagrįstus apribojimus. Analizuojant teismų praktiką, galima pastebėti, kad būtent reguliavimo *kodu* pažeidimų vertinimas kelia iš tiesų nemažai problemų.

Elektroninės erdvės ribų ir galimybių joje klausimas pirmiausia gali būti sprendžiamas *kompiuterio kodu*, kuris, anot L. Lessig, ir sukuria elektroninę erdvę tokią, kokia ji yra – su nustatytais suvaržymais ir leidimais. Atitinkamai IS konfidencialumo apsauga garantuojama būtent per jį[325]. *Reguliavimą kodu* savo darbuose taip pat analizavo ir O. S. Kerr, kuris tokį terminą pasiūlė, atsižvelgdamas į tai, kad prieigos kontrolė tiesiogiai priklauso nuo *kompiuterio kodo*, sudarančio kliūtį įgaliojimų ribas viršijančių vartotojų veiksmams[326]. Taigi toks veiksmų elektroninėje erdvėje reguliavimas siejamas su „techniniu barjeru“[327] – tam tikrais techninės ar programinės įrangos konfigūravimais, leidžiančiais nustatyti atitinkamo lygio apribojimus prieigai prie IS ar jos išteklių. Bendriausia prasme teigtina, kad prieigos kontrolės mechanizmas apsaugo sistemą nuo galimų nustatytos saugumo politikos pažeidimų, jungiantis prie sistemos „iš išorės“ arba joje atliekant veiksmus prieigos teisę prie sistemos turintiems vartotojams.

Tačiau *reguliavimo kodu* apėjimo sąvoka taip pat nėra monolitinė – ji atspindi dvi alternatyvias prieigos kontrolės nustatytų apribojimų pažeidimo rūšis: 1) autentifikavimo procedūros pažeidimus; 2) IS saugumo silpnų vietų išnaudojimą[328], siekiant paveikti jos atliekamas funkcijas[329]. Apie tokius neteisėtos prieigos būdus (tiesa, analizuojant prieigą

---

[322] Kerr, O. S., *supra* note 222, p. 1644.

[323] Clough, J., *supra* note 210, p. 166; Wong, M. W. S., *supra* note 252, p. 124.

[324] Susitarimu pagrįsti prieigos prie IS apribojimai siejami su nuostatomis ir sąlygomis, kurių turi laikytis asmuo gaudamas prieigą prie IS (toks būdas gali būti įvardijamas ir prieiga prie IS *per spustelėjimą* (angl. *click-through agreement*). Šie apribojimai pažeidžiami, kai asmuo gaudamas prieigą prie IS, nesilaiko nustatytų susitarimo sąlygų. Tokius atvejus mokslinėje literatūroje siūloma priskirti ne baudžiamosios, o civilinės teisės reguliavimo sričiai (plačiau žr. Kerr, O. S., *op. cit.*, p. 1649–1660).

[325] Lessig, L., *supra* note 261, p. 12.

[326] Kerr, O. S., *op. cit.*, p. 1644.

[327] Clough, J., *supra* note 210, p. 166.

[328] Nurodant programinės įrangos saugumo problemas vartojami įvairūs terminai – tai ir defektas, programavimo klaida, yda, apsirikimas, defektas ir pan. (plačiau žr. Plėštys, R., *et al.*, *supra* note 186, p. 50). Nors kiekvienas jų turi tam tikrą specifinę reikšmę, toliau darbe siekiant išvengti terminų painiavos vartojamas bendras *IS saugumo silpnų vietų* terminas

[329] *Computer and Information security handbook*. Vacca J. R. (red). Amsterdam: Elsevier: Morgan Kaufmann, 2009, p. 94; Kerr, O. S., *op. cit.*, p. 1644–1645.

ne prie IS, o kompiuterinių duomenų) yra užsiminęs ir D. Štitlis, analizuodamas Rusijos autorių nuomones, kokie veiksmai turėtų būti pripažinti neteisėta prieiga prie kompiuterinės informacijos[330]. Beje, panašų skirstymą įmanoma rasti ne tik mokslinėje literatūroje, bet ir užsienio valstybių baudžiamuosiuose įstatymuose. Pavyzdžiui, Estijos baudžiamojo įstatymo 217 paragrafe, numatančiame atsakomybę už neteisėtą kompiuterinės sistemos naudojimą, nurodoma neteisėta prieiga prie kompiuterinės sistemos pašalinant arba apeinant kodą, slaptažodį arba kitas apsaugos priemones.

Pirmieji – autentifikavimo procedūros[331] pažeidimo atvejai yra pakankamai akivaizdūs ir neturėtų kelti didesnių tokio pobūdžio veiksmų neteisėtumo konstatavimo problemų. Pačią galimybę gauti neteisėtą prieigą prie IS, panaudojant svetimus vartotojo tapatybę patvirtinančius duomenis, lemia asmens identifikavimo elektroninėje erdvėje specifika. Tiek fizinėje, tiek ir elektroninėje erdvėje asmenims, siekiant atlikti tam tikrus veiksmus, dažniausiai prireikia patvirtinti savo tapatybę. Tačiau, skirtingai nei fizinėje, elektroninėje erdvėje toks identifikavimas vyksta asmeniui tiesiogiai nedalyvaujant, t. y., kaip pastebi M. Laurinaitis, „norint identifikuoti, nereikia fiziškai būti atitinkamoje geografinėje vietoje“[332]. Kadangi elektroninė erdvė, kaip buvo minėta anksčiau, yra IS veiklos rezultatas, tai autentifikavimas joje vyksta atsižvelgiant į komunikavimo elektroninėje erdvėje ypatumus. Būtent jie leidžia tapatybę analizuoti grynai techniniu požiūriu ir ją laikyti tiesiog „skaitmeniniu pseudonimu“[333], kuris reprezentuoja asmenį. Atitinkamai technologijos turėtų užtikrinti ne tik tai, kad asmuo, identifikuodamas save, galės nevaržomai naudotis tokiu pseudonimu, bet ir tai, kad galimybė šiuo pseudonimu pasinaudoti kitiems asmenims nebus suteikta. Akivaizdu, kad tokia asmens tapatybės nustatymo procedūra yra kur kas sudėtingesnė, nes tarp asmenų įsiterpia tarpinė – informacinių ir komunikacijos technologijų – grandis. Būtent tokia komunikavimo elektroninėje erdvėje specifika rodo sąveiką ne tik tarp asmenų ir technologijų ar pačių technologijų, bet dažnai ir *automatizuotą* tam tikrų veiksmų pobūdį. Ne veltui T. L. Norman, apibrėždamas prieigos kontrolės sistemas, nurodė ir šį autorizuotų asmenų patvirtinimo procedūros aspektą[334]. Todėl dėl asmens tapatybės klaidinantys veiksmai elektroninėje erdvėje tiesiogiai nukreipiami ne prieš konkretų autentifikavimo procedūrą vykdantį asmenį, o prieš technologijas, taikomas autentifikavimo procedūrai palengvinti, kai minėtas asmuo tiesiogiai šioje procedūroje gali ir nedalyvauti.

Į IS suklaidinimo galimybę, kaltininkui save pateikiant kaip teisėtą IS vartotoją, atkreiptas dėmesys ir teismų praktikoje. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2001 m. spalio 9 d. nutartyje, priimtoje baudžiamojoje byloje

---

[330] Štitilis, D. Kai kurie neteisėtos prieigos prie kompiuterinės informacijos kriminalizavimo aspektai. *Jurisprudencija*. 2003, 47(39): 62.

[331] Identifikavimas, autentifikavimas ir autorizacija yra skirtingą turinį turinčios sąvokos. Autentifikavimo metu identifikavimo duomenys susiejami su autentifikavimo duomenimis, atitikimo atveju tariama, kad vartotojo tapatybė yra nustatyta. Autorizavimo metu autentifikuotam vartotojui suteikiamos įvairios jam numatytos galimybės atlikti veiksmus sistemoje (Plėštys, R., *et al*., *supra* note 186, p. 35). Darbe šios sąvokos vartojamos taip, kaip jos minimos analizuojamų autorių darbuose, taip pat parenkamos priklausomai nuo konteksto.

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

[333] *Ibid*., p. 31.

[334] Norman, T. L. *Electronic Access Control*. Elsevier Inc., 2012, p. 17.

(bylos Nr. 2K-682/2001), išaiškinta, kad *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 ir taip suklaidina elektroninę sistemą ir tuo pačiu banką. Pastarieji klaidos įtakoje nusprendę, kad toks asmuo teisėtai duoda komandą atlikti operaciją, suklydimo įtakoje savanoriškai perleidžia teisę į turtą, t. y. perveda pinigines lėšas kitam sąskaitos turėtojui, o vėliau išduoda pinigus.* Šis precedento reikšmę turintis išaiškinimas lėmė į sukčiavimo sudėtį įtraukto apgaulės požymio suvokimo pokyčius[335], o naujoji jos rūšis mokslinėje literatūroje vienų autorių įvardyta kaip išeinanti už klasikinės apgaulės ribų[336] arba, anot kitų, laikoma specifine apgaulės forma[337]. Nors šiuo Lietuvos Aukščiausiojo Teismo išaiškinimu siekta pagrįsti apgaulės kaip objektyvaus sukčiavimo sudėties požymio buvimą kaltininko veikoje, tačiau jis aktualus ir tuo, kad jame pripažinta ne tik asmens, bet ir IS suklaidinimo galimybė. Todėl šis IS suklaidinimo aspektas svarbus analizuojant ne tik finansinės operacijos inicijavimą, bet ir nustatant kitų kaltininko veiksmų neteisėtumą, panaudojus ne jam priklausančias autentifikavimo elektroninėje erdvėje priemones. Šiems atvejams galima būtų prisikirti ir apgaulingus veiksmus, kuriais jungiantis prie IS buvo pažeisti autentifikavimo procedūros nustatyti reikalavimai. Pačiam neteisėtam prisijungimui būtini duomenys kaltininko galėjo būti gauti įvairiai: panaudojant socialinės inžinerijos (pavyzdžiui, prisijungimo prie IS duomenų „žvejyba“ (angl. *phishing*)) ar apgaulingą IP taktiką (angl. *pharming*), kenkėjišką programinę įrangą ir daugelį kitų galimų būdų[338].

Apžvelgus teismų praktiką matyti, kad tokie autentifikavimo procedūrų pažeidimai nereti ir kaltininkui inkriminuojant BK 198[1] straipsnyje numatytą nusikalstamą veiką leidžia konstatuoti prisijungimo veiksmų prie IS neteisėtumą. Kaip pavyzdį galima paminėti Klaipėdos miesto apylinkės teismo 2009 m. liepos 1 d. teismo baudžiamąjį įsakymą baudžiamojoje byloje (bylos Nr. 1-770-795/2009), kuriame nurodoma, kad *T. J. laikotarpiu nuo 2006 metų spalio l d. iki 2007 m. spalio 17 d. (tiksli data nenustatyta), bute, esančiame (duomenys neskelbtini) naudodamas personalinį kompiuterį <...> ir jame įdiegtą interneto naršyklės kompiuterinę programą, per šiam butui suteiktą interneto prieigą, prisijungė prie UAB (duomenys neskelbtini) tarnybinėje stotyje administruojamo socialinio tinklalapio (duomenys neskelbtini) ir į šio tinklalapio registruotų vartotojų autentifikavimo langelius įvedė <...> neteisėtai įgytus prisijungimo kodus ir slaptažodžius. <...> Atlikęs šiuos veiksmus, T. J., pažeisdamas tinklalapio (duomenys neskelbtini) apsaugos priemonę, numatančią, jog teisę prisijungti prie šio tinklalapio turi tik registracijos anketą užpildę asmenys,*

[335] Tokį apgaulės suvokimą įtvirtino Lietuvos Aukščiausiojo Teismo senatas (Lietuvos Aukščiausiojo Teismo senato 2005 m. birželio 23 d. nutarimo Nr. 52 „Dėl teismų praktikos vagystės ir plėšimo baudžiamosiose bylose“, 9 punktas. *Teismų praktika*. 2005, Nr. 23.).

[336] Pranka, D., *supra* note 26, p. 666.

[337] Sinkevičius E., *supra* note 26, p. 51.

[338] Plačiau žr. Kalpokas, V.; Marcinauskaitė, R., *supra* note 221, p. 33–39.

autentifikuojami pagal UAB (duomenys neskelbtini) jiems priskirtus kodus ir slaptažodžius, neteisėtai prisijungė prie šios bendrovės administruojamo tinklalapio (duomenys neskelbtini) registruotų lankytojų S. G., J. K., A. K., J. R., V. S., Ž. M., V. P., D. L., V. G., E. S., M. K., J. Š., J. U., I. Ž., L. *M., J. S. paskyrų ir pakeitė šiems tinklalapio lankytojams priskirtus autentifikavimo slaptažodžius.* Panašūs apgaulingi veiksmai, leidę konstatuoti IS apsaugos priemonių pažeidimo faktą ir tokių veiksmų nusikalstamą pobūdį, aprašomi ir anksčiau aptartuose teismų sprendimuose – Vilniaus miesto 1 apylinkės teismo 2009 m. rugsėjo 14 d. teismo baudžiamajame įsakyme baudžiamojoje byloje (bylos Nr. N1-1470-88/2009), Vilniaus miesto 1 apylinkės teismo 2011 m. gruodžio 6 d. nuosprendyje baudžiamojoje byloje (bylos Nr. 1-1430-276/2011), Klaipėdos miesto apylinkės teismo 2009 m. birželio 29 d. teismo baudžiamąjį įsakymą baudžiamojoje byloje (bylos Nr. 1-740-93/2009) ir kt. Taigi tokie atvejai rodo, kad neteisėtam prisijungimui įvykdyti pakanka panaudoti teisėtam sistemos vartotojui suteiktus ir jo autentifikavimui skirtus duomenis. Tačiau galimi atvejai, kai neteisėta prieiga prie IS gaunama kitu – IS saugumo silpnų vietų išnaudojimo keliu.

Analizuojant šią antrą *reguliavimo kodu* apėjimo rūšį, atkreiptinas dėmesys į tai, kad toks neteisėtas prisijungimas prie IS gali būti padaromas „per pažeidžiamas vietas saugumo sistemoje, panaudojus nedokumentuotas operacinės sistemos galimybes“[339]. Tokių galimybių nustatymas ir išnaudojimas leidžia išvengti standartinės procedūros, kontroliuojančios prieigą prie IS. Kaip teigia Ch. Day, sėkmingo tokio pažeidžiamumo išnaudojimo atveju asmeniui gali būti suteikiamos administratoriaus ar jam prilyginamos teisės IS. Kai tik „pašalietis“ gauna tokio lygio prieigą, jis gali sistemą valdyti, įgyti joje esančius duomenis arba ją panaudoti atakuojant kitas sistemas[340]. Pažymėtina, kad įvairios galimybės apeiti kodu nustatytą reguliavimą gali atsirasti: 1) tiek dėl jau esamų IS saugumo silpnų vietų; 2) tiek ir dėl kaltininko tikslingų veiksmų jas sukuriant (pavyzdžiui, panaudojus kenkėjišką programinę įrangą).

Aptariant šį neteisėto prisijungimo prie IS būdą paminėtina, kad programą sudaro sudėtingi taisyklių rinkiniai ir tam tikra jų vykdymo seka, kuri nurodo IS, ką ši turėtų daryti. Anot J. Erickson, „programa gali atlikti tik tai, kas joje užprogramuota, skrupulingai iki paskutinio simbolio“[341]. Kadangi programa iš tiesų atlieka tik tai, kam ji buvo sukurta, tai kitokias jos funkcijas lemia pačios programos ar jos vykdymo aplinkos defektai arba tiesiog klaidos. Tokių IS saugumo silpnų vietų išnaudojimas sudaro galimybes, jas aptikus arba sukūrus, priversti programą veikti jai nenumatytu būdu. IS, kuri netinkamai sukonfigūruota arba kurios programinė įranga yra su žinomomis saugumo problemomis, gali suteikti prieigos teisę neautorizuotiems vartotojams. Pavyzdžiui, galima paminėti „buferio perpildymo“[342] (angl. *buffer overruns*) saugumo spragą, kuri leidžia suaktyvinti pasirinktą kodą ar komandas ir tokiu būdu gauti prieigą prie IS. Ši galimybė atsiranda tada, kai dėl perpildymo programos darbas tampa neprognozuojamas ar net prieštaraujantis jos paskirčiai. Todėl prieigos teisė prie IS kaltininkui suteikiama be tinkamo slaptažodžio. Išnaudojus

[339] Venčkauskas, A.; Toldinas, J., *supra* note 170, p. 10.

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

[341] Plačiau žr. Erickson, J. *Hakingas. Programų kodo narstymo menas*. 2-asis pataisytas ir papildytas leidimas. Kaunas: „Smaltijos“ leidykla, 2010, p. 117.

[342] Plačiau žr. Whitman, M. E., *et al*., *supra* note 170, p. 75; McClure S., *et al. Apsauga nuo hakerių: tinklo saugumo palaikymo paslaptys ir sprendimai*. Kaunas: „Smaltijos“ leidykla, 2006, p. 216–220.

šią spragą, sudaromos galimybės gauti „pagrindinio naudotojo statusą ir neribotą prieigą prie visų kompiuteryje esančių duomenų“[343]. Tokiems būdamas gali būti priskirta ir „SQL komandos įterpimo“[344] (angl. *SQL command injection*) ataka, kuri taip pat leidžia prisijungti prie IS nežinant teisėto jos vartotojo slaptažodžio, ir daugelis kitų būdų. Todėl akivaizdu, kad dėl esamų ar sukurtų IS saugumo silpnų vietų gauta prieiga prie IS, kaip ir anksčiau minėtais autentifikavimo procedūros pažeidimo atvejais, turėtų būti pripažįstama neteisėta.

Mokslinėje literatūroje, aptariant įvairius prieigos neteisėtumo nustatymo aspektus, tokiai išvadai padaryti pagrindą suteikė JAV apeliacinio teismo (2-osios apygardos) 1991 m. kovo 7 d. sprendime byloje *Jungtinės Amerikos Valstijos prieš R.T. Morris (US v. Morris)*[345] 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 kompiuterinės sistemos darbą. Teismas, priimdamas tokį sprendimą, kartu suformulavo naują neteisėtos prieigos nustatymo standartą, kuris mokslinėje literatūroje vėliau pavadintas „numatytų funkcijų“[346] 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, tačiau mokslinėje literatūroje jo interpretavimui skirtas nemažas dėmesys. Kaip teigė O. S. Kerr, šis kriterijus gali būti kildinamas iš „socialinių normų, susiformavusių kompiuterių naudotojų bendruomenėje, prasmės“[347]. Jos atspindi paprastą logiką – programinė įranga kuriama tam tikriems tikslams pasiekti, o sudarius galimybes programa naudotis, ji turėtų būti naudojama pagal jos paskirtį ir neiškreipiant jos atliekamų funkcijų. Galimybė naudotis programa neleidžia vartotojams neteisėtai išnaudoti jos silpnų vietų ir priversti programą atlikti jai nenumatytų (nebūdingų) funkcijų. Todėl kaltininkui gavus prieigą prie IS nenumatytu keliu, t. y. pasinaudojus programoje esančiomis saugumo spragomis, tokia prieiga turėtų būti laikoma neteisėta. Beje, šis aiškinimas tinkamas tiek tada, kai kaltininkas išnaudojo jau esamas IS saugumo silpnas vietas, tiek ir tada, kai jis tikslingais veiksmais pats jas sukūrė.

---

[343] Plačiau žr. Erickson, J., *supra* note 341, p. 124.

[344] Plačiau žr. Kazanavičius, E. *et al. Programų sauga [elektroninis išteklius]: mokomoji knyga*. Kaunas: TEV, 2011, p. 98; Whitman, M. E., *et al.*, *supra* note 170, p. 75.

[345] *United States v. Morris*, no. 774, United States Court of Appeals, 2 nd Circuit, 1991 [interaktyvus] [žiūrėta 2012-12-03] <http://www.loundy.com/CASES/US_v_Morris2.html>.

[346] Kerr, O. S., *supra* note 222, p. 1632.

[347] *Ibid.*

Analizuojant Lietuvos teismų praktiką matyti, kad tokių prisijungimų neteisėtumo vertinimo atvejų joje nėra daug. Tačiau pavieniai teismų sprendimai leidžia pastebėti, kad prieigos prie IS gavimas, išnaudojus programinės įrangos saugumo silpnąsias vietas, vis dėlto pripažįstamas neteisėtu. Kaip pavyzdys paminėtinas anksčiau aptartas Kupiškio rajono apylinkės teismo 2009 m. rugsėjo 2 d. nuosprendis baudžiamojoje byloje (bylos Nr. 1-53-100/2009), kuriame dėl banko programoje buvusių spragų gauta prieiga pripažinta neteisėta ir J. V., be kitų, taip pat inkriminuota BK 198[1] straipsnyje esanti nusikalstama veika.

Taigi, apibendrinus galima teigti, kad prisijungimo prie IS neteisėtumas konstatuotinas nustačius, jog šiam veiksmui nebuvo gautas IS savininko ar teisėto valdytojo leidimas. Nors paties prisijungimo neteisėtumo aiškinimas galimas iš įvairių pozicijų, tačiau BK 198[1] straipsnyje jis turėtų būti siejamas tik su neteisėtu, o ne su teisėtumo ribas viršijančiu prisijungimu. Prisijungimo prie IS neteisėtumą tokiu atveju turėtų padėti nustatyti tiek autentifikavimo procedūros pažeidimai, tiek ir IS saugumo silpnų vietų išnaudojimas.

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

Neteisėto prisijungimo prie IS padarymo būdas – šios sistemos apsaugos priemonių pažeidimas yra vienas iš kriterijų, apibrėžiančių neteisėto prisijungimo prie IS inkriminavimo ribas ir, kaip minėta, padedančių nuspręsti, kokia neteisėto prisijungimo koncepcija pasirinkta kriminalizuojant tokią veiką Lietuvos BK 198[1] straipsnyje. Šio sudėtyje esančio objektyviojo požymio ištakos siejamos su Konvencijos dėl elektroninių nusikaltimų 2 straipsnio ir Pamatinio sprendimo 2005/222/TVR 2 straipsnio nuostatomis. Jose tiesiogiai numatyta galimybė neteisėto prisijungimo prie IS veiką susiaurinti iki prisijungimų, kuriais pažeidžiamos IS apsaugos priemonės. Tikslumo dėlei atkreiptinas dėmesys į tai, kad šiuose teisės aktuose vartojamas tiek „saugumo priemonių“[348], tiek ir „apsaugos priemonių“[349] terminas.

Nors reikalavimas nustatyti apsaugos priemonių pažeidimą leidžia užtikrinti pakankamą neteisėto prisijungimo prie IS pavojingumo lygį (būtiną baudžiamajai atsakomybei kilti), tačiau vis dėlto šis technologinis nusikalstamos veikos aspektas kelia ir tam tikrų analizuojamo požymio interpretavimo problemų. Jų priežastys, kaip ir anksčiau aptartų objektyviųjų požymių atveju, susijusios su technologinio neutralumo principo taikymu aprašant neteisėto prisijungimo veiką. Be to, apsaugos priemonių pažeidimo aiškinimo sunkumus atspindi ir nuolat kylantis jau minėtas technologijų bei terminologijos klausimas. Detaliau analizuojant šias problemas keltini klausimai: 1) kaip turėtų būti suvokiamos IS apsaugos priemonės ir 2) kaip reikėtų interpretuoti tokių priemonių pažeidimus. Kadangi, kaip minėta, BK 198[1] straipsnyje numatytos veikos ašis yra IS, o ne elektroninių duomenų konfidencialumo pažeidimas, tai šios nusikalstamos veikos kontekste analizuotinos IS, o ne joje esančių elektroninių duomenų apsaugos priemonės.

---

[348] Konvencijos dėl elektroninių nusikaltimų 2 straipsnyje yra numatyta, jog „šalis gali reikalauti, kad toks nusikaltimas būtų padarytas pažeidžiant *apsaugos priemones* <...>“.

[349] Pamatinio sprendimo 2005/222/TVR 2 straipsnio 2 dalyje numatyta, kad „kiekviena valstybė narė gali nuspręsti, kad dėl 1 dalyje nurodytos veikos gali būti apkaltinama tik tada, kai nusikaltimas padarytas pažeidžiant kokią nors *saugumo priemonę*“.

Taigi, ieškant tokių priemonių sampratos, akcentuotina, kad, priklausomai nuo požiūrio, joms gali būti suteikta ir plati, ir pakankamai siaura prasmė. Pirmasis atvejis siejamas su kompleksiniu saugumo užtikrinimo požiūriu ir leidžia išskirti pačius įvairiausius būdus prieigai prie IS apsunkinti – „nuo organizacinių – administracinių draudimų iki specialių kompiuterių įrangos priemonių“[350]. Pritarus tokiai nuomonei svarbu suvokti ir šių būdų tarpusavio ryšį. Pavyzdžiui, organizacinės priemonės turi būti palaikomos fizinėmis ir techninėmis priemonėmis, ir iš kitos pusės „techninėms apsaugos priemonėms reikia atitinkamos organizacinės paramos“[351]. Daugeliui autorių (E. Kazanavičius, A. Venčkauskas, E. Toldinas ir kt.)[352] toks pakankamai platus požiūris leido joms bendriausia prasme priskirti moralines – etines[353], teisines[354], organizacines (administracines)[355], fizines[356] ir technines (aparatines ir programines) priemones. Be to, galima pastebėti, kad dėl glaudžios IS ir elektroninių duomenų sąsajos šis klasifikavimas dažnai naudojamas aptariant tiek IS, tiek ir elektroninių duomenų (informacijos) kompleksinius saugumo užtikrinimo sprendimus – įvairialypius metodus ir priemones. Pavyzdžiui, minint informacijos apsaugą literatūroje nurodomos bene analogiškos techninės ir organizacinės saugumo užtikrinimo priemonės[357].

Tuo tarpu siauresnis neteisėto prisijungimo padarymo būdo aiškinimas paremtas išimtinai technologiniu požiūriu ir leidžia vadovautis apsaugos priemonių technologine koncepcija. Apsaugos priemonės tuomet siejamos tik su anksčiau minėta aparatine ir programine įranga, „skirta apsaugoti informacinę sistemą nuo įvairaus pobūdžio pažeidimų ir duomenų praradimo dėl techninių priežasčių ar neteisėtų veiksmų“[358]. Kadangi šios priemonės vykdo apsaugos funkciją, tai literatūroje neretai jos yra įvardijamos ir „kompiuterių saugumo servisais“[359]. Anot A. Venčkausko ir E. Toldino, jos padeda spręsti pačius 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“[360]. Kadangi apsaugos priemonių yra pakankamai didelė įvairovė (pavyzdžiui, ugniasienės, prieigos kontrolė mechanizmai ir pan.), tai bendriausia prasme būtų galima teigti, kad neteisėtas prisijungimas prie IS turėtų pasireikšti aparatinės arba programinės įrangos nustatytų apribojimų pažeidimais.

---

[350] Venčkauskas, A.; Toldinas, J., *supra* note 170, p. 12.

[351] Kazanavičius, E., *et al.*, *supra* note 188, p. 24.

[352] Kazanavičius, E., *et al.*, *supra* note 344, p. 23; Venčkauskas, A.; Toldinas, J., *op. cit.*, p. 11.

[353] Tai „elgesio normos, kurios tradiciškai susiklostė arba formuojasi šalyje ir visuomenėje didėjant kompiuterių paplitimo lygiui“. (Kazanavičius, E., *et al.*, *op. cit.*, p. 23). Šios normos paprastai nėra privalomos kaip norminiai teisės aktai.

[354] 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, J., *op. cit.*, p. 11)

[355] Tai priemonės, „reglamentuojančios duomenų apdorojimo sistemos funkcionavimo procesus, jos išteklių naudojimą, personalo veiklą, taip pat vartotojų sąveikos su sistema tvarką, siekiant apsunkinti ir užkirsti saugumo grėsmių realizavimo galimybę“ Kazanavičius, E., *et al.*, *op. cit.*, p. 23–24.).

[356] Literatūroje techninės priemonės dažniausiai siejamos su įvairiais mechaniniais, elektriniais įrenginiais, skirtais sudaryti fizinėms kliūtims prieinant prie sistemos komponentų. Joms taip pat priklauso ryšio, apsaugos signalizacijos ir vizualaus stebėjimo techninės priemonės (Kazanavičius, E., *et al.*, *op. cit.*, p. 24).

[357] Budnikas, A., *et al.*, *supra* note 189, p. 52.

[358] Abramavičius, A., *et al.*, *supra* note 160, p. 436.

[359] Venčkauskas, A.; Toldinas, J., *op. cit.*, p. 12.

[360] *Ibid.*

Atsakymas į tai, kokiu požiūriu į apsaugos priemones vadovavosi įstatymų leidėjas, numatydamas baudžiamąją atsakomybę už neteisėtą prisijungimą prie IS, iš tiesų nėra aiškus. Kadangi BK 198[1] straipsnyje numatytos nusikalstamos veikos sudėties požymiai formuluoti pagal Konvencijos dėl elektroninių nusikaltimų ir Pamatinio sprendimo 2005/222/TVR nuostatas, tai viena vertus, galima kalbėti apie siauresnę apsaugos priemonių sampratą. Pavyzdžiui, Konvencijos dėl elektroninių nusikaltimų aiškinamojoje ataskaitoje minimi įvairūs tik technologiniai IS apsaugos priemonių aspektai (49 punkte). Apsaugos priemonių technologine koncepcija taip pat vadovavosi ir BK 198[1] straipsnį komentavę autoriai[361]. Tačiau, kita vertus, toks siauresnis nusikalstamos veikos padarymo būdo interpretavimas kelia ir diskusinių klausimų.

Vienas iš tokių momentų susijęs su IS, kuriose nėra jokių saugumo užtikrinimo mechanizmų, konfidencialumo apsauga. Neteisėto prisijungimo veikai suteikus gana siaurą apibrėžtį akivaizdu, kad prieiga prie neturinčios apsaugos priemonių sistemos negalės būti kvalifikuojama pagal BK 198[1] straipsnį[362]. Tokiose situacijose tiesiog nebūtų įmanoma nustatyti IS apsaugos priemonių buvimo, jų pažeidimo fakto, taigi atitinkamai ir šios veikos padarymo būdo kaltininko veikoje. Tačiau ši neteisėto prisijungimo koncepcija iš dalies gali būti pateisinama tuo, kad BK 198[1] straipsnyje esanti veika yra kriminalizuota *per se* be ryšio su kitomis jau sistemoje padaromomis nusikalstamomis veikomis. Tai yra BK kiekvienas nusikalstamų veikų elektroninėje erdvėje padarymo mechanizmo etapas yra išskaidytas į savarankiškas, taigi viena su kitomis nesusijusias veikas. Būtent toks atsakomybės už neteisėtą prisijungimą nustatymo būdas leidžia pakankamai ribotas plataus ir laisvo jos požymių interpretavimo galimybes. Šios problemos, kaip minėta anksčiau, susijusios su neteisėto prisijungimo veikos *perkriminalizavimo* rizika. Tačiau pažymėtina, kad toks neteisėto prisijungimo suvokimas neužkerta kelio kaltininko veikoje įžvelgti kitų nusikalstamų veikų, padarytų jau pačios IS viduje (pavyzdžiui, jei kaltininkas, prisijungęs prie sistemos, neteisėtai įgijo, laikė, pašalino, pakeitė ar darė kitą poveikį elektroniniams duomenims, sutrikdė ar nutraukė IS darbą ir pan.).

Kitas diskutuotinas technologinės koncepcijos aspektas susijęs su probleminėmis situacijomis, kada gali tekti vertinti pačių apsaugos priemonių (aparatinės ir programinės įrangos) pakankamumą. Kaip teigia I. Walden, „įvedus saugumo priemonių ribą, tikėtina, kad tai gali sukurti didesnį teisinį netikrumą <...>“[363]. Pirmiausia dėl to, kad, sudėtyje numačius apsaugos priemonių pažeidimo požymį, lieka neaišku, ar būtina įvertinti ir tokių priemonių „tinkamumą arba protingumą“[364]. Tokio pobūdžio abejonių gali kelti ir Konvencijos dėl elektroninių nusikaltimų aiškinamojoje ataskaitoje pateikti pastebėjimai (49 punktas). Joje teigiama, kad bendrai pritariama, jog neteisėtos prieigos prie IS veika turėtų būti kriminalizuota, tačiau tam tikrų dvejonių valstybėse kyla tokiais atvejais, kai šia veika nėra padaroma žala, arba net tada, kai buvo aptiktos sistemos saugumo silpnos vietos. Tačiau reikėtų pripažinti, kad toks požiūris, nesant aiškių kriterijų, kaip turėtų būti

[361] Abramavičius, A., *et al*., *supra* note 160, p. 436.

[362] Tai kelia klausimų dėl IS, kurioje nėra jokių saugumo užtikrinimo mechanizmų, pakankamos konfidencialumo apsaugos. Analogišką pastebėjimą, tačiau analizuodamas ne apie IS, o elektroninius duomenis, išsakė J. Clough, kuris minėtus reikalavimus pavadino *nesąžiningai diskriminuojančiais*. (Clough, J., *supra* note 210, p. 169).

[363] Walden, I., *supra* note 70, p. 162.

[364] *Ibid*.

vertinamas priemonių pakankamumas, dar labiau susiaurintų neteisėto prisijungimo veikos inkriminavimo galimybes ir keltų bereikalingas diskusijas konstatuojant šio požymio buvimą kaltininko veikoje. Todėl teigtina, kad įvairūs saugumo priemonių trūkumai neturėtų paneigti pačių apsaugos priemonių buvimo fakto. Taip pat toks reikalavimas galėtų būti laikomas nepagrįstu jį vertinant ir iš nukentėjusiojo pusės. Rūpestingumui nustatyti šiuo atveju turėtų pakakti to, kad jis ėmėsi atitinkamų saugumo priemonių, pašaliniam asmeniui rodančių, kad prisijungimas prie IS yra apribotas, o ne reikalauti, kad jis apsaugos priemones padarytų bene neįveikiamas. Prie tokios išvados leidžia prieiti ir ekvivalentus veiksmų fizinėje ir elektroninėje erdvėje vertinimas – norint konstatuoti įsibrovimą fizinėje erdvėje nėra būtina nustatyti, kad buvo imtasi tokių priemonių, kurios kaltininkui sudarė itin sunkiai įveikiamas kliūtis[365]. Todėl atitinkamai elektroninėje erdvėje, jei nukentėjusysis, pavyzdžiui, nepakeitė gamintojo nustatytų pirminių prisijungimo duomenų, neatnaujino programinės įrangos ar jo įdiegta programinė įranga yra su žinomais saugumo trūkumais ir daugelis kitų atvejų neturėtų paneigti pačių apsaugos priemonių pažeidimo fakto. Juo labiau kad apie tokio pobūdžio išimtis nesudaro sąlygų kalbėti ir pats BK 198[1] straipsnis.

Taip pat diskusijų gali sukelti situacijos, kai nukentėjusiajam priklausanti IS (kompiuteris), turinti įdiegtas apsaugos priemones, paliekama be priežiūros prieš tai teisėtam jos vartotojui atlikus būtinus jo autentifikavimo veiksmus ir prie šios sistemos prisijungus. Kaltininkui tokiais atvejais nėra būtina pažeisti sistemos apsaugos priemones, nes pati sistema, prieš tai leidusi prieigą, kaltininką atpažįsta kaip teisėtą jos vartotoją. Tokioms situacijoms apibūdinti taikant fizinės erdvės kriterijus ir žvelgiant iš *vidinės perspektyvos* pozicijų gali būti pasitelkiama atidarytų durų arba apgaulės panaudojimo patenkant į vidų analogija[366]. Analizuojant tokius atvejus elektroninėje erdvėje reikėtų atsižvelgti į tai, kad minėta sistema vis dėlto išlieka apsaugota iki tol, kol prieiga prie jos ribojama atitinkamomis priemonėmis. Todėl nustatytų apsaugos priemonių reikalavimai pažeidžiami ir tais atvejais, kai su sistema tyčinius veiksmus atlieka asmuo, kuriam nėra suteikta prie jos prieigos teisė, nors pačios autentifikavimo procedūros jis ir neturėjo pereiti. Šioje situacijoje visuomet bus įmanoma nustatyti IS apgaulę, kai sistema prieš teisėto vartotojo valią naudojosi kitas asmuo, nei tas, kuris buvo autentifikuotas.

Kitas anksčiau iškeltas klausimas taip pat susijęs su technologijų ir terminologijos problema, t. y. pačių IS apsaugos priemonių pažeidimo interpretavimu. Kadangi BK 198[1] straipsnio dispozicijoje nusikalstama veika aprašyta kaip neteisėtas prisijungimas prie IS pažeidžiant

[365] Įsibrovimo doktrinoje pagrindinis dėmesys skiriamas įvairių neteisėto patekimo į patalpą, saugyklą, saugomą teritoriją ar pan. būdų analizei. Pavyzdžiui, aptariamas neteisėtas patekimas įsilaužiant, panaudojant apgaulę 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 Baudžiamųjų bylų skyriaus 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 bei įsibrovimą į jas, tačiau bet kuriuo iš šių atvejų diskusija gali 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, jo veikos kvalifikavimui įtakos neturi turėti.

[366] Abiem šiais atvejais įsibrovimui konstatuoti netrukdo tai, kad kaltininkui patenkant į vidų nereikėjo įveikti atitinkamų kliūčių (pavyzdžiui, išlaužti durų, išjungti signalizaciją ar pan.) (plačiau žr. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2005 m. birželio 23 d. nutarimas Nr. 52 „Dėl teismų praktikos vagystės ir plėšimo baudžiamosiose bylose“ 15 punktas. *Teismų praktika*. 2005, Nr. 23).

IS apsaugos priemones, tai natūraliai gali kilti klausimas, ar apsaugos priemonių pažeidimas neturi būti siejamas su joms padaroma tam tikra žala. Ar vis dėlto tokia nusikalstamos veikos padarymo būdo formuluotė interpretuotina ir kitaip – kaip apsaugos priemonėmis nustatytų apribojimų (reikalavimų) pažeidimas. Būtent pastarasis aiškinimas gali būti išvedamas nors iš negausios ir dar tik besiformuojančios, tačiau šiuo aspektu aiškios teismų praktikos neteisėto prisijungimo prie IS baudžiamosiose bylose. Bene akivaizdžiausi atvejai, kai žala pačioms IS apsaugos priemonėms nėra padaroma, tie, kai kaltininko veiksmais pažeidžiami autentifikavimo mechanizmų nustatyti prisijungimo prie IS apribojimai, bet ne pačios IS apsaugos priemonės. Tokiais atvejais neigiamas poveikis sistemos apsaugai nėra būtinas, nes prieigai prie jos gauti pakanka apgaulės, naudojamos autentifikavimo procedūros metu (sistemai pateikiant jos teisėto vartotojo duomenis). Šis būdas leidžia suklaidinti IS, kuri suteikia prieigą kaltininkui be jokio jo neigiamo ir žalą sukeliančio poveikio pačioms sistemos apsaugos priemonėms. Taigi IS apsaugos priemonių pažeidimas turėtų būti konstatuotas tiek tada, kai apsaugos priemonėms padaroma žala (pavyzdžiui, sukuriamos saugumo silpnos vietos), tiek ir tada, kai pažeidžiami jų nustatyti apribojimai nesukeliant žalos pačioms apsaugos priemonėms (pavyzdžiui, esamų saugumo silpnų vietų išnaudojimas, autentifikavimo procedūros pažeidimai ir pan.)

Reikėtų priminti, kad vartotoją elektroninių paslaugų sistemoje leidžianti nustatyti autentiškumo patvirtinimo procedūra gali būti laikoma viena iš šios sistemos saugumo užtikrinimo priemonių. Taigi analizuojant teismų praktiką matyti, kad tokių priemonių pažeidimai sprendimuose aprašomi įvairiai, tačiau jie nėra siejami išimtinai tik su žala pačioms elektroninių paslaugų sistemos apsaugos priemonėms. Pavyzdžiui, minėtame Kupiškio rajono apylinkės teismo 2009 m. rugsėjo 2 d. nuosprendyje baudžiamojoje byloje (bylos Nr. 1-53-100/2009) teismas konstatavo banko internetiniame tinklalapyje įdiegtų apsaugos priemonių apėjimą, o ne jų pažeidimą, tai, manytina, pagrįstai nesutrukdė, be kitų nusikalstamų veikų, kaltininkui inkriminuoti ir BK 198[1] straipsnyje numatyto neteisėto prisijungimo prie IS veiką. Kituose teismų sprendimuose minimas apsaugos priemonių pažeidimas, tačiau toks nusikalstamos veikos padarymo būdas taip pat nėra siejamas tik su žala šioms priemonėms. Pavyzdžiui, Vilniaus miesto 1 apylinkės teismo 2010 m. kovo 5 d. teismo baudžiamajame įsakyme, priimtame baudžiamojoje byloje (bylos Nr. N1-724-276/2010), tiesiogiai minimas elektroninės bankininkystės sistemos apsaugos priemonių, skirtų užtikrinti, kad prie šių sistemų paskyrų galėtų prisijungti tik banko klientai, sudarę su banku elektroninės bankininkystės sutartis, pažeidimas. Teismas nustatė, kad kaltininkas prisijungė prie elektroninės bankininkystės sistemos neteisėtai naudodamas kitiems asmenims priklausančius jų identifikavimo sistemoje duomenis. Būtent tokiu būdu, anot teismo, buvo pažeistos elektroninės bankininkystės sistemos apsaugos priemonės, skirtos užtikrinti, kad prie šių sistemų paskyrų galėtų prisijungti tik banko klientai, sudarę su banku elektroninės bankininkystės sutartis. Panašiai IS apsaugos priemonių pažeidimas, sudarant sąlygas kalbėti apie apsaugos priemonių reikalavimų pažeidimą, aprašytas ir Klaipėdos miesto apylinkės teismo 2009 m. liepos 1 d. teismo baudžiamajame įsakyme baudžiamojoje byloje (bylos Nr. 1-770-795/2009). Jame konstatuota, kad kaltininkas prie elektroninio pašto sistemos prisijungdavo į tinklalapio registruotų vartotojų autentifikavimo langelius įvesdamas neteisėtai įgytus prisijungimo kodus ir slaptažodžius. Tai teismui leido padaryti išvadą, kad buvo pažeistos elektroninio pašto sistemos apsaugos priemonės, numatančios, jog teisę prisijungti prie šios sistemos turi tik registracijos anketą užpildę asmenys, autenti-

fikuojami pagal jiems suteiktus kodus ir slaptažodžius. Tačiau tikslumo dėlei reikėtų paminėti, kad teismų praktikoje vis dėlto galima sutikti siauresnių, todėl diskutuotinų, apsaugos priemonių pažeidimo interpretavimo atvejų, kurie suteikia apsaugos priemonių pažeidimo požymiui itin siaurą turinį. Pavyzdžiui, Vilniaus miesto apylinkės teismo 2013 m. sausio 25 d. nuosprendyje baudžiamojoje byloje (bylos Nr. 1-258-716/2013) nurodoma, kad *A. T. byloje buvo kaltinamas tuo, kad neteisėtai prisijungė prie informacinės sistemos, t. y. prie klientės R. K. elektroninės bankininkystės sistemos neturėdamas šios sistemos savininko ar teisėto valdytojo leidimo. Lietuvos Respublikos informacinės visuomenės paslaugų įstatymas informacinę sistemą apibrėžia kaip techninių ir programinių priemonių visumą, naudojamą informacijai kurti, siųsti, priimti, išsaugoti ar kitaip tvarkyti elektroniniu būdu. Teismas pripažįsta, kad elektroninės bankininkystės sistema atitinka šią sąvoką ir papuola į Lietuvos Respublikos baudžiamojo kodekso 198[1] str. reguliavimo sritį. Kita vertus, atsakomybei pagal minėtą straipsnį realizuoti būtinos sąlygos ir objektyvūs požymiai yra tai, kad prisijungimas prie informacinės sistemos turi būti neteisėta ir vykdomas pažeidžiant šios sistemos apsaugos priemones. Akivaizdu, kad A.T. prisijungdamas prie R.K. elektroninės bankininkystės sistemos ne savo vardu, be savininko sutikimo, tai padarė neteisėtai. Tuo tarpu išnagrinėjus bylą nenustatyta, kad neteisėtai prisijungdamas prie elektroninės bankininkystės A. T. tai padarė pažeisdamas apsaugos priemones, t. y. jas sugadindamas ar pakenkdamas apsaugos priemonių režimui. Byloje nustatyta priešingai, t. y. tai, kad A.T. prie elektroninės sistemos prisijungė kaip bet kuris teisėtas vartotojas, nepažeisdamas elektroninės bankininkystės apsaugos priemonių, jas įveikdamas tikrais banko klientei R. K. išduotais slaptažodžiais ir kodais, t. y. elektroniniais duomenimis. <...> Tokiu būdu teismas pripažįsta, kad savo nusikalstamais veiksmais A.T. nerealizavo visų Lietuvos Respublikos baudžiamojo kodekso 198[1] straipsnio dispozicijoje numatytų objektyvių požymių, t. y. nepažeidė informacinės sistemos apsaugos priemonių, jas pašalino neteisėtai panaudodamas neteisėtai S. G. turėtus tikrus elektroninius duomenis, todėl jo veikoje nėra šio nusikaltimo sudėties. Įvertinus visą tai teismas priverstas A. T. dalyje išteisinti.* Apeliacinis skundas dėl tokio BK 198[1] straipsnyje aprašytų neteisėto prisijungimo prie IS požymių aiškinimo šioje baudžiamojoje byloje nebuvo paduotas[367].

Taigi apibendrinus teigtina, kad IS apsaugos priemonės gali būti aiškinamos plačiai arba priešingai – taikant jų techninę koncepciją pakankamai siaurai. Apsisprendžiant, kuri pozicija atspindėtų įstatymo leidėjo valią, reikėtų atsižvelgti į tai, kad šios nusikalstamos veikos ištakos tiesiogiai siejamos su tarptautiniais ir Europos Sąjungos teisės aktais. Nors juose apsaugos priemonių turinys neatskleidžiamas, tačiau aiškinant neteisėtos prieigos įvairius aspektus jos dažniausiai aptariamos tik iš technologinių pozicijų. Tačiau toks požiūris nėra imperatyvus – apsaugos priemonių pažeidimas gali būti atviras įvairioms interpretacijoms, tačiau, be abejo, prieš tai įvertinus neteisėto prisijungimo prie IS *perkriminalizavimo* grėsmę.

2.4. Nusikalstamą veiką kvalifikuojančios aplinkybės

IS strateginės reikšmės ar jos didelės reikšmės valstybės valdymui, ūkiui ar finansų sistemai požymis naudojamas BK 198[1] straipsnio 2 dalyje formuluojant kvalifikuotą neteisėto prisijungimo prie IS sudėtį. Patys neteisėti prisijungimai prie tokio pobūdžio IS kaip *modus operandi* gali būti laikomi „informacinio karo“ elementu, kuris, anot D. Assaf,

[367] Apeliacinį skundą šioje byloje padavė nuteistieji A. T. ir S. G. (Vilniaus apygardos teismo 2013 m. gegužės 29 d. nutartis baudžiamojoje byloje (bylos Nr. 1A-294-166/2013).

yra asimetrinis ta prasme, kad „leidžia silpnesniam priešininkui nusverti stipresnės šalies <...> strateginį pranašumą, palyginti žema kaina naudojant kibernetinę ataką prieš pažeidžiamą kritinę informacinę infrastruktūrą“[368]. Minėto požymio įtraukimas į kvalifikuotą neteisėto prisijungimo prie IS sudėtį suprantamas, nes neteisėtas prisijungimas prie padidintą reikšmę turinčios IS sudaro galimybes sukelti didesnio masto neigiamus padarinius (tiek konfidencialumo, tiek ir integralumo bei vientisumo prasme).

BK 198 straipsnio 2 dalyje numatyto nusikalstamos veikos dalyko konstrukcija apima ne tik *technologinį*, bet taip pat *teisinį* jo aspektą. Su technologijomis susijęs ir technologijų bei terminologijos klausimą keliantis IS kaip nusikalstamos veikos dalyko požymis analizuotas ankstesnėse dalyse. Todėl šioje dalyje pagrindinis dėmesys bus skiriamas teisinei BK 198 straipsnio 2 dalyje numatyto nusikalstamos veikos dalyko pusei – jo strateginės reikšmės, didelės reikšmės valstybės valdymui, ūkiui ar finansų sistemai nustatymui.

Taigi aiškinant BK 198[1] straipsnio 2 dalyje didesnę IS reikšmę žyminčius strateginės reikšmės ir didelės reikšmės nurodytoms sritims (valstybės valdymui, ūkiui ar finansų sistemai) požymius pažymėtina, kad tiek teisės aktuose, tiek ir mokslinėje literatūroje jie naudojami apibūdinti ne tiek IS, kiek pačią infrastruktūrą, informacinę infrastruktūrą ar objektą. Be to, šalia strateginės reikšmės ir didelės reikšmės dažnai vartojami ir kiti terminai, nusakantys padidintą infrastruktūros, informacinės infrastruktūros ar objekto svarbą. Todėl atskleidžiant, kaip galėtų būti suvokiama IS, minima BK 198[1] straipsnio 2 dalyje, tikslinga: 1) aptarti tas sąvokas, kurios vartojamos apibūdinti infrastruktūros, informacinės infrastruktūros ar objekto ypatingą svarbą; 2) atskleisti tokio pobūdžio infrastruktūros, informacinės infrastruktūros ir IS ryšį.

Teisės aktuose ir, atsižvelgiant į sukurtą teisinį reguliavimą, mokslinėje literatūroje vartojami pakankamai įvairūs, tačiau tarpusavyje glaudžiai susiję terminai, nurodantys papildomus infrastruktūrai (informacinei infrastruktūrai) ar objektui būdingus ir padidintą jų reikšmę parodančius požymius. Pavyzdžiui, šalia strateginės reikšmės nacionaliniam saugumui turinčių įmonių teisės aktuose yra minimas ir *kitų nacionaliniam saugumui užtikrinti svarbių* įmonių[369] ar *valstybinės reikšmės objektų* terminai[370]. Taip pat ne tik nacionaliniuose[371], bet ir Europos Sąjungos teisės aktuose[372] bei itin dažnai mokslinėje literatūroje (D. Assaf, B. Lopez, S. Ghosh ir kt.)[373] vartojamas *ypatingos svarbos* infrastruktūros (informacinės

---

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

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

[370] 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 patvirtinimas. *Valstybės žinios*. 2010, Nr. 69-3442.

[371] 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.

[372] Europos Sąjungos Tarybos 2008 m. gruodžio 8 d. direktyva 2008/114/EC dėl Europos ypatingos svarbos infrastruktūros objektų nustatymo ir priskyrimo jiems bei būtinybės gerinti jų apsaugą vertinimo. [2008] OL L345/76.

[373] *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.

infrastruktūros) arba kitaip *kritinės* infrastruktūros (informacinės infrastruktūros) (angl. *critical infrastructure*) terminas. Tokia terminų gausa iš pirmo žvilgsnio iš tiesų leidžia kelti strateginės reikšmės ar didelės reikšmės požymių turinio nustatymo problemą. Tačiau vis dėlto sulyginus minėtų terminų apibrėžtis galima pastebėti daug jų tarpusavio panašumų – šių terminų sąsaja atsiranda nustatant esminius kriterijus, pagal kuriuos infrastruktūra (informacinė infrastruktūra) ar objektas galėtų būti pripažįstami ypatingos svarbos, o jų veiklos sutrikdymas sukeltų globalų neigiamą poveikį įvairiems svarbiems sektoriams. Patys vertinimo kriterijai leidžia net ir pakitus situacijai įvertinti tam tikrų objektų svarbą ir motyvuotai juos priskirti prie ypatingos svarbos infrastruktūros objektų. Be to, jų nustatymas aktualus sprendžiant, ar *mutatis mutandis* pagal išskirtus kriterijus gali būti apibrėžiama ir strateginės reikšmės arba didelės reikšmės valstybės valdymui, ūkiui ar finansų sistemai turinti IS.

Ar infrastruktūra yra ypatingos svarbos (kritinė) yra interpretavimo dalykas, be to, kaip mini S. Ghosh, pats sąvokos formulavimas, pavyzdžiui, ją apribojant tam tikrais objektais yra sudėtingas, nes sąvoka „kritinis visuomet susijęs su perspektyvos klausimu“[374]. Ypatingos svarbos suvokimas laikui bėgant gali keistis, priklausomai nuo to, kaip vystosi visuomenė, kaip plečiama informacinė infrastruktūra, kokie sektoriai susiejami su informacinėmis ir komunikacijos technologijomis ir pan.

Identifikuojant, kokia infrastruktūra gali būti pripažįstama kritine, kaip minėta, svarbi bendrų kriterijų paieška, kurios buvo imtasi Europos Sąjungos lygmeniu priėmus Europos Sąjungos Tarybos 2008 m. gruodžio 8 d. direktyvą 2008/114/EC dėl Europos ypatingos svarbos infrastruktūros objektų nustatymo ir priskyrimo jiems bei būtinybės gerinti jų apsaugą vertinimo (toliau – Direktyva 2008/114/EC)[375]. 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“. Poveikis bent dviem valstybėms narėms leistų tokio pobūdžio objektą pripažinti Europos ypatingos infrastruktūros objektu (2 straipsnio b punktas). Taip pat Direktyvoje 2008/114/EC pateikiami bendri kriterijai, kuriais vadovaujantis atliekamas objektų vertinimas – tai *nukentėjusiųjų kriterijus* (įvertinama atsižvelgiant į potencialų žuvusiųjų ar sužeistų skaičių), *ekonominio poveikio kriterijus* (įvertinama atsižvelgiant į ekonominio nuostolio ir (arba) produktų ar paslaugų pablogėjimo mastą; įskaitant galimą poveikį aplinkai) ir *poveikio visuomenei kriterijus* (įvertinama atsižvelgiant į poveikį visuomenės pasitikėjimui, fizines kančias ir kasdieninio gyvenimo sutrikdymą; įskaitant būtinų 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[376] (toliau – Nutarimas Nr. 943), kuriame vietoj ypatingos svarbos infra-

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

[375] Europos Sąjungos Tarybos 2008 m. gruodžio 8 d. direktyva 2008/114/EC dėl Europos ypatingos svarbos infrastruktūros objektų nustatymo ir priskyrimo jiems bei būtinybės gerinti jų apsaugą vertinimo. [2008] OL L345/76.

[376] 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.

struktūros vartojamas *valstybinės reikšmės* objektų terminas (2 punktas). Jo turinys minėtame nutarime susiejamas su Lietuvos Respublikos civilinės saugos įstatymu, kuriame valstybinės reikšmės objektu laikoma „valstybės institucija, įmonė, ūkio, energetikos, transporto, telekomunikacijų ar kitas infrastruktūros objektas, neatsižvelgiant į jo nuosavybės formą, kurio kontrolės ar funkcionavimo sutrikimas arba sutrikdymas keltų pavojų ar padarytų didelę žalą nacionaliniam saugumui – sutrikdytų valstybės valdymą, ūkio sistemos, valstybei svarbios ūkio šakos ar infrastruktūros funkcionavimą arba kuris karo, antpuolių ar teroro aktų metu gali būti pasirinktas kaip taikinys ir dėl to tapti ekstremaliosios situacijos židiniu“ (2 straipsnio 30 punktas). Beje, minėtame apraše taip pat nurodomi analogiški nukentėjusiųjų, ekonominio poveikio ir poveikio visuomenei kriterijai (12 punktas).

Pažymėtina, kad bene analogiška valstybinės reikšmės objekto sąvoka pateikiama ir Lietuvos Respublikos Vyriausybės 2010 m. birželio 7 d. nutarimu Nr. 717 patvirtintame Objektų pripažinimo valstybinės reikšmės objektais tvarkos aprašo (toliau – Nutarimas Nr. 717) 4 punkte[377]. Taip pat šio aprašo 2 punkte valstybinės reikšmės objektams *a priori* yra priskiriami objektai, kurie vadovaujantis Lietuvos Respublikos strateginę reikšmę nacionaliniam saugumui turinčių įmonių ir įrenginių bei kitų nacionaliniam saugumui užtikrinti svarbių įmonių įstatymu yra priskiriami prie strateginę reikšmę nacionaliniam saugumui turinčių įmonių ir įrenginių bei kitų nacionaliniam saugumui užtikrinti svarbių įmonių[378].

Tokia Direktyvoje 2008/114/EC, Nutarimuose Nr. 943 ir 717 vartojama terminija leidžia padaryti keletą svarbių išvadų:

1) Direktyvoje 2008/114/EC minimiems *ypatingos svarbos infrastruktūros objektams* nacionalinėje teisėje įvardyti parinktas *valstybinės reikšmės objekto* terminas;

2) valstybinės reikšmės objektais *inter alia* laikomos ir strateginę reikšmę nacionaliniam saugumui turinčios įmonės ir įrenginiai bei kitos nacionaliniam saugumui užtikrinti svarbios įmonės. Todėl, pavyzdžiui, valstybinės reikšmės objektu pripažįstama VĮ Ignalinos atominė elektrinė, VĮ Tarptautinis Vilniaus oro uostas, AB Lietuvos radijo ir televizijos centras bei daugelis kitų;

3) valstybinės reikšmės objektu gali tapti objektas, atitinkantis vertinimui naudojamus kriterijus, *neatsižvelgiant į jo nuosavybės formą* (jis gali priklausyti tiek privačiam, tiek ir viešam sektoriui);

4) nustatant ypatingos svarbos (valstybinės reikšmės) objektą esminę reikšmę turi šio objekto veiklos pobūdis ir (ar) paskirtis, kuri suponuoja, kad dėl neigiamo poveikio jam gali būti sukeliamas pavojus ar padaroma didelė žala įvairiems sektoriams. Sukeltų pa-

---

[377] 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.

Jame valstybinės reikšmės objektu „pripažįstama valstybės institucija, įmonė, ūkio, energetikos, transporto, telekomunikacijų ar kitas infrastruktūros objektas, neatsižvelgiant į jo nuosavybės formą, kurio kontrolės ar funkcionavimo sutrikimas arba sutrikdymas keltų pavojų ar padarytų didelę žalą nacionaliniam saugumui“.

[378] Strateginę ar svarbią reikšmę nacionaliniam saugumui turinčios įmonės ir įrenginiai pagal šio įstatymo 2 straipsnio 4 dalį tai „Lietuvos Respublikoje esančios ar steigiamos įmonės, projektuojami ar statomi įrenginiai, kuriems pagal jų paskirtį ir (ar) veiklos pobūdį šis įstatymas priskiria strateginę arba svarbią reikšmę nacionaliniam saugumui ir kuriems dėl esminių nacionalinio saugumo interesų apsaugos nustatomos sąlygos ir reikalavimai dėl įmonių ar įrenginių nuosavybės ar valdymo ar bet kurių kitų teisių, įmonių kapitalo struktūros ir jo pokyčių, taip pat reikalavimai, kuriuos turi tenkinti potencialūs dalyviai“.

darinių masto arba kilusios grėsmės vertinimui taikytini anksčiau minėti nukentėjusiųjų skaičiaus, poveikio ekonomikai ar visuomenei kriterijai.

Apibrėžiant ypatingos svarbos infrastruktūrą mokslinėje literatūroje taip pat orientuojamasi į šios infrastruktūros svarbą ir neigiamų padarinių, kuriuos gali sukelti neteisėtas poveikis jai, mastą. Pavyzdžiui, B. Lopez kalbėdamas apie kritinę infrastruktūrą atkreipė dėmesį į tai, kad ji „yra tiek gyvybiškai svarbi, jog jos nesugebėjimas veikti turės neigiamą poveikį saugumui arba ekonominiam saugumui“[379]. E. M. Brunner ir M. Suter taip pat akcentavo, kad komponentas arba visa infrastruktūra paprastai apibrėžiama kaip „kritinė“ dėl jos strateginės pozicijos visoje infrastruktūros sistemoje. Kartu šie autoriai išskyrė keletą tokio pobūdžio infrastruktūros suvokimo būdų, kas leido į infrastruktūros ypatingą svarbą pažvelgti iš *sisteminės* ir *simbolinės* pozicijų. *Sisteminis požiūris* reikštų, kad infrastruktūra arba infrastruktūros komponentai yra ypatingos svarbos (kritiniai) dėl jų struktūrinės pozicijos visoje sistemoje, ypač jei jie užtikrina ryšį tarp kitų infrastruktūrų. Tačiau toks požiūris, kaip pastebi patys autoriai, sukuria ir tam tikras problemas, nustatant, kokia infrastruktūra ar jos komponentai yra kritiniai – iš esmės viskas sujungta komunikacinėmis technologijomis ir net pavienis nedidelės reikšmės atvejis gali sukelti nenumatytą pakopinį efektą, turėsiantį įtakos daugeliui sektorių. Taigi, jei ypatinga svarba aiškinama per infrastruktūrų tarpusavio sąsają visos jos tampa potencialiai kritinės. Taikant *simbolinę sampratą* infrastruktūra arba infrastruktūros komponentai pripažįstami kritiniais patys savaime dėl savo vaidmens ar funkcijos visuomenėje. Probleminiai infrastruktūrų tarpusavio ryšio klausimai tokiais atvejais yra antraeiliai. Ypatingos svarbos infrastruktūrai identifikuoti nėra taikomas *tarpusavio sąsajos kriterijus*, nes pati infrastruktūros simbolinė reikšmė yra pakankama, kad ji taptų susidomėjimą keliančiu taikiniu. Vadovaujantis simboliniu požiūriu skirtingai nei sisteminiu kritinę infrastruktūrą apibrėžti yra daug paprasčiau – pagrindiniu akcentu čia tampa jos vaidmuo, svarba ir simbolinė reikšmė. Tačiau toks požiūris dažniausiai verčia orientuotis į pavienes infrastruktūras, didesnės reikšmės neteikiant infrastruktūrų tarpusavio sąsajai[380].

Sprendžiant, ar anksčiau minėti nukentėjusiųjų, ekonominio poveikio ir poveikio visuomenei kriterijai gali būti taikomi apibūdinant ir IS, aktualu nustatyti infrastruktūros, informacinės infrastruktūros ir IS ryšį.

Pati infrastruktūra suvokiama kaip „pagrindinė sistemos struktūra, ypač viešosios paslaugos ir įrenginiai (tokių kaip magistralės, mokyklos, tiltai ir vandens sistemos) reikalingi palaikyti prekybą, taip pat ekonomikos ir gyvenamųjų rajonų vystymąsi“[381]. Vystantis informacinėms ir komunikacijos technologijoms infrastruktūros plėtrai ir tinkamam jos funkcionavimui svarbi tampa informacinė infrastruktūra kaip viena iš visą infrastruktūrą sudarančių elementų. Taigi analizuojant ypatingos svarbos infrastruktūros ir ypatingos svarbos informacinės infrastruktūros sąsają atkreiptinas dėmesys į tai, kad šie terminai nėra sinonimai, o tarpusavyje sąveikauja kaip visuma ir jos dalis. Kadangi dauguma strategiškai svarbių sektorių yra priklausomi nuo technologijų, tai neišvengiamai tenka išskirti tiek *fizinį*, tiek

[379] *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.

[380] Brunner, E. M.; Suter, M. *International CIIP Handbook 2008/2009*. [interaktyvus]. p. 530–532, [žiūrėta 2013-06-01]. <http://www.css.ethz.ch/publications/pdfs/CIIP-HB-08-09.pdf>.

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

ir *virtualų* ypatingos svarbos infrastruktūros apsaugos lygmenis. Toks požiūris susijęs su mokslinėje literatūroje pateiktu gana taikliu pastebėjimu, kas „elektroninė erdvė turi sąlytį praktiškai su viskuo ir su kiekvienu“[382]. Būtent virtualus apsaugos lygmuo yra aiškiausiai siejamas su informacinės infrastruktūros kaip infrastruktūros dalies apsauga.

Kaip teigia D. Assaf, ypatingos svarbos (kritinė) informacinė infrastruktūra inkorporuoja 2 terminus: „ypatingos svarbos infrastruktūra“ ir „informacinė infrastruktūra“. Analizuodamas jų tarpusavio santykį autorius priėjo išvados, kad ypatingos svarbos informacinė infrastruktūra yra ta informacinės infrastruktūros dalis, kuri yra esminė užtikrinant ypatingos svarbos infrastruktūros paslaugų nenutrūkstamumą. Kitais žodžiais tariant tai „ryšių ir informacijos tinklai, sistemos, programinė įranga ir įrenginiai (įskaitant priežiūros ir kontrolės įrangą), esantys ypatingos svarbos infrastruktūros pagrindas“[383]. Šis aspektas kaip vienas iš galimų apibūdinant ypatingos svarbos informacinę infrastruktūrą minimas 2009 m. kovo 16 d. Lietuvos Respublikos valstybės kontrolės išankstinio tyrimo ataskaitoje Nr. IT-P-900-1-3 Strateginės informacijos sauga[384], kurioje ypatingos svarbos informacinė infrastruktūra apibrėžta kaip „elektroninių ryšių tinklas, informacinė sistema ar jų grupė, kurie patys yra priskirtini ypatingos svarbos infrastruktūrai arba kurių tinkamas veikimas yra būtina ypatingos svarbos infrastruktūros funkcionavimo prielaida“.

Panaši nuomonė, kaip turėtų būti suprantama ypatingos svarbos informacinė infrastruktūra, matyti ir nacionaliniu lygmeniu priimtuose teisės aktuose numačius ypatingos svarbos informacinės infrastruktūros apibrėžtį. Pavyzdžiui, Lietuvos Respublikos Vyriausybės 2011 m. birželio 29 d. nutarimo Nr. 796 „Dėl elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011-2019 metais programos patvirtinimo“ (Žin., 2011, Nr. 83-4033) 4 punkte ji apibūdinta kai „elektroninių ryšių tinklas, informacinė sistema ar informacinių sistemų grupė, kurioje įvykęs incidentas padaro ar gali padaryti didelę žalą nacionaliniam saugumui, šalies ūkiui ar visuomenės gerovei“. Kaip matyti, pati ypatingos svarbos informacinė infrastruktūra apibūdinama tiek *technologiniu* aspektu, kaip IS, IS grupės ir komunikacinės technologijos, tiek *teisiniu*, rodančiu padidintą informacinės infrastruktūros reikšmę visuomenėje – incidentas joje gali padaryti arba padaro didelę žalą nacionaliniam saugumui, šalies ūkiui ar visuomenės gerovei. Be abejo, paprastai tokius padarinius sukelia neteisėtas poveikis IS, kuri yra esminė užtikrinant nenutrūkstamą ypatingos svarbos infrastruktūros funkcionavimą. Taigi apibendrinus, galima būtų padaryti šias išvadas:

1) informacinė infrastruktūra yra infrastruktūros dalis, rodanti jos sąsają su informacinėmis ir komunikacijos technologijomis. Priklausomai nuo informacinės infrastruktūros sandaros ją gali sudaryti tiek viena IS, tiek ir keletas jų. Todėl sprendžiant, ar pati IS, o ne bendrai infrastruktūra ar informacinė infrastruktūra (jei ją sudaro keletas IS) yra ypatingos reikšmės, svarbu nustatyti, kad ši IS yra esminė užtikrinant pačios infrastruktūros funkcionavimą, yra jos tinkamo veikimo pagrindas;

2) analizuojant ypatingos svarbos, valstybinės reikšmės ir strateginės bei didelės reikšmės tam tikriems sektoriams terminų ryšį buvo prieita prie išvados, kad jie baudžiamąja

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

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

[384] 2009 m. kovo 16 d. Lietuvos Respublikos valstybės kontrolės išankstinio tyrimo ataskaita Nr. IT-P-900-1-3 Strateginės informacijos sauga. [interaktyvus], [žiūrėta 2013-08-29]. <http://www.vkontrole.lt/audito_ataskaitos.aspx?tipas=7>.

teisine prasme turėtų leisti įvardyti tą patį infrastruktūros, informacinės infrastruktūros ypatumą – jos išskirtinę, itin svarbią reikšmę. Atitinkamai strateginę reikšmę nacionaliniam saugumui arba didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinčioms IS apibūdinti taip pat gali būti kaip sinonimai taikomi bendri ypatingos svarbos, valstybinės reikšmės IS terminai[385];

3) strateginės reikšmės nacionaliniam saugumui arba didelės reikšmės valstybės valdymui, ūkiui ar finansų sistemai IS požymių kaltininko veikoje nustatymui ir jų pagrindimui taikytini minėti infrastruktūros objekto padidintą svarbą leidžiantys nustatyti nukentėjusiųjų skaičiaus, poveikio ekonomikai ar visuomenei kriterijai. Tokiu atveju IS reikšmė atitinkamiems sektoriams būtų vertinama atsižvelgiant ne tik į konkretaus sektoriaus, kuriame ji funkcionuoja, svarbą, bet ir naudojant *neigiamų padarinių masto kriterijus*. Todėl BK 198[1] straipsnio 2 dalyje numatytas neteisėtą prisijungimą prie IS 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. Pačios žalos mastui nustatyti gali būti taikomi nukentėjusiųjų, ekonominio poveikio ir poveikio visuomenei kriterijai;

4) kadangi ypatingos svarbos IS apibūdinantis požymis padidintą šios sistemos svarbą apibūdina pačia bendriausia prasme, tai BK 198[1] straipsnio 2 dalyje nurodomas konkrečios nacionalinio saugumo, valstybės valdymo, ūkio ir finansų sritys. Konstatuojant, kad neteisėtai buvo prisijungta prie IS, turinčios strateginės reikšmės nacionaliniam saugumui ar didelės reikšmės valstybės valdymui, ūkiui ar finansų sistemai, turėtų būti nurodoma viena (ar kelios) iš dispozicijoje nurodytų sričių. O pats neigiamų padarinių masto 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 IS yra didelės reikšmės finansų sistemai).

3. Subjektyvieji neteisėto prisijungimo prie informacinės sistemos sudėties požymiai

Neteisėto prisijungimo prie IS inkriminavimo apribojimus nustato ne tik aptarti objektyvieji, bet taip pat šios nusikalstamos veikos subjektyvieji požymiai. Kaip vienas iš pagrindinių ir, analizuojant IS konfidencialumo pažeidimus, galintis kelti 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 atsako pagal baudžiamąjį įstatymą tik tuo atveju, jeigu jis 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, anot G. Švedo, „išreiškia vieną svarbiausių šiuolaikinės baudžiamosios atsakomybės nuostatų – atsakomybę tik už

[385] Mokslinėje literatūroje dažnai galima sutikti ne tik ypatingos svarbos, valstybinės reikšmės, bet ir kitas sistemos lemiamą reikšmę apibūdinančių terminų variacijas. Pavyzdžiui, D. Bainbridge, analizuodamas neteisėtos prieigos veikų keliamas grėsmes ir *padidintos rizikos veiklas* minėto pobūdžio sistemas, įvardijo kaip *esmines su saugos užtikrinimu susijusias* sistemas (angl. *safety-critical system*) (Bainbridge, D., *supra* note 307, p. 381).

kaltai padarytą veiką“[386]. Šis aspektas aktualus analizuojant neteisėtą prisijungimą prie IS, nes tokios nusikalstamos veikos padarymo mechanizmas visuomet susijęs su informacinių ir komunikacijos technologijų galimybėmis, jų atliekamomis funkcijomis. Įsiterpus šiam elementui, akivaizdu, kad panaudojus technologijas įmanomos situacijos, kai sukeliami asmeniui nenumatyti jų veiklos rezultatai. Todėl iš tiesų vienais atvejais gali nekilti klausimų, ar asmens atlikti veiksmai naudojant kompiuterį yra nusikalstami, tačiau vis dėlto, kaip pastebi B. A. Howell, „technologijos sukuria problemą, ar nusikaltimas yra padarytas kompiuterio vartotojo, ar kompiuterio programos“[387]. Pavyzdžiui, dėl prieigos kontrolę užtikrinančios programinės įrangos spragų asmeniui gali būti suteikta galimybė prisijungti prie IS. Tačiau dėl programinės įrangos blogo funkcionavimo nustatytų apribojimų pažeidimas prieigą gavusio asmens gali būti ir nesuvoktas[388]. Būtent kaltės principas tokiais atvejais leidžia eliminuoti objektyvų pakaltinimą, taigi neleidžia kilti baudžiamajai atsakomybei, jei žala vertybėms buvo padaryta nesant kaltės.

Taigi aiškinant kaltės požymį atkreiptinas dėmesys į tai, kad neteisėto prisijungimo prie IS nusikalstama veika yra tyčinė. Kadangi šios veikos sudėtis formali, tai pagal šiuo metu galiojančio BK 15 straipsnio nuostatas ji gali būti padaroma tik tiesiogine tyčia. Neatsargios kaltės formos BK 198[1] straipsnis tiesiogiai nenumato, atitinkamai baudžiamoji atsakomybė už dėl neatsargumo padarytą tokią veiką negalima (BK 16 straipsnio 4 dalis). Tokia kaltės formų apribojimo galimybė numatyta tiek Pamatinio sprendimo 2005/222/TVR 2 straipsnyje, kuriame tiesiogiai minima tyčinė prieiga prie visos IS ar jos dalies, tiek 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 „sugaunančios viską“[389] nuo iš tiesų pavojingų veikų iki bet kokio netinkamo elgesio panaudojant kompiuterį konstrukcijos. Kaip teigiama mokslinėje literatūroje, kitokie nei tyčiniai veiksmai gali liudyti tiesiog apie „nerūpestingumą, kvailumą, neatidumą“[390], tačiau jų padarymas neturėtų būti vertinamas iš baudžiamosios teisės pozicijų. Todėl teigtina, kad tyčinės kaltės įtraukimas į neteisėto prisijungimo prie IS sudėtį susiaurina šios nusikalstamos veikos apibrėžtį ir padeda išvengti pernelyg plataus, taigi žiūrint iš baudžiamosios teisės pusės nepagrįsto, šios veikos taikymo.

Atskleidžiant neteisėto prisijungimo prie IS kaltės turinį reikėtų atsižvelgti į tai, kad, kaip minėta, šios nusikalstamos veikos sudėtis yra formali ir ji gali būti padaryta tik tiesiogine tyčia. Todėl konstatuojant tyčinę kaltę turėtų būti nustatoma, kad kaltininkas suvokia, jog darydamas žalą IS konfidencialumui neteisėtai prisijungia prie šios sistemos pažeisdamas jos apsaugos priemones, ir nori taip veikti. Kadangi neteisėto prisijungimo veika BK 198[1] straipsnyje kriminalizuota *per se* be sąsajos su kitomis nusikalstamomis veikomis ar kaltininko nusikalstamais ketinimais, tai toks kaltės turinys nereikalauja įrodyti, kad

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

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

[388] Tokie atvejai gali būti prilyginami kazusui ir nuo anksčiau aptartų tyčinių *kompiuterio kodu* nustatytų apribojimų pažeidimų skiriasi tuo, kad tokios programinės įrangos silpnosios vietos nėra žinomos vartotojui ir nėra sąmoningai išnaudojamos gaunant prieigą prie IS.

[389] Clough, J., *supra* note 210, p. 167.

[390] Clough, J., *supra* note 110, p. 92.

kaltininkas, gavęs neteisėtą prieigą prie IS, ketino pačioje sistemoje padaryti kitas nusikalstamas veikas (pavyzdžiui, pažeisti elektroninių duomenų konfidencialumą, sutrikdyti IS darbą ar pan.). Patys neteisėto prisijungimo prie IS tikslai ir motyvai, kaip pastebi R. Mockevičius ir D. Valatkevičius, gali būti įvairūs: tai ir chuliganiškos paskatos, siekis daryti kitas nusikalstamas veikas ir pan.[391] Tačiau šios veikos padarymo motyvų ir tikslų neįtraukus į jos sudėtį, jie veikos kvalifikavimui pagal BK 198[1] straipsnį įtakos neturi.

Toks kaltės turinys *inter alia* reiškia, jog kaltininkas jungdamasis prie IS turi suvokti ne tik tai, kad jis pažeidžia IS apsaugos priemones, bet ir tai, kad tokie jo veiksmai yra neteisėti. Šiuo aspektu galima būtų paminėti svarbią baudžiamajai teisei nuostatą, kad asmuo savo elgesio pavojingumą gali įvertinti tik tada, kai suvokia nusikalstamos veikos faktines aplinkybes. Kaip teigia S. Bikelis, „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 <...>“[392]. Taigi tyčinės kaltės reikalavimas leidžia eliminuoti atvejus, kai prie IS buvo prisijungta nesuvokiant tokio veiksmo neteisėtumo (pavyzdžiui, jau minėta, kad prieiga gali būti suteikta dėl blogo apsaugos priemonių funkcionavimo) arba kai esant leidimui atliekamas įsiskverbimo testavimas, siekiant nustatyti IS saugumo silpnąsias vietas (etiškas įsibrovimas).

Nagrinėjant patį neteisėtumo požymį, darbe buvo atkreiptas dėmesys į tai, kad teisėtų ir jiems priešingų veiksmų atskyrimas elektroninėje erdvėje bendriausia prasme priklauso nuo privačios ir viešos erdvių ribų joje nustatymo. Anot Y. Benkler, „ribų sukūrimas reiškia leidimą žmonėms suprasti, kad ribos egzistuoja, ar jos būtų fizinės, loginės ar teisinės“[393]. Tačiau kaltės požymis, analizuojant neteisėto prisijungimo prie IS veiką, lemia, kad vien tik apribojimų buvimas ir jų reikalavimų nepaisymas nėra pakankamas konstatuoti, kad buvo padaryta ši veika, – būtina nustatyti ir kaltininko tokių ribų bei jų pažeidimo suvokimą. Toks reikalavimas reiškia, kad neišvengiamai turi būti įvertintas ir elektroninėje erdvėje nustatytų apribojimų aiškumas. Todėl įvairios priemonės, kurių buvo imtasi apibrėžiant prisijungimo prie IS sąlygas, gali būti laikomos pakankamomis tik tada, jei jos vartotojui efektyviai praneša apie atitinkamų ribų egzistavimą. Mokslinėje literatūroje, tiesa, kalbant ne apie prisijungimo prie IS, o prieigos prie duomenų apribojimus, akcentuota, kad įvairūs apribojimai turi būti matomi ir suvokiami būtent iš vartotojo perspektyvos, tai ir atitiktų jo patyrimą *Internete kaip vietoje* (angl. *Internet-as-place*)[394]. Šio ribų numatomumo kriterijaus taikymas leidžia įžvelgti panašumų su *vidinės perspektyvos* teorijos idėjomis, kurios į elektroninę erdvę leido pažvelgti kaip į virtualią realybę, o patį prisijungimą tapatinti su virtualiu įėjimu į sistemą. Tokios analogijos sudaro galimybes taikyti ir ekvivalentaus vertinimo principą bei atsižvelgti į tai, kaip asmuo suvokė savo veiksmus elektroninėje erdvėje. Lygiavertis vertinimas tokiu atveju išreikštų idėją, kad nepriklausomai nuo to, kokioje erdvėje asmuo veikia, visais atvejais turi 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

[391] Abramavičius, A., *et al*., *supra* note 160, p. 437.
[392] Bikelis, S. *Tyčinė kaltė baudžiamosios teisės teorijoje ir praktikoje: daktaro disertacija*. Vilnius: Mykolo Romerio universitetas, 2007, p. 48.
[393] Madison, M. J., *supra* note 252, p. 490.
[394] *Ibid*., p. 491.

ribų suvokimas (pavyzdžiui, vertinant kaltininko įsibrovimo veiksmus)[395], tai mažesni suvokimo reikalavimai neturėtų būti nustatomi elektroninėje erdvėje.

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

[395] Pavyzdžiui, Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2010 m. gruodžio 7 d. nutartyje baudžiamojoje byloje (bylos Nr. 2K-555/2010) spręsta, 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. Todėl teismas atskirai pasisakė 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 stovėjo statinės su alumi, aiškiai matyti pašaliniams įeiti draudžiantis užrašas) ir padarė išvadą, kad nuteistasis tokius apribojimus suvokė.

IV. NETEISĖTAS ELEKTRONINIŲ DUOMENŲ PERĖMIMAS IR PANAUDOJIMAS (BK 198 straipsnis)

1. Neteisėto elektroninių duomenų perėmimo ir panaudojimo kriminalizavimo pagrindimas ir inkriminavimo 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 vadinta kompiuterinės informacijos pasisavinimu ir skleidimu bei savo apimtimi buvo siauresnė nei šiuo metu BK esanti elektroninių duomenų perėmimo ir panaudojimo veika. Būtent po 2007 m. viso BK XXX skyriaus pokyčių BK 198 straipsnyje kito ne tik jame esančios veikos baudžiamumas, bet ir bendrai vartojama su technologijomis susijusi terminija, taip pat į jame esančią dispoziciją buvo įtraukta daugiau alternatyvių veikų, išskirtos naujos nusikalstamą veiką kvalifikuojančios aplinkybės. Šiais pakeitimais buvo patikslintas ir nusikalstamos veikos dalykas – juo laikoma nebe įstatymo saugoma kompiuterinė informacija, o nevieši elektroniniai duomenys. Dispozicijoje šalia pasisavinimo ir įvairių informacijos paskleidimo variantų atsirado taip pat elektroninių duomenų neteisėto stebėjimo, fiksavimo, perėmimo, įgijimo, laikymo veikos. Be to, neteisėto elektroninių duomenų perėmimo ir panaudojimo sudėtyje numatyta šią veiką kvalifikuojanti aplinkybė, susijusi su padidinta neviešų elektroninių duomenų svarba – jų strategine reikšme nacionaliniam saugumui, didele reikšme valstybės valdymui, ūkiui ar finansų sistemai.

Pakeitimams tam tikra apimtimi turėjo įtakos tiek Konvencijos dėl elektroninių nusikaltimų, tiek Pamatinio sprendimo 2005/222/TVR nuostatos. Tačiau minint šiuos teisės aktus reikėtų atkreipti dėmesį į tai, kad Konvencijos dėl elektroninių nusikaltimų 3 straipsnyje kompiuterinių duomenų konfidencialumą pažeidžianti veika aprašyta daug siauriau nei ta, kuri įtvirtinta BK 198 straipsnyje. O Pamatinis sprendimas tokios nusikalstamos veikos tiesiogiai nenumato – jame elektroninių duomenų konfidencialumo apsauga gali būti susieta tik su IS konfidencialumu. Neišsamus Pamatiniame sprendime 2005/222/TVR esančių nusikalstamų veikų sąrašas koreguotas Direktyva 2013/40/ES. Jos 6 straipsnyje numatyta neteisėto duomenų perėmimo veika yra bene analogiška neteisėtos perimties veikai, apibrėžtai Konvencijos dėl elektroninių nusikaltimų 3 straipsnyje.

Taigi, analizuojant 2007 metų BK 198 straipsnio pokyčius, darytina išvada, kad jais pirminė šiai nusikalstamai veikai suteikta apimtis nebuvo siaurinta, o pagrindiniais pakeitimais siekta: 1) patikslinti sudėties požymius pagal konvencinių nuostatų reikalavimus; 2) perkeliant Pamatinį sprendimą 2005/222/TVR į nacionalinę teisę, suvienodinti visame BK XXX skyriuje vartojamą terminiją. Taip, atsižvelgiant į Konvencijos dėl elektroninių nusikaltimų 3 straipsnio reikalavimus, neteisėto elektroninių duomenų perėmimo ir panaudojimo nusikalstamoje veikoje atsirado elektroninių duomenų stebėjimo, fiksavimo ir perėmimo veikos. O įgyvendinant Pamatinio sprendimo nuostatas, straipsnyje įvestas elektroninių duomenų terminas bei numatytas BK XXX skyriui vieningas veikas kvalifikuojantis požymis, susijęs su padidinta IS ar elektroninių duomenų svarba.

Tačiau šis elektroninių duomenų konfidencialumo pažeidimų kriminalizavimo būdas nėra vienintelis. Konfidencialumo elektroninėje erdvėje apsaugai pasitelkus baudžiamosios teisės priemones užsienio valstybėse požiūris, kaip tai galima būtų padaryti ir kokia apimtimi elektroniniai duomenys turėtų būti saugomi, skiriasi.

Įvairią tokio pobūdžio nusikalstamų veikų elektroninėje erdvėje kriminalizavimo praktiką lėmė duomenų, kurie yra *laikomi IS*, ir duomenų, kurie yra *perduodami joje*, atskyrimas. Todėl elektroninių duomenų konfidencialumo pažeidimus bendriausia prasme galima analizuoti dviem aspektais: 1) kaip neteisėtą prieigą *prie duomenų, laikomų (saugojamų) IS* ir 2) kaip neteisėtą *duomenų, perduodamų IS*, perėmimą. Teigtina, kad tokiam atskyrimui pagrindą suteikė 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 suteikus atitinkamas diskrecijos ribas buvo sudarytos sąlygos skirtingai pažvelgti į galimus IS ir duomenų konfidencialumo pažeidimų kriminalizavimo variantus, atitinkamai atsirasti ir skirtingoms tokių veikų inkriminavimo problemoms.

Analizuojant pirmąjį elektroninių duomenų konfidencialumo pažeidimo aspektą – neteisėtą prieigą prie *duomenų, laikomų (saugomų) IS*, reikėtų priminti, kad kai kuriose užsienio valstybėse tokio pobūdžio veika dažnai susiejama su neteisėta prieiga prie IS. Šiais atvejais, kaip buvo minėta ankstesnėse dalyse, neteisėtos prieigos veikos esminiu aspektu laikomas elektroninių duomenų, o ne IS konfidencialumas[396]. Šis neteisėtos prieigos kriminalizavimo kelias pasirinktas, pavyzdžiui, Vokietijos baudžiamojo įstatymo 202a straipsnyje, kuriame kriminalizuotas duomenų šnipinėjimas (tokia veika pasireiškia duomenų, apsaugotų nuo neteisėtos prieigos, įgijimu, įveikiant apsaugą). Toks požiūris į neteisėtos prieigos veiką matyti ir Jungtinės Karalystės Netinkamo naudojimosi kompiuteriais akto 1 straipsnyje, kuriame ji aprašyta kaip neteisėtas privertimas kompiuterį atlikti bet kokią funkciją siekiant gauti prieigą prie programos arba duomenų, laikomų kompiuteryje, arba sudarant galimybes tokią prieigą gauti. Kaip nurodoma mokslinėje literatūroje (I. Walden, J. Clough, A. S. Blunn, C. Reed ir kt.)[397], tokiomis veikos kėsinamasi į duomenų, *laikomų (saugomų) IS, konfidencialumą*. Anot J. Clough, nusikalstamos veikos, „susijusios su neteisėta prieiga prie kompiuterio, išsivystė iki bendresnių, susijusių su duomenų, laikomų kompiuteryje, apsauga“[398]. I. Walden, taip pat atkreipė dėmesį į tai, kad šiais atvejais turimi mintyje „*nejudami duomenys*“ (angl. *data „at rest*“), t. y. duomenys, esantys sistemoje, prie kurios kaltininkas yra priėjęs arba joje padaręs pakeitimus“[399].

Antrasis elektroninių duomenų konfidencialumo pažeidimo aspektas, t. y. neteisėtas *duomenų, perduodamų IS*, perėmimas sietinas su kitu duomenų konfidencialumo pažeidimo lygmeniu. Apibūdinant šiuos duomenis, mokslinėje literatūroje apie juos bendriausia prasme kalbama kaip apie duomenis, perduodamus tinklais (angl. *data „in transmission*“)[400], per telekomunikacijos sistemą[401] ir pan. J. Clough, analizuodamas besikeičiantį elektroninių ryšių pobūdį, pažymėjo, kad nepriklausomai nuo to, ar „elektroninis paštas perduodamas telekomunikacijų tinklais, pranešimai vietiniais tinklais (LAN) ar vaizdai siunčiami be-

[396] Plačiau žiūrėti III dalies 1 skyriuje.

[397] Walden, I., *supra* note 70, p. 183; Clough, J., *supra* note 110, p. 135; Blunn, A. S. Report of the Review of the Regulation of Access to Communications. [interaktyvus]. Australija, 2005, p. 28, [žiūrėta 2013-06-01]. <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.

[398] Clough, J., *op. cit.*, p.135.

[399] Walden, I., *op. cit.*, p. 183.

[400] *Ibid*.

[401] Blunn, A. S., *op. cit.*, p. 28.

vieliu ryšiu yra potenciali galimybė, kad duomenys bus perimti“[402]. Iš tiesų vystantis ryšių technologijoms atsiranda ir nauji tokių veikų padarymo būdai („nusikalstama veika seka galimybę“)[403], todėl minėtas duomenų skirstymas į *laikomus IS* ir *perduodamus duomenis* leidžia akcentuoti visapusį duomenų saugumo poreikį. O analizuojamu aspektu ir apie būtiną subalansuotą duomenų, esančių elektroninėje erdvėje, konfidencialumo apsaugą.

Apžvelgus užsienio valstybių praktiką kriminalizuojant duomenų, esančių perdavimo procese, perėmimą, matyti, kad daugelyje valstybių tokie duomenų konfidencialumo pažeidimai kriminalizuoti kaip atskira veika (Vokietija, Jungtinė Karalystė, Kipras, Jungtinės Amerikos Valstijos ir kt.). Pavyzdžiui, minėta, kad Vokietijos baudžiamojo įstatymo 202a straipsnyje nustatyta atsakomybė už neteisėtą prieigą prie apsaugotų duomenų, jei buvo įveikta apsauga. Tuo tarpu 202b straipsnyje kalbama apie duomenų perėmimą techninėmis priemonėmis iš neviešo duomenų apdorojimo įrenginio arba iš duomenų apdorojimo įrenginio elektromagnetinio perdavimo. Toks neteisėtos prieigos prie IS laikomų ir perduodamų duomenų atskyrimas pasirinktas ir Jungtinėje Karalystėje. Atsakomybė už neteisėtą perėmimą yra nustatyta 2000 m. Tyrimo įgaliojimų reguliavimo akto[404] 1 dalyje. Joje neteisėtu perėmimu bendriausia prasme laikomas bet kokio pranešimo perėmimas jo perdavimo metu, jei tokie veiksmai buvo atlikti sąmoningai ir neturint teisėtų įgaliojimų atlikti perėmimą, be to, toks perėmimas turi būti padaromas bet kokioje Jungtinės Karalystės vietoje.

Reikalavimo numatyti baudžiamąją atsakomybę už *neteisėtą duomenų perėmimą* ištakos tiesiogiai siejamos su Konvencijos dėl elektroninių nusikaltimų 3 straipsniu. Jos aiškinamojoje ataskaitoje nurodoma, kad šiame straipsnyje esančių nuostatų tikslas yra „apsaugoti privatumo teisę perduodant duomenis“, nepriklausomai nuo tokios elektroninių duomenų perdavimo formos – telefonu, faksu, elektroniniu paštu ar rinkmenų perdavimą (51 punktas). Atitinkamai neteisėto perėmimo veikos požymių aprašymo baudžiamuosiuose įstatymuose variantai gali būti išvedami būtent iš konvencinių nuostatų. Konvencijos dėl elektroninių nusikaltimų 3 straipsnis įpareigoja nustatyti baudžiamąją atsakomybę už sąmoningą ir neteisėtą neviešo kompiuterinių duomenų perdavimo į kompiuterinę sistemą, iš jos ir jos viduje perimtį techninėmis priemonėmis. Šiame straipsnyje minima ir elektromagnetinės emisijos iš kompiuterinės sistemos, perduodančios tokius kompiuterinius duomenis, perimtis.

Analizuojant tiek pačios Konvencijos dėl elektroninių nusikaltimų 3 straipsnio nuostatas, tiek jos aiškinamojoje ataskaitoje pateiktus jų interpretavimo variantus, įmanoma išskirti keletą svarbių aspektų, kurie valstybėms suteikė galimybę apriboti šios nusikalstamos veikos „plotį“. Taigi siekiant išvengti neteisėto perėmimo veikos *perkriminalizavimo* grėsmės 1) konvencinės nuostatos numato galimybę susiaurinti neteisėto perėmimo veikos apibrėžtį į sudėtį įtraukiant tokius požymius kaip šios nusikalstamos veikos padarymas turint nesąžiningą ketinimą, taip pat jei buvo nustatyta, kad kompiuterinė sistema yra sujungta su kita kompiuterine sistema (3 straipsnis); 2) neteisėtos perimties veikoje taip pat numatyta galimybė reikalauti, kad tokia veika būtų padaryta panaudojant technines priemones – pasiekiant duomenis tiesiogiai (gavus prieigą ir naudojantis kompiuterine sistema) arba netiesiogiai (naudojant įvairias priemones, skirtas duomenų perėmimui). Kaip nurodoma Konvencijos aiškinamojoje ataskaitoje, techninių priemonių reikalavimas

[402] Clough, J., *supra* note 110, p. 135.

[403] Clough, J., *supra* note 210, p. 150.

[404] Regulation of Investigatory Powers Act. [interaktyvus], [žiūrėta 2013-06-01]. <http://www.legislation.gov.uk/ukpga/2000/23/section/1>.

gali būti laikomas tuo apribojimu, kuris leidžia išvengti neteisėto perėmimo nusikalstamos veikos *perkriminalizavimo* (53 punktas); 3) kadangi kompiuterinė sistema gali apimti ir radijo ryšį, tai Konvencijos aiškinamojoje ataskaitoje išaiškinta, kad valstybės nėra įpareigotos kriminalizuoti bet kokios radijo transliacijos perėmimą, kuri net ir būdama nevieša, yra pakankamai lengvai prieinama ir tokiu būdu gali būti perimta, pavyzdžiui, ir mėgėjo (56 punktas). Mokslinėje literatūroje aiškinama, kad tokie apribojimai tiesiogiai siejami su *Bluetooth* (angl. *blue tooth* – mėlynas dantis) technologijomis ir kitais įrenginiais, naudojančiais radijo bangas perduodant duomenis santykinai trumpais atstumais[405]. 4) Konvencijos 3 straipsnyje minimas neviešas duomenų perdavimo perėmimas. Pati sąvoka *neviešas* apibūdina perdavimo (komunikavimo) proceso, o ne perduotų duomenų pobūdį. Perduodami duomenys gali būti viešai prieinama informacija, bet perdavimas išlieka neviešu, jei jo dalyviai nori komunikuoti konfidencialiai. Todėl atitinkamai tokia nuostata *per se* nešalina atvejų, kai duomenimis yra keičiamasi viešai prieinamų ryšių tinklais (54 punktas).

Tuo tarpu analizuojant Lietuvos BK 198 straipsnyje numatytus neteisėto elektroninių duomenų perėmimo ir panaudojimo nusikalstamos veikos sudėties požymius matyti, kad tiek *duomenų, perduodamų IS*, tiek ir *duomenų, esančių joje,* konfidencialumo pažeidimai kriminalizuoti tame pačiame viename straipsnyje[406]. Be to, konstruojant šios nusikalstamos veikos sudėtį, nebuvo pasinaudota jos susiaurinimo galimybėmis bandant išspręsti neteisėto elektroninių duomenų perėmimo ir panaudojimo *perkriminalizavimo* problemas – nusikalstama veika nėra susieta, pavyzdžiui, nei su kaltininko nesąžiningais ketinimais, nei su techninių priemonių panaudojimu.

Taip numačius neteisėto elektroninių duomenų perėmimo ir panaudojimo nusikalstamą veiką BK, ji kelia nemažai inkriminavimo klausimų. Kadangi daugelis jų bus aptarti interpretuojant atskirus šios veikos sudėties požymius, tai prieš pereinant prie detalesnės jų analizės tikslinga aptarti bendresnes BK 198 straipsnio taikymo problemas. Viena svarbesnių – siejama su nusikalstamų veikų daugeto ir baudžiamojo įstatymo normų konkurencijos atskyrimu, atitinkamai ir teisingu kaltininko padarytų nusikalstamų veikų elektroninėje erdvėje kvalifikavimu.

Pirmiau minėta, kad daugeliui tradicinėmis laikomų nusikalstamų veikų „persikėlus“ į elektroninę erdvę, pakito jų sudėties požymių aiškinimas. Būtent pakankamai platus jų turinio interpretavimas leido užtikrinti ne tik ekvivalentų veiksmų fizinėje ir elektroninėje erdvėje vertinimą, bet taip pat padėjo „atrasti“ ir informacinių bei komunikacijos technologijų panaudojimo požymį. Tačiau šis aspektas iškėlė ir diskusinių klausimų, t. y. kokiais atvejais kvalifikuojant tradicines nusikalstamas veikas, padarytas elektroninėje erdvėje, yra būtinos nuorodos ir į BK XXX skyriuje esančias nusikalstamas veikas, o tiksliau į BK 198 straipsnį. Tokiai problemai atsirasti sudarė sąlygas plati neteisėto elektroninių duomenų perėmimo ir panaudojimo nusikalstamos veikos apibrėžtis, kai baudžiamoji atsakomybė nustatyta už įvairias alternatyvias veikas – neteisėtą neviešų elektroninių duomenų stebėjimą, fiksavimą, perėmimą, įgijimą, laikymą, pasisavinimą, paskleidimą ar kitokį pa-

[405] Clough, J., *supra* note 110, p. 138.

[406] 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).

naudojimą. Todėl dažni atvejai, 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 baudžiamųjų teisės normų konkurenciją.

Esant baudžiamosios teisės normų konkurencijai, anot V. Pavilonio, „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“[407]. Kadangi tokiais atvejais vieną nusikalstamą veiką visiškai atitinka keletas tarpusavyje konkuruojančių normų, tai pagal konkurencijos įveikimo taisykles sprendžiama, kurią iš jų taikyti. Analizuojamu aspektu aktuali bendrosios ir specialiosios normos konkurencijos įveikimo taisyklė, kai tokioms normoms tarpusavyje konkuruojant iš jų, kvalifikuojant veiką, taikoma speciali norma. Todėl atitinkamai, konkuruojant BK 198 straipsnyje esančiai bendrai normai ir kitoms normoms, numatančioms konkretesnius elektroninėje erdvėje padarytos nusikalstamos veikos požymius, taikytina būtent pastaroji speciali norma. Joje įtvirtintų nusikalstamos veikos sudėties požymiai visiškai atitinka padarytą nusikalstamą veiką. Tokie atvejai nėra pripažįstami nusikalstamų veikų daugetu ir veika papildomai pagal BK 198 straipsnį nėra kvalifikuojama. Tačiau literatūroje galima sutikti priešingų, todėl diskutuotinų bendros ir specialios normų konkurencijos įveikimo taisyklės aiškinimų. Komentuodami BK 198 straipsnį, R. Mockevičius ir D. Valatkevičius atkreipė dėmesį į tai, kad BK yra keletas straipsnių, numatančių atsakomybę už neteisėtus veiksmus su informacija, kuri, beje, gali būti ir elektroninių duomenų formos. Tačiau tokiomis veikomis tiesiogiai kėsinamasi ne į elektroninių duomenų saugumą, bet į kitus teisinius gėrius. Išskirdami keletą straipsnių, tarp jų, pavyzdžiui, BK 124, 210, 296 straipsnius, autoriai priėjo prie išvados, kad „jeigu padarytas nusikaltimas atitiks šiuose straipsniuose numatytą nusikaltimo sudėtį – o dalykas bus elektroniniai duomenys – veika turi būti papildomai kvalifikuojama ir pagal BK 198 straipsnį“[408].

Panaši nusikalstamų veikų kvalifikavimo taisyklė, nedarant skirtumo tarp baudžiamojo įstatymo normų konkurencijos ir nusikalstamų veikų daugeto, suformuluota ir I. Dauparaitės bei D. Štitilio. Šie autoriai, nagrinėdami įvairius tapatybės vagystės elektroninėje erdvėje kriminalizavimo aspektus Lietuvoje, išaiškino, kad „<...> tapatybės vagystės elektroninėje erdvėje atveju reikia kalbėti apie nusikalstamų veikų daugetą, t. y. šios pavojingos veikos atveju pavojingi ir priešingi teisei veiksmai gali būti kvalifikuojami kaip nusikalstamų veikų sutaptis pagal BK 198 str. ir kitus LR BK specialiosios dalies straipsnius <...>“[409]. Tarp kitų BK straipsnių yra minimi, pavyzdžiui, BK 182, 186, 207, 214, 215 straipsniai. Šiuo aspektu reikėtų pažymėti, kad kai apie sukčiavimą arba turtinės žalos padarymą apgaule ir tapatybės vagystę[410] galima iš tiesų kalbėti iš nusikalstamų veikų

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

[408] Abramavičius, A., *et al*., *supra* note 160, p. 431.

[409] Štitilis, D., *et al*., *supra* note 332, p. 257.

[410] Tai atvejai, kai baudžiamojo įstatymo norma joje numatytais nusikalstamos veikos sudėties požymiais neapima visų kaltininko padarytos nusikalstamos veikos aspektų. Todėl tiksliam kaltininko padarytos nusikalstamos veikos kvalifikavimui būtina parinkti keletą baudžiamojo įstatymo normų. Pavyzdžiui, Lietuvos Aukščiausiojo Teismo praktikoje suformuluota nuostata, kad „Neteisėtas elektroninės mokėjimo priemonės įgijimas bei inicijavimas ar atlikimas ja finansinės operacijos didesnės kaip 1 MGL dydžio sumos kvalifikuojamas kaip BK 182, 214, 215 straipsniuose numatytų nusikalstamų veikų sutaptis“ (Teismų praktikos sukčiavimo (Baudžiamojo kodekso 182 straipsnis) baudžiamosiose bylose apžvalgos 22 punktas. *Teismų praktika*.

daugeto pozicijų, tai vertinant BK 214, 215 ir 198 straipsniuose esančių normų santykį minėtos taisyklės taikymas abejotinas. BK 214 ir 215 straipsnyje numatytas dalykas – elektroninių mokėjimo priemonių naudotojų tapatybės patvirtinimo priemonių duomenys, pakankami finansinei operacijai inicijuoti, gali turėti nematerialią išraišką, atitinkamai šie duomenys būtų laikomi viena iš elektroninių duomenų rūšių, taigi ir konkrečiau įvardytais elektroniniais duomenimis. Kadangi šiuose straipsniuose numatytomis nusikalstamomis veikomis pirmiausia kėsinamasi į finansų sistemą, o ne elektroninių duomenų saugumą, tai padarytai nusikalstamai veikai atitinkant tiek BK 198 straipsnyje, tiek BK 214, tiek 215 straipsniuose numatytus nusikalstamos veikos požymius, turėtų būti taikomos specialios BK 214 ir 215 straipsnio normos – papildomos nuorodos į BK 198 straipsnį yra perteklinės. Priešinga praktika laikytina nukrypstančia nuo baudžiamosios teisės teorijoje ir teismų praktikoje nusistovėjusios bendrosios ir specialiosios normų konkurencijos įveikimo taisyklės. Beje, šiais atvejais minėtų nusikalstamų veikų daugetas nėra įžvelgiamas ir teismų praktikoje. Pavyzdžiui, Vilniaus miesto 1 apylinkės teismo 2009 m. rugsėjo 14 d. nuosprendyje baudžiamojoje byloje (bylos Nr. N1-1470-88/2009) konstatuota, kad M. J., be kitų nusikalstamų veikų, taip pat padarė BK 214 ir 215 straipsniuose numatytas veikas, t. y. jis neteisėtai įgijo elektroninės bankininkystės paslaugos naudotojo tapatybės patvirtinimo priemonių duomenis, pakankamus finansinei operacijai inicijuoti, kurie buvo įvesti į viešai prieinamus suklastotus elektroninės bankininkystės paslaugos internetinius tinklalapius, ir juos panaudodamas šią operaciją atliko. Šioje baudžiamojoje byloje pagrįstai kaltininko veiksmai papildomai pagal BK 198 straipsnį nekvalifikuoti. Pagal šį straipsnį neteisėtas tokio pobūdžio duomenų įgijimas ir panaudojimas inicijuojant finansinę operaciją nekvalifikuotas ir Kupiškio rajono apylinkės teismo 2009 m. rugsėjo 2 d. nuosprendyje baudžiamojoje byloje (bylos Nr. 1-53-100/2009).

Taigi BK 198 straipsnyje kriminalizuotas neteisėtas disponavimas *IS perduodamais* ir *joje laikomais* neviešais elektroniniais duomenimis. Suformuluota pakankamai plati šios nusikalstamos veikos apibrėžtis kelia nemažai jos inkriminavimo problemų, susijusių su šios nusikalstamos veikos *perkriminalizavimo* grėsme, taip pat su sunkumais sprendžiant, ar konkrečiu atveju susidurta su nusikalstamų veikų daugetu, ar su baudžiamosios teisės normų konkurencija.

2. Objektyvieji neteisėto elektroninių duomenų perėmimo ir panaudojimo sudėties požymiai

Neteisėto elektroninių duomenų perėmimo ir panaudojimo sudėties objektyvieji ir subjektyvieji požymiai padeda nustatyti, kiek plačiai įstatymų leidėjas siekė kriminalizuoti elektroninių duomenų konfidencialumo pažeidimus elektroninėje erdvėje. Sulyginus BK 198 straipsnio dispozicijoje aprašytos nusikalstamos veikos sudėties požymius su Konvencijos dėl elektroninių nusikaltimų nuostatomis (2, 3 straipsniai) matyti, kad nacionalinėje teisėje pasirinktas platesnis konfidencialumo pažeidimų kriminalizavimo variantas. Į nusikalstamos veikos sudėtį įtrauktos įvairios pavojingų veikų alternatyvos, sudarančios sąlygas ją inkriminuoti ne tik neteisėtos prieigos prie *IS perduodamų*, bet ir *joje laikomų (saugojamų) duomenų* atveju. BK 198 straipsnio taikymas nėra apribotas papildomais požymiais –

2010, Nr. 32). Neabejotina, kad tokia kvalifikavimo taisyklė būtų taikoma nustačius ir neteisėto naudotojo tapatybės patvirtinimo priemonių duomenų įgijimo, panaudojimo ir turtinės naudos gavimo atvejais.

tokiais kaip, pavyzdžiui, Konvencijoje numatytu nesąžiningu ketinimu, techninių priemonių panaudojimu ir pan. Viena vertus, tokia įstatymo leidėjo pozicija suprantama – gana plačiai kriminalizavus neteisėtą elektroninių duomenų perėmimą ir panaudojimą siekta nepalikti galimų spragų, kurios leistų išvengti baudžiamosios atsakomybės už veikas elektroninėje erdvėje. Tačiau, kita vertus, BK 198 straipsnyje numačius itin daug alternatyvių veikų, jų aiškiai nesusiejus su nusikalstamos veikos dalyku, pačios nusikalstamos veikos taikymo neapribojus papildomais požymiais, sukurtos šios elektroninių duomenų konfidencialumą pažeidžiančios nusikalstamos veikos inkriminavimo problemos.

Objektyviųjų požymių analizė rodo neteisėto elektroninių duomenų perėmimo ir panaudojimo sudėties netobulumą, atskleidžia gana chaotišką požiūrį į sudėties požymių tarpusavio santykį. Į BK 198 straipsnio dispoziciją įtrauktos įvairios pavojingų veikų alternatyvos, kurios tarpusavyje persidengia, palieka neaiškumų, kokiais neviešų elektroninių duomenų konfidencialumo pažeidimo atvejais turėtų būti taikomos. Be to, šiame straipsnyje naudojama terminija, dėl kurios išsamesnės diskusijos nekilo nei doktrinoje, nei teismų praktikoje, todėl iki dabar lieka neaišku, pavyzdžiui, kaip turėtų būti suprantamas neviešų elektroninių duomenų pasisavinimas, kai šalia jo numatytas ir neteisėtas duomenų įgijimas. Sukūrus vieną normą, skirtą tiek *IS perduodamų*, tiek ir *joje laikomų (saugomų) duomenų* konfidencialumo pažeidimams vertinti, kyla dvejonių, kokios veikų alternatyvos ir kokiais atvejais turėtų būti taikomos (ypač elektroninių duomenų stebėjimo, fiksavimo ir perėmimo atvejais). Nusikalstamos veikos dalyką įvardijus neviešais elektroniniais duomenimis, paliekamas atviras klausimas, kaip vertinti kaltininko veiksmus, jei visos nusikalstamos veikos metu duomenys keitė savo formą (pavyzdžiui, iš elektroninės į materialią juos užrašius, atspausdinus ir pan).

Kita probleminė situacija, kurią lemia pakankamai plačiai BK 198 straipsnyje aprašyta nusikalstama veika, susijusi su tokios nusikalstamos veikos *perkriminalizavimo* grėsme. Konstitucinio Teismo jurisprudencijoje ne kartą atkreiptas dėmesys į tai, kad įstatymų leidėjas baudžiamajame įstatyme nusikalstamomis gali įvardyti tik tas veikas, kurios iš tikrųjų pavojingos ir jomis daroma didelė žala asmens, visuomenės ir valstybės interesams arba dėl šių veikų kyla grėsmė, kad tokia žala bus padaryta (Konstitucinio Teismo 2004 m. gruodžio 29 d., 2006 m. sausio 16 d. nutarimai). Nustatant teisinius apribojimus bei atsakomybę už teisės pažeidimus, būtina laikytis protingumo reikalavimo, proporcingumo principo, pagal kurį nustatytos teisinės priemonės turi būti būtinos demokratinėje visuomenėje ir tinkamos siekiamiems teisėtiems, neturi varžyti asmens teisių labiau, nei reikia šiems tikslams pasiekti (Konstitucinio Teismo 2004 m. gruodžio 13 d., 2004 m gruodžio 29 d., 2005 m. rugsėjo 29 d., 2006 m. sausio 16 d. nutarimai). Tačiau analizuojant neteisėto elektroninių duomenų perėmimo ir panaudojimo veiką, tam tikrose situacijose gali kilti abejonių, ar šių Konstitucinio Teismo jurisprudencijoje suformuluotų reikalavimų konstruojant nusikalstamos veikos sudėtį buvo laikytasi. Pavyzdžiui, BK 198 straipsnyje minima neviešų elektroninių duomenų stebėjimo veika, kurios taikymas veda prie nenuspėjamos šio straipsnio apimties, kai bet koks žvilgtelėjimas į neviešus elektroninius duomenis gali būti vertinamas kaip apysunkis nusikaltimas. Todėl svarbu atkreipti dėmesį į tai, kad stebėjimas, kaip teisinis požymis, pavojingumo prasme gali turėti labai skirtingų formų, todėl negali būti nustatinėjamas ir pripažįstamas automatiškai. Beje, su panašiomis elektroninių duomenų perėmimo ir panaudojimo pakankamo pavojingumo nustatymo problemomis gali būti susiduriama taikant ir kitas sudėtyje numatytas veikų alternaty-

vas. Tokią situaciją lėmė įstatymo leidėjo pozicija kriminalizuojant elektroninių duomenų konfidencialumo pažeidimus – vieninteliai BK 198 straipsnyje numatyti šios nusikalstamos veikos taikymo apribojimai yra elektroninių duomenų neviešumas (objektyvusis požymis) ir tyčinės kaltės reikalavimas (subjektyvusis požymis).

2.1. Nevieši elektroniniai duomenys kaip nusikalstamos veikos dalykas

Duomenų konfidencialumą elektroninėje erdvėje pažeidžiančios nusikalstamos veikos dalyko apibrėžties problemos, atsižvelgiant į technologinio neutralumo principo taikymą, įvairiose valstybėse yra sprendžiamos skirtingai. Daugumoje jų baudžiamojo įstatymo lygmeniu šis nusikalstamos veikos sudėties požymis paliktas neapibrėžtas (pavyzdžiui, Prancūzija, Vokietija, Estija, Lietuva ir kt.). Kitose (pavyzdžiui, Kipras, Bulgarija, Dominikos Respublika, Rusija) priešingai – bandoma pateikti nors ir bendro pobūdžio, tačiau esmines elektroninių duomenų (informacijos) savybes numatančius apibrėžimus. Tokiais atvejais sulyginimo sunkumus, be kita ko, kelia ir dalykui įvardyti pasirinkti skirtingi terminai, pavyzdžiui kompiuterizuoti (Bulgarija), kompiuteriniai duomenys (Kipras, Dominikos Respublika), kompiuterinė informacija (terminas, išaiškintas Rusijos baudžiamojo įstatymo 272 straipsnio dispozicijoje) ir pan.

Neteisėtas elektroninių duomenų perėmimo ir panaudojimo dalykas Lietuvos BK 198 straipsnio 1 dalies dispozicijoje įvardytas kaip nevieši elektroniniai duomenys. Kitokia formuluotė aprašant šį sudėties požymį vartojama BK 198 straipsnio 2 dalyje esančioje kvalifikuotoje neteisėto elektroninių duomenų perėmimo ir panaudojimo sudėtyje – joje minimi strateginę reikšmę nacionaliniam saugumui arba didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turintys nevieši elektroniniai duomenys. Tačiau nepriklausomai nuo to, apie kurį – platesnę ar siauresnę reikšmę turintį dalyko požymį kalbama, jų struktūroje galima išskirti du aspektus: 1) technologinį (elektroniniai duomenys) ir 2) teisinį (elektroninių duomenų neviešumas).

Be to, reikėtų atkreipti dėmesį į tai, kad nors Lietuvos BK nėra pateikiamas autentiškas BK XXX skyriuje vartojamų sąvokų išaiškinimas, tačiau kriterijus, leidžiančius duomenis priskirti elektroninių duomenų rūšiai, galima nustatyti tiek iš Konvencijos dėl elektroninių nusikaltimų ir Pamatinio sprendimo nuostatų, tiek ir iš nacionalinės teisės aktų bei teismų praktikos.

2.1.1. Elektroninių duomenų samprata

Analizuojant tiesiogiai su technologijomis susijusį neteisėto elektroninių duomenų perėmimo ir panaudojimo dalyko aspektą – pačius elektroninius duomenis, tenka kalbėti ir apie technologijų ir terminologijos klausimą. Jis, kaip jau buvo galima pastebėti, yra neišvengiamas nusikalstamų veikų sudėtyse *expressis verbis* įtvirtinus technologijas žyminčius terminus. Taigi analizuojant minėtą nusikalstamos veikos dalyko aspektą, reikėtų aptarti tas baudžiamosios teisės kontekste kylančias elektroninių duomenų interpretavimo problemas, kurios bendriausia prasme susijusios su: 1) duomenų ir informacijos tarpusavio ryšio nustatymu; 2) elektroninių duomenų sąvokos apibrėžimu.

Pirmoji problema aktuali tuo, kad pasirinktas duomenų arba informacijos terminas lemia platesnį arba priešingai – siauresnį požiūrį į alternatyviomis veikomis (stebėjimu, fik-

savimu, įgijimu ir kt.) padaromus konfidencialumo pažeidimus. Be to, pagrindą analizuoti duomenų ir informacijos santykį suteikia 2007 metais priimti BK XXX skyriaus pakeitimai. Primintina, kad įsigaliojus 2000 m. BK, jo XXX skyriuje su elektroninių duomenų konfidencialumo pažeidimais susijusiose normose vietoj duomenų vartotas informacijos terminas (pavyzdžiui, BK 198 straipsnyje, kuriame buvo kriminalizuotas *kompiuterinės informacijos pasisavinimas ir skleidimas*). Toks pasirinktas sudėties požymių aprašymas mokslinėje literatūroje susilaukė nemažai kritikos, atkreipiant dėmesį į tai, kad įstatymų leidėjas duomenų ir informacijos skirtumo BK XXX skyriuje neįžvelgė[411]. Todėl ištaisant šį trūkumą, 2007 metų BK pakeitimais BK XXX skyriuje atsisakyta *kompiuterinės informacijos* sąvokos ir pradėta vartoti kita – *elektroniniai duomenys*. Tokios pasikeitusios įstatymo leidėjo pozicijos ištakų reikėtų ieškoti duomenų ir informacijos skirtumuose.

Dauguma autorių (B. Burgis, D. Dzemydienė, R. Naujikienė, R. T. Potter, K. C. Laudon, J. R. Gordon ir kt.), vertindami duomenų ir informacijos sąsają, yra priėję prie vieningos nuomonės, kad šios sąvokos nėra tapačios ir, siekiant tikslumo, turėtų būti vartojamos pagal jų tikrąją prasmę. Analizuojant duomenis, svarbu pažymėti, kad jie turi primityvią, vienetinę reikšmę, kuri mokslininkų, nagrinėjusių įvairius duomenų ir informacijos tarpusavio ryšio aspektus, išreiškiama vartojant *neapdorotų faktų*[412], *fundamentalių faktų be konteksto*[413], *pirminių apibūdinimų, neturinčių konkrečios reikšmės*[414], *simbolių grupių, kurių pranešimo reikšmės lygmuo yra žemiausias*[415] pasakymus. Jie reiškia ne ką kitą, o tai, kad duomenys nesiejami su jų galima reikšme adresatui. Taigi galima būtų pritarti nuomonei, kad duomenys yra potenciali informacija, t. y. „duomenys virsta informacija, kai tam tikram subjektui jie tampa suprantami“[416]. Todėl duomenų suvokimo, jų prasmės, naudos įgijimo žmogui akcentavimas, analizuojant informacijos sąvoką, matyti daugelio autorių darbuose[417]. Anot R. T. Potter, „informacija reiškia duomenis tada, kai jie yra pateikti taip, kad turi reikšmės ir vertės gavėjui“[418]. Artimą šiam apibrėžimui pateikė ir C. K. Laudon su J. P. Laudon – pagal juos informacija reiškia duomenis, kai jie „pateikti tokia forma, kad būtų prasmingi ir naudingi žmogui“[419]. Lietuvos autorių darbuose informacija taip pat suprantama panašiai: informacija tai „duomenys, turintys prasmę; kitaip sakant, duomenys virsta informacija, kai tam tikram subjektui jie tampa suprantami“[420]. Tam tikrais atvejais darbuose akcentuojamas ir duomenų formos bei turinio tinkamumas naudoti, kuris leidžia tenkinti žmonių informacinius poreikius[421]. Taigi apibendrinus, būtų galima teigti, kad duomenys yra tam tikra „žaliava“[422] informacijai gauti.

---

411 Civilka, M., *et al*., *supra* note 9, p. 529.
412 Laudon, K. C.; Laudon, J. P., *supra* note 225, p. 8.
413 Gordon, J. R.; Gordon, S. R., *supra* note 230, p. 6.
414 Potter, R. T., *et al*., *supra* note 243, p. 5.
415 Dzemydienė, D.; Naujikienė, R., *supra* note 227, p. 12.
416 Skyrius, R.; Mikalauskienė, A.; Zalieckaitė, L., *supra* note 103, p. 7.
417 Potter, R. T., *op. cit.*, p. 5; Laudon, K. C.; Laudon, J. P., *op. cit.*, p. 5; Skyrius, R.; Mikalauskienė, A.; Zalieckaitė, L., *supra* note 103, p. 7; Wacks, P., *Personal Information: Privacy and the Law*. Oxford: Clarendon Press, 1989, p. 25.
418 Potter, R. T., *et al*., *op. cit.*, p. 5.
419 Laudon, K. C.; Laudon, J. P., *op. cit.*, p. 8.
420 Skyrius, R.; Mikalauskienė, A.; Zalieckaitė, L., *op. cit.*, p. 7.
421 Saulis, A.; Vasilecas, O., *supra* note 226, p. 9–10.
422 Skyrius, R.; Mikalauskienė, A.; Zalieckaitė, L., *op. cit.*, p. 7.

Šios tam tikros informacijos apibrėžtys rodo, kad duomenų sąvoka yra platesnė nei informacija, ir tą itin svarbu suvokti kalbant apie duomenų ir informacijos santykį baudžiamosios teisės kontekste. Netinkamo termino pasirinkimas gali lemti pernelyg siauras nusikalstamų veikų, kuriomis pažeidžiamas konfidencialumas, apimtis. Juo labiau kad vartojant duomenų arba informacijos terminą reikėtų atsižvelgti į tai, kad informacinių procesų dalyviai yra ne tik žmonės, bet ir IS. Atitinkamai ne visi IS atliekami duomenų apdorojimo (tvarkymo) veiksmai ir šių veiksmų metu gauti duomenys suvokiami ir matomi žmogui, kaip potencialios informacijos gavėjui.

Todėl šios nusikalstamos veikos dalyką susiejus su informacijos terminu, jo reikalaujamas duomenų suvokimas gali lemti, kad nuo neteisėto poveikio konfidencialumui lieka neapsaugoti duomenys, egzistuojantys *iki informacinėje* stadijoje[423]. Tuo tarpu baudžiamojo įstatymo lygmeniu, autorės nuomone, 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. Į tokį duomenų konfidencialumo aspektą atkreipė dėmesį ir I. Walden, kurio nuomone, „grėsmės privatumui kyla surenkant neapdorotus duomenis prieš juos transformuojant į informaciją, kuri gali būti naudojama žmogaus“[424]. Todėl baudžiamajame įstatyme numačius duomenų, o ne informacijos terminą, akivaizdu, kad analogiškos baudžiamosios teisės priemonės, nustačius konfidencialumo pažeidimus, būtų taikomos ankstesnėje nei duomenų virtimo informacija stadijoje. Toks požiūris leidžia padaryti svarbią išvadą, kad informacinių technologijų srityje išsakoma nuomonė, jog *informacijos vertė sąlygiškai didesnė negu duomenų*[425], įtakos nustatant baudžiamąją atsakomybę už įvairius elektroninių duomenų konfidencialumo pažeidimus neturi. Konfidencialumo prasme tiek duomenys, tiek ir informacija, kvalifikuojant kaltininko padarytas veikas pagal BK 198 straipsnį, turėtų būti laikomi lygiaverčiais (pavyzdžiui, toks požiūris aktualus tais atvejais, kai duomenų konfidencialumas bandomas apsaugoti juos perduodant ryšių tinklais tarp IS, kai duomenys yra nei matomi, nei suprantami žmogui ir pan.).

Tačiau, analizuojant užsienio valstybių praktiką kriminalizuojant įvairius elektroninėje erdvėje padaromus konfidencialumo pažeidimus, matyti, kad teisėkūros lygmenyje ne visuomet suteikiama svarba duomenų ir informacijos skirtumams. Todėl vienose valstybėse (pavyzdžiui, Vokietijoje, Portugalijoje, Kipre ir kt.) nusikalstamų veikų, bendriausia prasme susijusių su neteisėta prieiga prie duomenų, dalykas įvardijamas kompiuterinių duomenų terminu, tuo tarpu kitose (Rusija, JAV ir kt.) vartojamas kompiuterinės informacijos arba tiesiog informacijos terminas. Tačiau šis pastebėjimas reikalauja tam tikro patikslinimo – nusikalstamos veikos dalyku laikant informaciją skirtumas tarp jos ir duomenų gali būti ir nedaromas. Tačiau tai kad šie terminai dažniausiai pripažįstami sinonimais, leidžia pastebėti, pavyzdžiui, Rusijos autorių pateikti *kompiuterinės informacijos* kaip Rusijos baudžiamojo įstatymo 272 straipsnyje numatytos nusikalstamos veikos (ne-

[423] Priklausomai nuo kaltininko tyčios kryptingumo tokie atvejai galėtų būti vertinama tik iš parengtinės nusikalstamos veikos pozicijų.

[424] Walden, I., *supra* note 70, p. 14.

[425] Dzemydienė, D.; Naujikienė, R., *supra* note 227, p. 12.
Tokia išvada daroma dėl to, kad su duomenimis turi būti atliekami įvairūs veiksmai juos padarant tinkamais naudoti žmogui. Informacija gaunama apdorojus duomenis, tai gali būti formatavimas, filtravimas, sumavimas, analizė ar kitos sudėtingesnės operacijos.

teisėtos prieigos prie kompiuterinės informacijos) dalyko apibrėžimai. Juose apibūdinant informaciją vartojamas būtent duomenų terminas. Anot N. I. Vetrov, kompiuterinė informacija – tai „patys įvairiausi duomenys apie asmenis, daiktus, faktus, įvykius, reiškinius ir procesus, nepriklausomai nuo jų pavaizdavimo formos, kurie užfiksuoti kompiuterinėje laikmenoje arba perduodami telekomunikacijos kanalais tokios formos, kuri yra tinkama apdoroti kompiuteriui“[426]. Duomenų terminas apibūdinant informaciją taip pat minimas kitų autorių darbuose, todėl kompiuterinės informacijos apibrėžimas yra panašus į anksčiau minėtą, t. y. kompiuterinė informacija suprantama kaip „duomenys, esantys vienoje iš kompiuterinės informacijos laikmenų (kietasis diskas, išorinės laikmenos <...>), kurie gali būti perduodami kompiuterių komunikacijos kanalais ir jų manipuliavimas galimas tik naudojant kompiuterį“[427].

Nustačius informacijos ir duomenų tarpusavio santykį, tikslinga pereiti prie antrojo anksčiau iškelto klausimo, kaip baudžiamosios teisės kontekste turėtų būti suvokiami elektroniniai duomenys. Tam tikrų sunkumų, atskleidžiant šią sąvoką, kelia tai, kad šalia jos taip pat vartojama kompiuterinių duomenų sąvoka. Be to, būtent pastaroji minima Konvencijoje dėl elektroninių nusikaltimų ir Pamatiniame sprendime 2005/222/TVR.

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 vykdyti tam tikrą funkciją“. Pamatinio sprendimo 2005/222/TVR 1 straipsnio b punkte kompiuteriniai duomenys apibūdinti kaip „faktai, informacija ar sąvokos, pateiktos tokia forma, kuri tinkama tvarkyti informacinėje sistemoje, įskaitant programą, tinkamą tam, kad informacinė sistema atliktų funkciją“. Kaip matyti, šių apibrėžimų esminis aspektas yra duomenų tinkamumas juos apdoroti IS (kompiuterinėje sistemoje). Atsižvelgiant į IS veiklos principus, akivaizdu, kad duomenų apdorojimo joje galimybės turėtų būti siejamos su duomenų forma, leidžiančia su jais atlikti įvairias operacijas (veiksmus). Todėl Konvencijos dėl elektroninių nusikaltimų aiškinamojoje ataskaitoje (25 punktas) kompiuteriniai duomenys susieti su elektroniniais ar kitos tiesiogiai apdorojamos formos duomenimis. Iš Pamatinio sprendimo 2005/222/TVR aiškinamajame memorandume pateikto išaiškinimo galima matyti, kad duomenys tampa kompiuteriniais duomenimis, kai jie sukuriami arba perkeliami į tokią formą, kuri tinkama juos apdoroti IS. Todėl ši sąvoka, pavyzdžiui, neapima tokių fizinių daiktų kaip knyga. Tačiau knyga bus laikoma kompiuteriniais duomenimis, jei ji išsaugota elektronine forma (laikoma kompiuterinių duomenų pavidalu) arba į tokią formą perkelta nuskaitymo būdu.

Atkreiptinas dėmesys į tai, kad Konvencijoje dėl elektroninių nusikaltimų ir Pamatiniame sprendime 2005/222/TVR suformuluotos kompiuterinių duomenų sąvokų ištakos siejamos su anksčiau darbe aptartu ISO/IEC 2382-1:1996 standartu. Šiame standarte duomenys apibrėžti kaip „formalizuotas informacijos vaizdinys, tinkamas perduoti kitiems, suvokti ir apdoroti“. Be to, jame nurodoma, kad duomenys gali būti apdorojami rankiniu būdu arba automatinėmis priemonėmis. Todėl tokia duomenų savybė kaip jų *tinkamumas apdoroti automatinėmis priemonėmis* tapo minėtuose teisės aktuose pateiktos kom-

[426] Vetrov, N. I. *Ugolovnoe pravo. Osobennaja chast: uchebnik* [Criminal law. Special Part: Textbook]. 2-oe izd. Moskva: JUNITI-DANA: Zakon i pravo, 2002, c. 369.

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

piuterinių duomenų sąvokos ašimi. Taip pat, manytina, būtent dėl to tiek Konvencijoje dėl elektroninių nusikaltimų, tiek Pamatiniame sprendime 2005/222/TVR kompiuteriniai duomenys apibrėžiami bene identiškai.

Kaip minėta, dėl technologinio neutralumo principo taikymo daugumos valstybių baudžiamuosiuose įstatymuose kompiuterinių duomenų sąvoka nėra pateikiama, taip sudarant galimybes vystytis su technologijomis susijusioms teisės normoms. Tačiau tose valstybėse, kur vis dėlto bandoma apibrėžti šį nusikalstamos veikos dalyką, kompiuterinių duomenų sąvoka suformuluota pakankamai abstrakčiai – jos esminiu aspektu paliekant duomenų formą, leidžiančią juos apdoroti IS (kompiuterinėje sistemoje). Pavyzdžiui, Bulgarijos Respublikos baudžiamojo įstatymo[428] 93 straipsnio 22 punkte kompiuterizuoti duomenys apibūdinti kaip „bet koks faktų, informacijos ar sąvokų pateikimas tokia forma, kuri yra tinkama automatiniam apdorojimui, įskaitant kompiuterio programą“. Panašiai kompiuteriniai duomenys apibrėžti Kipro Respublikos įstatymo Nr. 22 (III) 04[429] 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“. Kartu tokie kompiuterinių duomenų apibrėžimai leidžia pastebėti ir pakankamai didelę Konvencijos dėl elektroninių nusikaltimų ir Pamatinio sprendimo 2005/222/TVR nuostatų įtaką juos konstruojant. Taigi būtent šių teisės aktų nuostatos lėmė bene identišką valstybių, esančių Europos Sąjungos narėmis arba (ir) ratifikavusių minėtą Konvenciją, suvokimą, kas turėtų būti laikoma kompiuteriniais duomenimis. Beje, panašus požiūris į nusikalstamos veikos, pažeidžiančios kompiuterinės informacijos konfidencialumą, dalyką yra susiformavęs ir tose valstybėse, kurios nepriklauso minėtų valstybių grupei.

Pavyzdžiui, Rusijos Federacijos baudžiamajame įstatyme kompiuterinę informaciją, kaip vieną iš informacijos rūšių, apibūdinantys požymiai įtraukti į 272 straipsnyje esančios nusikalstamos veikos sudėtį (neteisėta prieiga prie kompiuterinės informacijos). Šiame straipsnyje kompiuterine informacija laikoma ta, kuri yra automatiniu būdu apdorojamose laikmenose, kompiuteryje, kompiuterinėje sistemoje arba jų tinkle. Nors, kaip matyti, kompiuterinė informacija apibrėžiama naudojant ne *tinkamumo apdoroti kompiuterinėje sistemoje*, o tokios *informacijos buvimo vietos* kriterijumi, tačiau būtent jos buvimas sistemoje (suvokiamoje bendriausia prasme), tam tikroje jos dalyje ar laikmenoje sudaro sąlygas šią informaciją apdoroti automatiniu būdu. Todėl įvairūs autoriai, interpretuodami, kaip turėtų būti suprantama kompiuterinė informacija, naudoja vieną iš šių kriterijų. Taip, pavyzdžiui, O. Ja. Baev ir V. A. Meshherkov kompiuterinę informaciją apibrėžė kaip tą, 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“[430]. Tuo tarpu kiti autoriai, akcentuodami tokių duomenų neatskiriamumą nuo kompiuterinės sistemos, laikosi

[428] Criminal Code of the Republic of Bulgaria. [interaktyvus], [žiūrėta 2013-06-01]. <http://www.vks.bg/english/vksen_p04_04.htm#Section_I_>.
Bulgarijos Respublika Konvenciją dėl elektroninių nusikaltimų ratifikavo 2005 m. balandžio 7 d.

[429] Cyprus Law No. 22(III)04. [interaktyvus], [žiūrėta 2013-01-19]. <http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/CountryProfiles/cyber_cp_%20Cyprus_2007_June.pdf>.
Kipro Respublika Konvenciją dėl elektroninių nusikaltimų ratifikavo 2005 m. sausio 19 d.

[430] Mazurov V. A., *supra* note 157, p. 33.

nuomonės, kad jų apibrėžimui pakanka to, kuris numatytas baudžiamajame įstatyme[431]. Atitinkamai, vadovaujantis *informacijos būvimo vietos kriterijumi*, bandoma konkretizuoti (išvardijant galimus variantus), kur tokio pobūdžio informacija gali būti randama. Pavyzdžiui, „operatyvioje kompiuterio atmintyje esanti informacija, informacija, esanti kitose kompiuterinėse laikmenose, tiek prijungtose prie kompiuterio, tiek ir išoriniuose kaupikliuose, įskaitant diskelius, lazerinius ir kitokius diskus“[432]. Be to, neteisėta prieiga prie kompiuterinės informacijos bus ir tais atvejais, kai informacija perimta ją perduodant kompiuterių tinklais. Taigi galima teigti, kad, naudojant skirtingus – *tinkamumo apdoroti kompiuterinėje sistemoje* ir *informacijos buvimo vietos* – kriterijus, kompiuterinės informacijos apibrėžimas neišvengiamai iš dalies skiriasi, tačiau neteisėtos prieigos prie informacijos dalyko specifinės savybės išlika tos pačios. Aiškus ryšys tarp duomenų formos, leidžiančios ją apdoroti IS (kompiuterinėje sistemoje), ir pačių duomenų buvimo tokioje sistemoje matomas analizuojant duomenis informacinių ir komunikacijos technologijų srityje. Bendriausia prasme joje duomenys apibrėžiami kaip „kompiuterio apdorojami objektai – visa, kas laikoma kompiuterio laikmenose“[433], arba kaip „faktų, sudarytų iš skaičių, ženklų ir simbolių, rinkinys, laikomas kompiuteryje tokiu būdu, kad jis gali būti apdorojamas kompiuteriu“[434].

Aptariant Lietuvos BK 198 straipsnio dispozicijoje nurodyto nusikalstamos veikos dalyko požymius, pastebėtina, kad įgyvendinus konvencines ir Pamatinio sprendimo 2005/222/TVR nuostatas vis dėlto pasirinkta ne kompiuterinių, o elektroninių duomenų sąvoka. Pats autentiškas elektroninių duomenų išaiškinimas dėl technologinio neutralumo principo taikymo BK nėra pateiktas, tačiau tam tikri elektroninių duomenų interpretavimo variantai matomi kituose nacionaliniuose teisės aktuose. Juose, beje, taip pat kaip BK XXX skyriuje, vartojamas būtent elektroninių, o ne kompiuterinių duomenų terminas. Pavyzdžiui, Lietuvos Respublikos elektroninio parašo įstatymo (toliau – Elektroninio parašo įstatymas)[435] 2 straipsnio 2 dalyje elektroniniai duomenys apibūdinti kaip „visi duomenys, kurie tvarkomi informacinių technologijų priemonėmis“. Panašus elektroninių duomenų apibrėžimas pateiktas 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“[436] 3 punkte. Jame elektroniniai duomenys apibrėžti kaip „duomenys, pateikti tokia forma,

---

[431] *Kommentarij k ugolovnomu kodeksu Rossijskoj Federacii* [Commentary to the Criminal Code of the Russian Federation]. Naumova, A. V. (red.). Moskva: Jurist, 1996, s. 663; *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, s. 502; *Ugolovnoe pravo Rossii. Osobennaja chast: uchebnik* [Russian criminal law. Special Part: The textbook]. Rarog A. I. (red.). Moskva: Ehksmo, 2010, s. 526.

[432] *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, s. 502.

[433] Dagienė, V., *et al*., *supra* note 251, p. 96.

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

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

[436] 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.

kuri tinkama juos tvarkyti informacinėje sistemoje“. Tokių bene identiškų sąvokų ištakos siejamos su anksčiau aptartu Konvencijoje dėl elektroninių nusikaltimų ir Pamatiniame sprendime 2005/222/TVR esamu kompiuterinių duomenų apibrėžimu. Todėl aiškinant neteisėto elektroninių duomenų perėmimo ir panaudojimo nusikalstamos veikos dalyką – elektroninius duomenis – akivaizdi šių teisės aktų įtaka.

Kaip matyti, būtent *tinkamumo apdoroti automatinėmis priemonėmis* kriterijus, kuris naudotas konstruojant elektroninių duomenų sąvoką nacionalinėje teisėje ir kuris buvo laikomas pagrindu formuluojant kompiuterinių duomenų sąvoką minėtuose tarptautiniuose ir Europos Sąjungos teisės aktuose, parodo daug elektroninių ir kompiuterinių duomenų panašumų. Analizuojant pateiktus apibrėžimus, iš pirmo žvilgsnio gali atrodyti, kad pagrindinis kriterijus, naudojamas atribojant šias sąvokas, yra technologijos, kuriomis duomenys apdorojami. Pavyzdžiui, Konvencijoje dėl elektroninių nusikaltimų minima kompiuterinė sistema, Pamatiniame sprendime 2005/222/TVR – IS, nacionalinėje teisėje – tiek IS, tiek ir IT. Ši atskyrimo problema siejama su minėtu *technologijų ir terminologijos klausimu*, kuris nuolat kyla bandant apibrėžti įvairias technologijas žyminčias sąvokas. Šiuo aspektu reikėtų atkreipti dėmesį į tai, kad anksčiau darbe nagrinėjant neteisėto prisijungimo prie IS (BK 198[1] straipsnis) dalyko problematiką, buvo prieita prie išvados, kad, analizuojant IS, IT ir kompiuterinę sistemą, bendriausia prasme turimos mintyje panašios technologijos[437]. Todėl ir kompiuteriniai bei elektroniniai duomenys, autorės nuomone, turėtų būti taip pat suvokiami panašiai[438], pirmumą teikiant būtent jų formai, o ne bandymams konkrečiai įvardyti šiuos duomenis apdorojančias technologijas[439]. Tai leistų išvengti nusikalstamos veikos, numatytos BK 198 straipsnyje, dalyko apibrėžties nepagrįsto susiaurinimo pavojaus.

Nuo minėtų 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. Pavyzdžiui, Vilniaus miesto 2 apylinkės teismo 2011 m. liepos 1 d. nuosprendyje baudžiamojoje byloje (bylos Nr. 1-188-387/2011) viena iš kaltininko padarytų nusikalstamų veikų kvalifikavimo problemų buvo susijusi su neteisėto elektroninių duomenų perėmimo ir panaudojimo inkriminavimo pagrįstumu. Teismas pabrėžė, kad BK 198 straipsnio 1 dalyje *numatyto nusikaltimo dalykas yra elektroniniai duomenys. Elektroniniai duomenys – tai duomenys, kurie tvarkomi informacinių technologijų priemonėmis. Elektroniniai duomenys turi būti sukurti elektronine forma arba perkelti į tokią formą. Elektroniniai duomenys apima ir kompiuterines programas ar programinę įrangą.* Nors kaltininko padarytų nusikalstamų veikų kvalifikavimo problema vėliau buvo sprendžiama tiek apeliacinės instancijos, tiek ir kasaciniame teisme[440], tačiau pats elektroninių duomenų suvokimas šioje byloje nekito. Vilniaus apygardos teismo 2011 m. gruodžio 23 d. nuosprendyje šioje baudžiamojoje byloje (bylos Nr. 1A-977/2011) taip pat pateiktas iš esmės identiškas elektroninių duomenų apibrėžimas. Teismas nurodė, kad *BK*

[437] Plačiau apie IS, IT ir kompiuterinės sistemos santykį žiūrėti III dalies 2.1 poskyryje.

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

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

[440] Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų 2012 m. birželio 26 d. nutartis baudžiamojoje byloje (bylos Nr. 2K-375/2012).

198 str. numatyto nusikaltimo dalykas yra elektroniniai duomenys, kurie įvardijami, kaip duomenys, tvarkomi informacinių technologijų priemonėmis ir yra sukurti elektronine forma arba perkelti į tokią formą. Taip pat elektroniniai duomenys įvardijami ir, kaip ženklų seka, skirta perduoti informacijai, naudojant informacines technologijas.

Taigi teigtina, kad, norint duomenis pripažinti elektroniniais duomenimis, jie turi būti arba sukurti, arba perkelti į elektroninę formą. Be to, akivaizdu, kad kaip tokie jie gali egzistuoti tik būdami IS, suvokiamoje pačia bendriausia prasme (ne tik kompiuteriuose, bet ir faksuose, mobiliuosiuose telefonuose, elektroninių ryšių tinkluose, internete[441], taip pat įvairiuose informacijos kaupikliuose, pavyzdžiui, kompaktiniuose diskuose, USB atmintinėse ir pan.). Todėl pagal BK 198 straipsnį nekvalifikuotini kėsinimaisi į tokių duomenų konfidencialumą, iš kurių tik gali būti formuojami elektroniniai duomenys (pavyzdžiui, įvairūs užrašai, schemos ir pan.), tačiau jie dar neperkelti į tokią formą. Šie duomenys neatitinka specifinių elektroninių duomenų perėmimo ir panaudojimo nusikalstamos veikos dalyko savybių. Tačiau toks aiškinimas kelia nemažai problemų sprendžiant, ar pagal BK 198 straipsnį kvalifikuotina veika, jei elektroniniai duomenys jos eigoje keitė šią formą[442].

Taigi elektroninių duomenų apibūdinimui gali būti pasitelkiami du – jų *tinkamumo apdoroti IS* ir tokių *duomenų buvimo vietos* – kriterijai. Pirmasis jų nurodo duomenų formą, kuri yra atpažįstama IS, atitinkamai su tokiais duomenimis IS gali atlikti įvairius veiksmus. Antrasis kriterijus taip pat gali padėti apibūdinti elektroninius duomenis, tačiau jis reikalauja gana detalių nuorodų į technologijas – kur konkrečiai IS elektroniniai duomenys gali būti randami. Vertinant šiuos kriterijus taip pat svarbi glaudi jų tarpusavio sąsaja – galimybės apdoroti duomenis siejamos su jų specifine (elektronine) forma, kuri išlaikoma, jei duomenys yra įvedami į IS. Taigi abu šie kriterijai padeda aiškiau suprasti, kokiomis savybėmis pasižymi BK 198 straipsnyje esančios nusikalstamos veikos dalykas. Analizuojant nacionalinėje teisėje pateiktus elektroninių duomenų apibrėžimus matyti, kad juose akcentuojama galimybė juos tvarkyti IT ar IS priemonėmis. Nors pačioms technologijoms įvardyti yra vartojami šie abu terminai, tačiau atsižvelgiant į BK XXX skyriuje esančią terminiją ir siekiant išvengti probleminių situacijų atribojant IS, IT bei komunikacijos technologijas, autorės nuomone, tiksliau elektroninius duomenis įvardyti kaip apdorojamus IS, o ne IT.

2.1.2. Elektroninių duomenų formos kitimo įtaka duomenis 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 pirmiau aptarti *tinkamumo juos apdoroti IS* ir tokių *duomenų buvimo vietos* kriterijai. Neteisėto elektroninių duomenų perėmimo ir panaudojimo nusikalstamos veikos aprašymo būdas suponuoja tai, kad kiekviena dispozicijoje nurodyta alternatyvi pavojinga veika (pavyzdžiui, įgijimas, laikymas, paskleidimas) turėtų būti siejama būtent su elektroniniais duomenimis ir jų konfidencialumo pažeidimais. Toks šios nusikalstamos veikos dalyko interpretavimas reiškia, kad įvairūs neteisėti veiksmai su duomenimis, esančiais ne elektroninės formos (neatitinkančiais minėtus kriterijus), į BK 198 straipsnio reguliavimo sritį

[441] Abramavičius, A., *et al*., *supra* note 160, p. 418.

[442] Plačiau apie duomenų formos kitimo įtaką nusikalstamos veikos kvalifikavimui pagal BK 198 straipsnį žiūrėti IV dalies 2.1.2 poskyryje.

nepatenka. Tačiau šis požiūris atskleidžia ir gana sudėtingas neteisėto elektroninių duomenų perėmimo ir panaudojimo inkriminavimo problemas, kurias sukūrė pasirinktas minėtos nusikalstamos veikos aprašymo būdas.

Sunkumų, sprendžiant, kokias ir kiek alternatyvių veikų padarė kaltininkas, paprastai neturėtų kelti tie atvejai, kai jų metu elektroniniai duomenys neprarado šios formos. Pavyzdžiui, Mažeikių rajono apylinkės teismo 2009 m. rugpjūčio 12 d. nuosprendyje baudžiamojoje byloje (bylos Nr. 1-188-785/2009) 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 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 internetiniame puslapyje* <...>. Atsižvelgiant į tai, teismas pripažino R. R. kaltu pagal BK 198 straipsnio 1 dalį.

Kiek kitokia situacija yra tada, kai neteisėtai disponuojama duomenimis, kurie elektroninę formą išsaugoja tik nusikalstamos veikos pradžioje, o vėlesni kaltininko veiksmai atliekami su duomenimis, kurie yra nebe elektroninės formos, o turi materialią išraišką (pavyzdžiui, yra užrašyti, atspausdinti ir pan.). Tokiais atvejais kyla abejonių, ar kaltininkui inkriminuotinos tos BK 198 straipsnyje numatytos alternatyvios veikos, kurios padarytos disponuojant elektroninę formą praradusiais duomenimis. Pavyzdžiui, faktinės bylos aplinkybės gali rodyti, kad kaltininkas neteisėtai stebėjo elektroninius duomenis, vėliau atsispausdindamas juos įgijo ir paskleidė jau nebe elektroninės formos, o užfiksuotus popieriuje. Būtent į tokią probleminę situaciją, analizuojant duomenų kopijavimo vertinimo variantus, atkreiptas dėmesys ir mokslinėje literatūroje. Šiuo klausimu joje yra susiformavusios dvi skirtingos pozicijos – vienų autorių nuomone (S. A. Pashin ir kt.), kopijavimu gali būti pripažinti tik tie veiksmai, kai duomenys yra perkeliami iš vienos kompiuterinės laikmenos (kompiuterio) į kitą kompiuterinę laikmeną (kompiuterį)[443]. Tuo tarpu kiti autoriai (N. I. Vetrov, A. V. Naumov ir kt.)[444] išreiškia kiek lankstesnį požiūrį, kopijavimu pripažindami ir tuos veiksmus, kuriais duomenys perkeliami iš elektroninės į bet kokią kitą formą. Pastaroji nuomonė reikšmės kopijavimo būdams nesuteikia – jie įtakos nusikalstamos veikos kvalifikavimui neturi, nes baudžiamosios teisės priemonėmis yra saugomi elektroniniai duomenys nepriklausomai nuo jų buvimo vietos (ar jie būtų užfiksuoti popieriuje, ar išsaugoti išorinėje informacijos laikmenoje ir pan.).

Šiuo aspektu analizuojant BK 198 straipsnyje numatytas alternatyvias veikas iš tiesų lieka neaišku, kaip turėtų būti vertinamos situacijos, kai elektroniniai duomenys neteisėtai atspausdinami ir kaip spausdintas variantas laikomi bei vėliau tokios formos paskleidžiami. Ar kaltininkui tokiais atvejais gali būti inkriminuojamas ne tik elektroninių duomenų įgijimas, bet ir elektroninių duomenų laikymas bei paskleidimas, kai įgyjami, laikomi ir paskleidžiami duomenys yra praradę elektroninę formą? Šios problemos sprendimas priklauso nuo to, kam aiškinant BK 198 straipsnį bus teikiamas prioritetas, ar duomenų

[443] Mazurov V. A., *supra* note 157, p. 107.

[444] Vetrov, N. I., *supra* note 426, p. 370; Naumov, A. V. Rossijskoe ugolovnoe pravo: kurs lekcij [Russian criminal law: the course of lectures]. 4-asis leidimas. Moskva: Volters Kluver, 2007, s. 283.

išraiškos formai (dalykui būdingoms savybėms), ar vis dėlto duomenų elektroninės formos reikalavimai bus keliami tik pirminiam duomenų šaltiniui. Kaip matyti, nors ir iš itin negausios teismų praktikos, elektroninių duomenų konfidencialumo pažeidimai pripažįstami ir tada, kai elektroniniai duomenys savo formos neišsaugoja visų kaltininko padarytų pavojingų veikų metu. Pavyzdžiui, Šiaulių miesto apylinkės teismo 2011 m. liepos 18 d. teismo baudžiamuoju įsakymu byloje (bylos Nr. 1-617-885/2011) V. Š., 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, šeimyninę padėtį, išduotus asmens tapatybės dokumentus, darbovietę, pajamas, šiuos duomenis neteisėtai įgijo, atspausdinant valstybinės mokesčių inspekcijos kompiuterinės duomenų bazės išrašus (pažymas), po to, neteisėtai įgytus neviešus minėtus elektroninius duomenis neteisėtai paskleidė <...> per kelis kartus perduodamas G. L.* Taigi, kaip matyti, ta aplinkybė, kad elektroniniai duomenys buvo atspausdinti ir tokio formos paskleisti, netrukdė teismui konstatuoti, kad V. Š. stebėjo, įgijo ir paskleidė elektroninius duomenis. Manytina, kad tokią teismo poziciją lėmė tai, jog įgyti ir paskleisti buvo nevieši duomenys, kurių pirminis šaltinis išliko elektroninės formos.

Tokiais ir jiems panašiais atvejais priėjus prie kitokios išvados būtų sukurta nelogiška situacija, kai, pavyzdžiui, asmens, įgijusio prieš tai neteisėtai atspausdintus elektroninius duomenis, veiksmai pagal BK 198 straipsnį negalėtų būti kvalifikuojami (jei nenustatytas bendrininkavimo faktas). Taip pat laikymo ir paskleidimo veikos negalėtų būti inkriminuojamos asmeniui, kuris laikė ir paskleidė neteisėtai atsispausdintus elektroninius duomenis.

Tačiau kita vertus reikėtų pripažinti, kad toks neteisėto elektroninių duomenų perėmimo ir panaudojimo sudėties požymių interpretavimas ne visiškai atitinka to, kaip ši nusikalstama veika yra aprašyta BK 198 straipsnio dispozicijoje, tačiau jis yra vienas iš būdų, kuriais sprendžiamos alternatyvių veikų inkriminavimo kaltininkui problemos. Jas, kaip minėta, kelia pats požymių parinkimas konstruojant neteisėto elektroninių duomenų perėmimo ir panaudojimo nusikalstamos veikos sudėtį. Nusikalstamos veikos dalyką įvardijus elektroniniais duomenimis, neišvengiamai tenka spręsti jau minėtą 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. Pastarasis požiūris, lemiantis pakankamai platų normos aiškinimą, gali sukelti ir papildomų problemų – pavyzdžiui, kaip vertintinos situacijos, kai duomenys išlieka tik materialioje formoje, t. y. nelieka pirminių elektroninių duomenų. Be to, dauguma neviešų elektroninių duomenų gali būti saugoma ir materialia forma, tada neteisėtai įgijus būtent tokios formos duomenis (nepriėjus prie elektroninių duomenų) nusikalstamai veikai kvalifikuoti taip pat turėtų būti taikomas BK 198 straipsnis. Įsitvirtinus tokiam nusikalstamos veikos dalyko interpretavimui ir atitinkamai padarytų pavojingų veikų vertinimui, galima spėti, kad, be kita ko, neišvengiamai tektų įrodinėti, jog materialią formą turintys duomenys anksčiau turėjo kitą – elektroninę formą. Be to, toks įrodinėjimas būtų būtinas ir tais atvejais, kai pirminiai elektroniniai duomenys yra išlikę, tiek ir tais atvejais, kai pirminių elektroninių duomenų nebėra.

Šiuo aspektu reikėtų atkreipti dėmesį į tai, kad nusikalstamos veikos sudėtyje numatant tiek elektroninę, tiek materialią formą galinčius turėti duomenis (informaciją) kaip

nusikalstamos veikos dalyką, BK yra vartojamas materialaus objekto, kurio turinys ar informacija apie jį yra, pavyzdžiui, tarnybos paslaptis (BK 296 straipsnis), valstybės paslaptis (BK 124 straipsnis). Tokiu atveju duomenų (informacijos) formos kitimas iš elektroninės į materialią ar atvirkščiai problemų inkriminuojant alternatyvias veikas neturėtų kelti. Tuo tarpu BK 198 straipsnyje tiesiogiai vartojant elektroninių duomenų terminą šių duomenų formos kitimo problema lieka neišspręsta. Todėl svarstytina, ar šiuos elektroninių duomenų požymio inkriminavimo sunkumus negalėtų išspręsti pakeista dalyko formuluotė iš neviešų elektroninių duomenų į materialų objektą, kurio turinys yra nevieši elektroniniai duomenys. Toks nusikalstamos veikos dalykas, be abejo, galėtų būti vartojamas tik vietoj *IS laikom*ų, o ne *joje perduodam*ų neviešų elektroninių duomenų.

2.1.3. Elektroninių duomenų ir informacinės sistemos ryšys

Savarankiška BK 198 straipsnyje numatytos nusikalstamos veikos dalyko interpretavimo problema susijusi su IS ir elektroninių duomenų tarpusavio ryšiu. Iš pirmo žvilgsnio atrodančios visiškai nesusijusios sąvokos iš tikro pagal Konvencijos dėl elektroninių nusikaltimų ir Pamatinio sprendimo 2005/222/TVR nuostatas yra tarpusavyje persipynusios. Jų sąsaja atspindi dar vieną technologijų ir terminologijos klausimo aspektą, svarbų sprendžiant, kiek nusikalstamų veikų kaltininkas padarė elektroninėje erdvėje ir ar jis pažeidė tik IS, ar ir elektroninių duomenų konfidencialumą.

Konvencijoje dėl elektroninių nusikaltimų ir Pamatiniame sprendime 2005/222/TVR kompiuteriniai duomenys ir kompiuterinė sistema (IS) bandyti vienas nuo kito atskirti, pateikiant savarankiškas 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 minint ne kompiuterinę, o IS, yra suformuluota Pamatiniame sprendime 2005/222/TVR. Jame IS apibrėžiama kaip „prietaisas arba tarpusavyje sujungtų ar susijusių prietaisų grupė, iš kurių vienas arba daugiau pagal programą vykdo automatinį kompiuterinių duomenų tvarkymą, taip pat juose saugomi, tvarkomi, iš jų išrenkami arba jais perduodami kompiuteriniai duomenys turint tikslą juos apdoroti, panaudoti, apsaugoti ir prižiūrėti“. Kaip matyti, šiuose apibrėžimuose elektroninių duomenų ir IS ryšys yra perteiktas per bene pagrindinę IS funkciją – elektroninių duomenų apdorojimą (tvarkymą) pagal programą. Detaliau analizuojant elektroninių duomenų ir IS ryšį galima pastebėti gana įdomią situaciją – elektroninių duomenų atskyrimas nuo IS tampa sudėtingu aiškinantis programinės įrangos statusą IS apdorojant elektroninius duomenis. Ši problema išryškėja minėtuose dokumentuose elektroniniams duomenims priskyrus ir programą (programinę įrangą), pagal kurią IS gali vykdyti tam tikrą funkciją[445].

Aiškinantis, kas yra programinė įranga, reikėtų atkreipti dėmesį į tai, kad ji minima Konvencijos aiškinamojoje ataskaitoje (23 punktas) ir Pamatinio sprendimo 2005/222/TVR

[445] 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 vykdyti tam tikrą 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*“.

aiškinamajame memorandume. Juose išaiškinta, kas turėtų būti laikoma IS ir kompiuterinės sistemos sąvokose minimu įtaisu ar tarpusavyje sujungtų įtaisų grupe. Tiek vienu, tiek ir kitu atveju įtaisas apibūdintas per jo sudedamąsias dalis – aparatinę (angl. *hardware*) ir programinę (angl. *software*) įrangą. Šie komponentai yra būtini, nes aparatinė įranga be programinės įrangos pati savaime neturi duomenų apdorojimo gebėjimų[446]. Todėl būtent dėl programinės įrangos kompiuteris yra laikomas *intelektualiu informacijos apdorojimo įrankiu*[447].

Toks minėtuose dokumentuose išreikštas požiūris į elektroninių duomenų ir programinės įrangos (programos) ryšį nėra naujas. Jis atitina bendrą suvokimą, kad tiek kalbant apie kompiuterio darbe naudojamas operacines sistemas, tiek apie taikomą programinę įrangą visais atvejais neišvengiamai bus turimi mintyje ir elektroniniai duomenys. Tai atspindi vieną iš klasikinių kompiuterių struktūros sudarymo idėjų, kad programą sudarančios komandos „užkoduojamos kaip ir apdorojamieji duomenys ir nesiskiria nuo kitos informacijos“[448]. Todėl, pavyzdžiui, anot D. Dulinsko ir J. Dulinskienės, „operacine sistema vadinamas specialių programų ir duomenų rinkinys, sukurtas kompiuterinės sistemos ištekliams valdyti, kompiuterio programų kūrimui palengvinti ir šių programų vykdymui valdyti“[449]. Operacinės sistemos vartotojui suteikia bendrąsias kompiuterio valdymo paslaugas, o konkrečioms užduotims vykdyti pasitelkiamos taikomosios programos. Tačiau ir taikomųjų programų atveju turimos mintyje ne tik komandos, bet ir elektroninių duomenų visuma, būtina konkretiems veiksmams atlikti[450].

Toks požiūris parodo ir dvejopą elektroninių duomenų statusą. Konvencijoje dėl elektroninių nusikaltimų ir Pamatiniame sprendime 2005/222/TVR atskirai apibrėžus elektroninius duomenis, jie bandyti atskirti nuo IS, tačiau, aiškinant IS sąvoką elektroniniai duomenys neišvengiamai tampa IS dalimi. Todėl pagrįstu galima laikyti I. Walden išsakytą pastebėjimą, kad „duomenys neturėtų būti matomi kaip kažkas atskiro nuo technologijų, nes visuomet egzistuoja dvejopumas vartojant šį terminą“[451]. Todėl, anot autoriaus, vienas diskusinių klausimų, sprendžiant duomenų ir IS atskyrimo problemą, yra tiesiogiai susijęs su kompiuterio programinės įrangos (programos) teisiniu vertinimu. Tokiu atveju galimybės atriboti duomenis ir IS priklausys nuo to, ar programinė įranga (programa) bus laikoma viena iš elektroninių duomenų formų, ar vis dėlto programinė įranga bus atskirta nuo duomenų ir laikoma priemone, padedančia apdoroti duomenis.

Šis vienas iš technologijų ir terminologijos problemos aspektų tiesiogiai siejamas su nusikalstamų veikų, pažeidžiančių elektroninių duomenų ir IS konfidencialumą, kvalifikavimo problemomis. Elektroninių duomenų ir IS atskyrimu pagrįstas visų *CIA nusikalstamų veikų* aprašymas Konvencijoje dėl elektroninių nusikaltimų. Joje atskirai numatytos veikos pažeidžiančios IS ir elektroninių duomenų saugumą (konfidencialumą, integralumą ir prieinamumą). Beje, šiuo atskyrimu, įgyvendinant konvencines nuostatas, vadovautasi ir konstruojant *CIA nusikalstamų veikų* sudėtis Lietuvos BK XXX skyriuje. Jame atskirai nustatyta atsakomybė už neteisėtą prisijungimą prie informacinės sistemos (198[1] straips-

[446] Jonušauskas, S.; Bilevičienė, T.; Kažemikaitis, V., *supra* note 136, p. 14.
[447] Kiškis, M. *et al*., *supra* note 8, p. 20.
[448] Kanapeckas, P., *et al. Kompiuterių elementai* [elektroninis išteklius]. Kaunas: Technologija, 2011, p. 475.
[449] Dulinskas, D.; Dulinskienė, J. *ECDL visiems: kompiuterinio raštingumo pagrindai*. Kaunas: Informacinių technologijų mokymo centas, 2006, p. 15.
[450] *Ibid*.
[451] Walden, I., *supra* note 70, p. 14–15.

nis) ir neteisėtą elektroninių duomenų perėmimą ir panaudojimą (198 straipsnis) kaip konfidencialumo pažeidimus. Taip pat atskirai kriminalizuotas neteisėtas poveikis elektroniniams duomenims (196 straipsnis) ir informacinei sistemai (BK 197 straipsnis) kaip integralumo ir prieinamumo pažeidimai. Viena vertus, toks atskyrimas yra pagrįstas (pavyzdžiui, elektroninių duomenų, kurie nėra programinė įranga, atveju), tačiau, kita vertus, elektroninių duomenų ir IS glaudi sąsaja gali kelti klausimų, kiek nusikalstamų veikų kaltininkui turėtų būti inkriminuojama.

Pavyzdžiui, nusikalstama veika kvalifikuojama pagal BK 198[1] straipsnį, jei nustatoma, kad kaltininkas neteisėtai prisijungė prie IS pažeisdamas jos apsaugos priemones. BK 198 straipsnyje numatyta atskira elektroninių duomenų konfidencialumą pažeidžianti veika, kuri, be kitų alternatyvų, gali pasireikšti ir neteisėtu neviešų elektroninių duomenų stebėjimu ar kitokiu panaudojimu. Taigi kaltininkas, neteisėtai prisijungdamas prie IS, gauna prieigą prie sistemos ir galimybes ja neteisėtai naudotis – prieiti prie sistemos išteklių, atitinkamai ir prie programinės įrangos. Atsižvelgiant į tai, ar programinė įranga laikoma IS dalimi ar elektroniniais duomenimis, neteisėtas jos panaudojimas ir veikimo stebėjimas gali būti arba priešingai – nekvalifikuotinas pagal BK 198 straipsnį. Todėl toks „definicinis neaiškumas“[452] kelia teisės problemų ir atitinkamai klausimų, kaip jos turėtų būti sprendžiamos. Bandant rasti galimus jų sprendimo variantus reikėtų atkreipti dėmesį į tai, kad galimybes IS funkcionuoti suteikia abi – tiek aparatinė, tiek ir programinė – įranga, todėl be vienos iš jų duomenų apdorojimas taptų neįmanomas. Atitinkamai kaltininkui gavus prieigą prie IS, tolesni jo neteisėti veiksmai sistemoje negalimi be vienokio ar kitokio programinės įrangos panaudojimo. Autorės nuomone, tokiais atvejais programinė įranga turėtų būti atskirta nuo elektroninių duomenų ir laikoma priemone, padedančia apdoroti duomenis IS. Todėl kaltininko veiksmai, atliekant įvairius neteisėtus veiksmus sistemoje tiesiog pasinaudojant programine įranga (programa), pagal BK 198 straipsnį kaip kitoks neteisėtas elektroninių duomenų panaudojimas nekvalifikuotini. Toks bendro pobūdžio pastebėjimas vis dėlto neneigia visų aplinkybių analizės svarbos, todėl galima pritarti mokslinėje literatūroje išsakomai nuomonei, kad „<...> skirtingas traktavimas galimas remiantis atliktos veikos pobūdžiu, patirta žala ir (ar), kaltininko kalte, bet ne abejotinu [elektroninių duomenų ir IS – aut. pastaba] ir neparemtu techniniu atskyrimu“[453].

Taigi apibendrinus galima būtų teigti, kad IS ir elektroninių duomenų atskyrimo problemos kyla dėl to, kad elektroniniais duomenimis pagal Konvencijos dėl elektroninių nusikaltimų ir Pamatinio sprendimo 2005/222/TVR nuostatas pripažįstama ir programinė įranga (programa). Pati programinė įranga yra neatskiriama IS dalis – tiek ji, tiek ir aparatinė įranga užtikrina IS galimybes atlikti įvairius duomenų apdorojimo veiksmus. Kadangi BK XXX skyriuje atskirai kriminalizuoti elektroninių duomenų (198 straipsnis) ir IS konfidencialumo (198[1] straipsnis) pažeidimai, tai gali kilti neaiškumų, ar kaltininko neteisėti veiksmai sistemoje, kurių atlikimui sąlygas sudaro programinės įrangos neteisėtas panaudojimas, turėtų būti kvalifikuojami pagal BK 198 straipsnį (kaip kitoks neteisėtas elektroninių duomenų panaudojimas). Autorės nuomone, programinė įranga tokiais atvejais turėtų būti atskirta nuo elektroninių duomenų ir laikoma tiesiog priemone, padedančia apdoroti duomenis IS. Be abejo, tokia išvada negali paneigti poreikio įvertinti visas aplinkybes – veikos pobūdį, sukeltas pasekmes, kaltininko tyčios kryptingumą ir pan.

[452] Walden, I., *supra* note 70, p. 160.
[453] *Ibid*.

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 tokių duomenų apsaugai nustatytų reikalavimų. Tai verčia analizuoti du tarpusavyje susijusius aspektus – neviešų elektroninių duomenų sampratą ir iš tokių duomenų neviešumo kylančius įvairius įpareigojimus elgtis su jais tinkamai (nesikišti, neatskleisti ir pan.).

Pats neviešumo požymis, apibūdinantis nusikalstamos veikos dalyką ir būtinas konstatuojant elektroninių duomenų konfidencialumo pažeidimus, yra tiesiogiai minimas tiek Konvencijos dėl elektroninių nusikaltimų 3 straipsnyje, tiek ir neteisėto elektroninių duomenų perėmimo ir panaudojimo nusikalstamos veikos sudėtyje, numatytoje BK 198 straipsnyje. Tačiau palyginus, kokiu aspektu neviešumas minimas šiuose teisės aktuose, galima pamatyti nemažai esminių skirtumų.

Konvencijoje dėl elektroninių nusikaltimų neviešumas apibūdina kompiuterinių duomenų perdavimo procesą. Jos aiškinamajame rašte neviešumas interpretuojamas jį siejant ne su kompiuteriniais duomenimis, o su tokių duomenų perdavimu, t. y. „terminas neviešas apibūdina perdavimo (komunikavimo) proceso pobūdį, bet ne perduodamų duomenų pobūdį“ (54 punktas). Taigi siunčiami duomenys gali būti viešai prieinama informacija, tačiau komunikavimo dalyviai gali siekti, kad pats toks duomenų perdavimas būtų konfidencialus. Tačiau analizuojant šios Konvencijos 3 straipsnyje numatytos neteisėtos perimties nusikalstamos veikos požymius akivaizdu, kad toks aiškinimas aktualus analizuojant IS perduodamų duomenų neteisėtą gavimą, bet ne tada, kai apie duomenis kalbama kaip apie „*nejudamus duomenis*“. Taip pat neviešas duomenų perdavimo pobūdis, o ne nevieši elektroniniai duomenys minimi Direktyvos 2013/40/ES 6 straipsnyje.

Aiškinant BK 198 straipsnyje kriminalizuotą nusikalstamą veiką, matyti, kad įstatymų leidėjas pasuko kiek kita linkme – jis neviešumą susiejo ne su duomenų perdavimo procesu, o su nusikalstamos veikos dalyku – elektroniniais duomenimis. Viena vertus, toks pasirinkimas gali būti suprantamas dėl to, kad minėtame BK straipsnyje kriminalizuoti ne tik perduodamų, bet taip pat ir IS laikomų duomenų konfidencialumo pažeidimai, tačiau, kita vertus, toks pasirinkimas kelia problemų. Viena jų – kaip turėtų būti vertinami tie atvejai, kai naudojant technines priemones perimami vieši elektroniniai duomenys, nors patį komunikavimo procesą buvo siekta išlaikyti konfidencialų. Taip pat nėra aišku, ar baudžiamoji atsakomybė kaltininkui galėtų kilti tais atvejais, kai, pavyzdžiui, pažeidus elektroninių duomenų apsaugos priemones, gaunama prieiga prie viešų elektroninių duomenų. Beje, elektroninių duomenų viešumo faktas nesusipažinus su pačiu elektroninių duomenų turiniu kaltininkui galėjo būti ir nežinomas. Šios situacijos kelia pagrindinį klausimą, ar neviešumas turėtų būti siejamas tik su duomenų turiniu, ar vis dėlto apie jį įmanoma kalbėti ir tada, kai prieiga prie tokių duomenų buvo apsunkinta. Pavyzdžiui, nustačius prieigos prie elektroninių duomenų kontrolę, siekta apriboti galimybę pašaliniams asmenims sužinoti, kokie duomenys yra laikomi IS. Aptartais atvejais, atsižvelgiant į esamą nusikalstamos veikos dalyko formuluotę, BK 198 straipsnyje numatytos nusikalstamos veikos inkriminavimas taptų probleminis arba net ir neįmanomas, nors tam tikru aspektu elektroninių duomenų konfidencialumo pažeidimai galėtų būti konstatuoti.

Aiškinantis neviešų elektroninių duomenų sampratą pirmiausia tikslinga aptarti patį viešumo suvokimą. Viešas, vadovaujantis lingvistiniu aiškinimu, apibūdinamas kaip visiems skirtas, visuomenės naudojamas[454] ir bendrinėje kalboje gali būti pakeičiamas sinonimais neuždaras, neslepiamas[455]. Neapriboto prieinamumo prie informacijos kriterijus naudojamas ir Lietuvos Respublikos visuomenės informavimo įstatymo 2 straipsnio 74 punkte apibūdinant viešąją informaciją, kuri apibrėžta kaip informacija, skirta viešai skleisti, išskyrus pornografinio pobūdžio informaciją, taip pat kaip informacija, kuri pagal Lietuvos Respublikos įstatymus negali būti viešai skleidžiama. Todėl suteikiant priešingą reikšmę viešumui, t. y. kalbant apie neviešus elektroninius duomenis, turėtų būti pabrėžiamas jų viešas neskelbtinumas, slaptumas, konfidencialumas. Prieigos prie informacijos suvaržymai, anot J. van der Hoven, gali būti laikomi „informacinio neteisingumo" prevencija. Patį „informacinį neteisingumą" šis autorius aiškino atsižvelgdamas į M. Walzen išsakytas idėjas apie „prieigos erdvę" ir susiejo su nepagarba riboms, kurias nustato minėta sfera[456]. Taigi elektroninių duomenų neviešumo pažeidimais gali būti laikomi neleistini ribų nepaisymai, duomenų sričių atskyrimo ignoravimai, duomenų perkėlimai už konfidencialumo erdvės ribų. Tokie atvejai galimi tiek tada, kai nevieši duomenys yra žinomi tik šių duomenų subjektui, tiek ir esant konfidencialiam ryšiui, t. y. tam tikromis sąlygomis patikėjus duomenis kitiems asmenis arba jiems leidus atlikti veiksmus, kurie suteikia galimybę sužinoti viešam skleidimui neskirtus duomenis. Mainais duomenų gavėjas prisiima įsipareigojimus nepadaryti žalos duomenų subjektui ir neperduoti jų trečiajam asmeniui be duomenų subjekto sutikimo[457].

Konfidencialumo aspektą turintys santykiai gali susiklostyti tarp įvairių subjektų, atitinkamai konfidencialumo įpareigojimai dažnai atsiranda įvairiuose kontekstuose. Bendriausia prasme galima būtų išskirti du neviešumo pagrindus: 1) objektyvų, kai elektroninių duomenų viešumo apribojimus nustato įstatymai ar kiti teisės aktai; 2) subjektyvų, kai prieigos prie elektroninių duomenų apribojimai atsiranda dėl asmenų tarpusavio susitarimų ir pan. Todėl sprendžiant, kas turėtų būti laikoma neviešais elektroniniais duomenimis, svarbu apibrėžti konfidencialumo (neviešumo) erdvės ribas. Kaip teigia N. C. Manson ir O. O'Neill, kalbant apie konfidencialumą turima mintyje įvairių rūšių turinio apsauga, kai komunikavo santykio šalys tokį turinį „siekia apsaugoti, yra susitarusios apsaugoti arba yra įpareigotos apsaugoti"[458]. Bendriausia prasme neviešumas tampa svarbus tada, kai duomenys gaunami konfidencialiai nuo kitų asmenų ir negali būti perduoti pašaliniams be duomenų subjekto sutikimo. Kadangi tokios situacijos yra įvairios, tai mokslinėje literatūroje[459] diskusijos dėl konfidencialumo užtikrinimo poreikio ar konkrečių įpareigojimų plėtojamos duomenis jungiant į grupes pagal

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

[455] Lyberis, A. *Sinonimų žodynas*. Vilnius: Lietuvos kalbos instituto leidykla, 2002, p. 558.

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

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

[458] *Ibid*., p. 126.

[459] 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., *supra* note 457, p. 126.

atitinkamus kriterijus. Tai, pavyzdžiui, gali būti asmens duomenys[460], komercinės, profesinės veiklos srityse naudojami duomenys ir daugelis kitų, kai tikimasi jų konfidencialumo apsaugos. Šis neviešų elektroninių duomenų grupavimo būdas yra pakankamai natūralus, nes tokių duomenų kategorija yra itin plati, į ją patenka pagal savo pobūdį įvairūs duomenys. Juos dažnai gali jungti ne pats duomenų turinys, bet ir tam tikri reikalavimai jų konfidencialumui užtikrinti. Būtent apsaugos lygis kaip vienas iš išorinių duomenis apibūdinančių požymių laikytinas tuo kriterijumi, kuris padeda duomenis suskirstyti į dvi grupes – viešus duomenis ir viešai neskelbiamus (neviešus) duomenis[461]. Vidinis neviešų elektroninių duomenų grupavimas sudarė sąlygas mokslinėje literatūroje suformuluoti „informacijos talpyklos modelį“, taip pat į duomenis metaforiškai pažvelgti kaip į asmens „kvazi – fizinius daiktus“, kurie kaip ir tam tikra informacija gali būti slepiami, laikomi arba perkeliami, perduodami[462].

Neviešų elektroninių duomenų skirstymas į grupes padeda aiškiau suvokti ir paties neviešumo ribas – kadangi į atskirą „talpyklą“ patenka tik tam tikros rūšies duomenys, tai paprasčiau atrasti ir vidinius šiuos duomenis jungiančius kriterijus, taip pat nustatyti įpareigojimus, kurie, atsižvelgiant į „talpykloje“ esančių duomenų pobūdį, apibrėžtų įvairių atliekamų veiksmų su jais reikalavimus. Neviešumo požymio, apibūdinančio teisinį elektroninių duomenų aspektą, nustatymui būtina kaskart įvertinti konkrečios rūšies elektroniniams duomenims nustatytą disponavimo jais režimą. Taigi būtina atsižvelgti į reikalavimus, kurie gali būti suformuluoti įvairiuose teisės aktuose (įstatymuose, poįstatyminiuose teisės aktuose, vidaus dokumentuose ir pan.), tiek ir nustatyti asmenų tarpusavio susitarimus bei kitas neatskleidimo įpareigojimą rodančias aplinkybes. Todėl akivaizdu, kad elektroninių duomenų priskyrimas neviešų elektroninių duomenų kategorijai yra fakto klausimas ir vertintinas kiekvienoje konkrečioje byloje atsižvelgiant į įvairias aplinkybes, pagrindžiančias arba priešingai – paneigiančias, kad yra disponavimo duomenimis apribojimai, specialūs reikalavimai arba procedūros. Mokslinėje literatūroje išsakoma nuomonė, kad tokias ribas atspindi „tikslų detalizavimo ir naudojimo apribojimų“[463] idėja, kuri užtikrina, kad duomenys nebus naudojami už tos srities ribų, kurioms buvo duotas duomenų subjekto leidimas[464]. Šie elektroninių duomenų apsikeitimo ribojimai

[460] Analizuojant asmens duomenis kaip nusikalstamos veikos dalyką reikėtų atkreipti dėmesį į nevienodą jų baudžiamojo teisinio vertinimo problemą. Teismų praktikoje nustačius neteisėto disponavimo tokiais elektroniniais duomenimis faktą kaltininkui paprastai inkriminuojama BK 198 straipsnyje numatyta nusikalstama veika (pavyzdžiui, Vilniaus miesto 1 apylinkės teismo 2008 m. rugsėjo 5 d. nuosprendis baudžiamojoje byloje (bylos Nr. 1-17-296/2008), Vilniaus miesto 1 apylinkės teismo 2011 m. gruodžio 6 d. nuosprendis baudžiamojoje byloje (bylos Nr. 1-1430-276/2011), Šiaulių miesto apylinkės teismo 2011 m. liepos 18 d. teismo baudžiamasis įsakymas baudžiamojoje byloje (bylos Nr. 1-617-885/2011 ir kt.). Tačiau pavieniais atvejais galima pastebėti ir BK 167 straipsnio taikymo atvejų (pavyzdžiui, Lazdijų rajono apylinkės teismo 2012 m. lapkričio 5 d. nuosprendis baudžiamojoje byloje (bylos Nr. 1-40-743/2012).

[461] Tokius išorinius informacijos požymius kaip apsaugos lygis (informacijai taikomi apsaugos reikalavimai), savalaikiškumas (operatyvumas), nematerialus pobūdis ir kt. A. Panomariovas analizavo kalbėdamas apie viešai neskelbiamos informacijos bendrąją sampratą baudžiamojo proceso kontekste (plačiau žr. Panomariovas, A., *op. cit.*, p. 10).

[462] Manson, N. C.; O'Neill, O., *supra* note 457, p. 102, 107.

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

[464] Tokia idėja atsispindi ir teisės aktuose – pavyzdžiui, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo (*Valstybės žinios*. 1996, Nr. 63-1479) 3 straipsnyje aptariant asmens duomenų tvarkymo reikalavimus, be kitų, minima ir tai, kad duomenys turi būtų renkami apibrėžtais ir teisėtais tikslais ir toliau nebūtų tvarkomi tikslais, nesuderinamais su nustatytaisiais prieš renkant asmens duomenis (3 straipsnio 1 dalies 1 punktas).

sudaro galimybes 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 numatytos nusikalstamos veikos inkriminavimo pagrįstumą, paprastai nurodomi tie teisės aktai, kuriuose nustatytos disponavimo elektroniniais duomenimis ribos (ir kurių konkrečiu atveju nebuvo laikytasi). Pavyzdžiui, Mažeikių rajono apylinkės teismo 2009 m. rugpjūčio 12 d. nuosprendyje baudžiamojoje byloje (bylos Nr. 1-188-785/2009) nurodoma, 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* <...>. Teismas detaliai išvardijo ribojimus, kurie buvo taikomi duomenų skaitymui, keitimui, įtraukimui, kopijavimui, ištrynimui, taip pat duomenų perdavimui pašaliniams asmenims, ir nustatęs, kad prisiimtų įsipareigojimų kaltininkas nesilaikė, konstatavo, kad jis padarė nusikalstamą veiką, numatytą BK 198 straipsnyje, t. y. neteisėtai įgijo, laikė, pasisavino ir paskleidė neviešus elektroninius duomenis (vaizdo įrašą apie AB įvykusį gaisrą, kurį vėliau paskleidė internete). Detaliai teisės aktų įpareigojimų pažeidimai aptarti ir Šiaulių miesto apylinkės teismo 2011 m. liepos 18 d. teismo baudžiamajame įsakyme baudžiamojoje byloje (bylos Nr. 1-617-885/2011). Šioje byloje, be Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo nuostatų, susijusių su teisėtais asmens duomenų tvarkymo kriterijais, minima daugelis kitų teisės aktų[465], kurie nustatė apribojimus prieigai prie mokesčių mokėtojų duomenų: asmens vardo, pavardės, asmens kodo, šeiminės padėties, išduotų asmens tapatybės dokumentų, užimtumo ir pajamų. Teismui nustačius, kad šie reikalavimai kaltininkui duomenis įgijus ir paskleidus pašaliniam asmeniui buvo pažeisti, konstatuota, kad jis, be kitų nusikalstamų veikų, padarė ir veiką, numatytą BK 198 straipsnyje.

Taigi vienas iš kriterijų inkriminuojant neteisėto elektroninių duomenų perėmimo ir panaudojimo nusikalstamą veiką siejamas su teisiniu elektroninių duomenų požymiu – jų neviešumu. Šis požymis bendriausia prasme reiškia, kad tai slepiami, viešam naudojimui neskirti elektroniniai duomenys. Atitinkamai jų konfidencialumo apsaugai, priklausomai nuo duomenų pobūdžio, nustatomi atitinkami ribojimai. Jie sudaro galimybes neviešus elektroninius duomenis analizuoti kaip duomenų rūšį, kuriai taikomas tam tikras apsaugos lygis – atitinkami apsaugos reikalavimai. Jie gali būti suformuluoti įvairiuose teisės aktuose, kilti iš asmenų tarpusavio susitarimų bei kitų aplinkybių, rodančių neatskleidimo įpareigojimus.

[465] Šiame baudžiamajame įsakyme nurodyti, pavyzdžiui, Lietuvos Respublikos mokesčių administravimo įstatymo 32 straipsnio 2, 5 ir 6 punktai; Valstybės tarnautojų veiklos etikos taisyklių, patvirtintų Lietuvos Respublikos Vyriausybės 2002 m. birželio 24 d. nutarimu Nr. 968, 2.1, 2.2, 2.3, 3.2, 3.3, 4.2 punktai; Valstybinės mokesčių inspekcijos valstybės tarnautojo elgesio kodekso, patvirtinto Valstybinės mokesčių inspekcijos prie Lietuvos Respublikos finansų ministerijos viršininko 2005 m. liepos 25 d. įsakymu Nr. V-141 „Dėl Valstybinės mokesčių inspekcijos valstybės tarnautojo elgesio kodekso patvirtinimo", 15.3, 16.1, 26, 27, 28 ir 29 punktai; Šiaulių apskrities valstybinės mokesčių inspekcijos viršininko 2009 m. birželio 5 d. įsakymo Nr. 1-184 „Dėl išorinių duomenų bazių naudojimo Šiaulių apskrities valstybinėje mokesčių inspekcijoje" 3.3, 3.5, 3.6, 3.7 punktai; Mokesčių mokėtojų asmens duomenų tvarkymo Valstybinėje mokesčių inspekcijoje taisyklių, patvirtintų Valstybinės mokesčių inspekcijos prie Lietuvos Respublikos finansų ministerijos viršininko 2008 m. balandžio 4 d. įsakymu Nr. V-130, 51 punktas ir daugelis kitų.

2.2. Pavojingos veikos

Nusikalstama neteisėto elektroninių duomenų perėmimo ir panaudojimo veika gali pasireikšti alternatyviomis neteisėto stebėjimo, fiksavimo, perėmimo, įgijimo, laikymo, pasisavinimo, paskleidimo ar kitokio neviešų elektroninių duomenų panaudojimo veikomis. Dispozicijoje aprašius įvairius neteisėto duomenų įgijimo ir jų vėlesnio panaudojimo veiksmus BK 198 straipsnyje neteisėtam disponavimui elektroniniais duomenimis suteiktas platus turinys. Tokia įstatymo leidėjo pozicija leidžia spręsti ir apie pasirinktą šios nusikalstamos veikos koncepciją – baudžiamąją atsakomybę siekta nustatyti už elektroninių duomenų konfidencialumo pažeidimus įvairiuose jų apdorojimo proceso etapuose. Pats duomenų apdorojimas, anot M. Webster, iš esmės „reiškia bet ką, kas gali būti padaryta duomenims arba su duomenimis“[466], todėl šis procesas autorei leido kalbėti apie duomenų įgijimą, naudojimą, laikymą, sunaikinimą ir kitas operacijas. Beje, duomenų tvarkymas plačiai apibrėžiamas ir Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo (*Valstybės žinios*. 1996, Nr. 63-1479) 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“. Kadangi duomenų saugumas svarbus įvairių veiksmų su jais atlikimo metu, tai pats duomenų apdorojimo terminas vartojamas pačia plačiausia prasme. Manytina, kad būtent dėl to įstatymų leidėjas BK 198 straipsnio dispozicijoje numatė įvairias pavojingas veikas, rodančias duomenų konfidencialumo pažeidimus kažkuriame iš duomenų apdorojimo etapų.

Aptariant minėtas alternatyvias veikas, matyti, kad daugelis jų pagal savo formuluotę panašios į tas, kurios įtvirtintos tradicinėmis laikomų nusikalstamų veikų sudėtyse. Pavyzdžiui, tokias kaip įgijimas, laikymas, platinimas, pasisavinimas ar kitokį neteisėtą disponavimą rodančias pavojingas veikas galima sutikti 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, sprogstamosiomis medžiagomis (pavyzdžiui, 253 straipsnis), disponavimo narkotinėmis ar psichotropinėmis medžiagomis (pavyzdžiui, 259, 260, 263 straipsniai) ir daugelio kitų sudėtyse. Be to, panašiai įvairių BK straipsnių dispozicijose aprašytos veikos, kuriomis daromas neteisėtas poveikis nusikalstamos veikos dalykui, galinčiam ir neturėti materialios išraiškos (pavyzdžiui, 124, 166, 170, 296, taip pat anksčiau minėti 214, 215 straipsniai). Kadangi pastarosios nusikalstamos veikos dėl savo prigimties negalėjo būti taikomos visų elektroninių duomenų konfidencialumo pažeidimo atvejais, tai BK 198 straipsnyje buvo numatyta bendra neteisėto elektroninių duomenų perėmimo ir panaudojimo veika. Toks požiūris į elektroninės erdvės saugumą, kaip ir anksčiau aptartos neteisėtos prieigos prie IS atveju, rodo apie tradicinių doktrinų vystymąsi. Kaip teigia M. J. Madison, „probleminiai prieigos prie informacijos, duomenų ir kompiuterio programų klausimai tampa probleminiais prieigos prie vietos, erdvės ir daikto <...> klausimais“[467]. Tokia išvada autoriui sudarė galimybes

[466] Webster, M. *Data protection in the financial services industry*. Aldershot; Burlington (Vt.): Gower, 2006, p. 13.

[467] Madison, M. J., *supra* note 252, p. 434.

analizuoti dviejų – *Interneto kaip vietos* (angl. *Internet-as-place*) ir *Informacijos kaip daikto* (angl. *Information-as-thing*) – metaforų derinį. Kai neteisėtas prisijungimas prie IS rodo įsibrovimo doktrinos plėtrą, tai neteisėtas disponavimas elektroniniais duomenimis tam tikra apimtimi yra susijęs su pagrobimo (neteisėto įgijimo) doktrinos vystymusi ir jos taikymu, be abejo, ne fizinėje, o elektroninėje erdvėje. Reikėtų atkreipti dėmesį į tai, kad šie doktrininiai pokyčiai nėra nauji – su panašiomis problemomis, kriminalizuojant įvairius neteisėtus veiksmus su materialios išraiškos neturinčiais nusikalstamos veikos dalykais, buvo susidurta įsigaliojus 2000 m. BK. Pavyzdžiui, numačius baudžiamąją atsakomybę už neteisėtą naudojimąsi energija ir ryšių paslaugomis (BK 179 straipsnis).

BK 198 straipsnyje įtvirtinus, kaip matyti, pakankamai platų neteisėto disponavimo elektroniniais duomenimis turinį, kai baudžiamoji atsakomybė kyla ne tik už elektroninių duomenų neteisėtą stebėjimą, fiksavimą, perėmimą, įgijimą, pasisavinimą, bet taip ir už jų laikymą bei įvairius šio nusikalstamos veikos dalyko panaudojimo veiksmus, neišvengiamai tenka kelti ir tokių požymių inkriminavimo problemas. Keletas bendresnių diskusinių klausimų yra šie:

1) BK 198 straipsnyje nusikalstamos veikos dalyku, kaip minėta, pripažįstami tiek elektroniniai duomenys, kurie *laikomi IS*, tiek ir *perduodami joje*. Šio straipsnio dispozicijoje, be perėmimo veikos, tiesiogiai numačius ir stebėjimą bei fiksavimą lieka neaišku, į kurių iš minėtų duomenų konfidencialumą jomis yra kėsinamasi. Ši problema kyla dėl to, kad Konvencijos dėl elektroninių nusikaltimų aiškinamojoje ataskaitoje elektroninių duomenų perėmimas techninėmis priemonėmis apibūdinamas per klausymąsi, kontroliavimą ir sekimą (53 punktas). Akivaizdu, kad perėmimo veika dėl savo specifikos neišvengiamai bus susijusi tik su perduodamų duomenų neteisėtu gavimu, tačiau nėra aišku, kaip šiame kontekste turėtų būti vertinamas, pavyzdžiui, elektroninių duomenų sekimas (stebėjimas). Kadangi BK 198 straipsnio dispozicijoje nusikalstamos veikos dalyku įvardyti elektroniniai duomenys, nekonkretizuojant jų iki *laikomų IS* ar *joje perduodamų* duomenų, tai tokia nusikalstamos veikos sudėtis nesuteikia galimybės stebėjimo kaip veikos apriboti tik iki *IS perduodamų duomenų* stebėjimo. Kartu ši išvada rodo nusikalstamos veikos, numatytos BK 198 straipsnyje, *perkriminalizavimo* problemas, aptartas anksčiau;

2) BK 198 straipsnio dispozicijoje neteisėtas elektroninių duomenų gavimas nėra siejamas tik su jų perėmimu, t. y. tik su tomis veikomis, kuriomis yra neteisėtai gaunami *IS perduodami elektroniniai duomenys*. Šiame straipsnyje aprašyta nusikalstama veika gali pasireikšti ir kitomis alternatyvomis, todėl dabartinis straipsnio pavadinimas, turintis nurodyti jame esančios nusikalstamos veikos esmę, yra klaidinantis. Kadangi ši nusikalstama veika ją įvardijus *neteisėtu elektroninių duomenų perėmimu ir panaudojimu* apibūdinta pernelyg siaurai, tai, autorės nuomone, tikslesniu pavadinimu galima būtų laikyti *neteisėtą disponavimą neviešais elektroniniais duomenimis*. Tiesa, teisės aktuose galima sutikti 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 apibūdinta kaip elektroninių duomenų pasisavinimas, platinimas, paskelbimas ar kitoks neteisėtas jų naudojimas. Tačiau, atsižvelgiant į BK straipsnių, kuriuose aprašytos įvairios ir *inter alia* neteisėtą poveikį materialios išraiškos galinčiam neturėti dalykui darančios veikos, pavadinimus, tikslesnis būtų ne manipuliavimo, o disponavimo terminas (pavyzdžiui, neteisėtas disponavimas in-

formacija, kuri yra valstybės paslaptis (BK 124 straipsnis). Juo labiau kad BK manipuliavimo terminas yra vartojamas kiek kitame kontekste ir siejamas su tikrovės neatitinkančios ar neišsamios informacijos skleidimu (BK 218 straipsnis).

Prieš pereinant prie konkrečių BK 198 straipsnyje numatytų veikų analizės ir probleminių jų aiškinimo aspektų atkreiptinas dėmesys į tai, kad šiame straipsnyje pavojingos veikos aprašytos kaip alternatyvos. Todėl baudžiamajai atsakomybei už neteisėtą elektroninių duomenų perėmimą ir panaudojimą kilti pakanka nustatyti bent vienos iš šių veikų padarymo faktą. Taip pat BK 198 straipsnyje aprašytos veikos laikomos viena tęstine nusikalstama veika, jei nustatoma, kad jos sudaro vienos tos pačios savarankiškos nusikalstamos veikos atskiras sudėtines dalis (epizodus) ir jas jungia vieninga kaltininko tyčia. Kadangi tęstinė veika pripažįstama paviene nusikalstama veika, tai ji nėra skaidoma dalimis dėl atskirų alternatyvių veikų ir kvalifikuojama pagal vieną minėto straipsnio atitinkamą dalį. Kai faktinės bylos aplinkybės rodo, kad kaltininkas galėjo padaryti keletą alternatyvių veikų, svarbiu tampa draudimas preziumuoti pavojingas veikas – kiekviena jų turi savarankišką baudžiamąją teisinę reikšmę kaltininkui, todėl turi būti savarankiškai įrodinėjama, o ne išvedama iš kitų BK 198 straipsnyje nurodytų ir byloje neginčijamai įrodytų veikų. Toks reikalavimas Lietuvos Aukščiausiojo Teismo praktikoje susietas ir su draudimu kelti skirtingus, t. y. mažesnius arba didesnius, reikalavimus įrodinėjant bei pagrindžiant padarytas veikas[468].

Taip pat kitas veikų analizei svarbus aspektas yra tas, kad Konvencijos dėl elektroninių nusikaltimų 3 straipsnyje aprašyta tik neteisėtos perimties nusikalstama veika. Likusių alternatyvų tinkamam interpretavimui aktualu nustatyti, kaip tokios veikos yra suvokiamos BK esančių kitų nusikalstamų veikų sudėtyse. Tokia analizė gali padėti tinkamai atskleisti neteisėto elektroninių duomenų perėmimo ir panaudojimo sudėties požymių turinį, be abejo, susiformavusį tradicinį požiūrį pritaikant „skaitmeniniame kontekste".

2.2.1. Perėmimas

Perėmimo kaip pavojingos veikos ištakos išimtinai siejamos su Konvencijos dėl elektroninių nusikaltimų 3 straipsnio, kuriame aprašyta kompiuterinių duomenų neteisėta perimtis, nuostatomis. Ši sąsaja leidžia perėmimo veiką analizuoti tik *IS perduodamų*, bet ne anksčiau minėtų „*nejudamų*" elektroninių duomenų neteisėto gavimo kontekste. Nors toks sukonkretinimas rodo perėmimo ir kitų neteisėto elektroninių duomenų gavimo veikų atskyrimo kriterijų, tačiau kartu verčia nustatyti ir pavojingos veikos pripažinimo perėmimu sąlygas. O tiksliau apsispręsti: 1) kada elektroniniai duomenys yra perduodami IS ir 2) kokių elektroninių duomenų neteisėtas perėmimas, atsižvelgiant į šių duomenų perdavimo IS ypatumus, kriminalizuotas BK 198 straipsnyje.

Analizuojant pirmąjį klausimą pažymėtina, kad Konvencijos dėl elektroninių nusikaltimų 3 straipsnyje minimas duomenų, perduodamų iš kompiuterinės sistemos ir jos

[468] 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 (bylos Nr. 2K-P-218/2009), Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2011 m. gruodžio 6 d. nutartis baudžiamojoje byloje (bylos Nr. 2K-482/2011), Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2011 m. balandžio 5 d. nutartis baudžiamojoje byloje (bylos Nr. 2K-159/2011) ir kt.).

viduje perėmimas. Šios Konvencijos aiškinamojoje ataskaitoje tokios situacijos detalizuojamos, išaiškinant, kad komunikavimas perduodant duomenis gali vykti tiek pavienėje kompiuterinėje sistemoje (pavyzdžiui, duomenims patenkant iš CPĮ į ekraną arba spausdintuvą), tiek ir tarp keleto sistemų, priklausančių vienam asmeniui, keleto kompiuterių, komunikuojančių tarpusavyje, arba asmeniui komunikuojant su kompiuteriu (t. y. naudojant klaviatūrą). Taip pat nurodoma, jog baudžiamajai atsakomybei kilti gali būti reikalaujama papildomo elemento, kad komunikavimas vyktų tarp dviejų sujungtų, tačiau veikiančių per atstumą kompiuterinių sistemų (55 punktas). Taigi pagrindinė problema kaltininkui inkriminuojant duomenų perėmimą kyla sprendžiant, kada duomenys gali būti laikomi perduodamais IS, ir atitinkamai, kada galima kalbėti apie tokių duomenų perėmimą. Patys pavojingi perėmimo veiksmai yra tiesiogiai susiję su neteisėtu duomenų gavimu *jų perdavimo metu*, tačiau iš Konvencijos aiškinamosios ataskaitos matyti, kad toks perdavimas galimas tiek iš kompiuterinės sistemos, tiek ir jos viduje (pavyzdžiui, asmeniui komunikuojant su kompiuteriu). Todėl aktualu nuspręsti, ar BK 198 straipsnio dispozicijoje minima perėmimo veika yra tik tie veiksmai, kuriais neteisėtai gauti elektroninių ryšių tinklais[469] siųsti duomenys, ar ir tie, kuriais gauti duomenys juos perduodant tik kompiuterio viduje.

Vidiniai duomenų perdavimo procesai, kai duomenys lieka kompiuteryje, yra neišvengiamai susiję su jo atliekamomis funkcijomis, kai vartotojas per įvesties įrenginius nurodo įvairias komandas kompiuteriui ir taip jame atlieka savo pageidaujamus veiksmus. Vartotojo siekiamų apdoroti duomenų perėmimas tokiais atvejais galimas nepriklausomai nuo to, ar turimas mintyje pavienis kompiuteris, ar tas, kuris sujungtas elektroninių ryšių tinklais su kitomis IS. Bene klasikiniu pavyzdžiu, kaip yra atliekami šie neteisėti perėmimo veiksmai, gali būti laikomas kenkėjiškos programinės įrangos panaudojimas (pavyzdžiui, *Keylogger*), kai ji, be kitų funkcijų, gali fiksuoti kiekvieno vartotojo kompiuterio klaviatūra įvestą informaciją.

Analizuojant kitą – išorinį elektroninių duomenų perdavimo variantą, kai duomenys yra siunčiami elektroninių ryšių tinklais, aktualu nustatyti, kada jie yra tokios būsenos. Mokslinėje literatūroje atkreiptas dėmesys į tai, kad teisės normos, susijusios su duomenų perėmimu, pirmiausia vystėsi realiuoju laiku perduodamų duomenų perėmimo kontekste[470]. Tačiau kintant situacijai, kai vis dažniau naudojamasi balso pašto (VoIP) paslaugomis[471], taip pat itin paplito elektroninio pašto, trumpųjų žinučių ir kitų elektroninių duomenų perdavimo paslaugos, aktualūs tapo įvairūs konfidencialumo užtikrinimo aspektai vertinant paslaugų teikėjo laikomus duomenis, kai jie: 1) jau yra pristatyti ir 2) dar nėra perduoti, o laukia pristatymo. Tokiais atvejais bandoma nustatyti skirtumus tarp *saugojimo po duomenų perdavimo* ir *duomenų tarpinio saugojimo*. Kai pirmasis atvejis leidžia

[469] Pagal Elektroninių ryšių įstatymo 2 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".

[470] Clough, J., *supra* note 110, p. 164.

[471] Plačiau žr. Kašėta, S.; Adomkus, T., *supra* note 185.

kalbėti apie „saugomų komunikacijų konfidencialumą“[472], tai antrasis verčia dvejoti, ar duomenys vertintini kaip saugomi (laikomi) IS, ar vis dėlto kaip perduodami elektroninių ryšių tinklais. Pastarąją problemą kelia pats duomenų perdavimo tinklais būdas.

Kadangi šiuo atveju susiduriama su komunikacijos technologijomis ir įvairiais jų funkcionavimo aspektais, tai tenka prisiminti galimas jų veikimo vertinimo pozicijas – *išorinę* ir *vidinę perspektyvas*. Pavyzdžiui, žiūrint iš *vidinės perspektyvos* Internetas vartotojui sudaro vienos vientisos komunikavimo sistemos iliuziją, tačiau ši perspektyva nesuteikia informacijos, kaip veikia įrenginių visuma ar pavieniai įrenginiai atlikdami įvairias funkcijas elektroninių ryšių tinklais perduodant duomenis. Todėl į duomenų perdavimo procesus aktualu pažvelgti ir iš *išorinės perspektyvos*. Dauguma IS yra tarpusavyje sujungtos, kad galėtų komunikuoti, taigi keistis elektroniniais duomenimis ir dalytis per atstumą esančiais ištekliais. Kaip teigia A. A. El Gamal ir Y.–H. Kim, į tinklą sujungta sistema – tai „kompleksas informacijos šaltinių ir komunikavimo mazgų, sujungtų tinklu“[473]. Kiekvienas iš šių mazgų atlieka savarankišką galutinę funkciją arba yra skirtas kokiam nors tikslui pasiekti.

Kad tinklo įrenginiai galėtų apsikeisti duomenimis, prieš tai duomenys turi būti sutvarkyti tokiu būdu, kuris leistų įrenginiui sėkmingai juos nukreipti į jų paskyrimo vietą, o kitam – juos priimti. Todėl, anot B. G. Blunndell, „perdavimas yra kompleksinis procesas ir priklauso nuo daugelio skirtingų operacijų“[474]. Pirmiausia duomenys skaidomi į mažesnius vienetus (paketus), prie kiekvieno tokio fragmento pridedama informacija (antraštė), kuri leidžia šiuos duomenų fragmentus perduoti įvairiais tinklais kelionės metu iki jiems numatytos vietos. Tokį duomenų „pakavimo“ procesą Internete vaizdžiai pavaizdavo D. Štitilio, aiškindamas, kaip keičiamasi duomenimis naudojant TCP (angl. *Transmission Control Protocol*)/IP (angl. *Internet Protokol*) protokolą. TCP protokolas „suskaido siunčiamą informaciją porcijomis (paketais), sudeda juos į elektroninius vokus, ant jų užrašo gavėjo bei siuntėjo adresus“[475]. Tuo tarpu IP protokolas nustato, kokiu optimaliausiu būdu suformuotas paketas turėtų būti siunčiamas Internetu. Jį siunčiant per interneto mazginius punktus, kiekviename jų nuskaitomas gavėjo adresas ir suformuotas paketas siunčiamas toliau. Taigi, kaip teigia autorius, „kiekvienas interneto elektroninis laiškas gali būti padalytas į kelis duomenų paketus, kurie gali keliauti pas adresatą visiškai skirtingais keliais“[476]. Tokius paketus vėliau padeda surinkti ir vėl atkurti pradinę informaciją TCP protokolas.

Panašus duomenų perdavimo principas būdingas įvairioms paslaugoms Internete – anot J. Clough „kiekviena paslauga Internete naudoja savo protokolą perduodant duomenų paketus iš vienos vietos į kitą“[477]. O pats informacijos paketų perdavimo būdas autoriui leido apie pranešimų siuntimo procesą bendriausia prasme kalbėti kaip apie „saugomą ir persiunčiamą“[478] pristatymą. Apie saugojimą duomenų perdavimo procese užsimenama todėl, kad galimi atvejai, kai suformuoti paketai dėl įvairių priežasčių negali būti iš karto

[472] Clough, J., *supra* note 110, p. 164.
[473] El Gamal, A. A.; Kim, Y.–H. *Network Information Theory*. Cambridge: Cambridge University Press, 2011, p. 1.
[474] Blundell, B. G., *supra* note 109, p. 244.
[475] Štitilis, D. *supra* note 7, p. 13.
[476] *Ibid*.
[477] Clough, J., *op. cit.*, p. 165.
[478] 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 2013-06-02]. <http://media.ca1.uscourts.gov/cgi-bin/getopn.pl?OPINION=03-1383EB.01A>.

nusiųsti iš vieno tinklo taško į kitą, todėl tinklo mazguose yra tam tikram laikui sulaikomi ir vėlinami pristatyti (laikinai saugomi, kol pasieks galutinę jų paskyrimo vietą). To priežastys yra įvairios – tai ir paketų aptarnavimo mazge laikas, reikalingas tinklo mazgui atlikti tiesiogines savo funkcijas (pavyzdžiui, parinkti maršrutą), paketų aptarnavimas eilėje, kai jie laukia, kol bus aptarnauti anksčiau į tinklo mazgą patekę paketai, ir pan.[479] Todėl teigtina, kad siunčiami duomenys dažnai, o galimas dalykas, kad ir nuolat, yra tiek siuntime, tiek ir tam tikra prasme „saugykloje" to paties siuntimo metu (net jei saugojimas trunka ne ilgiau kaip mikrosekundės dalį). Būtent tai ir sukelia sunkumų sprendžiant, kuriais atvejais duomenys yra perduodami, o kuriais – gali būti laikomi „*nejudamais*" (saugomais ar laikomais IS).

Nustatant duomenų perdavimo IS pradžios ir pabaigos momentus, A. S. Blunn atkreipė dėmesį į tai, kad mokslinėje literatūroje išsakomos trys tarpusavyje konkuruojančios nuomonės, t. y. pranešimas laikomas gautu, jei: 1) jį perskaitė numatytas gavėjas; 2) pranešimas pasiekė kažkurią iš tarpinių grandžių; 3) pranešimas yra saugojamas ta prasme, kad jis yra „*nejudamas*", t. y. nėra automatiškai persiunčiamas ir pasiekė tą adresą, iš kurio gali būti tiesiogiai prieinamas numatyto gavėjo[480]. Akivaizdu, kad duomenų fragmentus (paketus) siekiant pristatyti numatytam gavėjui jie parinkto maršruto įvairiose tarpinėse grandyse bus sulaikomi. Tokie trumpalaikiai duomenų saugojimai yra vienas esminių perdavimo proceso etapų, todėl bandymai atskirti visus šiuos užlaikymus nuo persiuntimų iš tiesų netenka prasmės. Į perdavimą, autorės nuomone, turėtų būti žiūrima kaip į vientisą procesą, apimantį neišvengiamą trumpalaikį duomenų saugojimą ir jų persiuntimą siekiant duomenis pristatyti numatytam adresatui. Todėl šiuo aspektu pavojingą veiką vertinant kaip perėmimą nėra svarbu, kad duomenys jų siuntimo metu galėjo tam tikru momentu būti elektroniniu būdu saugomi, jei tai yra duomenų perdavimo proceso sudedamoji dalis. Tokiu atveju duomenų perdavimo pabaigos momentas neturėtų būti siejamas nei su gavėjo veiksmais susipažįstant su duomenimis (pranešimu), nei su tarpiniais saugojimais – pirmuoju atveju perdavimo pabaigos momentas kaskart gali skirtis, priklausomai nuo to, kada su duomenimis bus susipažinta, nors patys duomenys jau nėra perdavimo procese (pavyzdžiui, yra saugomi serveryje). Tuo tarpu antruoju atveju vientisas perdavimo procesas yra nepagrįstai skaidomas dalimis. Atsižvelgiant į tai, sėkmingu perdavimu turėtų būti laikomas momentas, kai duomenys pasiekė tą adresą, iš kurios jie gali būti tiesiogiai prieinamas numatyto gavėjo.

Šiame kontekste analizuojant BK 198 straipsnio dispozicijoje numatytą neteisėto perėmimo veiką, galima pastebėti, kad gilesnė diskusija, kaip ji galėtų būti suvokiama, Lietuvos baudžiamosios teisės doktrinoje nėra sutinkama. Kai kuriais jos vertinimo aspektais yra pasisakę tik keletas autorių, pavyzdžiui, D. Valatkevičiaus ir R. Mockevičiaus nuomone, „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"[481]. Kaip matyti, šie autoriai nenurodo galimybės neteisėtu perėmimu laikyti veiksmus, kuriais gaunami tik kompiuterio viduje perduodami elektroniniai duomenys. Tačiau toks vertinimo variantas, atsižvelgiant į abstraktų neteisėto elektroninių duomenų perėmimo ir panaudo-

[479] Plačiau žr. Plėštys, R., *et al*., *supra* note 186, p. 37–41.
[480] Blunn, A. S., *supra* note 397, p. 28–29.
[481] Abramavičius, A., *et al*., *supra* note 160, p. 432.

jimo nusikalstamos veikos aprašymą, neatmestinas. BK 198 straipsnio dispozicijoje nėra nuorodų į elektroninio ryšio tinklus, IS būtiną sąsają su kitomis sistemomis, reikalavimus nustatyti kitą nei siuntėjas duomenų gavėją ar į kitas šios nusikalstamos veikos apibrėžtį siaurinančias aplinkybes. Pakankamai plati nusikalstamos veikos apimtis bent jau baudžiamojo įstatymo lygmeniu nesuteikia pagrindo elektroninių duomenų perėmimą analizuoti tik išorinio duomenų perdavimo kontekste (duomenis perduodant elektroninių ryšių tinklais arba į išorinius IS įrenginius). Todėl diskutuotina, ar elektroninių duomenų perėmimu negalėtų būti laikomi ir tokie pavojingi kaltininko veiksmai, kai šie duomenys buvo neteisėtai gauti juos perduodant pačiame kompiuteryje. Beje, apie tokią neteisėtų veiksmų vertinimo galimybę užsiminta ir Konvencijos dėl elektroninių nusikaltimų aiškinamojoje ataskaitoje, kurioje, kaip minėta, yra nurodoma ir į asmens sąveiką su paviene kompiuterine sistema bei vidinius duomenų perdavimus (55 punktas).

Tuo tarpu iš baudžiamosios teisės pozicijų vertinant išimtinai išorinius duomenų perdavimo procesus ir sprendžiant perėmimo inkriminavimo kaltininkui galimybes, būtina atskirti *neteisėtą elektroninių ryšių tinklais jau perduotų* ir *dar tik siuntimo procese esančių duomenų* neteisėtą gavimą. Pirmuoju atveju duomenų perdavimo procesas jau yra pasibaigęs juos pristačius numatytam gavėjui, taigi apie tokius duomenis galima kalbėti kaip apie saugomus (laikomus) IS, t. y. kaip apie „*nejudamus*“ duomenis. Kadangi perėmimo veika išimtinai siejama su duomenų konfidencialumo pažeidimais jų siuntimo metu, tai tokiais atvejais tiksliau taikyti ne duomenų perėmimo požymį, o kitas alternatyvias duomenų neteisėtą gavimą žyminčias veikas (pavyzdžiui, neteisėtą elektroninių duomenų įgijimą). Todėl elektroninių duomenų perdavimo inkriminavimas galimas tik antruoju atveju, kai duomenys neteisėtai gaunami jų perdavimo metu, t. y. tol, kol jie nėra pristatyti numatytam gavėjui. Tokiam sprendimui tai, kad perdavimo metu neišvengiami tarpiniai duomenų saugojimai kaip šio proceso dalis įtakos, atsižvelgiant į anksčiau išsakytus argumentus, neturi turėti.

Antrasis probleminis aspektas, analizuojant pavojingos veikos pripažinimo perėmimu sąlygas, buvo tiesiogiai susijęs su nusikalstamos veikos dalyku, t. y. kokių elektroninių duomenų neteisėtas perėmimas, atsižvelgiant į jų perdavimo IS ypatumus, yra kriminalizuotas BK 198 straipsnyje. Kaip minėta, elektroniniams duomenims identifikuoti gali būti pasitelkiamas *tinkamumo apdoroti IS* arba *duomenų būvimo vietos* kriterijus, tačiau jie tik sudaro galimybes duomenis priskirti elektroninių duomenų rūšiai. Todėl aptariant elektroninių ryšių tinklais siunčiamus duomenis, reikėtų atkreipti dėmesį ir į jų struktūrą – šie duomenys apima ne tik turinio (angl. *Content data*), bet taip pat ir srauto duomenis (angl. *Traffic data*).

Srauto duomenys Konvencijos dėl elektroninių nusikaltimų 1 straipsnio d punkte apibūdinti kaip duomenys, kurie 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 priskirti kompiuterinių duomenų, kuriems taikomas specifinis teisinis režimas, kategorijai. Šie duomenys sukurti kompiuterio komunikacijos grandinėje siekiant nustatytu maršrutu nusiųsti informaciją iš kilmės į paskyrimo vietą (28 punktas). Panašiai srauto duomenys, kaip tie duomenys, kurie „tvarkomi siekiant perduoti informaciją elektroninių ryšių tinklu ir (arba) tokio perdavimo apskaitai“ suvokiami ir Lietuvos Respublikos elektroninių ryšių įstatymo

2 straipsnio 57 punkte[482]. Pranešimo turinio ir informacijos, kuri yra būtina jam pasiekti numatytą vietą, atskyrimas gana vaizdžiai apibūdinamas mokslinėje literatūroje. Pasitelkdamas tradicinio laiško pavyzdį, J. Clough srauto duomenis prilygino siuntėjo ir gavėjo adresui, pašto ženklui ir antspaudui, kurie paprasčiausiai leidžia laiškui pasiekti adresatą arba grįžti atgal pas siuntėją, o laiškas voke laikomas pranešimo turiniu, todėl gali būti lyginamas su turinio duomenimis[483]. Kaip matyti, apie tokį elektroninių duomenų atskyrimą verčia kalbėti pats anksčiau aptartas duomenų perdavimo elektroninių ryšių tinklais principas – duomenis suskaidžius į mažesnius fragmentus (paketus), prie kiekvieno tokio fragmento pridedama informacija (antraštė), kuri leidžia juos perduoti įvairiais tinklais kelionės metu iki jiems numatytos vietos. BK 198 straipsnio kontekste elektroninių duomenų konfidencialumo pažeidimai konstatuotini nustačius tiek turinio duomenų, tiek ir su jais susijusių tinklo srauto duomenų neteisėtą gavimą. Tokia išvada darytina dėl pakankamai bendrai, t. y. technologijų atžvilgiu neutraliai, įvardyto šios nusikalstamos veikos dalyko – elektroninių duomenų. Tačiau, kuri iš straipsnio dispozicijoje minimų pavojingų veikų – perėmimas ar fiksavimas – tinkamesnė srauto duomenų neteisėtam gavimui, įmanoma nuspręsti tik išsiaiškinus, koks yra perėmimo ir fiksavimo veikų tarpusavio santykis.

2.2.2. Stebėjimas, fiksavimas

Bene daugiausiai interpretavimo sunkumų, analizuojant BK 198 straipsnio dispozicijoje numatytas pavojingas veikas, kelia stebėjimo ir fiksavimo veikos. Įvairūs probleminiai klausimai, atskleidžiant jų turinį, neišvengiami todėl, kad šios veikos nėra dažnai sutinkamos BK, nekilus diskusijoms tiek teismų praktikoje, tiek baudžiamosios teisės doktrinoje nėra suformuluotos galimos šių alternatyvų aiškinimo kryptys. Be to, pati neteisėto elektroninių duomenų perėmimo ir panaudojimo sudėtis, tokia kaip ji įtvirtinta BK 198 straipsnyje, rodo neapibrėžtą ir neaiškumų keliantį stebėjimo ir fiksavimo veikų turinį. Interpretavimo įvairovę lemia tai, kad minėtos pavojingos veikos analizuotinos atskirai *IS laikomų* ir *joje perduodamų elektroninių duomenų* neteisėto gavimo kontekste. Tokia situacija susidaro todėl, kad BK 198 straipsnio dispozicijoje elektroniniai duomenys kaip nusikalstamos veikos dalykas nėra konkretizuojami iki minėtų rūšių, o pati dispozicija nesuteikia galimybių stebėjimą ir fiksavimą susieti tik su *IS perduodamais* duomenimis. Nors, autorės nuomone, klausimas dėl tokios sąsajos natūraliai gali kilti analizuojant, pavyzdžiui, BK 166 straipsnį, kuriame minimas ne laikomų, o išimtinai elektroninių ryšių tinklais siunčiamų pranešimų stebėjimas, fiksavimas ir perėmimas. Be to, dvejonių sukelia ir Konvencijos dėl elektroninių nusikaltimų aiškinamojoje ataskaitoje pateiktas perėmi-

[482] Elektroninių ryšių įstatymo nuostatos yra suderintos su 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių) (OL 2004 m. *specialusis leidimas*, 13 skyrius, 29 tomas, p. 514) su paskutiniais pakeitimais, padarytais 2009 m. lapkričio 25 d. Europos Parlamento ir Tarybos direktyva 2009/136/EB.[2009] OL L 337/11.

Šioje direktyvoje, pagrindžiant asmens duomenų apsaugos svarbą elektroninių ryšių sektoriuje, nurodoma, kad srauto duomenys gali, *inter alia*, apimti duomenis, nurodančius pranešimo maršrutą, trukmę, laiką ar apimtį, naudojamą protokolą, siuntėjo ar gavėjo galinio įrenginio vietą, tinklą, kuriame pranešimas atsirado ar pasibaigė, ryšio pradžios bei pabaigos laiką ir trukmę. Be to, jie taip pat gali apimti ir formatą, kuriuo pranešimas perduodamas tinklu.

[483] Clough, J., *supra* note 110, p. 152.

mo, naudojant technines priemones, interpretavimas jį aiškinant per klausymąsi, sekimą ir kontroliavimą (53 punktas).

Taigi, kaip matyti, elektroninių duomenų stebėjimas ir fiksavimas gali būti aiškinamas dviem aspektais – atskirai kaip *IS perduodamų duomenų* ir kaip šioje sistemoje laikomų („*nejudamų*“) duomenų stebėjimas ir fiksavimas. Tačiau toks skirstymas kelia nemažai jų atribojimo nuo kitų analizuojamos nusikalstamos veikos sudėtyje numatytų alternatyvių veikų, o tiksliau elektroninių duomenų perėmimo ir įgijimo.

Aiškinantis *IS perduodamų duomenų* stebėjimo ir fiksavimo interpretavimo problemas, aktualu aptarti jų atskyrimo nuo perėmimo veikos kriterijus. Pavojingi perėmimo veiksmai, kaip minėta, yra tiesiogiai susiję su neteisėtu duomenų gavimu *jų perdavimo metu.* Problemų atribojant perėmimo, stebėjimo ir fiksavimo veikas kyla todėl, kad paprastai perėmimo procesas siejamas ir su elektroninių duomenų stebėjimu ir fiksavimu. Aiškiau šį veikų ryšį įmanoma pavaizduoti prieš tai išsiaiškinus, kaip suvokiamos pačios stebėjimo ir fiksavimo veikos.

Stebėjimas BK 198 straipsnį komentavusių autorių, tiesa, neišskiriant „*nejudamų*“ ir perduodamų duomenų, apibūdintas „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“[484]. Taigi neteisėtas stebėjimas siejamas su elektroninių duomenų užfiksavimu kaltininko mintyse, kai duomenys lieka jo atmintyje ir nėra atkuriami elektroninėje ar materialioje formoje (neužrašomi, nekopijuojami ir pan.).

IS perduodamų elektroninių duomenų fiksavimas palygintinas su jų „sugavimu“ ir atvaizdavimu. IS siunčiamų duomenų „gaudymas“ tarsi leidžia jų srautą sustabdyti ir taip duomenis padaryti prieinamais kaltininko stebėjimui, analizei ir pan. Toks aiškinimas atitiktų ir bendrą fiksavimo supratimą. Fiksuoti (lot. *fixus* – tvirtas, stiprus, nesuardomas), kaip aiškinama Tarptautinių žodžių žodyne, reiškia užrašyti, registruoti, žymėti, padaryti nejudamą, įtvirtinti[485]. Arba toks veiksmas gali būti apibūdintas kaip „komanda veiksmui sustabdyti, „įšaldyti“[486]. Kadangi paprastai srauto stebėjimui būtinos specialios priemonės (programinė įranga, pavyzdžiui, įvairios tinklo srauto perėmimo programos, techninės priemonės), tai perduodamų elektroninių duomenų fiksavimas yra kaltininko pasitelktų priemonių veiklos rezultatas. Priklausomai nuo jų ypatumų, šios priemonės gali leisti stebėti, analizuoti duomenis, interpretuoti duomenų paketus ir perrinkti jų srautą į originalius duomenis[487]. Akivaizdu, kad tokiais ir panašiais atvejais konfidencialių siunčiamų duomenų stebėjimui (elektroninių duomenų matymui, jų atpažinimui) yra būtinas šių duomenų fiksavimas – programinė įranga, „sugavusi“ perduodamus duomenis, juos atvaizduoja programos lange kaltininkui susipažinti. Taigi: 1) stebėjimas paprastai neatsiejamas nuo prieš tai atlikto ar stebėjimo metu vykdomo perduodamų duomenų fiksavimo; 2) pats neteisėtas programinės įrangos veikimas tinkle (fiksuojant duomenis) gali būti prilyginamas tinklo srauto stebėjimui; 3) fiksavimas bendriausia prasme gali būti laikomas tuo pačiu elektroninių duomenų perėmimu. Pavyzdžiui, D. Valatkevičius ir R. Mockevi-

[484] Abramavičius, A., *et al*., *supra* note 160, p. 432.

[485] Vaitkevičiūtė V. *Tarptautinių žodžių žodynas*. 4-asis pataisytas ir papildytas leidimas. Vilnius: Žodynas, 2007, p. 336.

[486] Dagienė, V., *et al*., *supra* note 251.

[487] Česnys, A.; Juknius, J., *supra* note 218, p. 71.

čius elektroninių duomenų perėmimą apibrėžė per elektroninių ryšių tinklais ar tarp kelių kompiuterių ar jo komponentų siunčiamų ir perduodamų duomenų užfiksavimą[488]. Be to, kaip minėta Konvencijos dėl elektroninių nusikaltimų aiškinamajame rašte, perėmimas yra suvokiamas pačia bendriausia prasme, kaip klausymasis, sekimas ar kontroliavimas.

Taigi toks stebėjimo, fiksavimo ir perėmimo veikų išskyrimas į savarankiškas BK 198 straipsnyje numatytas alternatyvas sukelia nemažai jų atribojimo problemų, nes artimoms pagal savo prasmę veikoms įvardyti pasirinkti skirtingi terminai. Beje, galimų užuominų, kokie kriterijai leistų šias veikas vieną nuo kitos atriboti, nesuteikia nei baudžiamosios teisės doktrina, nei teismų praktika. Todėl bandant suteikti minėtiems požymiams specifinę reikšmę, atitinkamai ir savarankišką turinį, diskutuotina:

1) ar atskiriant fiksavimo ir perėmimo veikas negalėtų būti daromas skirtumas tarp srauto ir turinio duomenų gavimo. Tokiu atveju fiksavimas sietinas su srauto duomenų nusikaitymu, t. y. tų duomenų (antraščių), kuriais buvo pažymėti duomenų paketai ir kurie atpažįstami tinklo įrenginiuose, fiksavimu. Tuo tarpu duomenų perėmimas reikštų turinio duomenų gavimą, t. y. pačios siunčiamos informacijos, kuri siuntimo proceso metu buvo suskaidyta į tam tikro dydžio duomenų paketus. Nors ir netiesiogiai, tačiau tokiam spėjimui pagrindą gali sudaryti 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 susietos 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 rodo apie pokalbio turinio sužinojimą. Galima spėti, kad asmens pokalbių turinio neteisėtam girdėjimui vietoj perėmimo buvo pasirinkta tinkamesnė – būtent klausymo – veika. Todėl darytina prielaida, kad BK 166 straipsnyje neteisėtas pranešimų perėmimas siejamas būtent su jų turinio gavimu. Taikant analogišką aiškinimą, elektroninių duomenų turinio sužinojimą BK 198 straipsnyje numatytos nusikalstamos veikos kontekste galėtų atspindėti būtent šių duomenų perėmimo veika. Tačiau šiuo aspektu atkreiptinas dėmesys į tai, kad neteisėtas elektroninių ryšių tinklais perduodamų duomenų gavimas bene visuomet bus susijęs tiek su srauto, tiek su turinio duomenų gavimu;

2) ar įstatymų leidėjas atskirdamas fiksavimą ir perėmimą nesiekė fiksavimo susieti tik su siunčiamų duomenų nuskaitymu, kai duomenų srautui, t. y. pačiam duomenų perdavimui, įtaka nėra daroma – srautas toliau keliauja nuo siuntėjo iki gavėjo. Tuo tarpu perėmimu būtų laikomi kaltininko veiksmai, pasireiškę neteisėtu poveikiu pačiam duomenų srautui tinkle. Tai galėtų būti tiek siunčiamų duomenų perėmimas, kai jie nebepasiekia numatyto gavėjo, tiek ir veiksmais, kuriais yra, pavyzdžiui, perimama sesijos kontrolė, kai serveryje buvo sėkmingai nustatyta teisėto vartotojo tapatybė[489];

3) ar atskyrus fiksavimo ir perėmimo veikas nebuvo siekta diferencijuoti patį nusikalstamos veikos, numatytos BK 198 straipsnyje, baigtumo momentą. Neteisėto neviešų elektroninių duomenų fiksavimo baigtumo momentas galėtų būti siejamas su duomenų srauto nuskaitymo pradžia (pradėjus fiksuoti duomenis), o perėmimu būtų laikomi veiksmai, kuriais kaltininkas šiuos duomenis gauna ir gali jais disponuoti. Nors dažniausiai fiksavimo ir perėmimo momentas sutaps, tačiau retai, bet galimos situacijos, kai užfiksa-

[488] Abramavičius, A., *et al*., *supra* note 160, p. 432.
[489] Plačiau apie sesijų perėmimo metodus žr.: Česnys, A.; Juknius, J., *supra* note 218, p. 76–78.

vus duomenis kaltininkas prie jų iš karto neprieina (pavyzdžiui, jei programai fiksuojant duomenis kaltininko nėra šalia).

Apibendrinant šiuos bandymus atskirti fiksavimą nuo perėmimo pažymėtina, kad pateikti aiškinimai nėra išvedami iš Konvencijos dėl elektroninių nusikaltimų nuostatų – joje skirtumas tarp srauto ir turinio duomenų gavimo, duomenų srauto nuskaitymo ir poveikio pačiam srautui veikų baigtumo momentu nėra daromas. Todėl, pasirinkus vieną iš atribojimo problemos sprendimo variantų, akivaizdu, kad jis būtų laikomas tik nacionalinėje teisėje numatytu neteisėto perėmimo veikos aiškinimo ypatumu. Autorės nuomone, artimiausias Konvencijos dėl elektroninių nusikaltimų nuostatoms ir tam tikrą paaiškinimą nacionalinėje teisėje (atsižvelgiant į BK 166 straipsnyje numatytos nusikalstamos veikos požymius) galėtų turėti pirmasis pastebėjimas, kad fiksavimui ir perėmimui atskirti turėtų būti daromas skirtumas tarp srauto ir turinio duomenų neteisėto gavimo. Šis aiškinimas, beje, nebūtų ir itin specifinis žiūrint iš technologinės pusės, nors, be abejo, atsižvelgiant į tokio pobūdžio nusikalstamų veikų padarymo mechanizmą, kaltininkui bene visuomet tektų inkriminuoti ne tik perėmimo, bet ir fiksavimo su stebėjimu veikas. Aišku tokiam požymių interpretavimui įsitvirtinti būtina tolimesnė diskusija baudžiamosios teisės doktrinoje, taip pat šios nuomonės pagrindimą arba priešingai – paneigimą ateityje gali lemti ir besiklostanti teismų praktika.

Antrasis elektroninių duomenų stebėjimo ir fiksavimo interpretavimo probleminis aspektas, kaip minėta, iškyla šias veikas analizuojant *IS laikomų* („*nejudamų*“) duomenų neteisėto gavimo kontekste. Stebėjimą ir fiksavimą susiejant su neteisėta prieiga prie šios rūšies duomenų, jų inkriminavimas kaltininkui taip pat kelia tam tikrų problemų: 1) nustatant stebėjimo veikos pakankamą pavojingumą, būtiną baudžiamajai atsakomybei kilti; 2) fiksavimo veiką atribojant nuo kitos BK 198 straipsnio dispozicijoje numatytos alternatyvos – elektroninių duomenų įgijimo.

Skirtingai nei IS perduodamų duomenų stebėjimo ir fiksavimo atveju, IS laikomų duomenų stebėjimas ir fiksavimas yra aiškiai viena nuo kitos atskirtos veikos – elektroninių duomenų stebėjimui nėra būtini ankstesni kaltininko atlikti šių duomenų fiksavimo veiksmai. Pereinant prie „*nejudamų*“ duomenų stebėjimo analizės reikėtų atkreipti dėmesį į tai, kad pats stebėjimo suvokimas didesnių problemų nekelia – tokia veika gali būti apibūdinta kaip jų matymas, analizavimas, duomenų užfiksavimas kaltininko mintyse, kai jie nėra atkuriami elektroninėje arba materialioje formoje. Šios veikos vertinimo sunkumų kelia kitas jos aspektas, t. y. kaip nustatyti pakankamą baudžiamajai atsakomybei kilti stebėjimo pavojingumą. Neteisėto elektroninių duomenų perėmimo ir panaudojimo sudėtyje stebėjimą numačius kaip alternatyvią veiką vien jos pakanka baudžiamajai atsakomybei pagal BK 198 straipsnį kilti. Esant taip aprašytai nusikalstamai veikai ją inkriminuojant nereikalaujama nustatyti papildomas tokios veikos pavojingumą rodančias aplinkybes kaip, pavyzdžiui: techninių priemonių panaudojimą, kaltininko nusikalstamus ketinimus, tam tikrą besitęsiantį veikos pobūdį ar kitas veikos pavojingumą didinančias aplinkybes. Apie vieną iš tokių, t. y. techninių priemonių panaudojimą, užsiminta ir Konvencijos dėl elektroninių nusikaltimų aiškinamajame rašte – jame, nors ir kalbant apie perėmimą, atkreiptas dėmesys į tokio pobūdžio nusikalstamos veikos *perkriminalizavimo* grėsmę. Sprendžiant šią problemą, valstybėms suteikta galimybė apriboti neteisėto perėmimo nusikalstamos veikos taikymą jos sudėtyje numatant ir techninių priemonių panaudojimo reikalavimą (53 punktas).

Šiuo aspektu atkreiptinas dėmesys į tai, kad Lietuvos Aukščiausiojo Teismo praktikoje, siekiant išvengti formalaus baudžiamojo įstatymo taikymo, ne kartą akcentuota nusikalstamų ir vertinant iš baudžiamosios teisės pozicijų nepavojingų veikų atskyrimo svarba. Teismas pabrėžė, 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*[490]. Kadangi neviešų elektroninių duomenų stebėjimo veika yra baigta nuo stebėjimo veiksmų pradžios, tai diskusiniais atvejais pagrindžiant tokių veiksmų pavojingumą, autorės nuomone, svarbu nustatyti ne tik patį stebėjimo faktą, bet ir kitas aplinkybes, rodančias žalos baudžiamojo įstatymo saugomiems teisiniams gėriams kilimą arba akivaizdžią tokios žalos kilimo grėsmę. Stebėjimo pavojingumą, pavyzdžiui, gali pagrįsti kaltininko ketinimai padaryti kitas nusikalstamas veikas gavus duomenis, duomenų apsaugos priemonių pažeidimai, įvairių techninių priemonių, skirtų gauti duomenis, panaudojimas, kaltininko neteisėti veiksmai prisijungiant prie IS ir tokiu būdu gaunant prieigą prie duomenų, stebėjimo veiksmų pastovumas, stebėtų duomenų kiekis, žalos sukėlimas ir pan. Beje, apibūdindami stebėjimą, autoriai, komentavę BK 198 straipsnį, taip pat atkreipė dėmesį į tai, kad šie veiksmai „pasižymi tam tikru pastovumu ir užima tam tikrą laiko tarpą“[491].

Kitas iškeltas klausimas buvo susijęs su dviejų BK 198 straipsnio dispozicijoje numatytų alternatyvų – fiksavimo ir įgijimo – atskyrimo problemomis. Fiksavimas, anot D. Valatkevičiaus ir R. Mockevičius, pasireiškia „elektroninių duomenų paėmimu savo dispozicijon bei jų fiziniu perkėlimu į savo kontroliuojamą informacijos laikmeną“[492]. Kartu autoriai nurodo, 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.“[493] Tačiau toks fiksavimo suvokimas kelia problemų šią veiką atribojant nuo elektroninių duomenų įgijimo, kuris bendriausia prasme gali būti apibūdintas kaip elektroninių duomenų gavimas, nepriklausomai nuo jų gavimo būdo[494]. Toks dubliavimasis kelia diskusijų, kokiais kriterijais vadovaujantis gali būti atskiriamos šios bene analogiškos veikos. Pačių kriterijų, kaip ir anksčiau aptarto fiksavimo ir perėmimo atribojimo atveju, nei baudžiamosios teisės doktrina, nei teismų praktika nesuteikia. Tiesa, teismų praktikoje galima sutikti pavienių atvejų, kai kaltininkas pripažintas kaltu padaręs nusikalstamą veiką, numatytą BK 198 straipsnio 1 dalyje, t. y. neteisėtai stebėjęs ir fiksavęs neviešus elektroninius duomenis. Tačiau kriterijai, kodėl jam inkriminuotos būtent šios alternatyvos, teismų sprendimuose nepateikiami. Pavyzdžiui, Vilniaus rajono apylinkės teismo 2009 m. rugsėjo 8 d. nuosprendyje baudžiamojoje byloje (bylos

[490] Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2006 m. sausio 24 d. nutartis baudžiamojoje byloje (bylos Nr. 2K-86/2006), Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2010 m. gruodžio 21 d. nutartis baudžiamoje byloje (bylos Nr. 2K-560/2010) ir kt.

[491] Abramavičius, A., *et al*., *supra* note 160, p. 432.

[492] *Ibid*.

[493] *Ibid*.

[494] Pavyzdžiui, aiškinant neteisėtą *informacijos* įgijimą BK 124 straipsnio (neteisėtas disponavimas informacija, kuri yra valstybės paslaptis) kontekste tarp įvairių įgijimo būdų nurodomas ir įrašymas, fotografavimas (Abramavičius, A., *et al*., *supra* note 160, p. 102).

Nr. 1-278-298/2009) teismas konstatavo, 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. Nuosprendyje taip pat nurodoma, kad Ž. Š. savo reikmėm prisijungdavo prie Registro centro duomenų bazės iš skirtingų kompiuterių, kurie priklausė jam, draugams, internetinėms kavinėms. Prisijungdavo tikslu gauti duomenis apie asmenų nekilnojamąjį turtą.* Kadangi elektroninių duomenų įgijimas bendriausia prasme suvokiamas kaip jų gavimas, tai nėra aišku, kokiais kriterijais vadovaujantis kaltininkui buvo inkriminuotas neviešų elektroninių duomenų fiksavimas, o ne jų įgijimas.

Nors, autorės nuomone, fiksavimo ir įgijimo veikos iš esmės yra analogiško turinio, tačiau jas kaip alternatyvas numačius BK 198 straipsnio dispozicijoje neišvengiamai tenka ieškoti galimų jų atribojimo kriterijų. Galima būtų diskutuoti, ar, pavyzdžiui, fiksavimo ir įgijimo veikų atskyrimas nėra siejamas su skirtingu šių veikų baigtumo momentu (konstatuojant elektroninių duomenų įgijimą turėtų būti nustatoma ir disponavimo jais galimybė, tuo tarpu inkriminuojant fiksavimą ši galimybė nebūtų būtina). Taip pat svarstytina, ar fiksavimą nuo elektroninių duomenų įgijimo neskiria tai, kad inkriminuojant fiksavimą problemų nekeltų duomenų formos pakeitimas iš elektroninės į materialią (pavyzdžiui, elektroninius duomenis užrašant, atspausdinant ir pan.)[495].

Taigi atskiriant *IS perduodamų duomenų* fiksavimą ir perėmimą siūlytina fiksavimo veiką susieti su srauto, o perėmimo su turinio duomenų gavimu. *IS laikomų duomenų* fiksavimas ir įgijimas yra bene analogiškos veikos, todėl bandant jas atskirti diskutuotina, ar fiksavimas negalėtų būti inkriminuojamas tais atvejais, kai kaltininkas neteisėtai gaudamas elektroninius duomenis pakeitė jų formą į materialią.

2.2.3. Įgijimas

Neteisėtas elektroninių duomenų įgijimas nors ir laikomas viena iš neteisėtos prieigos prie duomenų išraiškos formų, tačiau ši veika, kaip ji įtvirtinta BK 198 straipsnio dispozicijoje, tiesioginės sąsajos su Konvencijos dėl elektroninių nusikaltimų nuostatomis neturi. Neteisėta prieiga prie duomenų, kaip minėta, daugelyje valstybių tam tikra dalimi yra susieta su neteisėta prieiga prie IS, taip pasirinkus vieną iš galimų neteisėtos prieigos prie IS kriminalizavimo variantų. Todėl neteisėto elektroninių duomenų įgijimo turinio atskleidimui ir nuosekliam aiškinimui svarbu nustatyti, kaip tokio pobūdžio pavojinga veika interpretuojama kitų kategorijų baudžiamosiose bylose.

Analizuojant baudžiamosios teisės teorijoje išsakomas nuomones, taip pat teismų praktikoje pateikiamus neteisėto įgijimo aiškinimus, matyti, kad bendriausia prasme įgijimas suprantamas kaip bet kokie kaltininko veiksmai, kuriais jis neteisėtai gauna nusikalstamos veikos dalyką. Štai, pavyzdžiui, teismų praktikoje nusikalstamų veikų finansų sistemai bylose įgijimas apibūdinamas kaip „veiksmai, kuriuos atlikę asmenys *gauna* ne-

[495] Plačiau apie duomenų formos kitimo įtaką nusikalstamos veikos kvalifikavimui žiūrėti IV dalies 2.1 poskyryje.

tikrą, 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“[496]. Bene analogiška įgijimo sąvoka naudojama BK 214 straipsnį komentavusių autorių. Jų nuomone, įgijimas tai bent vienos elektroninės mokėjimo priemonės „gavimas už atlygį ar be jo bet kokia forma“[497]. Įgijimas (įsigijimas) kaip „bet kokie veiksmai, kuriais asmuo realiai *gauna* tam tikrą daiktą“[498] yra suprantamas mokslinėje literatūroje analizuojant disponavimo pornografinio turinio dalykais sudėties požymius. Neteisėtas nusikalstamos veikos dalyko įgijimas kaip jo gavimas taip pat aiškinamas ir nusikalstamų veikų, susijusių su disponavimu narkotinėmis ar psichotropinėmis medžiagomis, bylose. Jose pagal susiformavusią teismų praktiką įgijimas yra veiksmai, „kuriuos atlikęs asmuo *gauna* psichotropinių ar narkotinių medžiagų“[499], bei daugeliu kitų atvejų. Taigi matyti, kad pati įgijimo veika aiškinama plačiai, į jos turinį įtraukiant bet kokius veiksmus, kuriais gaunamas nusikalstamos veikos dalykas. Tačiau analizuojant BK 198 straipsnio dispozicijoje aprašytas alternatyvas matyti, kad neteisėto elektroninių duomenų įgijimo turinys analizuojamos nusikalstamos veikos kontekste susiaurintas.

Neteisėto elektroninių duomenų perėmimo ir panaudojimo nusikalstamos veikos sudėtyje elektroninių duomenų gavimas išreikštas keliomis alternatyviomis veikomis – stebėjimas, fiksavimas, perėmimas ir įgijimas. Nors įgijimui paprastai suteikiama pakankamai plati reikšmė, tačiau BK 198 straipsnio dispozicijoje įgijimas suskaidytas į tam tikrus specifinius aspektus turinčias veikas. Kadangi įgijimo ir fiksavimo atskyrimo probleminiai aspektai analizuoti anksčiau, tai šioje dalyje aktualu kiek plačiau aptarti perėmimo ir įgijimo veikų tarpusavio santykį. Elektroninių duomenų perėmimas ir įgijimas yra pagal savo prasmę artimos veikos, tačiau jas abi įtvirtinus nusikalstamos veikos sudėtyje, neišvengiamai tenka elektroninius duomenis skirstyti į *laikomus (saugomus) IS* ir šioje sistemoje perduodamus duomenis. Kai perėmimas siejamas išimtinai su perduodamų elektroninių ryšių tinklais ar pačiame kompiuteryje elektroninių duomenų gavimu, tai tokie veiksmai, autorės nuomone, vengiant dubliavimo, turėtų būti eliminuojami iš alternatyvios neteisėto įgijimo veikos. Todėl apie neteisėtą įgijimą reikėtų kalbėti tik tais atvejais, kai neteisėtai gaunami IS laikomi (saugomi), t. y. „*nejudami*“ elektroniniai duomenys. Šių duomenų įgijimo būdai gali būti įvairūs – kaltininkui pačiam tiesiogiai priėjus prie elektroninių duomenų, elektroninius duomenis nusipirkus, gavus veltui arba mainais, juos parsisiuntus elektroninių ryšių tinklais, gavus apgaule, panaudojus grasinimus ar bet kokiu kitu būdu.

---

[496] 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.

[497] Abramavičius, A., *et al. Lietuvos Respublikos baudžiamojo kodekso komentaras. Specialioji dalis (213-330 straipsniai)*. Vilnius: Registrų centras, 2010, p. 32.

[498] Žėkas, T. Vaiko išnaudojimas pornografijai: baudžiamieji teisiniai ir kriminologiniai aspektai: daktaro disertacija: socialiniai mokslai, teisė (01 S). – Vilnius: Vilniaus universitetas, 2011, p. 130.

[499] Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus plenarinės sesijos 2009 m. spalio 20 d. nutartis baudžiamojoje byloje (bylos Nr. 2K-P-218/2009), Lietuvos Aukščiausiojo Teismo teisėjų senato 2002 m. birželio 21 d. nutarimo Nr. 37 „Dėl teismų praktikos nagrinėjant psichotropinių ar narkotinių medžiagų grobimo, neteisėto šių medžiagų ir jų pirmos kategorijos pirmtakų (prekursorių) gaminimo, įgijimo, laikymo, gabenimo, siuntimo, pardavimo ar kitokio platinimo baudžiamąsias bylas“ 11 punktas. *Teismų praktika*. 2002, Nr. 17.

Taip aiškinant šias veikas tiek perėmimas, tiek įgijimas įgauna savarankišką reikšmę, todėl nėra laikomos viena kitą lemiančiomis veikomis. Vienais atvejais iš tiesų perimti duomenys vėliau kaltininko iš šiuos duomenis perėmusių asmenų gali būti neteisėtai įgyti (pavyzdžiui, perkant), tačiau perėmimas nėra vienintelis būdas gauti elektroninius duomenis. Todėl galimi atvejais, kai duomenys kaltininko yra įgyjami iš kitų asmenų, kurie juos gavo ne šių duomenų perėmimo būdu. Atitinkamai negalima būtų sutikti su literatūroje išsakoma nuomone, kad „elektroninių duomenų įgijimas yra vėliau po perėmimo vykstantis veiksmas, kurio metu asmuo realiai gauna šiuos duomenis“[500]. Vis dėlto, autorės nuomone, perėmimas neturėtų būti laikomas pirminiu duomenų įgijimo etapu, o šioms nusikalstamoms veikoms suteikus savarankišką reikšmę, jos liudytų apie skirtingus ir dažnai nesusijusius neteisėto elektroninių duomenų gavimo variantus.

Elektroninius duomenis apibrėžus taikant *tinkamumo juos apdoroti IS kriterijų*, akivaizdu, kad neprarasdami šios formos jie gali egzistuoti tik būdami IS, tam tikroje jos dalyje ar išoriniuose informacijos kaupikliuose (pavyzdžiui, kompaktiniuose diskuose, USB atmintinėse ir pan.). Todėl diskusijų, kiek ir kokias nusikalstamas veikas padarė kaltininkas, gali sukelti situacijos nustačius, kad jis pagrobė kažkurią iš minėtų priemonių su joje laikytais neviešais elektroniniai 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 materialių objektų pagrobimo, ar kaltininko veikai kvalifikuoti taip pat turėtų būti taikoma atitinkama BK 198 straipsnio dalis dėl elektroninių duomenų neteisėto įgijimo. Analizuojant elektroninių duomenų neteisėtą įgijimą šiuo aspektu literatūroje pagrįstai neginčijama galimybė kaltininkui inkriminuoti ir neteisėtą elektroninių duomenų įgijimą, jei nustatoma, kad jo tyčia buvo nukreipta į tokių duomenų gavimą. Tai yra, pagal BK 198 straipsnį, anot D. Valatkevičiaus ir R. Mockevičiaus, „kvalifikuojami ir tie atvejai, kai kaltininkas, siekdamas perimti elektroninius duomenis, pasisavina patį kompiuterį ar jo techninę įrangą (standųjį diską), išorinės atminties įrenginius (diskelius, magnetooptinius diskus, kompaktinius diskus, DVD diskus ar magnetines juostas), kuriuose tokie duomenys yra“[501]. Panašios nuomonės yra ir rusų autoriai, kurie siūlo neteisėtą prieigą prie įstatymo saugomos informacijos konstatuoti ne tik tada, kai prie jos prasiskverbiama naudojant mokslo pasiekimus ir techniką, bet ir tada, kai neteisėta prieiga gaunama tradiciniais būdais – pagrobiant pačias informacijos laikmenas, techninę įrangą, kurioje yra saugoma informacija[502].

Apibendrinus siūlytina neteisėto perėmimo ir įgijimo veikas skirti pagal tai, kokie duomenys – *IS laikomi* ar *joje perduodami* – buvo gauti. Taip pat neviešų elektroninių duomenų įgijimu, priklausomai nuo kaltininko tyčios kryptingumo, pripažintinas ir IS komponentų, kuriuose laikomi elektroniniai duomenys, gavimas. Tokiais atvejais kaltininko veika, be nuorodų į BK 178 ir 180 straipsnius, taip pat kvalifikuotina pagal BK 198 straipsnio atitinkamą dalį.

---

[500] Abramavičius, A., *et al*., *supra* note 160, p. 432.

[501] *Ibid*.

[502] *Ugolovnoe pravo Rossii. Osobennaja chast: uchebnik* [Russian criminal law. Special Part: The textbook]. Borzenkova, G.N.; Komissarova, V. S. (red.), Moskva: Zercalo-M, 2005, s. 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, s. 252.

2.2.4. Laikymas

BK 198 straipsnio dispozicijoje esančios pavojingo laikymo veikos, kaip ir anksčiau aptarto įgijimo, ištakų turėtų būti ieškoma ne tarptautinėje ar Europos Sąjungos, o nacionalinėje teisėje. Ši su elektroninių duomenų konfidencialumo pažeidimais susijusi veika nėra numatyta nei Konvencijos dėl elektroninių nusikaltimų, nei Pamatinio sprendimo 2005/222/TVR nuostatose. Taigi nuosekliai aiškinant laikymo veiką būtina atsižvelgti į tai, kaip ji suprantama kitų nusikalstamų veikų, numatančių tokį sudėties požymį, kontekste.

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*, nepriklausomai nuo jų turėjimo laiko trukmės ar buvimo vietos (su savimi, patalpoje ar kitoje vietoje)“[503]. Palyginti analogiška laikymo sąvoka pateikiama ir nusikalstamų veikų, susijusių su disponavimu narkotinėmis ar psichotropinėmis medžiagomis, bylose aiškinant šių medžiagų laikymo požymį. Jose laikymu taip pat pripažįstamas nusikalstamos veikos dalykų „*buvimas kaltininko žinioje* nepriklausomai nuo jų turėjimo laiko trukmės ar buvimo vietos (su savimi, patalpoje, slėptuvėje ar kitose vietose)[504] arba „bet koks faktinis psichotropinių ar narkotinių medžiagų *turėjimas* nepriklausomai nuo laiko, kiekio ar jų buvimo vietos“[505]. Panašus laikymo veikos aiškinimas matomas ir mokslinėje literatūroje, pavyzdžiui, interpretuojant disponavimo pornografinio turinio dalykais sudėties požymius. Anot T. Žėko, šiose bylose „laikymas apibrėžiamas per *turėjimo* ir *valdymo* sąvokas“[506]. Į tokį veikos interpretavimą turėtų būti orientuojamasi aiškinant ir neteisėtą neviešų elektroninių duomenų laikymą, tačiau, palyginus su tradiciniu suvokimu, praplečiant jų turėjimo galimybes ne tik fizinėje, bet ir elektroninėje erdvėje. Apie laikymą elektroninės erdvės kontekste verčia kalbėti pati analizuojamos nusikalstamos veikos dalyko specifika – duomenys pripažįstami elektroniniais duomenimis, jei jie gali būti apdorojami IS. Kadangi elektroninę formą duomenys paprastai išsaugo, jeigu jie yra IS (jos dalyse arba išoriniuose informacijos kaupikliuose), tai ir neteisėtas laikymas siejamas su jų buvimu tokioje vietoje. Nuorodas į duomenų laikymą elektroninėje erdvėje galima pastebėti ir BK 198 straipsnį komentavusių autorių pateiktoje laikymo sąvokoje. Laikymas, kaip teigiama, yra „bet koks faktinis elektroninių duomenų turėjimas nepriklausomai nuo turėjimo laiko, jų buvimo vietos (su savimi, patalpoje, kompiuterio atmintyje, savo elektroninio pašto serveryje ir pan.)“[507].

---

[503] 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.

[504] Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus plenarinės sesijos 2009 m. spalio 20 d. nutartis baudžiamojoje byloje (bylos Nr. 2K-P-218/2009), Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2011 m. balandžio 19 d. nutartis baudžiamojoje byloje (bylos Nr. 2K-162/2011), Lietuvos Aukščiausiojo Teismo teisėjų senato 2002 m. birželio 21 d. nutarimo Nr. 37 „Dėl teismų praktikos nagrinėjant psichotropinių ar narkotinių medžiagų grobimo, neteisėto šių medžiagų ir jų pirmos kategorijos pirmtakų (prekursorių) gaminimo, įgijimo, laikymo, gabenimo, siuntimo, pardavimo ar kitokio platinimo baudžiamąsias bylas“ 11–12 punktai. *Teismų praktika*. 2002, Nr. 17.

[505] Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2010 m. gegužės 11 d. nutartis baudžiamojoje byloje (bylos Nr. 2K-185/2010).

[506] Žėkas T., *supra* note 498, p. 134.

[507] Abramavičius, A., *et al*., *supra* note 160, p. 432–433.

Nors paprastai nei teismų praktikoje, nei mokslinėje literatūroje nėra ginčijama, kad neteisėtas laikymas gali būti apibūdinamas per nusikalstamos veikos dalyko turėjimą (buvimą) kaltininko žinioje, tačiau šią veiką analizuojant BK 198 straipsnio kontekste kai kurių autorių darbuose laikymui ir turėjimui nepagrįstai bandomos suteikti skirtingos prasmės. Pavyzdžiui, sunkiai galima būtų sutikti su 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“[508]. Kalbant apie tapatybės vagystę[509] elektroninėje erdvėje vis dėlto reikėtų pripažinti, kad su asmens tapatybe susijusių elektroninių duomenų laikymas ir yra jų turėjimas kaltininko žinioje (nepriklausomai nuo to, ar būtų kalbama apie BK 198, 198[2], 214 ar kitus straipsnius).

Kadangi laikymo veika yra trunkamoji, tai jos pradžios momentas 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). Taigi vien pats elektroninių duomenų turėjimo faktas rodo baigtą neteisėto elektroninių duomenų perėmimo ir panaudojimo veiką, nepriklausomai nuo ankstesnių (pavyzdžiui, įgijimo, perėmimo) ar tolesnių kaltininko veiksmų (pavyzdžiui, paskleidimo).

Atsižvelgiant į tai, kad baudžiamoji atsakomybė už elektroninių duomenų laikymą kyla nuo tokių duomenų atsiradimo pas kaltininką pradžios, būtina nustatyti, kada jis gavo įvairių materialių priemonių, kuriose laikomi elektroniniai duomenys (pavyzdžiui, USB atmintinės, kompaktiniai diskai ir pan.), arba kada šie duomenys yra kaltininko gauti jam prieinamoje vietoje elektroninėje erdvėje (pavyzdžiui, elektroninio pašto serveryje, kitame serveryje, žinant prisijungimo kelią prie jo bei būtinus prisijungimo duomenis ir pan.). Visais šiais atvejais inkriminuojant laikymo veiką yra svarbu konstatuoti ir kaltininko galimybę prieiti prie elektroninių duomenų, daryti jiems poveikį, t. y. spręsti jų tolesnį likimą. Pagal teismų praktiką šią aplinkybę rodo tai, kad, pavyzdžiui, kaltininkas duomenis laikė savo kontroliuojamose informacijos laikmenose (išoriniame duomenų kaupikliuose, asmeniniame nešiojamajame kompiuteryje)[510], duomenis įrašė į išorinę laikmeną ir juos turėjo su savimi[511].

Darant išvadą, kad kaltininkas neteisėtai laikė neviešus elektroninius duomenis, aktualus tampa ir subjektyvus momentas, t. y. ar jis suvokė, jog savo žinioje neteisėtai turi neviešus elektroninius duomenis. Šis aspektas svarbus tais atvejais, kai duomenys yra gauti, pavyzdžiui, elektroniniu paštu ar yra kitose kaltininko prieinamose vietose, jei su šiais duomenimis jis dar nespėjo susipažinti. Subjektyvus momentas tokiais atvejais leidžia pagrįsti arba priešingai – paneigti laikymo veiką. Jei kaltininkui žinoma, kad jis neteisėtai gavo neviešus elektroninius duomenis, susipažinimo arba nespėjimo su jais susipažinti faktas veikos pripažinimui laikymu ar jos baigtumui įtakos neturi turėti. Beje, tokios pozicijos laikomasi ir disponavimo pornografinio turinio dalykais bylose, kai „ži-

[508] Štitilis, D., *et al*., *supra* note 332, p. 256.

[509] Tapatybės vagystės sąvoka, vertinant ją iš baudžiamosios teisės pozicijų, nėra tiksli, nes vagystės dalyku tiek baudžiamosios teisės teorijoje, tiek ir teismų praktikoje neginčijamai pripažįstami *inter alia* tik materialią išraišką, ekonominę vertę turintys objektai. Tačiau ši sąvoka vartojama kaip tiesioginis *identity theft* vertinys.

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

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

nojimo“ momentas tampa svarbus sprendžiant, ar kažkas laiko (turi) savo žinioje pornografinę medžiagą[512].

2.2.5. Pasisavinimas

Pasisavinimo požymis neteisėto elektroninių duomenų perėmimo ir panaudojimo nusikalstamos veikos sudėtyje buvo numatytas jau 2003 metais įsigaliojus naujajam BK[513]. Nors šis požymis BK 198 straipsnio dispozicijoje išliko ir po 2007 metų BK XXX skyriaus pakeitimų, tačiau, autorės nuomone, elektroninių duomenų pasisavinimo turinys iš esmės kito. Skirtingo nors ir vienodai įvardyto sudėties požymio interpretavimo poreikį rodo po 2007 metų BK 198 straipsnyje atsiradusios įvairios pavojingų veikų alternatyvos. Kai iki 2007 metų pasisavinimas minėto straipsnio dispozicijoje buvo numatytas kaip vienintelis požymis, reiškiantis kompiuterinės informacijos gavimą, tai po 2007 metų neteisėtam elektroninių duomenų gavimui aprašyti pasitelktos stebėjimo, fiksavimo, perėmimo ir įgijimo veikos. Todėl pasisavinimą siekiant atskirti nuo jų, šiam požymiui turėtų būti suteikiamas savarankiškas turinys, taip išvengiant dispozicijoje esančių požymių persidengimo. Be to, užtikrinant nuoseklų pasisavinimo požymio aiškinimą ir BK vidinę darną, būtina atsižvelgti į jo interpretavimą kitų nusikalstamų veikų sudėtyse.

Pavieniai bandymai atskleisti elektroninių duomenų pasisavinimo turinį literatūroje bendriausia prasme šį požymį susieja su elektroninių duomenų gavimu. Pavyzdžiui, galima sutikti 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“[514]. Šis apibrėžimas kelia klausimų, kaip taip aiškinant pasisavinimo požymį jis galėtų būti atskirtas nuo elektroninių duomenų neteisėto įgijimo. Tiesa, šią nuomonę išsakę BK 198 straipsnį komentavę autoriai elektroninių duomenų įgijimą laikė po perėmimo einantį etapą, „kurio metu asmuo realiai gauna šiuos duomenis“[515]. Matyti, kad toks aiškinimas yra chaotiškas, neleidžiantis nustatyti ne tik įgijimo ir perėmimo, bet taip pat ir įgijimo bei pasisavinimo požymių skirtumų, lemiantis jų dubliavimą. Todėl darytina prielaida, kad įstatymų leidėjas, BK 198 straipsnio dispozicijoje įtvirtinęs pakankamai daug alternatyvių neteisėtą elektroninių duomenų gavimą žyminčių požymių, pasisavinimui siekė suteikti savarankišką turinį. Atsižvelgiant į pasisavinimo nuoseklaus aiškinimo svarbą, jo interpretavimas turėtų kisti gana radikaliai – randant elektroninių duomenų pasisavinimo ir turto pasisavinimo bendrumų. Be abejo, elektroninės erdvės kontekste bandant pritaikyti turtinių nusikalstamų veikų doktrinoje ir teismų praktikoje pateiktus pasisavinimo išaiškinimus turėtų būti apsisprendžiama, ar tokie šio požymio aiškinimai ir kokia apimtimi gali būti pritaikomi „skaitmeniniame kontekste“.

Pagal susiformavusią teismų praktiką turto pasisavinimas yra tada, 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 nuosavu ir taip padaro žalos turto savinin-

[512] Žėkas T., *supra* note 498, p. 142.

[513] Iki 2007 metų BK 198 straipsnio pakeitimų ši nusikalstama veika vadinta kompiuterinės informacijos pasisavinimu ir skleidimu.

[514] Abramavičius, A., *et al*., *supra* note 160, p. 433.

[515] *Ibid*., p. 432.

kui[516]. Toks aiškinimas svarbus keliais aspektais: 1) jis nurodo specifinį subjekto santykį su nusikalstamos veikos dalyku. Būtent šis santykis, mokslinėje literatūroje (D. Bukelienės, E. Sinkevičius ir kt.)[517] ir teismų praktikoje laikomas vienu iš kriterijų, leidžiančių turto pasisavinimą atskirti nuo kitų turtinių nusikalstamų veikų; 2) konstatuojant pasisavinimą turėtų būti nustatomas turtinės žalos padarymo faktas kaltininkui neteisėtai užvaldžius svetimą turtą[518]. Tačiau šie kriterijai kelia nemažai problemų juos taikant elektroninės erdvės kontekste, t. y. sprendžiant, ką įstatymų leidėjas siekė kriminalizuoti elektroninių duomenų pasisavinimu.

Pirmasis kriterijus, apibūdinantis specifinį kaltininko santykį su turtu, reikalauja, kaip tai matyti iš BK 183 straipsnio dispozicijos, konstatuoti, kad turtas buvo jam patikėtas arba buvo jo žinioje. Tokių specialių įgaliojimų išaiškinimas suformuluotas teismų praktikoje, taip pat įvairūs šių įgaliojimų aiškinimo aspektai pateikiami ir mokslinėje literatūroje. Nevystant plačiau diskusijos dėl turto pripažinimo patikėtu ar esančio kaltininko žinioje, bendriausia prasme teigtina, kad patikėtas turtas – „tai einamų pareigų, specialių pavedimų bei sutarčių pagrindu teisėtai kaltininko valdomas svetimas turtas, kurio atžvilgiu kaltininkas turi teisiškai apibrėžtus įgalinimus“[519]. Mokslinėje literatūroje apie patikėtą turtą kalbama kiek plačiau: patikėto turto požymis nustatomas ir tada, kai, pavyzdžiui, „įsakymo, administracinio akto, darbinių santykių ar sutarčių pagrindu bei pagal teisiškai apibrėžtus įgaliojimus valdo, tvarko, naudoja ar net disponuoja jam patikėtais svetimais daiktais ir svetimomis turtinėmis ar realizuoja svetimus turtinius reikalavimus, t. y. disponuoja svetimu turtu“[520]. Tuo tarpu kaltininko žinioje esantis turtas pagal teismų praktiką yra „toks turtas, kai kaltininkas dėl savo einamų pareigų turi teisę pavaldiniams, kuriems patikėtas turtas, duoti nurodymus dėl šio turto panaudojimo“[521]. Tokius aiškinimus įprasta taikyti kaltininkui inkriminuojant turto pasisavinimą, tačiau BK 198 straipsnyje numačius elektroninių duomenų pasisavinimo požymį neišvengiamai kyla klausimų, kokia apimtimi ir kaip mi-

[516] Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2009 m. gegužės 5 d. nutartis baudžiamojoje byloje (bylos Nr. 2K-104/2009), Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2007 m. kovo 20 d. nutartis baudžiamojoje byloje (bylos Nr. 2K-123/2007), Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2006 m. balandžio 25 d. nutartis baudžiamojoje byloje (bylos Nr. 2K-396/2006), Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2006 m. gegužės 30 d. nutartis baudžiamojoje byloje (bylos Nr. 2K-330/2006).

[517] Bukelienė, D. *Baudžiamoji atsakomybė už turto pasisavinimą ir turto iššvaistymą (teoriniai ir praktiniai aspektai)*. Vilnius: Eugrimas, 2008, p. 132; Sinkevičius, E., *supra* note 26, p. 169–172.

[518] Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2008 m. gruodžio 9 d. nutartis baudžiamojoje byloje (bylos Nr. 2K-368/2008), Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2009 m. kovo 31 d. nutartis baudžiamojoje byloje (bylos Nr. 2K-76/2009) ir kt.

[519] Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2009 m. balandžio 28 d. nutartis baudžiamojoje byloje (bylos Nr. 2K-90/2009), Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2007 m. lapkričio 27 d. nutartis baudžiamojoje byloje (bylos Nr. 2K-733/2007), Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2006 m. balandžio 11 d. nutartis baudžiamojoje byloje (bylos Nr. 2K-213/2006), Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2006 m. birželio 27 d. nutartis baudžiamojoje byloje (bylos Nr. 2K-467/2006), Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2010 m. kovo 23 d. nutartis baudžiamojoje byloje (bylos Nr. 2K-198/2010) ir kt.

[520] Sinkevičius, E., *supra* note 26, p. 170.

[521] Lietuvos Aukščiausiojo Teismo senato 1998 m. gruodžio 22 d. nutarimo Nr. 8 „Dėl teismų praktikos sukčiavimo ir turto pasisavinimo arba iššvaistymo baudžiamosiose bylose (BK 274–275 straipsniai)“ 10 punktas. *Teismų praktika*. 1998, Nr. 10.

nėtas kriterijus turėtų būti aiškinamas elektroninių duomenų konfidencialumą pažeidžiančioje nusikalstamoje veikoje. Juo labiau kad apie ne kartą minėtą *elektroninių duomenų kaip daikto* (angl. *informatikon-as-thing*) palyginimą įmanoma kalbėti tik metaforiškai.

Pagrindinė problema taikant kaltininko specifinio santykio su elektroniniais duomenimis kriterijų yra ta, kad dažnai prie neviešų elektroninių duomenų nustatytomis sąlygomis teisėtą prieigą turi keletas kategorijų asmenų: 1) tie, kurie tiesiogiai tvarko elektroninius duomenis, kaip pirminį šaltinį (pavyzdžiui, užtikrina elektroninių duomenų įvedimą į duomenų bazę, jų tvarkymą joje ir pan.); 2) tie, kurie tiesiogiai veiksmų su pirminiu šaltiniu neatlieka, tačiau dėl darbinių funkcijų ar sutarčių pagrindu turi prieigą prie tokių duomenų (pavyzdžiui, duomenų bazių naudotojai, kurie gali susipažinti su jose esančiai neviešais elektroniniais duomenimis ir pan.). Nei baudžiamosios teisės doktrinoje, nei teismų praktikoje nekilus diskusijai šiuo klausimu iš tiesų sudėtinga spręsti, kuriems iš minėtų asmenų galėtų būti taikoma pasisavinimo veika. Tikslumo dėlei reikėtų atkreipti dėmesį į tai, kad teismų praktikoje sutinkami reti atvejai, kai, kaltininkui inkriminuojant BK 198 straipsnyje numatytą nusikalstamą veiką, nustatoma, kad jis turėjo teisėtą prieigą prie elektroninių duomenų. Tačiau apie nuoseklią BK 198 straipsnyje numatytų požymių taikymo praktiką kalbėti yra sudėtinga – kaltininkui tokiais atvejais inkriminuojamas duomenų neteisėtas stebėjimas ir fiksavimas[522], neteisėtas stebėjimas ir įgijimas[523] arba neteisėtas įgijimas ir pasisavinimas[524].

Antrasis išskirtas turto pasisavinimo požymis sietas 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[525]. Tačiau, skirtingai nei turto pasisavinimo atveju, kai dėl turto netekimo nukentėjusiajam yra padaroma turtinė žala, elektroninių duomenų pasisavinimo atveju kalbėti apie panašią žalą sudėtinga. Kaltininkas, turėdamas teisėtą prieigą prie duomenų, juos gali gauti daug paprasčiau – jam nėra būtinas originalas, nes elektroniniai duomenys gali būti atspausdinami, užrašomi ar gaunami kitais panašiais veiksmais. Tokiais atvejais, kai poveikis pirminiam elektroninių duomenų šaltiniui nėra padaromas, tenka kelti klausimą ir dėl pačios žalos nustatymo: tiesioginio elektroninių duomenų netekimo nustatyti nepavyktų, nes duomenys lieka pas nukentėjusįjį (nors žala konfidencialumui yra padaryta).

Kol kas nei baudžiamosios teisės doktrinoje, nei teismų praktikoje aiškiai neapibrėžtas elektroninių duomenų pasisavinimo požymis, autorės nuomone, sudaro galimybes bendriausia prasme diskutuoti dėl keleto jo aiškinimo būdų. Pavyzdžiui: 1) laikantis pakankamai plataus požiūrio pasisavinimas galėtų būti inkriminuojamas tais atvejais, kai neviešus

---

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

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

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

[525] Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2006 m. gegužės 30 d. baudžiamojoje byloje (bylos Nr. 2K-330/2006), Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2006 m. balandžio 25 d. nutartis baudžiamojoje byloje (bylos Nr. 2K-396/2006), Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2008 m. gruodžio 9 d. nutartis baudžiamojoje byloje (bylos Nr. 2K-368/2008), Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2009 m. kovo 31 d. nutartis baudžiamojoje byloje (bylos Nr. 2K-76/2009).

elektroninius duomenis neteisėtai gauna asmuo, kuriam buvo suteikta prieigos teisė prie jų. Kadangi tokiu elektroninių duomenų gavimu neigiamas poveikis jų pirminiam šaltiniui nėra daromas, tai šie duomenys išlieka, nors kartu ir atitenka kaltininkui; 2) pakankamai siauras požiūris į elektroninių duomenų pasisavinimą būtų artimesnis turto pasisavinimo aiškinimui. Pasisavinimas tuomet inkriminuotinas nustačius, kad kaltininkas priklausė tai kategorijai asmenų, kurie yra tiesiogiai atsakingi už elektroninių duomenų, kaip pirminio šaltinio, tvarkymą. Pati žala pasireikštų tokių duomenų netekimu, kai elektroniniai duomenys lieka tik pas kaltininką. Tokiais atvejais turėtų būti sprendžiama ir dėl BK 196 straipsnio, numatančio baudžiamąją atsakomybę už neteisėtą poveikį elektroniniams duomenims, taikymo, nes kaltininkas elektroninius duomenis bus sunaikinęs, pašalinęs ar pan. Taip pat neatmestinos ir kitos galimos specialaus subjekto bei žalos kilimo arba priešingai – jos kaip požymio atsisakymo variacijos.

Taigi akivaizdu, kad neviešų elektroninių duomenų pasisavinimas gali būti sunkiai aiškinamas pagal tradicinio turto pasisavinimo suvokimą. Tokia situacija neišvengiama dėl paties turto pasisavinimo specifikos ir pernelyg didelės jo sąsajos su turtinių nusikalstamų veikų doktrina – aiškinant turtinę žalą, specialaus subjekto požymius, materialų atsakingumą už turtą, jei jis kaltininkui buvo patikėtas, paties turto patikėjimo ar jo buvimo kaltininko žinioje požymius ir pan. Todėl galima būtų diskutuoti, ar interpretuojant elektroninių duomenų pasisavinimą neturėtų būti nutolstama nuo tų jį apibūdinančių požymių, kurie glaudžiai susiję su turtu. Atsisakius elektroninės erdvės kontekste sunkiai pritaikomų kriterijų, apie elektroninių duomenų pasisavinimą galima būtų kalbėti kaip apie neteisėtą kaltininko tapimą faktiniu elektroninių duomenų turėtoju, kai jam konkrečiomis sąlygomis buvo suteikta prieigos prie tokių duomenų teisė, tačiau jis peržengė jos teisėtumo ribas.

2.2.6. Paskleidimas

Apibūdindamas neteisėtus neviešų elektroninių duomenų perdavimo kitiems asmenims veiksmus, įstatymų leidėjas į analizuojamos nusikalstamos veikos sudėtį įtraukė duomenų paskleidimo požymį. Analizuojant BK nuostatas matyti, kad tokia pavojinga veika nėra vienintelė, kuri BK apibūdina informacijos kaip nusikalstamos veikos dalyko atskleidimo veiksmus. Todėl artimi savo prasme paskleidimui požymiai gali būti laikomi informacijos perdavimas (BK 119, 210, 217, 296 straipsniai), atskleidimas (125, 211, 297 straipsniai), perleidimas (124 straipsnis), jos paskelbimas (168 straipsnis) ir pan. Be to, ir BK 198 straipsnio redakcijoje, galiojusioje iki 2007 metų, paskelbimas buvo minimas šalia kitų pagal savo pobūdį panašių – informacijos paskelbimo ir platinimo veikų. Tik po 2007 metų pakeitimų minėtiems kaltininko veiksmams apibūdinti pasirinkta ši viena elektroninių duomenų paskleidimo veika, kuri, galima spėti, turėjo sujungti bet kokias kitas neteisėtas duomenų perdavimo tretiesiems asmenims veikas.

Aiškinantis, koks turinys suteiktas elektroninių duomenų paskleidimo veikai, aktualu nustatyti, kokiuose kituose BK straipsniuose ji numatyta ir kaip tų nusikalstamų veikų kontekste yra interpretuojama. BK tokių nusikalstamų veikų 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, tačiau kartu galima pastebėti, kad tokios veikos suvokimas pa-

našus ir kitų minėtų nusikalstamų veikų atveju. Taigi paskleidimas bendriausia prasme suvokiamas kaip informacijos pranešimas bent vienam kitam asmeniui, nepriklausomai nuo kaltininko pasirinkto tokio pranešimo būdo. Taip, pavyzdžiui, paskleidimą apibūdino BK 154 straipsnį komentavę autoriai: anot jų, paskleidimas tai „informacijos pranešimas kuriuo nors būdu bent vienam asmeniui, išskyrus nukentėjusįjį“[526]. Panašiai šmeižimo nusikalstamos veikos kontekste analizuojant platinimą yra pasisakę ir rusų mokslininkai. Platinimu, anot jų, laikomas informacijos pranešimas „bent vienam pašaliniam asmeniui, nepriklausomai nuo to, ar šis pranešimas buvo išplatintas toliau“[527] ar nukentėjusysis dalyvavo tokių kaltininko veiksmų metu[528], taip pat nepriklausomai nuo pasirinkto tokių veiksmų atlikimo būdo (beje dažnai minimas ir informacijos platinimas elektroninėje erdvėje)[529]. Žvelgiant į platesnį paskleidimo teisinį kontekstą matyti, kad taip paskleidimo veiksmai suvokiami ne tik baudžiamosios, bet taip pat civilinės teisės doktrinoje. Joje paskleidimas aiškinamas kaip „duomenų perdavimas bet kokiomis priemonėmis <...> bent vienam asmeniui, išskyrus tą, apie kurį tie duomenys skleidžiami“[530]. Patys paskleidimo būdai gali būti labai įvairūs – tai ir jų pranešimas vienam ar daugeliui asmenų pokalbio metu, viešuose pasisakymuose, per visuomenės informavimo priemones, paskleidžiant elektroninėje erdvėje, perduodant už atlygį arba be jo ir pan.

Toks turinys tinkamas ir paskleidimo veikai, numatytai neteisėto elektroninių duomenų perėmimo ir panaudojimo sudėtyje, tačiau šis aiškinimas reikalauja ir tam tikro patikslinimo, atsižvelgiant į paskleidimo specifiką elektroninėje erdvėje. Minėtose paskleidimo interpretacijose daugiau dėmesio skiriama aktyviems kaltininko veiksmams perduodant duomenis, tačiau nieko nesakoma apie tam tikras duomenų siūlymo apraiškas elektroninėje erdvėje. O tiksliau, problema ta, ar paskleidimas turėtų būti siejamas tik su duomenų perdavimu (apimančio įvairius būdus, pavyzdžiui, siuntimą elektroninėje erdvėje, duomenų perdavimą laikmenoje ir pan.), ar tokia veika galėtų būti pripažįstamas ir duomenų padarymas prieinamais elektroninėje erdvėje (pavyzdžiui, juos paskelbiant tinklalapyje, padarant prieinamais per P2P kompiuterių tinklą ir pan.). Toks kaltininko veiksmų atskyrimas mokslinėje literatūroje (I. Walden, U. Sieber ir kt.) daugiausia analizuojamas neteisėto turinio medžiagos platinimo kontekste, tačiau akivaizdu, kad ši problema aktuali analizuojnat ir BK 198 straipsnyje numatytą nusikalstamą veiką. Kai pirmuoju atveju kaltininko veiksmai yra daugiau siejami tarsi su informacijos „stūmimu“ iš siuntėjo šios informacijos gavėjui, tai antruoju atveju, anot I. Walden, „procesas yra labiau panašus į gavėjo informacijos traukimą iš siuntėjo“[531]. Šis skirtumas leido U. Sieber, analizuojant jurisdikcijos nustatymo problemas, išskirti atskirus „stūmimo“ ir „traukimo“ duomenų

[526] Abramavičius, A., *et al*., *supra* note 160, p. 196.

[527] *Kurs ugolovnogo prava: uchebnik* [The course of criminal law: The textbook]. Kuznecoba, N. F.; Tjazhkova, I. M. (red). Moskva: Zercalo-M, 2002, s. 233.

[528] Naumov, A. V., *supra* note 444, p. 154.

[529] *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, s. 98; *Rossijskoe ugolovnoe pravo: v dvukh tomakh: uchebnik* [Russian criminal law: In two volumes: The textbook]. Rarog A.I. (red). 5-as pataisytas ir papildytas leidimas. Moskva: Proftekhobrazobanie, 2005, s. 107.

[530] *Lietuvos Respublikos civilinio kodekso komentaras. Antroji knyga. Asmenys*. Mikelėnas V. *et al*. Vilnius: Justitia, 2002, p. 66.

[531] Walden, I., *supra* note 70, p. 183.

perdavimo būdus (angl. *push and pull techniques*)[532]. Akivaizdu, kad duomenų „stūmimo" veiksmai rodo aktyvų kaltininko veikimą paskleidžiant elektroninius duomenis, tuo tarpu galimybių prieiti prie duomenų sudarymas yra susijęs su pasyviu kaltininko elgesiu, kai „traukimo" veiksmai atliekami elektroninių duomenų gavėjo.

Analizuojant elektroninių duomenų paskleidimą BK 198 straipsnio kontekste, reikėtų pripažinti, kad tokia veika, nesiaurinant paskleidimo turinio, turėtų apimti abu anksčiau minėtus atvejus. Taigi nepriklausomai nuo to, kieno – siuntėjo ar gavėjo – duomenų perdavimo procesas buvo inicijuotas, tiek aktyvūs duomenų perdavimo veiksmai (konkrečiam asmeniui ar neapibrėžtam jų ratui), tiek ir sąlygų prieiti prie duomenų sudarymas turėtų būti pripažinti elektroniniu paskleidimu. Apie tokią interpretavimo galimybę yra užsiminę ir D. Valatkevičius bei R. Mockevičius komentuodami BK 198 straipsnį. Anot jų, „elektroninių duomenų paskleidimas reiškia elektroninių duomenų teikimą viešumai, jų garsinimą ir darymą žinomais arba bet kokį perdavimą kitiems asmenims"[533]. Kartu autoriai pripažįsta, kad paskleidimu turėtų būti laikomas ir „elektroninių duomenų <...> patalpinimas į vietas (pvz., tinklalapį internete), iš kur tampa prieinami kitiems asmenims (tai apima ir nuorodų į tokias vietas kūrimą <...> siekiant palengvinti priėjimą prie šių duomenų)"[534]. Beje, tokios elektroninio paskleidimo vertinimo tendencijos matyti ir teismų praktikoje – joje paskleidimu laikomi ne tik aktyvūs kaltininko veiksmai neteisėtai perduodant duomenis tretiesiems asmenims, bet taip pat ir sąlygų, leidžiančių susipažinti su duomenų turiniu, sudarymas, kai jie paskelbiami elektroninėje erdvėje. Pavyzdžiui, Šiaulių miesto apylinkės teismo 2011 m. liepos 18 d. teismo baudžiamajame įsakyme baudžiamojoje byloje (bylos Nr. 1-617-885/2011) paskleidimas pasireiškė atspausdintų Valstybinės mokesčių inspekcijos kompiuterinės duomenų bazės išrašų (pažymų) perdavimu trečiajam asmeniui. Tuo tarpu sąlygų prieiti prie elektroninių duomenų sudarymo vertinimas matyti Mažeikių rajono apylinkės teismo 2009 m. rugpjūčio 12 d. nuosprendyje baudžiamojoje byloje (bylos Nr. 1-188-785/2009), kurioje paskleidimu pripažintas neviešų elektroninių duomenų apie AB kilusį gaisrą paskelbimas internetiniame puslapyje (http://rutube.ru). Beje, pastaruoju atveju veikos baigtumo momento nustatymui tai, ar bent vienas kitas žmogus spėjo susipažinti su neviešais elektroniniais duomenimis, įtakos neturi turėti.

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 – šis požymis rodo nebaigtinį neteisėto disponavimo elektroniniais duomenimis veikų sąrašą. Jo formuluotė leidžia teigti, kad tokia veika itin dažnai gali būti vertinama kaip kitų nusikalstamų veikų padarymo būdas, pavyzdžiui, jei neteisėtai panaudojant neviešus elektroninius duomenis padaromas sukčiavimas (BK 182 straipsnis), neteisėtai prisijungiama prie IS (elektroninės bankininkystės sistemos, elektroninio pašto ar pan.) ir daugelis kitų atvejų. Kaip pavyzdys paminėtinas Šilalės rajono apylinkės teismo 2010 m. lapkričio 4 d. teismo baudžiamasis įsakymas baudžiamojoje

[532] *Cybercrime and Jurisdiction: a global survey*. Koops B.–J., Brenner S. (eds). The Hague: T.M.C. Asser Press, 2006, p. 198–201.
[533] Abramavičius, A., *et al*., *supra* note 160, p. 433.
[534] *Ibid*.

byloje (bylos Nr. 1-121-799/2010) – jame neteisėtu elektroninių duomenų panaudojimu pripažintas banko naudotojo ID, banko slaptažodžio ir banko kodo panaudojimas prisijungiant prie elektroninės bankininkystės IS. 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), tačiau diskutuotina, kodėl kaltininkui nebuvo inkriminuota BK 198[1] straipsnyje numatyta neteisėto prisijungimo prie IS nusikalstama veika.

Nors kitoks neviešų elektroninių duomenų panaudojimo požymis tiesiogiai numatytas BK 198 straipsnio dispozicijoje, tačiau mokslinėje literatūroje galima sutikti nuomonių, kad baudžiamoji atsakomybė pagal dabartinį teisinį reguliavimą nekyla už veiksmus, „kai asmuo, neteisėtai panaudodamas prisijungimo duomenis, neteisėtai prisijungė prie kito asmens *Facebook* profilio ir pastarojo asmens vardu per šį profilį pradėjo platinti seksualinio pobūdžio informaciją“[535]. Su tokia išsakyta pozicija sunkiai galima būtų sutikti, nes baudžiamąją atsakomybę už neteisėtą prisijungimą prie IS numato BK 198[1] straipsnis, o nustačius, kad prisijungiant buvo panaudoti nevieši elektroniniai duomenys, svarstytina galimybė kaltininko veikos kvalifikavimui taikyti ir BK 198 straipsnį[536].

Todėl problemos analizuojant kitokio neviešų elektroninių duomenų panaudojimo veiką turėtų kilti ne tiek dėl to, ar ji gali būti inkriminuojama kaltininkui panaudojus duomenis darant kitas nusikalstamas veikas, kiek sprendžiant baudžiamojo įstatymo normos visumos ir dalies konkurencijos įveikimo klausimą. Šis klausimas aktualus tuo, kad kitokio neviešų elektroninių duomenų panaudojimo veika dažnai gali tapti kitų nusikalstamų veikų padarymo būdu. Minėtos konkurencijos sprendimui didelės įtakos turi nusikalstamos veikos baudžiamumas: baudžiamosios teisės doktrinoje laikomasi vieningos nuomonės, kad nusikalstamos veikos yra kvalifikuojamos pagal sutaptį, jeigu į visumą įtraukta dalis yra pavojingesnė nei pati visuma. Tokiais atvejais, kaip teigia V. Pavilonis, „ji negali būti aprėpta tokios visumos ir turi būti kvalifikuota atskirai, t. y. pagal dviejų arba daugiau nusikaltimų sutaptį“[537]. Elektroninių nusikalstamų veikų kontekste sprendžiant šį normų konkurencijos įveikimo klausimą neišvengiamai tenka atsižvelgti į neteisėto elektroninių duomenų perėmimo ir panaudojimo nusikalstamos veikos baudžiamumą. BK 198 straipsnio 1 dalies sankcijoje numatyta maksimali laisvės atėmimo bausmė siekia ketverius metus, atitinkamai šioje dalyje numatyta nusikalstama veika priskiriama apysunkių nusikaltimų kategorijai (BK 11 straipsnio 4 dalis). Todėl akivaizdu, kad praktikoje gali pasitaikyti atvejų, kai neteisėto neviešų elektroninių duomenų panaudojimo neapims kitos nusikalstamos veikos. Pavyzdžiui, sprendžiant jau anksčiau minėto neteisėto prisijungimo prie IS, sukčiavimo (BK 182 straipsnio 1, 3 dalys) ir kitų nusikalstamų veikų, kurios buvo padarytos neteisėtai panaudojant neviešus elektroninius duomenis, inkriminavimo klausimus. Tokiais atvejais, autorės nuomone, iš tiesų gali kilti dilema, ar tokio teisinio reguliavimo nelemia blogas baudžiamojo įstatymo normų suderinamumas ir ar tikrai įstatymų leidėjas siekė nustatyti būtent tokias plačias BK 198 straipsnio taikymo galimybes.

[535] Štitilis, D., *et al*., *supra* note 332, p. 260.

[536] Plačiau apie neteisėto prisijungimo prie IS ir neviešų elektroninių duomenų panaudojimo santykį žiūrėti V skyriaus 1 dalyje.

Be to, atsižvelgiant į tai, ar platinama seksualinio pobūdžio informacija susijusi su asmens privataus gyvenimo neliečiamumo pažeidimais, taip pat, ar ji pažeidžia asmens garbę ir orumą, kaltininkui gali būti inkriminuojamos nusikalstamos veikos numatytos BK 154 ar 168 straipsniuose.

[537] Pavilonis, V., *supra* note 407, p. 45.

2.2.8. Pavojingų veikų neteisėtumo vertinimas

Lietuvos BK neteisėtas disponavimas neviešais elektroniniais duomenimis nėra susietas su neteisėta prieiga prie IS, šios nusikalstamos veikos kriminalizuotos *per se* skirtinguose BK 198 ir 198[1] straipsniuose. Todėl, nors neteisėta prieiga prie IS paprastai suponuos ir neteisėtą prieigą prie joje laikomų duomenų, tačiau teisėta prieiga prie IS neleidžia *ex ante* preziumuoti, kad šioje sistemoje nebuvo padaryti neviešų elektroninių duomenų konfidencialumo pažeidimai. Kadangi toks įstatymo leidėjo požiūris atskiria elektroninių duomenų ir IS konfidencialumo pažeidimus, tai būtų galima pritarti J. Clough, kad „tose jurisdikcijoje, kuriose dėmesio centre yra prieiga prie duomenų, leistinumo klausimas turėtų būti užduodamas dėl kiekvienos tokios prieigos“[538]. Autorius taip pat pažymi, kad net tais atvejais, kai pirminė prieiga yra teisėta, tolesni asmens veiksmai, kuriais yra pažeidžiamos nustatytos sąlygos, yra neteisėti[539].

Iš BK 198 straipsnyje aprašytos elektroninių duomenų perėmimo ir panaudojimo nusikalstamos veikos matyti, kad BK konfidencialumo pažeidimai, atliekant įvairius neteisėtus veiksmus su neviešais elektroniniais duomenimis, kriminalizuoti pakankamai plačiai. Toks nusikalstamos veikos sudėties požymių aprašymas galėjo būti pasirinktas dėl to, kad pati „informacinio privatumo“[540] sritis, kaip ją įvardijo N. C. Manson ir O. O'Neill, yra plati, todėl sudaro galimybes analizuoti įvairius nepageidaujamus veiksmus, kuriais nesilaikoma nustatytų įpareigojimų be leidimo konkretiems asmenims arba bet kam kitam sužinoti duomenis ar juos platinti. Taigi tokie apribojimai bendriausia prasme gali apimti reikalavimus susilaikyti nuo mėginimų sužinoti neviešus elektroninius duomenis, neatskleisti jų kitiems, nenaudoti jų nenumatytiems tikslams ir pan. Atsižvelgiant į tai, BK 198 straipsnio dispozicijoje įtvirtinta daug pavojingų veikų alternatyvų, 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 – neteisėtumo konstatavimas yra būtinas dėl kiekvienos pavojingos veikos atskirai. Kadangi, kaip minėta, BK 198 straipsnis yra siejamas tiek su *IS laikomų* („*nejudamų*“), tiek ir *IS perduodamų* neviešų elektroninių duomenų konfidencialumo pažeidimais, tai neteisėtumą taip pat galima analizuoti duomenų konfidencialumo ir komunikacijos konfidencialumo kontekste.

Disponavimo neviešais elektroniniais duomenimis neteisėtumui nustatyti taikant objektyvų kriterijų, neteisėtumas reikštų, kad asmuo, gaudamas prieigą ar atlikdamas kitus veiksmus su neviešais elektroniniais duomenimis, neturi teisėto leidimo tokiems veiksmams arba nors toks leidimas yra suteiktas, tačiau šiuos veiksmus jis atlieka pažeisdamas nustatytą neviešų elektroninių duomenų disponavimo tvarką (įpareigojimus). Kaip buvo minėta, elektroninių duomenų priskyrimas neviešų duomenų kategorijai priklauso nuo daugelio aplinkybių *inter alia* ir pačių duomenų rūšies. Be to, šios aplinkybės svarbios nustatant, ar tarp asmens gavusio duomenis ar atlikusio su jais tam tikrus veiksmus ir

[538] Clough, J., *supra* note 110, p. 76.
[539] *Ibid.*
[540] Manson, N. C.; O'Neill, O., *supra* note 459, p. 98.

duomenų subjekto egzistavo įpareigojimas išlaikyti elektroninių duomenų konfidencialumą. Toks gana bendro pobūdžio reikalavimas reikštų, kad asmuo, siekiantis gauti neviešus elektroninius duomenis ar atlikti su jais kitus disponavimo veiksmus, turi laikytis nustatytų reikalavimų, kokiu būdu jis gali gauti duomenis, atlikti su jais veiksmus ir kokiu tikslu jais disponuoti. Taigi, vertinant konfidencialumo įpareigojimus, galima būtų pritarti mokslinėje literatūroje išsakomai minčiai, kad nustatytos pareigos „garantuoja duomenų subjektui teisę, jog informacija apie jį nebūtų naudojama kitais tikslais arba nebūtų atskleista be jo sutikimo nebent yra kitos su viešuoju interesu susijusios svarbesnės priežastys tam padaryti“[541].

Pavyzdžiui, prieigos prie asmens duomenų[542] teisėtumo sąlygas nustato Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas (*Valstybės žinios*. 1996, Nr. 63-1479) (toliau – Teisinės apsaugos įstatymas), kurio nuostatos yra suderintos su 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (toliau – Direktyva 95/46/EB)[543]. Šiuo įstatymu siekiama apginti žmogaus privataus gyvenimo neliečiamumą tvarkant asmens duomenis, atitinkamai šis įstatymas numato pagrindinius asmens duomenų tvarkymo reikalavimus (3 straipsnis), teisėto tvarkymo kriterijus (5 straipsnis), asmens duomenų teikimo tvarką (6 straipsnis) ir kitas asmens veiksmų, atliekamų su asmens duomenimis, teisėtumo vertinimui svarbias nuostatas. Todėl asmens duomenys, pavyzdžiui, gali būti renkami tik apibrėžtais ir teisėtais tikslais, toliau negali būti tvarkomi tikslais, nesuderinamais su nustatytaisiais prieš renkant asmens duomenis, tvarkomi tiksliai, sąžiningai ir teisėtai (3 straipsnio 1 dalies 1, 2 punktai), asmens duomenys gali būti teikiami tik pagal nustatytą tvarką – esant duomenų valdytojo ir duomenų gavėjo sudarytai asmens duomenų teikimo sutarčiai (daugkartinio teikimo atveju) arba duomenų gavėjo prašymui (vienkartinio teikimo atveju) (6 straipsnis), taip pat šis įstatymas numato ir daugelį kitų svarbių reikalavimų. Atitinkamai Teisinės apsaugos įstatymo nuostatos bus pažeidžiamos tiek tais atvejais, kai asmuo nesilaiko nustatytos asmens duomenų gavimo tvarkos (pažeisdamas 6 straipsnio reikalavimus), tiek ir tada, kai, turėdamas teisėtą prieigą prie duomenų, juos naudos nenumatytiems tikslams. Paskutinįjį atvejį D. Roeland ir E. Macdonald, analizuodami Direktyvos 95/46/EB numatytus teisėtumo ir duomenų surinkimo aiškiai apibrėžtais bei teisėtais tikslais principus (6 straipsnio 1 dalies a, b punktai), susiejo su *ultra vires* veikimu, t. y. jei asmuo, turintis teisėtą prieigą prie asmens duomenų, juos gauna, tvarko ar laiko tais tikslais, kurių jam nesuteikia teisės normos, jis veikia *ultra vires* ir todėl neteisėtai laiko, gauna bei tvarko tokius duomenis[544].

---

[541] Rowland, D.; Macdonald, E. *Information Technology Law*. 3–as leidimas. Sydney; Portland (Or.): Cavendish Publishing, 2005, p. 349.

[542] Anksčiau darbe atkreiptas dėmesys į tai, kad teismų praktikoje neteisėtas disponavimas elektroninę formą turinčiais asmens duomenimis iš baudžiamosios teisės pozicijų vertinamas nevienodai. Dažniausiai tokie neteisėti kaltininko veiksmai kvalifikuojami pagal BK 198 straipsnį, tačiau galima sutikti atvejų, kai jam inkriminuojamas BK 167 straipsnyje esanti neteisėto informacijos apie privatų asmens gyvenimą rinkimo veika (plačiau žr. 460 išnaša).

[543] 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo. [1995] OL L 281/31.

[544] Rowland, D.; Macdonald, E., *supra* note 541, p. 350.
Šie autoriai atkreipė dėmesį į tai, kad neteisėtumas yra pakankamai platus terminas ir vienodai pritaikomas tiek viešam, tiek privačiam sektoriui, ir rodo tuos pažeidimus, kurie gali būti vertinami tiek iš baudžiamosios, tiek ir iš civilinės teisės pozicijų.

Analizuojant nors ir negausią teismų praktiką matyti, kad BK 198 straipsnyje esanti nusikalstama veika inkriminuojama ir tais atvejais, kai kaltininkas, turėdamas prieigą prie tvarkomų asmens duomenų, savo veiksmais pažeidė nustatytus Teisinės apsaugos įstatymo ir kitų teisės aktų reikalavimus. Pavyzdžiui, Šiaulių miesto apylinkės teismo 2011 m. liepos 18 d. teismo baudžiamuoju įsakymu baudžiamojoje byloje (bylos Nr. 1-617-885/2011) V. Š. nuteistas pagal BK 228 straipsnio 1 dalį (piktnaudžiavimas) ir pagal BK 198 straipsnio 1 dalį. Šioje byloje teismas konstatavo, kad *V. Š., veikdamas bendrininkų grupėje su G. L, būdamas valstybės tarnautoju – (duomenys neskelbtini), turėdamas tarnybinę prieigą prie valstybinės mokesčių inspekcijos kompiuterinės duomenų bazės apie fizinių asmenų asmens duomenis, <...> naudodamasis tarnybiniu kompiuteriu, 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, šeimyninę padėtį, išduotus asmens tapatybės dokumentus, darbovietę, pajamas, šiuos duomenis neteisėtai įgijo, atspausdinant valstybinės mokesčių inspekcijos kompiuterinės duomenų bazės išrašus (pažymas), po to, neteisėtai įgytus neviešus minėtus elektroninius duomenis neteisėtai paskleidė <...> per kelis kartus perduodamas G. L.* Apie šių V. Š. veiksmų neteisėtumą teismas sprendė atsižvelgdamas į įvairius teisės aktuose numatytų reikalavimų pažeidimus, tarp kurių paminėtas Teisinės apsaugos įstatymas, nustatantis teisėtus asmens duomenų tvarkymo kriterijus (pažeista 5 straipsnio 1 dalis), Lietuvos Respublikos mokesčių administravimo įstatymas, *inter alia* numatantis ir mokesčių administratoriaus pareigas (pažeisti 32 straipsnio 2, 5 ir 6 punktai), Lietuvos Respublikos valstybės tarnybos įstatymas, nustatantis valstybės tarnautojo pareigas (pažeisti 15 straipsnio 1 dalies 5 ir 9 punktai), ir daugeli kitų.

Pavyzdžiui, neviešų elektroninių duomenų konfidencialumo pažeidimai konstatuotini, kai neviešų elektroninių duomenų disponavimo apribojimus numato juridinių asmenų informacijos saugos politika ir ją įgyvendinantys dokumentai. Pavyzdžiui, Mažeikių rajono apylinkės teismo 2009 m. rugpjūčio 12 d. nuosprendyje baudžiamojoje byloje (bylos Nr. 1-188-785/2009) 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* <...>. Byloje taip pat konstatuota, kad R. R., pažeisdamas prisiimtus įsipareigojimus[545], *iš įrašymo įrenginio ir šiame įrenginyje esančio vaizdo archyvo, bylos „Incident2", kuriame buvo aplankalas „Footage» su jame esančiu vaizdo*

[545] 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, taip pat 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 turi būti numatytos informacijos saugos sąlygos ir taikoma atsakomybė".

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 internetiniame puslapyje <...>. Atsižvelgdamas į tai, teismas padarė išvadą, kad R. R. nusikalstama veika kvalifikuotina pagal BK 198 straipsnio 1 dalį. Taigi, kaip galima pastebėti, pagal besiformuojančią teismų praktiką kaltininko veiksmų neteisėtumas paprastai nustatomas, jei su neviešais elektroniniais duomenimis buvo atliekami veiksmai nesilaikant nustatytos tokio pobūdžio duomenų disponavimo tvarkos.

Neteisėtumą analizuojant kitu – elektroninių ryšių konfidencialumo pažeidimų aspektu aktualios Konvencijos dėl elektroninių nusikaltimų 3 straipsnio nuostatos ir šios Konvencijos aiškinamojoje ataskaitoje pateiktas tokių nuostatų išaiškinimas. Aiškinamojoje ataskaitoje atkreipiamas dėmesys į tai, kad baudžiamoji atsakomybė už kompiuterinių duomenų perimtį kyla tada, jei tokia veika yra padaroma tyčia ir neturint tokiems veiksmams teisės. Patys perėmimo veiksmai gali būti ir leistini, pavyzdžiui, jei duomenis perimantis asmuo turi teisę tokius veiksmus atlikti, jeigu veikia pagal nurodymus arba suteiktus įgaliojimus (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, tokias elektroninių duomenų perėmimo teisėtumo sąlygas numato ir nacionalinių teisės aktų, pavyzdžiui, Lietuvos Respublikos baudžiamojo proceso kodekso (*Valstybės žinios*. 2002, Nr. 37-1341) nuostatos, reglamentuojančios kitų procesinių prievartos priemonių taikymą (pavyzdžiui, elektroninių ryšių tinklais perduodamos informacijos kontrolę, jos fiksavimą ir kaupimą (154 straipsnis). Teisėtumo sąlygas nustato ir Lietuvos Respublikos kriminalinės žvalgybos įstatymas (*Valstybės žinios*. 2012, Nr. 122-6093), kurio 10 straipsnyje numatyta susirašinėjimo ir kitokio susižinojimo slaptos kontrolės atlikimo tvarka. Taip pat svarbu atkreipti dėmesį į tai, kad neviešų elektroninių duomenų perėmimo sąlygas gali numatyti ir įvairūs susitarimai tarp komunikavimo dalyvių, pavyzdžiui, jei elektroninių duomenų perėmimas vyksta testuojant IS veikimą, ieškant IS pažeidžiamų vietų ir pan. Taigi neviešų elektroninių duomenų perėmimo neteisėtumą rodo tai, kad padaryti veiksmai neatitinka jiems atlikti nustatytų teisėtumo kriterijų. Draudimas be faktinių elektroninių ryšių paslaugų naudotojų sutikimo klausytis, įrašyti, kaupti ar kitu būdu perimti pranešimų turinį ir srauto duomenis ar su jais susipažinti, taip pat atskleisti tokio pobūdžio duomenis arba sudaryti sąlygas juos gauti yra suformuluotas Elektroninių ryšių įstatymo 61 straipsnyje (išskyrus jame konkrečiai nurodytus atvejais). Šiais draudimais siekiama apsaugoti ryšio slaptumą, kurio nepaisymas, be abejo, sudaro sąlygas pažeisti ir neviešų IS perduodamų elektroninių duomenų konfidencialumą.

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 padidintą neviešų elektroninių duomenų svarbą ir naudojamas 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 IS atveju, leidžia išskirti ne tik *technologinį*, bet ir *teisinį* nusikalstamos veikos dalyko aspektą. Technologijų ir terminologijos klausimą keliantis elektroninių duomenų požymis analizuotas pirmiau, todėl pagrindinis dėmesys šioje dalyje skiriamas teisiniam jo aspektui – strateginei reikšmei nacionaliniam saugumui, didelei reikšmei valstybės valdymui, ūkiui ar finansų sistemai.

Pasirinktas nusikalstamų veikų elektroninių duomenų ir IS konfidencialumui kriminalizavimo būdas, kai baudžiamoji atsakomybė už neviešų elektroninių duomenų ir IS konfidencialumo pažeidimus yra numatyta skirtinguose BK 198 ir 198[1] straipsniuose, verčia atskirti ypatingą reikšmę turinčias IS nuo ypatingos reikšmės elektroninių duomenų. Todėl padidinta tiek IS, tiek ir elektroninių duomenų reikšmė pagal esamą nusikalstamų veikų aprašymą įrodinėtina savarankiškai. IS pripažinus turinčią strateginės reikšmės nacionaliniam saugumui arba didelės reikšmės valstybės valdymui, ūkiui ar finansų sistemai, joje tvarkomi duomenys paprastai taip pat gali turėti padidintos reikšmės nurodytoms sritims. Tačiau pagrindinė problema tokiais atvejais ta, ar taikytina prezumpcija, kad *visi* duomenys, tvarkomi ypatingos svarbos IS, taip pat yra didelės reikšmės valstybės valdymui, ūkiui ar finansų sistemai, o jų konfidencialumo pažeidimai kriminalizuoti BK 198 straipsnio 2 dalyje. Kaip minėta, pati IS, į ją žvelgiant plačiau, t. y. kartu su jos taikomuoju aspektu, yra skirta įvairiems organizacijos tikslams siekti, numatytoms funkcijoms įgyvendinti, taigi tam tikro darinio funkcionavimui užtikrinti, todėl IS gali būti apdorojami patys įvairiausi pagal savo reikšmę duomenys net ir tuo atveju, jei pati IS yra ypatingos svarbos. Dėl to, autorės nuomone, neteisėtas prisijungimas prie IS, atitinkančios BK 198[1] straipsnio 2 dalyje numatytus jos požymius, ne visais atvejais leidžia kalbėti apie padidintą reikšmę turinčių elektroninių duomenų konfidencialumo pažeidimus – duomenų, kuriais buvo neteisėtai disponuojama, reikšmė turi būti įvertinama savarankiškai. Atitinkamai ypatingos reikšmės IS konfidencialumo pažeidimai gali būti laikomi tik viena iš vertintinų, bet ne lemiamą reikšmę turinčių aplinkybių duomenis pripažįstant nusikalstamos veikos dalyku, numatytu BK 198 straipsnio 2 dalyje.

Strateginės reikšmės nacionaliniams saugumui, didelės reikšmės valstybės valdymui, ūkiui ar finansų sistemai turinčių elektroninių duomenų interpretavimą apsunkina tai, kad aiškių kriterijų, kaip nustatyti tokio pobūdžio duomenis, nei doktrina, nei nacionaliniai teisės aktai, nei teismų praktika nesuteikia. Lingvistinis BK 198 straipsnio 2 dalyje vartojamų terminų aiškinimas taip pat neinformatyvus, pavyzdžiui, viena iš žodžio *strateginis* reikšmių, ją susiejus su elektroniniais duomenimis, bendriausia prasme leidžia kalbėti apie suteikiančius pranašumą[546] elektroninius duomenis arba esminius, svarbius bendriesiems kovos tikslams pasiekti[547] duomenis. Nacionaliniuose teisės aktuose taip pat pateikiami tik bendro pobūdžio informacinių išteklių skirstymai į rūšis ir gana abstraktus tokio skirstymo kriterijus. Pavyzdžiui, analizuojant valstybės IS ir informacinius išteklius, galima paminėti Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo[548] 3 straipsnį, kuriame pateikiamos valstybės informacinių išteklių rūšys – ypatingos svarbos, svarbūs, žinybinės svarbos ir kiti valstybės informaciniai ištekliai. Šis skirstymas pagrįstas gana abstrakčiu grupavimo kriterijumi, t. y. kokiu mastu valstybės IS apdorojama

[546] Khokins, Dzh. M., *supra* note 179, p. 704.

[547] *Tarptautinių žodžių žodynas*. Sudarytojai Bendorienė, A., *et al*. Atsakomasis redaktorius Kinderys A. Vilnius: Alma litera, 2001, p. 707.

[548] Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas. *Valstybės žinios*. 2011, Nr. 163–7739.

informacija yra svarbi. Ypatingos svarbos valstybės informaciniai ištekliai siejami su visai valstybei svarbia informacija, svarbūs valstybės informaciniai ištekliai su kelioms institucijoms svarbia informacija, žinybinės svarbos – su informacija, svarbia vienai institucijai, tačiau pačios informacijos svarbos vertinimo kriterijai šiame įstatyme nėra pateikiami.

Viena vertus, tokia interpretavimo laisvė gali būti vertinama teigiamai, nes ypatingos svarbos elektroninių duomenų suvokimas laikui bėgant gali keistis. Kaip buvo pažymėta, analizuojant kritines IS, ypatinga svarba yra visuomet susijusi su perspektyvos klausimu. Tačiau, kita vertus, toks nusikalstamos veikos dalyko aiškinimo lankstumas sukelia ir tam tikro lygio neapibrėžtumą, kokie duomenys priskirtini strateginės reikšmės nacionaliniam saugumui, didelės reikšmės valstybės valdymui, ūkiui ar finansų sistemai turintiems elektroniniams duomenims. Vienas iš šios problemos sprendimo variantų – kaip orientacinius kriterijus *mutatis mutandis* pasitelkti tuos, kurie leido spręsti apie IS ypatingą svarbą atitinkamoms BK 198[1] straipsnio 2 dalyje nurodytoms sritims. Todėl *nukentėjusiųjų*, *ekonominio poveikio* ir *poveikio visuomenei* kriterijai leistų atsižvelgti bendriausia prasme į potencialių nukentėjusiųjų skaičių, žalos mastą, ekonominius nuostolius, poveikį visuomenės pasitikėjimui ir pan.

Pavyzdžiui, sprendimas, ar elektroniniai duomenys pasižymi ypatinga svarba sritims, nurodytoms BK 198 straipsnio 2 dalyje, galėtų būti susijęs ne tik su duomenų turiniu, bet ir su jų kiekiu. Autorės nuomone, tam tikrais atvejais neviešų elektroninių duomenų kiekis gali rodyti, kad pavieniai duomenys, kurie dėl savo turinio nėra laikomi ypatingos svarbos, šią savybę įgyja dėl neteisėto disponavimo tokiais duomenimis kiekio. Pavyzdžiui, svarstytina, ar negalėtų būti pripažinta, 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 pan.), jei buvo nustatytas neteisėtas disponavimas itin dideliu ir už ilgesnį laiką sukauptu tokių elektroninių duomenų kiekiu. Taip pat, ar neteisėtu disponavimu ypatingos svarbos duomenimis negalėtų būti pripažintas disponavimas itin dideliu ir už ilgesnį laiką sukauptu elektroninių duomenų, esančių *Sodros* Centrinėje klientų duomenų bazėje, kiekiu. Analizuojant teismų praktiką matyti, kad tokių atvejų joje kol kas nepasitaikė, tiesa, neteisėtas disponavimas minėtais duomenimis konstatuotas Šiaulių miesto apylinkės teismo 2011 m. liepos 18 d. teismo baudžiamajame įsakyme baudžiamojoje byloje (bylos Nr. 1-617-885/2011) ir Vilniaus miesto 1 apylinkės teismo 2008 m. rugsėjo 5 d. nuosprendyje baudžiamojoje byloje (bylos Nr. 1-17-296/2008). Šiaulių miesto apylinkės teismo 2011 m. liepos 18 d. teismo baudžiamajame įsakyme baudžiamojoje byloje (bylos Nr. 1-617-885/2011) nustatyta, kad V. Š. neteisėtai disponavo Valstybinės mokesčių inspekcijos duomenų bazėje kaupiamais duomenimis apie fizinius asmenis – jis įgijo ir paskleidė duomenis apie dvidešimt du fizinius asmenis. Autorės nuomone, tokia V. Š. veika pagrįstai kvalifikuota pagal BK 198 straipsnio 1 dalį, nes šis elektroninių duomenų kiekis yra nepakankamas kalbėti apie tokių duomenų didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai. Kiek kita situacija matyti Vilniaus miesto 1 apylinkės teismo 2008 m. rugsėjo 5 d. nuosprendyje baudžiamojoje byloje (bylos Nr. 1-17-296/2008), kuriame konstatuotas neteisėtas disponavimas *Sodros* Centrinės klientų duomenų bazės 1999–2004 metų duomenimis. Tačiau galimybės įvertinti ypatingą tokių elektroninių duomenų reikšmę šioje byloje nesuteikė nusikalstamos veikos padarymo metu (2003–2004 metai) galiojęs BK – jo 198 straipsnis tokios veiką kvalifikuojančios aplinkybės tuo metu nenumatė.

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 taip pat subjektyvieji požymiai, o tiksliau tyčinės kaltės nustatymo reikalavimas. Į tokio pobūdžio nusikalstamų veikų sudėtis įtraukus tik tyčinę kaltės formą, išvengta jų, kaip „sugaunančių viską“[549] – nuo pavojingo iki bet kokio netinkamo elgesio su informacinėmis ir komunikacijos technologijomis – konstrukcijos. Ne išimtis ir neteisėto elektroninių duomenų perėmimo ir panaudojimo nusikalstama veika – tyčinės kaltės požymis apriboja baudžiamosios atsakomybės taikymo galimybes: 1) kai panaudojant informacines ir komunikacijos technologijas dėl blogo šių technologijų funkcionavimo sukeliami nenumatyti jų veiklos rezultatai, 2) kai elektroninių duomenų konfidencialumas pažeidžiamas elgiantis lengvabūdiškai arba nerūpestingai; 3) kai atliekami teisėti IS testavimo veiksmai, siekiant nustatyti silpnąsias saugumo vietas.

Vertinant šiuos ir panašius atvejus iš baudžiamosios teisės pozicijų, aktualios tampa pagrindinės baudžiamosios atsakomybės nuostatos – tai, kad asmuo atsako pagal baudžiamąjį įstatymą 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). Šios nuostatos probleminiais informacinių ir komunikacijos technologijų panaudojimo atvejais (pavyzdžiui, kilus neprognozuotam jų veiklos rezultatui) leidžia išvengti objektyvaus pakaltinimo, kai elektroninių duomenų konfidencialumo pažeidimai padaryti nesant šių technologijų naudotojo kaltės arba veikoje nustačius kitą nei sudėtyje numatytą kaltės forma ir pan.

Pati kaltės formų apribojimo galimybė kildinama iš Konvencijos dėl elektroninių nusikaltimų 3 straipsnio, kuriame aprašius neteisėtos perimties nusikalstamą veiką, tiesiogiai numatyta galimybė atsakomybę susiaurinti iki *sąmoningos* neteisėtos kompiuterinių duomenų perimties. Į šią baudžiamosios atsakomybės kilimo sąlygą atkreiptas dėmesys ir Konvencijos dėl elektroninių nusikaltimų aiškinamojoje ataskaitoje, kurioje išaiškinta, kad baudžiamoji atsakomybė už neteisėtą perimtį galima tada, jei neteisėta perimtis padaryta tyčia (58 punktas). Įstatymų leidėjas tik tyčinę kaltę numatė BK 198 straipsnyje esančios neteisėto elektroninių duomenų perėmimo ir panaudojimo nusikalstamos veikos sudėtyje. Kadangi minėtame straipsnyje nėra tiesioginių nuorodų į neatsargią kaltės formą, tai pagal esamą baudžiamąjį teisinį reguliavimą baudžiamoji atsakomybė už dėl neatsargumo padarytą tokio pobūdžio veiką yra negalima (BK 16 straipsnio 4 dalis). Taigi konstatuojant tyčinę kaltę būtina nustatyti, kad kaltininkas suvokė, jog darydamas žalą elektroninių duomenų konfidencialumui neteisėtai stebi, fiksuoja, perima, įgyja, laiko, pasisavina, paskleidžia ar kitaip panaudoja neviešus elektroninius duomenis ir norėjo taip veikti.

Kaip teigia S. Bikelis, „<...> asmens, tyčia darančio nusikalstamą veiką, suvokimo dalykas yra <...> visi baudžiamojo įstatymo specialiosios dalies straipsnio dispozicijoje įvardyti objektyvieji požymiai ir iš įstatymo išplaukiančios jų ypatybės <...>“. Taigi BK 198 straipsnio dispozicijoje tiesiogiai numačius elektroninių duomenų neviešumo ir alternatyvių pavojingų veikų neteisėtumo požymius akivaizdu, kad tyčinė kaltė galės būti konstatuojama *inter alia* nustačius ir šių objektyviųjų požymių suvokimą. Beje, jei nusikalstama veika

[549] Clough, J., *supra* note 210, p. 167.

padaroma elektroninėje erdvėje, toks suvokimas turėtų būti vertinamas atsižvelgiant į asmens patyrimą būtent šioje erdvėje.

Ankstesniuose skyriuose prieita prie išvados, kad *Interneto kaip vietos* (angl. *Internet-as-place*) metafora ir *vidinės perspektyvos* pozicija bene geriausiai atspindi, kaip elektroninės erdvės naudotojai įgauna patirtį šioje erdvėje, taip pat suvokia įvairias vietas ir apribojimus joje. Ši, kaip ir mokslinėje literatūroje (M. J. Madison, M. W. S. Wong ir kt.)[550] minima kita – *Informacijos kaip daikto* (angl. *Information-as-thing*) metafora gali būti pasitelkiamos aiškinant prieigos prie elektroninių duomenų apribojimų (neteisėtumo ir duomenų neviešumo) numatomumą. Pati prieiga prie informacijos, anot M. J. Madison, „<...> reiškia, kad egzistuoja prieigos tarpusavio santykių objektas, kažkas, kas gali būti gaunama“[551]. Šiam santykiui paaiškinti pasitelkus fizinės erdvės analogiją, elektroniniai ištekliai, esantys virtualioje erdvėje arba tiksliau apčiuopiamoje IS (ar laikmenoje) bendriausia prasme metaforiškai prilyginami „daiktui“, prie kurio asmuo turi arba neturi prieigos, gali arba negali jo naudoti[552]. Todėl kaip prieigos prie materialaus daikto fizinėje erdvėje, taip ir prieigos prie elektroninių duomenų ir kitų veiksmų su jais atlikimo atveju svarbu nustatyti, ar elektroninių duomenų disponavimo apribojimai buvo nurodyti tinkamai ir leido elektroninės erdvės vartotojams suvokti, kad tam tikri jų veiksmai peržengia leidžiamas ribas. Reikėtų pripažinti, kad šis aiškių ribų nustatymo poreikis aktualus visų *CIA nusikalstamų veikų* padarymo atvejais (pavyzdžiui, aiškinant neteisėto prisijungimo prie IS inkriminavimo probleminius aspektus buvo svarbus privačios ir viešos ribų aiškus atskyrimas). Toks aiškinimas yra pakankamai natūralus, nes, nepriklausomai nuo fizinės ir elektroninės erdvės skirtumų, vartotojas elektroninę erdvę dažniausiai suvokia būtent kaip virtualią realybę, 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“[553]. Taigi tokiam vietų, erdvių ribų suvokimui įtakos neturi tai, ar asmuo veiksmus atlieka fizinėje ar elektroninėje erdvėje.

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 būtų pritarti J. Clough išsakytai minčiai, kad „kol turimas faktines žinias, jog kaltininkas neturėjo leidimo, daugeliu atvejų yra sunku įrodyti, tol tai padės akcentuoti aiškių apribojimų nustatymo svarbą“[554]. Net ir konstatavus neteisėtą prieigą 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. Taigi, kaip matyti, atskiriant viešus ir neviešus elektroninius duomenis, teisėtus ir reikalavimus neatitinkančius veiksmus būtina apie esamas ribas efektyviai informuoti elektroninės erdvės vartotoją.

Toks suvokimas kartu atkreipia dėmesį į jau minėtą nustatytų apribojimų numatomumo kriterijų, kuris leidžia į elektroninėje erdvėje nustatytas ribas pažvelgti iš jos naudotojo, elektroninę erdvę suvokiančio kaip virtualią realybę, pozicijos. Pats numato-

[550] Madison, M. J., *supra* note 252, p. 438–446; Wong, M. W. S., *supra* note 252, p. 102–103.
[551] Madison, M. J., *op. cit.*, p. 442.
[552] *Ibid*., p. 434.
[553] *Ibid*., p. 437.
[554] Clough, J., *supra* note 210, p. 167.

mumo kriterijus bendriausia prasme išreikštų idėją, kad siekiant nustatyti disponavimo elektroniniais duomenimis barjerus, t. y. duomenims suteikti neviešų duomenų statusą, potencialūs pažeidėjai, vadovaujantis elektroninės erdvės kaip vietos metafora, turi būti efektyviai informuojami, kad jų atliekami veiksmai pažeidžia elektroninių duomenų konfidencialumą. Atitinkamai šis kriterijus reikalauja nustatyti, kad elektroninių duomenų buvimo aplinkoje buvo sukurtos „ryškios, matomos ribos tarp atviros, viešos informacijos ir informacijos, kuriai nustatyti prieigos apribojimai“[555]. Pakankamas teisiškai reikšmingų apribojimų informatyvumas palengvina įrodinėjimą, kad kaltininkas, nesilaikęs aiškiai nustatytų ribų suvokė, jog jis esamų apribojimų nepaiso ir pažeidžia neviešų elektroninių duomenų disponavimo tvarką. Priešingu atveju nustatyti apribojimai nesuteiks jokios prasmingos informacijos elektroninės erdvės naudotojui ir žvelgiant iš *vidinės perspektyvos* pozicijų neturės įtakos jo patyrimui ir atliekamiems veiksmams elektroninėje erdvėje.

Nors prieigos prie neviešų elektroninių duomenų apribojimai gali būti įvairūs (kodu sukurti prieigos ribojimai, prieiga prie duomenų esant aiškiai apibrėžtoms veiksmų su jais atlikimo galimybėms ir pan.), tačiau visi jie rodo priemones, kurių buvo imtasi elektroninių duomenų konfidencialumui užtikrinti. Kaip teigia O. S. Kerr, sujungtos teisinės ir techninės priemonės „suteikia galimybes Interneto vartotojams nustatyti privatumo ir saugumo zoną, apsaugotą nuo pašalinių įsikišimo“[556]. Todėl, pavyzdžiui, vienas iš atvejų, kai pažeidžiamas neviešų elektroninių duomenų konfidencialumas nesant asmens kaltės yra tada, kai apribojimus nustatančios priemonės dėl blogo funkcionavimo suteikia prieigą prie tokių duomenų, sudaro sąlygas susipažinti su jų turiniu, daryti tokių duomenų kopijas ir pan. Šią situaciją gerai apibūdina jau minėta dilema, ar, panaudojus informacines ir komunikacijos technologijas, nusikalstama veika buvo padaryta tyčia šių technologijų naudotojo, ar vis dėlto pažeisti elektroninių duomenų konfidencialumą sudarė sąlygas nenumatyti pačių technologijų veikimo sutrikimai. Nustačius, kad asmens veiksmais nebuvo iškreiptos programinės įrangos atliekamos funkcijos, jis nesiekė prasiskverbti pro nustatytus apribojimus, o naudojosi programinės įrangos suteiktomis galimybėmis pagal jų paskirtį (numatytas funkcijas), jo veiksmuose nebus įmanoma nustatyti kaltės. Jei prieiga prie neviešų elektroninių duomenų suteikiama dėl blogo programinės įrangos funkcionavimo, žiūrint iš *vidinės perspektyvos* pozicijų, elektroninės erdvės vartotojui nustatyti prieigos apribojimai nebus suvokiami, tokie apribojimai neatitiks jų numatomumo kriterijaus, atitinkamai nebus suvoktas ir pats atliktų veiksmų neteisėtumas. Taigi akivaizdu, kad tokiais atvejais baudžiamoji atsakomybė pagal BK 198 straipsnį yra negalima.

Apibendrinus galima būtų teigti, kad kiekvienu konkrečiu atveju konstatuojant elektroninių duomenų konfidencialumo pažeidimų suvokimą, būtiną tyčinei kaltei, įvairūs apribojimai elektroninėje erdvėje turėtų būti vertinami nuosekliai, atsižvelgiant į naudotojo patirtį šioje erdvėje. Vienas iš tokio vertinimo metu taikomų kriterijų – nustatytų apribojimų, padedančių atskirti viešus ir neviešus duomenis, numatomumas. Šis kriterijus tinkamai atspindi elektroninės erdvės naudotojo patyrimą elektroninėje erdvėje pirmiausia kaip virtualioje realybėje (laikantis *vidinės perspektyvos* požiūrio), leidžia pagrįsti, kad kaltininkas atpažino aiškiai nustatytas ribas ir jų nesilaikydamas suvokė, jog pažeidžia elektroninių duomenų konfidencialumą.

[555] Madison, M. J., *supra* note 252, p. 491.
[556] Kerr, O. S., *supra* note 222, p. 1650.

V. NUSIKALSTAMŲ VEIKŲ ELEKTRONINIŲ DUOMENŲ IR INFORMACINIŲ SISTEMŲ KONFIDENCIALUMUI ATSKYRIMAS NUO PANAŠIŲ NUSIKALSTAMŲ VEIKŲ

Dėl informacinių ir komunikacijos technologijų panaudojimo pakitus nusikalstamų veikų padarymo galimybėms, atsirado esminės veikų kriminalizavimo pakankamumo problemos, kurios bandytos spręsti įvairiai – kurtos naujos nusikalstamų veikų sudėtys, jos apibrėžtos pakankamai abstrakčiai, praplėstas senųjų sudėčių aiškinimas. Tačiau šie bandymai sukūrė ir visai kitas – baudžiamojo įstatymo normų tarpusavio santykio problemas. Nustačius tradicinių nusikalstamų veikų sąlytį su elektronine erdve, neišvengiamai tenka kalbėti apie baudžiamojo įstatymo normų konkurenciją ir spręsti, ar padarytai veikai kvalifikuoti taikytina tradicinės veikos požymius numatanti, ar išimtinai elektroninei erdvei sukurta norma. Beje, abi jos visada tarsi persidengs, dubliuos viena kitą, skirtinga apimtimi numatys tos pačios nusikalstamos veikos sudėties požymius. Be to, be normų konkurencijos įveikimo klausimo yra neapsieinama analizuojant ir pačių nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui tarpusavio santykį[557].

Tinkamas normų konkurencijos išsprendimas leidžia ne tik formuotis nuosekliai baudžiamojo įstatymo taikymo praktikai, bet taip pat užtikrina ekvivalentaus vertinimo principo reikalavimų įgyvendinimą, taigi ir vienodą tų pačių vertybių apsaugos lygį abiejose erdvėse. Šio principo pažeidimai, veikos kvalifikavimui parinkus ne tą baudžiamojo įstatymo normą, pirmiausia turėtų įtakos teisiniams padariniams – elektroninėje erdvėje padaryta tradicinė veika būtų laikoma pavojingesne arba priešingai – mažiau pavojinga nei analogiška veika fizinėje erdvėje. Pavyzdžiui, 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 pasirinkus ne BK 296 straipsnio 1 dalį, o 198 straipsnio 1 dalį (tuo atveju, jei tarnybos paslaptis yra elektroninių duomenų formos), padaryta veika būtų laikoma nebe baudžiamuoju nusižengimu, o apysunkiu nusikaltimu.

Lietuvos Respublikos Konstitucinis Teismo jurisprudencijoje[558] baudžiamojo įstatymo vidinės darnos poreikis susietas su konstituciniu teisinės valstybės principu, suponuojančiu reikalavimą įstatymų leidėjui sukurti vientisą baudžiamąjį įstatymą, kuriame visos teisės normos sudarytų darnią sistemą. Tačiau analizuojant nusikalstamų veikų elektroninių duomenų ir IS konfidencialumui santykį su kitomis veikomis tokios dermės pasigendama, ypač tuomet, kai lyginamas baudžiamajame įstatyme nustatytas nusikalstamų veikų baudžiamumas. Be to, baudžiamojo įstatymo normų gana nenuoseklus taikymas matyti ir besiformuojančioje teismų praktikoje elektroninių nusikalstamų veikų bylose. Bene daugiausia atribojimo problemų kyla tarp pačių iš pirmo žvilgsnio atrodytų nesusijusių nusikalstamų veikų elektroninių duomenų ir IS saugumui, taip pat konfidencialumo pažeidimus bandant atskirti nuo nusikalstamų veikų finansų sistemai ar asmens privataus gyvenimo neliečiamumui.

---

[557] Žr. disertacijos priede pateiktą pavojingų alternatyvių veikų, numatytų BK 166, 168, 198, 198[2], 214 ir 215 straipsniuose, išsidėstymą.

[558] Lietuvos Respublikos Konstitucinio Teismo 2006 m. sausio 16 d. nutarimas.

1. Nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui tarpusavio santykis (BK 196, 198, 198[1] straipsniai)

Nusikalstamomis veikomis elektroninių duomenų ir informacinių sistemų saugumui dažnai gali būti padaroma žala ne tik elektroninių duomenų arba IS konfidencialumui, bet ir jų integralumui ar prieinamumui. BK XXX skyriuje atskirai kriminalizavus elektroninių duomenų ir IS saugumo pažeidimus, baudžiamojo įstatymo lygmeniu patį veikų padarymo mechanizmą išskaidžius į smulkias dalis, dažnai tenka aiškintis šiame skyriuje numatytų nusikalstamų veikų tarpusavio santykį. Viena aktualesnių problemų susijusi su neteisėto prisijungimo prie IS teisiniu vertinimu, kai šios veikos metu neteisėtai panaudojami nevieši elektroniniai duomenys arba jiems padaromas neteisėtas poveikis. Tokiais atvejais gali kilti klausimų, ar, be neteisėto prisijungimo prie IS, kaltininkui, atsižvelgiant į jo panaudotą neteisėto prisijungimo būdą, turėtų būti inkriminuojamos ir nusikalstamos veikos, numatytos BK 198 ar 196 straipsniuose.

Anksčiau darbe buvo prieita prie išvados, kad galimybių elektroninėje erdvėje ribos *inter alia* gali būti sprendžiamas kompiuterio kodu, padedančiu nustatyti atitinkamo lygio apribojimus prieigai prie IS. O šių apribojimų nepaisymas rodo IS apsaugos priemonių pažeidimus ir atitinka BK 198[1] straipsnyje numatytą nusikalstamos veikos padarymo būdą, kuris, beje, ir kelia BK 198[1], 198 bei 196 straipsnių santykio problemą. Vienas iš prieigos kontrolės pažeidimų – autentifikavimo procedūros apėjimas – pasireiškia neviešų elektroninių duomenų (pavyzdžiui, teisėto vartotojo prisijungimo vardo, slaptažodžio, kodo ar pan.)[559] neteisėtu panaudojimu suklaidinant IS, kuri kaltininką identifikuoja kaip teisėtą sistemos vartotoją ir suteikia prie jos prieigą. Taigi toks IS apsaugos priemonių apėjimas atitinka BK 198 straipsnyje numatytos nusikalstamos veikos požymius. Antrasis būdas yra susijęs su IS apsaugos priemonių silpnųjų vietų, kurios gali atsirasti ir dėl tikslingų kaltininko veiksmų, išnaudojimu. Spragų sukūrimas galimas padarius neteisėtą poveikį elektroniniams duomenims, taigi ir žalą pačioms IS apsaugos priemonėms, o tai atitiktų BK 196 straipsnyje aprašytą nusikalstamą veiką. Tokiais atvejais spręstina, kuri iš BK 198[1], 198, 196 straipsniuose numatytų normų taikytina kvalifikuojant neteisėto prisijungimo prie IS veiksmus.

[559] Analizuojant šį klausimą reikėtų atkreipti dėmesį ir į BK 198 ir 198[2] straipsniuose aprašytų nusikalstamų veikų tarpusavio santykio klausimą. Pagrindinė priežastis, kelianti šių veikų inkriminavimo problemų, yra ta, kad BK 198[2] straipsnyje numatytas nusikalstamos veikos dalykas – slaptažodžiai, prisijungimo kodai ar kitokie panašūs duomenys, tiesiogiai skirti daryti nusikalstamas veikas, gali būti ir BK 198 straipsnyje numatytu dalyku, jei jie turės neviešų elektroninių duomenų požymius. Autorės nuomone, sprendžiant šių normų taikymo klausimą turėtų būti atsižvelgta į tai, kad: 1) BK 198[2] straipsnyje tiesiogiai nurodžius slaptažodžius, prisijungimo kodus ar kitokius panašius duomenis suformuluotas konkretesnis nusikalstamos veikos dalykas palyginus su neviešais elektroniniais duomenimis. Įstatymų leidėjui išskyrus specifinį neteisėto disponavimo tokiais dalykais atvejį, teigtina, kad BK 198[2] straipsnyje įtvirtinta speciali norma lyginant su esančia BK 198 straipsnyje; 2) BK 198[2] straipsnyje, skirtingai nei BK 198 straipsnyje, neminima neteisėto duomenų panaudojimo veika, o tai sukuria gana įdomią situaciją sprendžiant, kaip turėtų būti kvalifikuojama kaltininko padaryta veika, jei jis neteisėtai įgijo slaptažodžius ar prisijungimo kodus ir vėliau juos panaudojo neteisėtai prisijungdamas prie IS (pavyzdžiui, keleto asmenų elektroninių paštų, socialinių tinklų ar pan.). Esant dabartiniam nusikalstamų veikų aprašymui, neteisėtam slaptažodžių, prisijungimo kodų ar kitų panašių duomenų įgijimui kvalifikuoti turėtų būti taikomas BK 198[2] straipsnis, o jų panaudojimui prisijungiant prie IS – BK 198 straipsnis, nes BK 198[2] straipsnis, numatęs konkretesnį nusikalstamos veikos dalyką, šio dalyko panaudojimo veikos neįtvirtino. Šiuo aspektu taip pat aktualu atkreipti dėmesį ir į BK 198[2] ir 214 straipsnyje numatytų nusikalstamų veikų tarpusavio santykį, kuris plačiau aptariamas V dalies 2 skyriuje.

Vertinant IS konfidencialumo pažeidimus matyti, kad tiek neteisėtas neviešų elektroninių duomenų panaudojimas, tiek ir neteisėtas poveikis elektroniniams duomenims tik iš dalies atitinka padarytą veiką, nes atspindi vien neteisėto prisijungimo prie IS padarymo būdą – IS apsaugos priemonių pažeidimą. Kaltininkui inkriminavus tik šias veikas, liktų neįvertintas pats neteisėto prisijungimo prie IS veiksmas. Taigi tokia situacija leidžia kelti baudžiamosios teisės normų konkurencijos, apibūdinamos kaip situacija, kai vieną padarytą nusikalstamą veiką atitinka kelios normos[560], sprendimo problemas. O tiksliau, šiuo atveju turėtų būti kalbama apie vieną iš jos rūšių – normos visumos ir normos dalies konkurenciją bei jos įveikimo sunkumus. Baudžiamosios teisės teorijoje esant tokiai situacijai pripažįstama, kad kaltininko veikoms vertinti taikytina norma, kurioje išsamiai aprašyti padarytos veikos požymiai[561], t. y. norma visuma. Autorės nuomone, būtent BK 198[1] straipsnyje numatyta nusikalstama veika visapusiškai atitinka kaltininko padarytus veiksmus neteisėtai jungiantis prie IS, o neteisėtas neviešų elektroninių duomenų panaudojimas ir neteisėtas poveikis elektroniniams duomenims juos atspindi tik iš dalies. Todėl tokiose situacijose norma visuma turėtų būti laikoma ta, kuri yra numatyta BK 198[1], o ne BK 197 ar 198 straipsniuose.

Tačiau tokia visumos ir dalies konkurencijos įveikimo taisyklė reikalauja tam tikro patikslinimo – esant jai būtina įvertinti ir į visumą įeinančių nusikalstamų veikų baudžiamumą. Nustačius, kad bet kuri visumos dalį sudaranti nusikalstama veika yra pavojingesnė nei pati visuma, ji tokios visumos negali būti apimta ir kvalifikuojama atskirai, t. y. pagal nusikalstamų veikų sutaptį. Palyginus BK 198[1], 198 ir 196 straipsnių sankcijas matyti, kad neteisėto prisijungimo prie IS nusikalstama veika laikoma nesunkiu nusikaltimu (BK 11 straipsnio 3 dalis), tuo tarpu neteisėtas poveikis elektroniniams duomenims ir neteisėtas elektroninių duomenų perėmimas ir panaudojimas priskiriami apysunkių nusikaltimų kategorijai (BK 11 straipsnio 4 dalis). Taigi, nors paprastai norma visuma turėtų būti pavojingesnė nei ją sudarančios dalys, tačiau pagal esamą teisinį reguliavimą IS konfidencialumo pažeidimą numatanti norma niekada neapims normos dalies – neteisėto elektroninių duomenų panaudojimo (BK 198 straipsnis) ar neteisėto poveikio elektroniniams duomenims (BK 196 straipsnis). Atitinkamai vadovaujantis minėta taisykle, neteisėtas prisijungimas prie IS, priklausomai nuo kaltininko panaudoto šios sistemos apsaugos priemonių pažeidimo būdo, turėtų būti kvalifikuojamas pagal nusikalstamų veikų sutaptį, t. y. 198[1] straipsnį ir pagal BK 198 ar 196 straipsnius. Be abejo, toks nusikalstamų veikų elektroninių duomenų ir IS saugumo tarpusavio santykis gali kelti ir nemažai klausimų, tačiau šiuo metu baudžiamajame įstatyme pasirinktas tokių nusikalstamų veikų aprašymo būdas ir nustatytas jų baudžiamumas daryti kitokios išvados, kaip šias veikas kvalifikuoti, kol kas nesuteikia galimybių.

Apžvelgus teismų praktiką matyti, kad tokia normų konkurencijos problema joje nėra sprendžiama, o kaltininko veiksmai neteisėtai prisijungus prie IS kvalifikuojami tik pagal BK 198[1] arba tik pagal 198 straipsnį. Kaip pavyzdys pirmajam atvejui paminėtini anksčiau analizuoti teismų sprendimai, kuriuose konstatuotas neteisėto prisijungimo prie IS faktas ir tokia veika kvalifikuota pagal BK 198[1] straipsnį. Pavyzdžiui, Vilniaus miesto 1 apylinkės teismo 2010 m. kovo 5 d. teismo baudžiamajame įsakyme baudžiamojoje byloje (bylos Nr. N1-724-276/2010) ir Vilniaus miesto 1 apylinkės teismo 2009 m. rugsėjo 14 d. teismo

[560] Girdenis, T. Nusikalstamų veikų daugetas Lietuvos baudžiamojoje teisėje: daktaro disertacija: socialiniai mokslai, teisė (01 S). – Vilnius: Mykolo Romerio universitetas, 2010, p. 26.; Abramavičius, A., *et al. Baudžiamoji teisė.* Bendroji dalis. 3-iasis pataisytas ir papildytas leidimas. Vilnius: Eugrimas, 2001, p. 335.

[561] Girdenis, T., *op. cit.,* p. 27; Abramavičius, A., *et al.*, *op. cit*., p. 342.

baudžiamajame įsakyme baudžiamojoje byloje (bylos Nr. N1-1470-88/2009) nustatytas neteisėtas prisijungimas prie bankų klientų paskirų elektroninės bankininkystės sistemose panaudojant autentifikavimo kodus ir slaptažodžius. Tokie veiksmai kvalifikuoti pagal BK 198[1] straipsnį. Neviešų elektroninių duomenų, t. y. autentifikavimo kodų ir slaptažodžių, panaudojimas neteisėtai prisijungiant prie elektroninės bankininkystės sistemos atskirai pagal BK 198 straipsnį nevertintas.

Antrasis atvejis rodo, kad pirmumas kvalifikuojant veiką teikiamas sudedamajai BK 198[1] straipsnyje esančios veikos daliai – jos padarymo būdui, t. y. neviešų elektroninių duomenų panaudojimui. Toks kvalifikavimo variantas palieka iš baudžiamosios teisės poziciją neįvertintą patį prisijungimo prie IS veiksmą. Pavyzdžiui, Ukmergės rajono apylinkės teismo 2012 m. gruodžio 17 d. teismo baudžiamajame įsakyme baudžiamojoje byloje (bylos Nr. 1-312-627/2012) konstatuota, kad, be kitų veikų, M. Ž. taip pat padarė dvi veikas, 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 tinklapio „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 tinklapio „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) <...>.* Panašiai padarytų nusikalstamų veikų teisinio vertinimo klausimas išspręstas ir Šilalės rajono apylinkės teismo 2010 m. lapkričio 4 d. teismo baudžiamajame įsakyme baudžiamojoje byloje (bylos Nr. 1-121-799/2010). Jame neteisėtas prisijungimas prie elektroninės bankininkystės sistemos panaudojant neviešus elektroninius duomenis taip pat kvalifikuotas pagal BK 198 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) santykis

Paplitus elektroninės komercijos paslaugomas, jų teikimas tapo neatsiejamas nuo asmens tapatybės nustatymo elektroninėje erdvėje. Šis nustatymas – tai vartotojo identifikavimo tam tikroje IS procesas[562], kurio metu IS pateikiami vartotojui suteikti ir sistemoje jį leidžiantys atpažinti duomenys. Dėl šių identifikavimo proceso ypatumų kaltininkui, siekiančiam save IS pateikti kaip kitą asmenį ir joje atlikti teisėtam vartotojui leidžiamus veiksmus (pavyzdžiui, mokėjimo operacijas)[563], konfidencialūs duomenys tampa būtini.

[562] Štitilis D.; Laurinaitis M. Tapatybės vagystė elektroninėje erdvėje. *Informacijos mokslai*. 2009, 50: 242.

[563] Pagal Lietuvos Respublikos mokėjimų įstatymo (*Valstybės žinios*. 1999, Nr. 97-2775) 2 straipsnio 15 punktą mokėjimo operacija tai „mokėtojo arba gavėjo inicijuotas lėšų įmokėjimas, pervedimas arba išėmimas neatsižvelgiant į mokėtojo ir gavėjo pareigas, kuriomis grindžiama operacija". Kiekviena mokėjimo operacija yra autorizuojama, todėl vartotojui nurodžius unikalų identifikatorių, toks mokėjimo nurodymas laikomas tinkamai įvykdytu unikaliu identifikatoriumi nurodyto gavėjo ir (arba) jo mokėjimo sąskaitos atžvilgiu (Mokėjimų įstatymo 40 straipsnio 1 dalis).

Atitinkamai, vertinant tokių duomenų konfidencialumo pažeidimus, tenka spręsti, pagal kokius baudžiamojo įstatymo straipsnius turėtų būti kvalifikuojamas neteisėtas duomenų gavimas ir panaudojimas.

Atsižvelgiant į teismų praktiką, tokie probleminiai aspektai geriausiai išryškėja analizuojant sukčiavimo elektroninėje erdvėje etapus[564], o tiksliau vieną jų, susijusį su neteisėtu duomenų, leidžiančių atpažinti vartotoją įvairiose elektroninių paslaugų sistemose, *inter alia* elektroninėje bankininkystėje, disponavimu. Tokiais atvejais spręstinas klausimas, ar šiais veiksmais pažeidžiamas elektroninių duomenų konfidencialumas ar vis dėlto jais yra kėsinamasi į elektroninių mokėjimo priemonių naudojimo ir disponavimo tvarką. Ši 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 198[2], bet tam tikra dalimi ir BK XXXII skyriuje numatytuose 214 bei 215 straipsniuose. Kadangi neteisėtą disponavimą elektroniniais duomenimis apibūdina įvairios alternatyvios veikos, tai aiškumo dėlei nusikalstamų veikų atribojimo klausimai gali būti aptartini atskirai dėl: 1) elektroninių duomenų įgijimo ir laikymo; 2) šių duomenų panaudojimo.

Analizuojant neteisėtą elektroninių duomenų įgijimą ir laikymą atkreiptinas dėmesys į tai, kad tokio pobūdžio neteisėti veiksmai kriminalizuoti tiek BK 198, 198[2], tiek ir BK 214 straipsnyje. BK 198 straipsnyje šalia įvairių alternatyvų minimas neviešų elektroninių duomenų įgijimas ir laikymas. BK 198[2] straipsnyje, be kitų veikų, kriminalizuotas 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 naudotojo tapatybės patvirtinimo priemonių duomenys, pakankami finansinei operacijai inicijuoti. Taigi akivaizdu, kad tokia situacija susijusi su baudžiamosios teisės normų konkurencija, kai padarytos nusikalstamos veikos sudėties požymius numato ne viena, o keletas baudžiamojo įstatymo normų. Analizuojant minėtus BK straipsnius matyti, kad BK 198 straipsnyje esantys nusikalstamos veikos požymiai yra bendresnio pobūdžio – nekonkretizuojama, kokios rūšies elektroniniai duomenys yra neteisėtai įgyjami ir laikomi. Tuo tarpu 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 naudotojo tapatybės patvirtinimo priemonių duomenys, pakankami finansinei operacijai inicijuoti. Šią kvalifikavimo problemą padeda išspręsti doktrinoje suformuluota baudžiamosios teisės normų konkurencijos įveikimo taisyklė, kad, esant bendrosios ir specialiosios normos konkurencijai, taikoma specialioji norma[565]. Todėl 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 vertinimo pavyzdžių galima rasti ir teismų praktikoje. Pavyzdžiui, Vilniaus miesto 1 apylinkės teismo 2009 m. rugsėjo 14 d. teismo baudžiamajame įsakyme, priimtame baudžiamojoje byloje (bylos Nr. N1-1470-88/2009), nustačius, kad kaltininkas laikė elektroninės bankininkystės paslaugos vartotojų tapatybės patvirtinimo priemonių duomenis, pakankamus finansinei operacijai inicijuoti, konstatuota, jog jo veikoje yra BK 214 straipsnyje numatytos nusikalstamos veikos sudėties požymiai: *M. J. <...> neteisėtai įgijo bei laikė*

[564] Plačiau žr. Kalpokas, V.; Marcinauskaitė, R., *supra* note 221, p. 30.
[565] Pavilonis, V., *supra* note 407, p. 40.

AB banko (duomenys neskelbtini) elektroninės bankininkystės paslaugos vartotojų S. B., J. V., Ž. O. ir E. B. naudotojo tapatybės patvirtinimo priemonių duomenis, pakankamus finansinei operacijai inicijuoti, kuriuos šios pilietės suvedė į M. J. viešai patalpintus suklastotus AB banko (duomenys neskelbtini) elektroninės bankininkystės paslaugos (duomenys neskelbtini) paslaugos internetinius tinklalapius, ir kurie vėliau buvo persiųsti į jo sukurtas elektroninio pašto dėžutes (duomenys neskelbtini). Šiais veiksmais M. J. padarė nusikalstamą veiką, numatytą LR BK 214 str. 1 d. Toks atvejis teismų praktikoje nėra vienintelis – neteisėtas elektroninės bankininkystės neviešų naudotojo tapatybės patvirtinimo elektroninių duomenų įgijimas ir laikymas pagal BK 214 straipsnį taip pat kvalifikuotas Kupiškio rajono apylinkės teismo 2009 m. rugsėjo 2 d. nuosprendyje baudžiamojoje byloje (bylos Nr.1-53-100/2009) ir Vilniaus miesto 1 apylinkės teismo 2010 m. kovo 5 d. teismo baudžiamajame įsakyme baudžiamojoje byloje (bylos Nr. N1-724-276/2010).

Kiek sudėtingesnė, nei anksčiau aptarta, yra BK 198[2] ir 214 straipsniuose numatytų nusikalstamų veikų santykio problema. Pagrindinė šios problemos priežastis ta, kad BK 198[2] straipsnyje, taip pat kaip 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, jei jie yra elektroninės mokėjimo priemonės naudotojo tapatybės patvirtinimo priemonių duomenys, pakankami finansinei operacijai inicijuoti. Todėl sprendžiant BK 198[2] ir 214 straipsnių taikymo klausimą turėtų būti atsižvelgta į tai, kad BK 214 straipsnyje kriminalizuota veika, kuria pirmiausia yra pažeidžiama elektroninių mokėjimo priemonių disponavimo tvarka[566], todėl nustačius, kad kaltininkas neteisėtai įgijo tuos elektroninius duomenis, kurie yra pakankami finansinei operacijai inicijuoti, jo veika turėtų būti kvalifikuojama taikant BK 214, o ne BK 198[2] straipsnį. Šiuo aspektu svarbu atkreipti dėmesį ir į tai, kad pagal Lietuvos Respublikos mokėjimų įstatymo 2 straipsnio 21 punktą mokėjimo priemonė nėra tapatinama tik su materialia priemone, o yra apibūdinta kaip personalizuota priemonė ir (arba) tam tikros procedūros, dėl kurių susitaria mokėjimo paslaugų vartotojas ir mokėjimo paslaugų teikėjas ir kurias mokėjimo paslaugų vartotojas naudoja mokėjimo nurodymui inicijuoti. Todėl, autorės nuomone, elektronine mokėjimo priemone turėtų būti pripažįstama ir banko paslaugų teikimo internetu elektroninė sistema (pavyzdžiui, programinė įranga, esanti banko įstaigos interneto tarnybinėje stotyje), kuri susijusi su tam tikromis procedūromis, naudojamomis autentifikuoti šių paslaugų vartotoją, mokėjimo nurodymui inicijuoti ir pan.[567], ir dėl kurių susitarė mokėjimo paslaugų vartotojas ir mokėjimo paslaugų teikėjas. Analizuojant teismų praktiką taikant BK 198[2] ir 214 straipsnius, vis dėlto galima pastebėti atvejų, kai pirmumas kvalifikuojant veiką (net ir nustačius, kad kaltininkas neteisėtai įgijo pakankamus duomenis elektroninės bankininkystės sistemoje inicijuoti

[566] Abramavičius, A., *et al*., *supra* note 497, p. 28.

[567] Iki 2009 m. galiojusios Mokėjimų įstatymo redakcijos 2 straipsnyje elektronine mokėjimo priemone laikytos nuotolinės prieigos mokėjimo priemonės ir elektroniniai pinigai. Analizuojamu aspektu svarbu atkreipti dėmesį, kad nuotolinės prieigos mokėjimo priemonėmis šiame įstatyme pripažintos priemonės, leidžiančios naudotojui elektroniniu būdu sudaryti nurodymus kredito įstaigai dėl disponavimo toje kredito įstaigoje jo sąskaitoje turimomis lėšomis. Naudojantis šiomis priemonėmis (naudotojo kompiuteryje įdiegta kredito įstaigos programine įranga, programine įranga, esančia kredito įstaigos interneto tarnybinėje stotyje, telefono ryšio įranga, kredito įstaigos išleista kortele (debeto, kredito ar kt.) ir kitomis priemonėmis), paprastai reikia tapatybės patvirtinimo (2 straipsnio 21 punktas).

finansinei operacijai) teikiamas BK 198[2] straipsnyje esančiai normai. Pavyzdžiui, Vilniaus miesto 1 apylinkės teismo 2011 m. kovo 25 d. nuosprendyje baudžiamojoje byloje (bylos Nr. 1-68-203/2011) konstatuota, kad kaltininkas įgijo minėtus duomenis, tačiau jam inkriminuota veika, esanti 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 198[2] str. 1 d.*

Kitas iškeltas probleminis klausimas buvo susijęs su vartotoją elektroninės bankininkystės sistemoje leidžiančių identifikuoti duomenų neteisėto panaudojimo atliekant įvairias pinigines operacijas teisėto vartotojo banko sąskaitoje vertinimu. Kadangi baudžiamajame įstatyme atsakomybę už neteisėtą neviešų elektroninių duomenų panaudojimą numato keletas 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, panaudojant svetimos elektroninės priemonės naudotojo tapatybės patvirtinimo priemonių duomenis, požymį galima pastebėti, kad jis, palyginus su BK 198 straipsnyje numatytu neteisėto neviešų elektroninių duomenų panaudojimo požymiu, yra konkretesnis. Todėl BK 215 straipsnyje, išskyrus specifinį neviešų elektroninių duomenų panaudojimo atvejį, ši, o ne BK 198 straipsnyje numatyta norma, vadovaujantis anksčiau minėtos bendrosios ir specialiosios normų konkurencijos įveikimo taisykle, taikytina, jei nustatoma, kad nusikalstama veika pasireiškė neteisėtu finansinės operacijos inicijavimu panaudojant tapatybės patvirtinimo priemonių duomenis. Toks aiškinimas nuosekliai išplaukia ir iš šio BK straipsnio paskirties: kriminalizavus tokią veiką pirmiausia siekta apsaugoti elektroninių mokėjimo priemonių disponavimo tvarką. Elektroninių mokėjimo priemonių duomenų ir kredito įstaigų informacinių sistemų saugumas šiuo atveju laikoma tik kaip papildoma baudžiamojo įstatymo saugoma vertybė, kuriai sukeliama žala arba tokios žalos grėsmė[568].

Aiškinimas, kad BK 215 straipsnis taikytinas ir tais atvejais, kai neteisėtos mokėjimo operacijos inicijuojamos ar atliekamos elektroninėje sistemoje įvedus naudotojo tapatybės patvirtinimo priemonių duomenis, matyti ir Lietuvos Aukščiausiojo Teismo praktikoje. Šio teismo 2012 m. birželio 26 d. nutartyje baudžiamojoje byloje (bylos 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 naudotojo 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, identifikuo-*

[568] Abramavičius, A., *et al*., *supra* note 497, p. 36.

jantis 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 panaudojant elektroninės bankininkystės naudotojo tapatybės patvirtinimo priemonių duomenis pagal BK 215 straipsnį kvalifikuojamas ir žemesnių instancijų teismų praktikoje. Tačiau joje vis dėlto galima pastebėti ir diskutuotinų BK 198 ir 215 straipsniuose esančių normų konkurencijos įveikimo variantų, kai pirmumas, kvalifikuojant veiką, teikiamas bendresnius požymius numatančiai BK 198 straipsnio normai. Pavyzdžiui, Vilniaus miesto 3 apylinkės teismo 2010 m. sausio 27 d. nuosprendyje baudžiamojoje byloje (bylos Nr. 1-182-498/10) A. Š. padarytos nusikalstamos veikos perkvalifikuotos iš BK 214 straipsnio 1 dalies ir 215 straipsnio 1 dalies į 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.*

3. Neteisėto elektroninių duomenų perėmimo ir panaudojimo bei nusikaltimų privataus gyvenimo neliečiamumui santykis

Baudžiamojo įstatymo saugomos vertybės, privatumo ir konfidencialumo tarpusavio santykio analizė parodė, kad asmens teisės į privatumą turinys yra pakankamai platus – taigi apie jį bendriausia prasme gali būti kalbama privataus, šeimos gyvenimo apsaugos, būsto ar asmens susižinojimo, asmeninių faktų slaptumo, draudimo skelbti gautą ar surinktą konfidencialią informaciją ir pan. kontekste. Įvairūs neteisėti įsikišimai į asmens privatumo sritį žvelgiant iš elektroninės erdvės saugumo perspektyvos, t. y. tiek, kiek šie pažeidimai padaromi elektroninėje erdvėje, yra kriminalizuoti ir BK 166, 167, 168 straipsniuose – tai asmens susižinojimo neliečiamumo pažeidimai, neteisėtas informacijos apie privatų asmens gyvenimą rinkimas, taip pat neteisėtas informacijos apie asmens priva-

tų gyvenimą atskleidimas ar panaudojimas. Šiuo atveju būtent ekvivalentaus vertinimo principas leidžia užtikrinti anksčiau minėtų BK straipsnių pritaikomumą nusikalstamoms veikoms, kuriomis kėsinamasi į asmens privatumo neliečiamumą nebe fizinėje, o elektroninėje erdvėje, kvalifikuoti.

Tačiau tokia situacija kartu kelia ir baudžiamojo įstatymo normų konkurencijos problemą, kai kelios normos – esančios BK 166, 167, 168 straipsniuose ir BK 198 straipsnyje – gali būti pritaikomos 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 *inter alia* ir elektroninėje erdvėje. Todėl neteisėto įsikišimo į privatumo sferą 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 pritaikoma BK 166, 167 ar 168 straipsniuose esanti norma turi ir visus BK 198 straipsnio normos požymius. Kaip minėta, nevieši elektroniniai duomenys (neteisėto disponavimo elektroniniais duomenimis dalykas) apima konfidencialumo aspektą turinčius įvairių rūšių duomenis, todėl nebūtų suklysta teigiant, kad duomenys, susiję su asmens privatumu, yra kartu ir nevieši duomenys. Taip pat BK 198 straipsnyje numatytos bene analogiškos pavojingos veikos kaip ir BK 166, 167 ar 168 straipsniuose: stebėjimas, fiksavimas, perėmimas, įgijimas kaip BK 167 straipsnyje minimas rinkimas, taip pat paskleidimas ar kitoks panaudojimas. Tačiau kartu matyti, kad BK 166, 167 ir 168 straipsniuose, palyginus su BK 198 straipsniu, išskirti specifiniai atvejai ir juos atitinkančios normos, kurios taikytinos būtent privatumo pažeidimams elektroninėje erdvėje kvalifikuoti. Todėl bendriausia prasme galima būtų teigti, kad BK 198 straipsnyje esanti norma yra lyg ir „rezervinė“ tiems atvejams, kurie nepatenka į specialių normų taikymo sritį. Šios bendrosios ir specialiosios normos konkurencijos įveikimo taisyklės taikymo pavyzdį galima būtų detaliau aptarti analizuojant BK 166 ir 198 straipsniuose esančių normų tarpusavio santykį.

BK 166 ir 198 straipsnių atskyrimo problema kyla sprendžiant, pagal kurį straipsnį kvalifikuotina veika, jei neteisėtai gauti elektroninių ryšių tinklais siunčiami ar saugomi po jų perdavimo asmens pranešimai, kurie gali būti laikomi ir neviešais elektroniniais duomenimis. Šiuo aspektu apie *komunikacinį privatumą*[569] kaip vieną iš teisės į privatumo turinį sudarančių elementų galima analizuoti tiek IS perduodamų, tiek ir po perdavimo saugomų („*nejudamų*“) pranešimų kontekste.

Pirmasis atvejis parodo asmens susižinojimo neliečiamumo pažeidimus neteisėtai gavus asmens pranešimus jų perdavimo IS proceso metu. 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 <...>“ (be abejo, išskyrus įstatymuose numatytas išimtis). Kaip teigia I. Jarukaitis, „ši nuostata detalizuoja Konstitucijos 22 straipsnyje įtvirtinto privataus gyvenimo apsaugos principą elektroninių ryšių kontekste“[570]. Žiūrint iš baudžiamosios teisės pozicijų, susižinojimo slaptumo pažeidimai galėtų būti kvalifikuojami tiek pagal BK 198, tiek ir pagal 166 straipsnį. BK 198 straipsnyje kriminalizuotas neteisėtas neviešų elektroninių duome-

[569] Kiškis, M. *et al.*, *supra* note 8, p. 116.

[570] Jarukaitis, I., *et al. Elektroninių ryšių teisė*. Vilnius: Eugrimas, 2005, p. 340.

nų 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 pagal tai, ar elektroninių ryšių kontekste kalbama apie susižinojimo slaptumo kaip garantuotos galimybės „laisvai keistis asmeninio pobūdžio informacija jos neatskleidžiant tretiesiems asmenims“[571] pažeidimus, ar vis dėlto perimami kiti konfidencialumo aspektą turintys, tačiau asmens privatumo sričiai nepriskirti elektroniniai duomenys (beje, elektroninių ryšių naudotojai yra ne tik fiziniai, bet ir juridiniai asmenys). Taigi nusikalstamos veikos dalyko specifika šiuo atveju leistų apie BK 166 straipsnyje numatytą normą kalbėti kaip apie specialiąją BK 198 straipsnyje esančios normos atžvilgiu. Todėl 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 galima sutikti nors ir negausioje teismų praktikoje. Pavyzdžiui, Vilniaus miesto 2 apylinkės teismo 2008 m. liepos 2 d. nuosprendyje baudžiamojoje byloje (bylos Nr. 1-5-655/2008) 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 specialia 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.* Šis nuosprendis buvo skųstas apeliacine tvarka, tačiau 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, bet nekeitė A. J. padarytų nusikalstamų veikų teisinio vertinimo.

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 asmens pranešimų siuntimo metu neteisėtai fiksuoti srauto duomenys, tačiau neperimti siunčiamo pranešimo turinio duomenys. Abejonė, ar BK 166 straipsnis taikytinas ir neteisėtam srauto duomenų fiksavimui kvalifikuoti, 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 vientisą turinio ir srauto duomenų visumą – tiek turinio, tiek srauto duomenys yra būtini siekiant užtikrinti komunikavimą tarp asmenų. Elektroninių ryšių

[571] Jarukaitis, I., et al., *supra* note 570, p. 333.

tinklais siunčiami turinio duomenys rodo asmenų bendravimą, o šiems duomenims perduoti sukurti srauto duomenys leidžia tarpusavyje „bendrauti" IS komponentams siekiant pristatyti turinio duomenis numatytam adresatui. Toks elektroninių ryšių tinklais siunčiamo pranešimo technologiškai neutralus interpretavimas užtikrintų ir nuoseklų asmens susižinojimo neliečiamumo pažeidimų baudžiamąjį teisinį vertinimą – BK 166 straipsnis būtų taikomas tiek neteisėtai perėmus su asmens privatumu susijusius turinio duomenis, tiek ir fiksavus šiems duomenims perduoti tiesiogiai skirtus srauto duomenis. Priešingu atveju srauto duomenų fiksavimas būtų kvalifikuojamas pagal kitame skyriuje esantį BK 198 straipsnį, o tai asmens privatumo pažeidimo veiką išskaidytų po skirtingus BK skyrius.

Be to, autorės nuomone, apie BK 166 straipsnio taikymo galimybes kvalifikuoti neteisėtą srauto duomenų gavimą gali rodyti ir jame numatyta viena iš alternatyvių veikų – pranešimų fiksavimas. Šią pavojingą veiką, tiesa, ją analizuojant BK 198 straipsnio kontekste, siūlyta susieti būtent su neteisėtu srauto duomenų gavimu. Toks fiksavimo aiškinimas, siekiant nuoseklumo, galėtų būti taikomas atskleidžiant ir BK 166 straipsnyje numatyto fiksavimo turinį. Taip pat paminėtina, kad nors šiuo klausimu literatūroje pasigendama gilesnės diskusijos, tačiau pavieniais atvejais, kalbant apie BK 166 straipsnio pritaikomumą minėtoms situacijoms, vis dėlto prieinama išvados, kad šiame straipsnyje yra numatyta atsakomybė ne tik už turinio, bet ir srauto duomenų neteisėtą gavimą. Pavyzdžiui, I. Jarukaitis, analizuodamas Konvencijos dėl elektroninių nusikaltimų 3 straipsnio nuostatas ir įvairius su jomis susijusius nacionalinės teisės suderinimo aspektus teigia, 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"[572].

Pereinant prie išskirto antrojo komunikacijos privatumo pažeidimo atvejo, kai neteisėtai gaunama prieiga prie pranešimų, kurie yra saugomi po jų perdavimo elektroninių ryšių tinklais (pavyzdžiui, elektroninio pašto serveryje, mobiliajame telefone ar pan.), galima pastebėti, kad problema 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, Šilutės rajono apylinkės teismo 2006 m. birželio 28 d. nuosprendžiu baudžiamojoje byloje (bylos Nr. N1- 249-299/2005) S. G. pripažinta kalta pagal BK 284 straipsnio 1 dalį ir 166 straipsnio 1 dalį. Nustatyta, kad *Šilutės mieste (duomenys neskelbtini) stadione, S. G. neteisėtai, prieš nukentėjusiosios valią, paėmė iš V. B. mobilaus ryšio telefoną „Samsung X640" ir skaitė mobilaus ryšio telefone esančias trumpąsias žinutes, toliau tęsdama savo nusikalstamą veiką, <...> būdama Šilutės mieste (duomenys neskelbtini), skaitė nukentėjusiosios mobilaus ryšio telefone „Samsung X640" esančias trumpąsias žinutes ir tuo pažeidė V. B. susirašinėjimo techninėmis priemonėmis siunčiamų pranešimų slaptumą.* Susižinojimo slaptumo pažeidimai neteisėtai gavus prieigą prie mobiliojo ryšio telefone esančių pranešimų pagal BK 166 straipsnį kvalifikuoti ir Šiaulių rajono apylinkės teismo 2010 m. liepos 19 d. teismo baudžiamajame įsakyme baudžiamojoje byloje (bylos Nr. 1-199-776/2010). Taigi nustačius, jog saugomi pranešimai yra susiję su asmens privatumu, įvairiems įsikišimams į susižinojimo neliečiamumo sferą

[572] Jarukaitis I., *et al*., *supra* note 570, p.348.

kvalifikuoti taikytinas ne BK 198, o 166 straipsnis. Beje, tokiais atvejais, autorės nuomone, siūlytina inkriminuoti ne perėmimo, fiksavimo ar stebėjimo veikas, kurios straipsnio dispozicijoje tiesiogiai susietos su elektroninių ryšių tinklais *siunčiamų* (perduodamų) pranešimų privatumo pažeidimais, o dispozicijoje minimą požymį – kitokį asmens susižinojimo neliečiamumo pažeidimą. Jis, atsižvelgiant į BK 166 straipsnyje aprašytus nusikalstamos veikos požymius, laikytinas tikslesniu kalbant apie neteisėtą prieigą prie pranešimų ne jų siuntimo metu, o tada, kai jie yra saugomi (laikomi) po jų pristatymo.

Taigi nusikalstamų veikų, aprašytų BK 198 ir 166 straipsniuose, požymiai leidžia nubrėžti ribą, kuriais atvejais kaltininko veika pažeidžiamas asmens susižinojimo neliečiamumas, o kuriais neviešų elektroninių duomenų konfidencialumas. Tačiau šių straipsnių lyginimas kelia nemažai sudėtingų problemų, 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 sąryšį sukurta situacija, kai asmens privatumo pažeidimai baudžiami dvigubai švelniau nei neviešų elektroninių duomenų konfidencialumo pažeidimai – BK 166 straipsnyje esanti nusikalstama veika yra nesunkus nusikaltimas, o BK 198 straipsnio 1 dalyje numatyta veika – apysunkis nusikaltimas. Beje, tinkamas sąryšis nenustatytas ir tarp kitų nusikalstamų veikų – 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 169 straipsnis) ir daugelis kitų. Toks teisinis reguliavimas reikštų, kad daugelis bendrajai normai, esančiai BK 198 straipsnyje, sukurtų specialių normų numato privilegijuotas nusikalstamų veikų sudėtis, o pačios veikos pavojingumą dažniausiai mažina nusikalstamos veikos dalyko specifika: pavyzdžiui, mažesnį veikos pavojingumą rodo, jei neteisėtai disponuojama duomenimis, sudarančiais valstybės, tarnybos paslaptį, asmens siunčiamais pranešimais ar pan. Autorės nuomone, toks teisės normų ryšys neparodo tikrosios baudžiamojo įstatymo saugomų vertybių tarpusavio sąsajos ir negali būti laikomas tinkamu.

IŠVADOS

1. Ekvivalentinio vertinimo principas bendriausia prasme atspindi idėją, kad baudžiamojo įstatymo normos turi užtikrinti vienodą vertybių apsaugos lygį fizinėje ir elektroninėje erdvėse. Praktiškai įgyvendinant lygiavertį veikų vertinimą Lietuvos baudžiamajame įstatyme, tradicinėms veikoms, padarytoms elektroninėje erdvėje, kvalifikuoti taikomas tas pats BK straipsnis, pagal kurį kvalifikuojamos analogiškos veikos fizinėje erdvėje. Įgyvendinant funkcinį ekvivalentiškumą *CIA nusikalstamoms veikoms* kvalifikuoti baudžiamajame įstatyme įtvirtintos savarankiškos normos (BK 196–198[2] straipsniai).

2. Technologinio neutralumo principas yra aktualus siekiant išvengti baudžiamojo įstatymo normų taikymo apribojimų, galinčių kilti dėl jose naudojamų su technologijomis susijusių požymių. Tačiau šį principą pasitelkiant baudžiamojoje teisėje, jo apimtis neišvengiamai siaurina baudžiamosios teisės principai, leidžiantys išvengti pernelyg plataus ir nepagrįsto veikų kriminalizavimo, atitinkamai ir nepagrįsto baudžiamosios atsakomybės ribų išplėtimo.

3. Elektroninių duomenų ir informacinių sistemų saugumo turiniui atskleisti taikytina ne abstrakti saugumo samprata, o klasikinis *CIA triados* saugumo modelis, leidžiantis nustatyti trijų elektroninių duomenų ir informacinių sistemų savybių – konfidencialumo, integralumo ir prieinamumo – išsaugojimo poreikį. Šio modelio pagrindu BK XXX skyriuje esančios veikos gali būti grupuojamos į konfidencialumo, integralumo ar prieinamumo pažeidimus.

Tiek neviešų elektroninių duomenų, tiek informacinių sistemų konfidencialumas rodo prieigos prie jų apribojimus, t. y. duomenys ar sistemos, atliekančios duomenų apdorojimo funkcijas, yra prieinamos tik vartotojams, turintiems prieigos prie jų teisę, ir tik ta apimtimi, kuria jiems ši teisė buvo suteikta.

4. Neteisėto prisijungimo prie informacinės sistemos nusikalstama veika yra kriminalizuota *per se* be tiesioginės sąsajos su kitomis elektroninių duomenų ir informacinių sistemų saugumą pažeidžiančiomis veikomis. Kadangi paprastai galimybes atlikti bet kokias veikas pačioje sistemoje sudaro pirminiai kaltininko neteisėto prisijungimo veiksmai, tai neturėtų stebinti dažni BK 198[1] straipsnyje numatytos veikos inkriminavimo atvejai.

5. Siekiant išvengti akivaizdžiai nepavojingų veikų kriminalizavimo, neteisėto prisijungimo prie IS apibrėžtis susiaurinta į šios veikos sudėtį įtraukus veikos padarymo būdą – IS apsaugos priemonių pažeidimą. Šioms priemonėms aiškinti taikytina technologinė IS apsaugos priemonių koncepcija. Platesnis šių priemonių interpretavimas galimas tik tuo atveju, jei prieš tai įvertinama neteisėto prisijungimo prie IS *perkriminalizavimo* grėsmė.

IS apsaugos priemonių pažeidimas interpretuotinas ne tik kaip žalos apsaugos priemonėms padarymas, bet ir kaip tokių priemonių nustatytų apribojimų (reikalavimų) pažeidimas, kai žala pačioms apsaugos priemonėms gali būti ir nesukeliama.

6. Neteisėtą prisijungimą prie IS kriminalizavus *per se* sudarytos ribotos galimybės prieigos neteisėtumu pripažinti ir teisėtumo ribas peržengiančią prieigą. Siauresnis aiškinimas leidžia išvengti baudžiamajai atsakomybei kilti būtino pavojingumo lygio nesiekiančių veiksmų kriminalizavimo.

Prisijungimo prie IS neteisėtumas konstatuotinas nustačius tiek autentifikavimo procedūros pažeidimo, tiek ir IS apsaugos silpnų vietų išnaudojimo faktą.

7. Prisijungimo aiškinimui taikytinas *vidinės perspektyvos* požiūris, kuris elektroninę erdvę apibūdina kaip virtualią realybę. Todėl, nepriklausomai nuo to, ar prisijungimas yra suvokiamas kaip komanda, kuria pradedamas darbo seansas su IS, ar jis suprantamas kaip galimybė prieiti prie IS išteklių, prisijungimas būtų metaforiškai prilyginamas *virtualiam įėjimui* į sistemą. Toks aiškinimas reikštų, kad prisijungimo veiksmui konstatuoti nepakanka tik sąveikos su IS.

Nors galimybės prieiti prie IS išteklių kriterijus padeda aiškiau suvokti prisijungimo veiką, tačiau jos baigtumo momentui neturi būti svarbi kaltininko reali galimybė atlikti tolesnius veiksmus IS.

8. BK 198[1] straipsnyje numatytas nusikalstamos veikos dalykas – IS – baudžiamosios teisės kontekste turėtų būti suvokiamas be jos funkcionavimo konteksto ir bendriausia prasme laikomas IT (apimančių ir komunikavimo technologijas) arba kompiuterinės sistemos sinonimu.

Strateginę reikšmę nacionaliniam saugumui arba didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinti IS yra neteisėto prisijungimo prie IS veiką kvalifikuojanti aplinkybė. Ypatingai IS svarbai BK 198[1] straipsnio 2 dalyje nurodytoms sritims konstatuoti taikytini *nukentėjusiųjų*, *ekonominio poveikio* ir *poveikio visuomenei* kriterijai.

9. Pagrindžiant tyčinę kaltę svarbus *vidinės perspektyvos* požiūris į elektroninę erdvę, kuris sudaro galimybes į ribų ir jų peržengimo neteisėtumo suvokimą pažvelgti iš elektroninės erdvės vartotojo pozicijos. Todėl šioje erdvėje nustatytų apribojimų suvokimui vertinti taikytinas tokių apribojimų ir jų pažeidimo *numatomumo kriterijus* – jis leidžia atsižvelgti į asmens patyrimą elektroninėje erdvėje kaip *vietoje*.

10. Neteisėtas elektroninių duomenų perėmimas ir panaudojimas BK 198 straipsnyje kriminalizuotas plačiai – į vieną nusikalstamą veiką sujungti tiek *duomenų, perduodamų IS* (angl. *data in transmission*), tiek ir *duomenų, laikomų joje* (angl. *data „in rest"*), konfidencialumo pažeidimai. Ši veika taip pat nėra susieta su papildomais požymiais (pavyzdžiui, techninių priemonių panaudojimu, kaltininko nusikalstamais ketinimais), galinčiais padėti išvengti jos „perkriminalizavimo" problemų.

11. Apibūdinant neteisėto elektroninių duomenų perėmimo ir panaudojimo nusikalstamos veikos dalyką, būtina išskirti du – *teisinį* ir *technologinį* – jo aspektus. Teisinis aspektas siejamas su elektroninių duomenų neviešumu, o technologinis – su tokių duomenų elektronine forma.

Elektroninių duomenų neviešumas rodo, kad jie priklauso duomenų, kuriems taikomas tam tikras apsaugos lygis – atitinkami konfidencialumo apsaugos reikalavimai, rūšiai. Neviešumo pagrindai gali būti kildinami tiek iš įstatymų ar kitų teisės aktų (objektyvūs), tiek ir asmenų susitarimų, privačių tikslų ir pan. (subjektyvūs).

Duomenų elektroninei formai konstatuoti taikytini jų *tinkamumo apdoroti IS* arba tokių *duomenų buvimo IS (tam tikroje jos dalyje ar išorinėje laikmenoje)* 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 pasitelktini *nukentėjusiųjų*, *ekonominio poveikio* ir *poveikio visuomenei* kriterijai. Ypatingą elektroninių duomenų svarbą *inter alia* gali rodyti ne tik duomenų turinys, bet ir itin didelis jų kiekis. Tokiais atvejais pavieniai duomenys, kurie dėl savo turinio nėra laikomi ypatingos svarbos, šią savybę gali įgyti dėl neteisėto disponavimo tokiais duomenimis kiekio.

12. BK 198 straipsnyje nusikalstamos veikos dalykas – nevieši elektroniniai duomenys nėra konkretizuoti iki *IS laikomų* ir *IS perduodamų duomenų*, todėl minėto straipsnio dispozicija nesuteikia galimybių alternatyvias veikas susieti tik su viena iš šių duomenų rūšių.

12.1. Stebėjimo, fiksavimo ir perėmimo veikų atskyrimo problemos kyla šias alternatyvas analizuojant *IS perduodamų duomenų* kontekste. Stebėjimas paprastai neatsiejamas nuo prieš tai atlikto ar stebėjimo metu vykdomo perduodamų duomenų fiksavimo; pats neteisėtas programinės įrangos veikimas tinkle fiksuojant duomenis gali būti prilyginamas tinklo srauto stebėjimui; fiksavimas bendriausia prasme gali būti laikomas tuo pačiu elektroninių duomenų perėmimu. Bandant atrasti šių alternatyvų skirtumus siūlytina skirti neteisėtą srauto ir turinio duomenų gavimą – fiksavimo veiką susieti su srauto duomenų, o perėmimo su turinio duomenų neteisėtu gavimu. Atsižvelgiant į tokio pobūdžio veikų padarymo mechanizmą, kaltininkui dažnai teks inkriminuoti ne tik perėmimo, bet ir fiksavimo bei stebėjimo veikas.

12.2. Fiksavimo ir įgijimo santykio problemos kyla šias veikas susiejus su *IS laikomais duomenimis*, nes joms suteiktas bene analogiškas turinys. BK 198 straipsnyje tokias veikas atskyrus, tenka ieškoti galimų šių alternatyvų atribojimo kriterijų. Diskutuotina, ar jais negali būti laikomi skirtingas fiksavimo ir įgijimo veikų baigtumo momentas arba galimybė veikos metu keisti elektroninių duomenų formą iš elektroninės į materialią.

12.3. Elektroninių duomenų perėmimas ir įgijimas yra pagal savo prasmę artimos veikos, tačiau jas abi įtvirtinus BK 198 straipsnyje neišvengiamai tenka atskirti *IS laikomus* ir *IS perduodamus* duomenis. Perėmimo veika išimtinai sietina su neteisėtu *IS perduodamų* duomenų gavimu. Vengiant dubliavimo, apie įgijimą galėtų būti kalbama tik tais atvejais, kai neteisėtai gaunami *IS laikomi* elektroniniai duomenys.

12.4. Stebėjimo veiką numačius kaip savarankišką alternatyvą, vien šio veiksmo su *IS laikomais duomenimis* pakanka baudžiamajai atsakomybei pagal BK 198 straipsnį kilti. Tokiais atvejais siekiant užtikrinti pakankamą veikos pavojingumą svarbu nustatyti ne tik patį stebėjimo faktą, bet ir kitas aplinkybes, liudijančias žalos baudžiamojo įstatymo saugomiems teisiniams gėriams kilimą. Siūlytina atsižvelgti į kaltininko ketinimus gavus duomenis padaryti kitas nusikalstamas veikas, duomenų apsaugos priemonių pažeidimus, įvairių techninių priemonių, skirtų duomenims gauti, panaudojimu, kaltininko neteisėtus veiksmus prisijungiant prie IS ir taip gaunant prieigą prie duomenų, stebėjimo veiksmų pastovumą, stebėtų duomenų kiekį, jų reikšmę, žalos sukėlimą ir pan.

12.5. Elektroninių duomenų laikymu pripažįstamas šių duomenų buvimas kaltininko žinioje – jo kontroliuojamose materialiose priemonėse, kuriose yra elektroniniai duomenys, arba jam prieinamoje vietoje elektroninėje erdvėje (pavyzdžiui, elektroninio pašto serveryje). Konstatuojant laikymą būtina nustatyti kaltininko galimybę prieiti prie elektroninių duomenų, daryti jiems poveikį.

12.6. Elektroninių duomenų pasisavinimo aiškinimui aktualūs kai kurie tradicinio turto pasisavinimo aspektai. Tačiau, atsižvelgiant į turto pasisavinimo specifiką ir pernelyg didelę jo sąsają su turtinių nusikalstamų veikų doktrina, aiškinant elektroninių duomenų pasisavinimą siūlytina atsisakyti elektroninės erdvės kontekste sunkiai pritaikomų kriterijų ir apie elektroninių duomenų pasisavinimą kalbėti kaip apie neteisėtą kaltininko tapimą faktiniu elektroninių duomenų turėtoju. Tai yra, kai kaltininkui konkrečiomis sąlygomis buvo suteikta prieigos prie duomenų teisė, tačiau jis peržengė jos teisėtumo ribas ir elektroniniais duomenimis disponavo pažeisdamas nustatytus apribojimus.

12.7. Elektroninių duomenų neteisėto paskleidimo veika sietina ne tik su aktyviais veiksmais perduodant duomenis tretiesiems asmenims, bet ir su sąlygų prieiti prie duomenų sudarymu. Tokiu atveju paskleidimui konstatuoti tai, kieno iniciatyva – siuntėjo ar gavėjo – duomenų perdavimo procesas buvo inicijuotas, neturės reikšmės.

12.8. Kitokio elektroninių duomenų panaudojimo požymis rodo nebaigtinį neteisėto disponavimo elektroniniais duomenimis veikų sąrašą. Šios veikos formuluotė leidžia teigti, kad tokia veika dažnai yra kitų nusikalstamų veikų padarymo būdas – vienas dažnesnių atvejų yra neviešų elektroninių duomenų neteisėtas panaudojimas prisijungiant prie IS.

13. Disponavimo neviešais elektroniniais duomenimis neteisėtumas reiškia, kad asmuo gaudamas prieigą arba atlikdamas kitas veikas su neviešais elektroniniais duomenimis neturi teisėto leidimo tokiems veiksmams arba nors toks leidimas yra suteiktas, tačiau veiksmus jis padaro pažeisdamas nustatytą neviešų elektroninių duomenų disponavimo tvarką (įpareigojimus).

14. Konstatuojant tyčinę kaltę *inter alia* elektroninių duomenų konfidencialumo pažeidimo suvokimą, apribojimai elektroninėje erdvėje vertinti iš *vidinės perspektyvos pozicijos*, sudarančios galimybę atsižvelgti į elektroninės erdvės vartotojo patirtį šioje erdvėje. Apribojimų vertinimui taikytinas jų *numatomumo kriterijus*, leidžiantis pagrįsti, kad asmuo suvokė nustatytas ribas, jų nesilaikydamas pažeidė elektroninių duomenų konfidencialumą.

15. Nustačius, kad neteisėtai prisijungiant prie IS panaudoti nevieši elektroniniai duomenys arba padarytas neteisėtas poveikis elektroniniams duomenims, spręstina, ar, be BK 198[1] straipsnyje aprašytos veikos, inkriminuotinos ir BK 196 ar 198 straipsnyje numatytos veikos. BK 198[1] straipsnyje esančią normą laikant *norma visuma*, o BK 196 ir 198 straipsnių normas – jos dalimi, neteisėtas prisijungimas prie IS, priklausomai nuo apsaugos priemonių pažeidimo būdo, kvalifikuotinas pagal nusikalstamų veikų sutaptį, t. y. BK 198[1] ir 196 ar 198 straipsnius. Šiuo metu už minėtų veikų padarymą nustatytos sankcijos lemia, kad IS konfidencialumą pažeidžianti norma niekada neapims *normos dalies* – neteisėto poveikio elektroniniams duomenims (BK 196 straipsnis) ar neteisėto elektroninių duomenų perėmimo ar panaudojimo (BK 198 straipsnis).

16. Baudžiamoji atsakomybė už įvairaus pobūdžio neteisėto disponavimo elektroniniais duomenimis veiksmus numatyta ne tik BK 198 straipsnyje, bet tam tikra dalimi ir BK 198[2] bei 214, 215 straipsniuose. Nustačius, kad kaltininkas įgijo visus BK 214 straipsnyje nurodytus požymius turinčius duomenis, jo veikai kvalifikuoti taikytinos ne BK 198 ar 198[2] straipsniuose numatytos normos, o specialioji, esanti BK 214 straipsnyje.

Pavojinga veika, pasireiškusi neteisėtu finansinės operacijos inicijavimu panaudojant elektroninės mokėjimo priemonės naudotojo tapatybės patvirtinimo priemonių duomenis, kvalifikuojama taikant ne BK 198, o 215 straipsnį.

17. BK XXIV skyriuje kriminalizuotos įvairios asmens privatumo pažeidimo apraiškos *inter alia* ir elektroninėje erdvėje, o tai kelia BK 198 straipsnyje ir šiame skyriuje aprašytų nusikalstamų veikų atskyrimo problemų. Nustačius, kad padaryti neteisėti įsikišimo į privatumo sritį veiksmai, jie kvalifikuotini pagal BK 166, 167 ar 168 straipsnius. Šiuose straipsniuose esančios normos yra specialios normai, esančiai BK 198 straipsnyje.

PASIŪLYMAI

Atsižvelgiant į disertacijoje iškeltas problemas ir pateiktus galimus jų sprendimo variantus siūlytini tokie BK 198 ir 198[1] straipsnių pakeitimai:

1. Pakeisti BK 198 straipsnį ir jį išdėstyti taip:

198 straipsnis. ~~Neteisėtas elektroninių duomenų perėmimas ir panaudojimas~~ Neteisėtas disponavimas neviešais elektroniniais duomenimis

1. Tas, kas neteisėtai stebėjo, fiksavo, perėmė~~,~~ **elektroninių ryšių tinklais siunčiamus neviešus elektroninius duomenis arba neteisėtai** įgijo, laikė, pasisavino, paskleidė ar kitaip panaudojo neviešus elektroninius duomenis arba **materialų objektą, kurio turinys yra** ~~neviešus elektroninius duomenis~~ **tokie duomenys**,

baudžiamas bauda **arba laisvės apribojimu, arba areštu, arba** laisvės atėmimu iki ~~ketverių metų~~ **dvejų metų**.

2. Tas, kas **atliko šio straipsnio 1 dalyje numatytus veiksmus neteisėtai prisijungęs prie informacinės sistemos arba neteisėtai** stebėjo, fiksavo, perėmė~~,~~ **ryšių tinklais siunčiamus strateginę reikšmę nacionaliniam saugumui arba didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinčius neviešus elektroninius duomenis arba neteisėtai** įgijo, laikė, pasisavino, paskleidė ar kitaip panaudojo ~~strateginę reikšmę nacionaliniam saugumui arba didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinčius neviešus elektroninius duomenis,~~ **tokius elektroninius duomenis arba materialų objektą, kurio turinys yra tokie duomenys,**

baudžiamas **bauda arba** laisvės atėmimu iki ~~šešerių metų~~ **ketverių metų**.

3. Už šiame straipsnyje numatytas veikas atsako ir juridinis asmuo.

2. Pakeisti BK 198[1] straipsnį ir jį išdėstyti taip:

198[1] straipsnis. Neteisėtas prisijungimas prie informacinės sistemos

1. Tas, kas neteisėtai prisijungė prie informacinės sistemos pažeisdamas **arba apeidamas** informacinės sistemos apsaugos priemones,

baudžiamas viešaisiais darbais arba bauda, **arba laisvės apribojimu,** arba areštu, arba laisvės atėmimu iki vienerių metų.

2. Tas, kas neteisėtai prisijungė prie strateginę reikšmę nacionaliniam saugumui arba didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinčios informacinės sistemos,

baudžiamas bauda arba areštu, arba laisvės atėmimu iki trejų metų.

3. Už šiame straipsnyje numatytas veikas atsako ir juridinis asmuo.

LITERATŪRA

I. 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 informacinės visuomenės paslaugų įstatymas. *Valstybės žinios*. 2006, Nr. 65-2380.
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 elektroninių ryšių įstatymas. *Valstybės žinios*. 2004, Nr. 69-2382.
10. Lietuvos Respublikos strateginę reikšmę nacionaliniam saugumui turinčių įmonių ir įrenginių bei kitų nacionaliniam saugumui užtikrinti svarbių įmonių įstatymas. *Valstybės žinios*. 2002, Nr. 103-4604.
11. Lietuvos Respublikos elektroninio parašo įstatymas. *Valstybės žinios*. 2000, Nr. 61-1827
12. Lietuvos Respublikos mokėjimų įstatymas. *Valstybės žinios*. 1999, Nr. 97-2775.
13. Lietuvos Respublikos civilinės saugos įstatymas. *Valstybės žinios*. 1998, Nr. 115-3230.
14. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas. *Valstybės žinios*. 1996, Nr. 63-1479.
15. Lietuvos Respublikos visuomenės informavimo įstatymas. Valstybės žinios. 1996, Nr. 71-1706.
16. 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.
17. 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.
18. 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.
19. Lietuvos Respublikos Vyriausybės 2010 m. birželio 7 d. nutarimas Nr. 717 Dėl objektų pripažinimo valstybinės reikšmės objektais tvarkos aprašo patvirtinimas. *Valstybės žinios*. 2010, Nr. 69-3442.

II. Užsienio valstybių norminiai teisės aktai

20. Computer Misuse Act. [interaktyvus], [žiūrėta 2013-06-01]. <http://www.legislation.gov.uk/ukpga/1990/18/section/1>.
21. Cyprus Law No. 22(III)04. [interaktyvus], [žiūrėta 2013-01-19]. <http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/CountryProfiles/cyber_cp_%20Cyprus_2007_June.pdf>.
22. Criminal Code of the Republic of Bulgaria. [interaktyvus], [žiūrėta 2013-06-01]. <http://www.vks.bg/english/vksen_p04_04.htm#Section_I_>.
23. Criminal Code of the Republic of Estonia. [interaktyvus], [žiūrėta 2013-06-01]. <http://www.legislationline.org/download/action/download/id/1280/file/4d16963509db70c09d23e52cb8df.htm/preview>.
24. Penal Code of the Republic of France. [interaktyvus], [žiūrėta 2013-06-01]. <http://www.legifrance.gouv.fr/Traductions/en-English/Legifrance-translations>.
25. Criminal Code of the Federal Republic of Germany. [interaktyvus], [žiūrėta 2013-06-01]. <http://www.gesetze-im-internet.de/englisch_stgb/index.html>.
26. Penal Code of the Republic of Latvia. [interaktyvus], [žiūrėta 2013-06-01]. <http://www.legislationline.org/download/action/download/id/1280/file/4d16963509db70c09d23e52cb8df.htm/preview>.
27. Criminal Code of the Republic of Poland. [interaktyvus], [žiūrėta 2013-06-01].<http://www.legislationline.org/documents/section/criminal-codes/country/10>.
28. Criminal Code Of The Russian Federation. [interaktyvus], [žiūrėta 2013-06-01]. <http://www.russian-criminal-code.com>.
29. The Code of the United States. [interaktyvus], [žiūrėta 2012-09-04]. <http://www.law.cornell.edu/uscode/text/18/1030>.
30. The Code of Maryland. [interaktyvus], [žiūrėta 2013-06-02]. <http://law.justia.com/codes/maryland/2010/criminal-law/title-7/subtitle-3/7-302>.
31. The Statutes of Kanzas. [Interaktyvus], [žiūrėta 2012-11-16]. <http://kansasstatutes.lesterama.org/Chapter_21/Article_37/21-3755.html>.
32. Regulation of Investigatory Powers Act. [interaktyvus], [žiūrėta 2013-06-01]. <http://www.legislation.gov.uk/ukpga/2000/23/section/1>.

III. Tarptautiniai ir Europos Sąjungos teisės aktai

33. Visuotinė žmogaus teisių deklaracija. *Valstybės žinios*. 2006, Nr. 68-2497.
34. Tarptautinis pilietinių ir politinių teisių paktas. *Valstybės žinios*. 2002, Nr. 77-3288.
35. Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija. *Valstybės žinios*. 1995, Nr. 40-987.
36. Europos Tarybos konvencija dėl elektroninių nusikaltimų. *Valstybės žinios*. 2004, Nr. 36-1188.
37. 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.
38. Europos Sąjungos Tarybos 2008 m. gruodžio 8 d. direktyva 2008/114/EC dėl Europos ypatingos svarbos infrastruktūros objektų nustatymo ir priskyrimo jiems bei būtinybės gerinti jų apsaugą vertinimo. [2008] OL L345/76.
39. Europos Sąjungos Tarybos 2005 m. vasario 24 d. pamatinio sprendimo 2005/212/TVR dėl nusikalstamu būdu įgytų lėšų, nusikaltimo priemonių ir turto konfiskavimo [2005] OL L 68/49.

40. Europos Sąjungos Tarybos 2005 m. vasario 24 d. pagrindų sprendimas 2005/222/TVR dėl atakų prieš informacines sistemas [2005] OL L 69/67.
41. Europos Parlamento ir Tarybos 2002 m. liepos 12 d. direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių) (OL 2004 m. *specialusis leidimas*, 13 skyrius, 29 tomas, p. 514) su paskutiniais pakeitimais, padarytais 2009 m. lapkričio 25 d. Europos Parlamento ir Tarybos direktyva 2009/136/EB. [2009] OL L 337/11.
42. Europos Parlamento ir Tarybos 1995 m. spalio 24 d. direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo. [1995] OL L 281/31.
43. 2007 m. gegužės 22 d. Europos Komisijos Komunikatas Europos Parlamentui, Tarybai ir Europos Regionų komitetui Bendrosios politikos, skirtos kovai su elektroniniais nusikaltimais, linkme KOM/2007/0267 galutinis. [interaktyvus], [žiūrėta 2012-01-24] <http://eur-lex.europa.eu>.
44. 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 2013-06-02]. <*www.ictregulationtoolkit.org/en/Document.1501.pdf*>.
45. Council of Europe Committee of Ministers Recommendation No. R (89) 9 Of the Committee of Ministers to Member States on Computer – related Crimes (Adopted by the Committee of Ministers on 13 September 1989 at the 428th meeting of the Ministers' Deputies) [interaktyvus], [žiūrėta 2012-01-24]. <https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=610660&SecMode=1&DocId=702280&Usage=2>.
46. Pasaulinio aukščiausio lygio susitikimo informacinės visuomenės klausimais, vykusio Ženevoje 2003 m. gruodžio 10–12 d., metu priimta principų deklaracija „Informacinės visuomenės sukūrimas – globalus naujojo tūkstantmečio uždavinys". [interaktyvus], [žiūrėta 2012-04-20]. <http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1161%7C1160>.

III. Mokslinė ir kita specialioji literatūra

47. *A Dictionary of Computing*. 5-asis leidimas. Daintith, J. (gen. ed.). Oxford: Oxford University Press, 2004.
48. Abramavičius, A., *et al. Lietuvos Respublikos baudžiamojo kodekso komentaras. Specialioji dalis (213–330 straipsniai)*. Vilnius: Registrų centras, 2010.
49. Abramavičius, A., *et al. Lietuvos baudžiamojo kodekso komentaras. Specialioji dalis (99–212 straipsniai)*. Vilnius: Registrų centras, 2009.
50. Abramavičius, A., *et al. Baudžiamoji teisė.* Bendroji dalis. 3-iasis pataisytas ir papildytas leidimas. Vilnius: Eugrimas, 2001.
51. Abramavičius, A., *et al. Baudžiamoji teisė*. Specialioji dalis. Vilnius: Eugrimas, 2000.
52. Ali, R. Technological Neutrality. *Lex Electronica*, 2009, 14(2).
53. Arlauskas, S. Metaforos ir normos: autorinių teisių samprata skaitmeninėje visuomenėje/ Knygos recenzija. Socialinių mokslų studijos. 2013, 5(1).
54. Ashworth, A. Conceptions of Overcriminalization. *Ohio State Journal Of Criminal Law*. 2008, 5.

55. Bainbridge, D. *Introduction to Computer Law*. 5-oji laida. Harlow: Pearson: Longman, 2004.
56. Barlow, J. P. A Declaration of Independence of Cyberspace. [interaktyvus], [žiūrėta 2012-09-29]. <https://projects.eff.org/~barlow/Declaration-Final.html>.
57. *Baudžiamasis procesas: nuo teorijos iki įrodinėjimo (prof. Eugenijaus Palskio atminimui)*. Mokslo studija. Vilnius: Mykolo Romerio universiteto leidykla, 2011.
58. Bikelis, S. *Tyčinė kaltė baudžiamosios teisės teorijoje ir praktikoje: daktaro disertacija*. Vilnius: Mykolo Romerio universitetas, 2007.
59. Bishop, M. *Computer Security: Art and Science.* Addison Wesley Professional, 2003.
60. *Black's Law Dictionary*. 9-asis leidimas. Garner, B. A. (ed. in chief). St. Paul (Minn.): West: Thomson Reuters busines, 2009.
61. Blundell, B. G. *Computer Systems and Networks*. London: Thomson: Middesex University Press, 2007.
62. Blunn, A. S. Report of the Review of the Regulation of Access to Communications. [interaktyvus]. Australija, 2005, [žiūrėta 2013-06-01]. <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>
63. Brenner, S. W. Cybercrime Metrics: Old Wine, New Bottles? *Virginia Journal of Law & Technology*, 2004, 9(13).
64. Brunner, E. M.; Suter, M. *International CIIP Handbook 2008/2009*. [interaktyvus], [žiūrėta 2013-06-01]. <http://www.css.ethz.ch/publications/pdfs/CIIP-HB-08-09.pdf>.
65. Budnikas, A., *et al*. *Elektroninės valdžios sauga*. Kaunas: Vitae Litera, 2008.
66. Bukelienė, D. *Baudžiamoji atsakomybė už turto pasisavinimą ir turto iššvaistymą (teoriniai ir praktiniai aspektai)*. Vilnius: Eugrimas, 2008.
67. Castells, M. *Tinklaveikos visuomenės raida*. Kaunas: Poligrafija ir informatika, 2005.
68. Civilka, M., *et al*. *Informacinių technologijų teisė*. Vilnius: NVO Teisės institutas, 2004.
69. Clough, J. *Principles of Cybercrime*. Cambridge: Cambridge University Press, 2010.
70. Clough, J. Data Theft? Cybercrime and the Increasing Criminalization of Access to Data. *Criminal Law Forum.* 2011, 22.
71. *Computer law***.** Reed, C. (ed). Oxford: Oxford University Press, 2011
72. *Computer Law: The Law and Regulation of Information Technology*. 6-asis leidimas. Reed, C.; Angel, J. (eds.). Oxford: Oxford University Press, 2007.
73. *Computer security handbook*. 4-oji laida. Hutt, A. E.; Bosworth, S.; Hoyt, D. B. (eds). New York, *et al*.: Wiley, 2002.
74. *Computer and Information security handbook.* Vacca, J. R. (red). Amsterdam: Elsevier: Morgan Kaufmann, 2009.
75. Convention on Cybercrime Explanatory Report. [interaktyvus], [žiūrėta 2012-01-24] <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>.
76. *Crime Online*. Jewkes, Y. (ed.). Willan Publishing, 2007.
77. *Cybercrime and Jurisdiction: a global survey*. Koops, B.–J.; Brenner, S. (eds). The Hague: T.M.C. Asser Press, 2006.
78. *Cybercrime: Digital Cops in a Networked Environment.* Balkin, J., *et al*. (eds.). New York (N.Y.): New York University Press, 2007.

79. *Cybercrimes: A Multidisciplinary Analysis*. Ghosh, S.; Turrini, E. (eds). Berlin: Springer, 2010.
80. Česnys, A.; Juknius, J. *Saugumo patikros ir etiško įsilaužimo technologijos*. Kaunas: KTU leidykla „Technologija“ 2011.
81. *Dabartinės lietuvių kalbos* žodynas. Keinys, S., *et al.* (red.). 4-asis leidimas. Lietuvių kalbos institutas, 2000.
82. *Dabartinės lietuvių kalbos žodynas*. Keinys, S. (vyr. red.). 7-asis pataisytas ir papildytas leidimas. Vilnius: Lietuvių kalbos institutas, 2012.
83. Dagienė, V., *et al*. *Enciklopedinis kompiuterijos žodynas*. 2-asis papildytas leidimas. Vilnius: TEV, 2008.
84. *Dictionary of Information Science and Technology*. I tomas. Khosrow–Pour, M. (ed.). Hershey, Pa., *et al*: Idea Group Reference, 2007.
85. *Dictionary of Information Technology*. 2-asis leidimas. Greasby, L.; Green, Th. (eds). Teddington: Peter Collin Publishing, 1996.
86. Drakšienė, A. Baudžiamoji atsakomybė už vagystę. *Teisė*, 2000, Nr. 37.
87. Domeika, P. *Apskaitos informacinė sistema*. Kaunas: „Spalvų kraitė“, 2008.
88. 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).
89. Dulinskas, D.; Dulinskienė, J. *ECDL visiems: kompiuterinio raštingumo pagrindai*. Kaunas: Informacinių technologijų mokymo centas, 2006.
90. Dzemydienė, D.; Naujikienė, R. *Informacinės sistemos. Duomenų struktūros ir valdymas*. Vilnius: Lietuvos teisės universiteto Leidybos centras, 2004.
91. El Gamal, A. A.; Kim, Y.–H. *Network Information Theory*. Cambridge: Cambridge University Press, 2011.
92. *Enciklopedinis kompiuterijos žodynas*. 2-asis papildytas leidimas. Vilnius: TEV, 2008.
93. Erickson, J. *Hakingas. Programų kodo narstymo menas*. 2-asis pataisytas ir papildytas leidimas. Kaunas: „Smaltijos“ leidykla, 2010.
94. Fedosiuk, O. Baudžiamoji atsakomybė kaip kraštutinė priemonė (*ultima ratio*): teorija ir realybė. *Jurisprudencija*, 2012. Nr. 19 (2).
95. Fedosiuk O. Nuosavybė ir turtas Civiliniame ir Baudžiamajame kodeksuose. *Jurisprudencija*. 2002, 28 (20).
96. Floridi, L. Open Problems in the Philosophy of Information. *Metaphilosophy*. 2004, 35(4).
97. *Funk & Wagnalls standard dictionary of the English language: combined with Britannica world language dictionary*. I tomas. Chicago: Encyclopaedia Britannica, 1960.
98. Girdenis, T. Nusikalstamų veikų daugetas Lietuvos baudžiamojoje teisėje: daktaro disertacija: socialiniai mokslai, teisė (01 S). – Vilnius: Mykolo Romerio universitetas, 2010.
99. Goranin, N.; Mažeika, D. *Nusikaltimai elektroninėje erdvėje ir jų tyrimo metodikos*. Mokomoji knyga. Kaunas: TEV [i.e. Technologija], 2011.
100. Gordon, J. R.; Gordon, S. R. *Information systems*. 2-asis leidimas. The Dryden Press: Harcourt Brace College Publisher, 1999.
101. Gupta, U. *Information Systems*. Upper Saddle River, New Jersey: Prentice-Hall Inc, 2000.
102. *Information technology and Moral Philosofy*. Hoven, van den J.; Weckert, J. (eds). Cambridge *et al*: Cambridge Univesity Press, 2008.

103. Johnson, D. R., Post, D. G. Law and Borders – The Rise of Law in Cyberspace. *Stanford Law Review.* 1996, 48.
104. Jarukaitis, I. *et al*. *Elektroninių ryšių teisė*. Vilnius: Eugrimas, 2005.
105. Jonušauskas S., Bilevičienė T., Kažemikaitis, V. Įvadas į informatiką. Vilnius: Lietuvos teisės universiteto Leidybos centras, 2002.
106. Jonušauskas, S.; Naujikienė, R.; Petrauskas, R. *Kompiuterinio raštingumo pagrindai, reikalingi Europos kompiuterių vartotojo pažymėjimui gauti*. Vilnius: Lietuvos teisės universiteto Leidybos centras, 2004.
107. Kašėta, S.; Adomkus, T. *Telefonijos informacijos ir VoIP sauga*. Kaunas: Vitae Litera, 2008.
108. Kalpokas, V.; Marcinauskaitė, R. Tapatybės vagystė elektroninėje erdvėje: technologiniai aspektai ir baudžiamasis teisinis vertinimas. *Teisės problemos*. 2012, Nr. 3(77).
109. Kanapeckas, P., *et al. Kompiuterių elementai* [elektroninis išteklius]. Kaunas: Technologija, 2011.
110. Kazanavičius, E., *et al*. *Informacijos saugos vadyba*. Kaunas: Vitae Litera, 2008.
111. Kazanavičius, E. *et al*. *Programų sauga [elektroninis išteklius]: mokomoji knyga*. Kaunas: TEV, 2011.
112. Kerr, O. S. Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes. *NYU Law Review.* 2003, 78(5).
113. Kerr, O. S. The Problem of Perspective in Internet Law. *Georgetown Law Journal*. 2003, 91.
114. Khokins, Dzh. M. *The Oxford Dictionary of the English Language*. Moskva: OOO «Izdatelstvo Actrel», OOO «Izdatelstvo AST», 2001.
115. Kiškis, M., *et al. Teisės informatika ir informatikos teisė*. Vilnius: Mykolo Romerio universiteto Leidybos centras, 2006.
116. Kirby, C. A**.** Defining Abusive Software to Protect Computer Users from the Threat of Spyware. *Science and Law Review*, X(3).
117. 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).
118. Kommentarij k ugolovnomu kodeksu Rossijskoj Federacii [Commentary to the Criminal Code of the Russian Federation]. Naumov, A.V. (red.). Moskva: Jurist, 1996.
119. *Kompiuterija*. Burgis, B.; Kulikauskas, A. (red.). Kaunas: „Naujasis LANKAS", 2000.
120. Koops, B.–J. *Should ICT regulation be Technology-Neutral?* [interaktyvus], [žiūrėta 2013-04-24]. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=918746>.
121. *Kurs ugolovnogo prava: uchebnik* [The course of criminal law: The textbook]. Kuznecoba, N.F.; Tjazhkova, I.M. (red). Moskva: Zercalo-M, 2002.
122. Lankauskas, M.; Mulevičius, M.; Zaksaitė, S. *Teisės į privatumą, minties, sąžinės, religijos laisvę ir saviraišką užtikrinimo problemos*. Mokslo studija. Vilnius: Lietuvos teisės institutas, 2013.
123. Laudon, K. C.; Laudon, J. P. *Essentials of Management Information Systems*. 3–ias leidimas. New Jersey: Prentice-Hall, Inc., 1999.
124. Laučius, J.; Vasilecas, O. *Informacinių technologijų projektų ir kokybės valdymas. Mokomoji knyga*. Vilnius: Technika, 2007.
125. Lessig, L. *Code and other Laws of Cyberspace*. New York (N.Y.): Basic books, 1999.
126. *Lietuvos Respublikos civilinio kodekso komentaras. Antroji knyga. Asmenys*. Mikelėnas, V. *et al*. Vilnius: Justitia, 2002.

127. *Lietuvos Respublikos konstitucijos komentaras*. Jovaišas, K. (atsakingas redaktorius). Vilnius: Teisės institutas, 2000.
128. Lyberis, A. *Sinonimų žodynas*. Vilnius: Lietuvos kalbos instituto leidykla, 2002.
129. *Longman dictionary of Contemporary English*. Summers, D. (edit. director). Berlin; München: Langenscheidt. Longman, 1987.
130. Madison, M. J. Rights of Access and the Shape of the Internet. *Boston College Law Review*. 44(2). 2003.
131. Manson, N. C.; O'Neill, O. *Rethinking Informed Consent in Bioethics*. Cambridge *et al*: Cambridge University Press, 2007.
132. Marcinauskaitė, R. Nusikalstamomis veikomis elektroninėje erdvėje pažeidžiamos pagrindinės baudžiamojo įstatymo saugomos vertybės nustatymo problema. *Socialinių mokslų studijos*. 2011, 3(3).
133. Mazurov V.A. *Kompiuternye prestuplenija: klasifikacija i sposoby protivodeistvija* [Computer crime: classification and ways of counteraction]. Moskva: Paletip, 2002.
134. McClure, S.; Scambray, J.; Kurtz, G. *Apsauga nuo hakerių: tinklo saugumo palaikymo paslaptys ir sprendimai*. Kaunas: „Smaltijos" leidykla, 2006.
135. Melnikas, B. *Transformacijos: visuomenės pokyčiai, naujas tūkstantmetis, valdymas ir savireguliacija, Rytų ir Vidurio Europa*. Vilnius: Vaga, 2002.
136. Mitra, A. From Cyber Space to Cybernetic Space: Rethinking the Relationship Between Real and Virtual Spaces. *Journal of Computer – Mediated Communication*. 2001, 7(1).
137. Moor, J. H. What is Computer Ethics? [interaktyvus], [žiūrėta 2012–09–09]. <http://www.blackwellpublishing.com/content/BPL_Images/Content_store/Sample_chapter/9781855548442/CEAC01.pdf >.
138. Moor, J. H. *Reason, Relativity and Responsability in Computer Ethics*. [interaktyvus], [žiūrėta 2012-08-04] <http://www.site.uottawa.ca/~stan/csi2911/moor1.pdf>.
139. Naumov, A. V. Rossijskoe ugolovnoe pravo: kurs lekcij [Russian criminal law: the course of lectures]. 4-asis leidimas. Moskva: Volters Kluver, 2007.
140. *Nepriklausomos Lietuvos teisė: praeitis, dabartis ir ateitis: recenzuotų mokslinių straipsnių rinkinys: liber amicorum profesoriui Jonui Prapiesčiui*. Švedas, G. (vyr. mokslinis redaktorius). Vilnius: Vilniaus universiteto Teisės fakulteto Alumni draugija, 2012.
141. *None-State Actors as Standard Setters*. Peters, A., *et al*. (eds). Cambridge: Cambridge University Press, 2009.
142. Norman, T. L. *Electronic Access Control*. Elsevier Inc., 2012.
143. Ohm, P. The Arguments against Technology – Neutral Surveillance Laws. *Texas Law Review*, 2010, 88(7).
144. Panomariovas, A. Asmens privataus gyvenimo paslaptis ir su ja susijusios problemos baudžiamajame procese. *Jurisprudencija*, 2001, 23(15).
145. Panomariovas, A. Viešai neskelbiama informacija (paslaptis) baudžiamajame procese: daktaro disertacija: socialiniai mokslai, teisė (01 S). – Vilnius: Lietuvos teisės universitetas, 2001.
146. Paulauskas, K. V. *Aiškinamasis kompiuterijos terminų santrumpų žodynas*. Kaunas: Technologija, 2000.
147. Pavilonis, V., Abramavičius, A. Lietuvos Respublikos baudžiamojo kodekso novelos. *Teisė*, 1994, 1.

148. Pavilonis, V. Baudžiamosios teisės normų konkurencija. *Teisės problemos*. 1996, 2(12).
149. Petrauskas, R.; Štitilis, D. *Kompiuteriniai nusikaltimai ir jų prevencija*. Vilnius: Lietuvos teisės akademijos Leidybos centras, 2000.
150. Piesliakas, V. Grobimas įsibraunant į butą, patalpą ar kitokią saugyklą. *Socialistinė teisė*. 1984. Nr. 1.
151. Pikelis, A. *Baudžiamosios teisėkūros labirintai*. Vilnius: UAB „Petro ofsetas", 2011.
152. Plėštys, R., *et al. Tinklų sauga*. Kaunas: Vitae Litera, 2008.
153. Pobedonoccev, K. Kurs grazhdanskago prava. Pervaja chast. [The course of civil law. First part]. Sanktpeterburg, 1896.
154. Potter, R. T., *et al. Introduction to Information Systems: Supporting and Transforming Business*. John Wiley & Sons, Inc., 2007.
155. Pranka, D. Apgaulės samprata ir reikšmė atribojant sukčiavimą ir civilinės teisės pažeidimą. *Socialinių mokslų studijos*, 2012, 4(2).
156. Reed, C. Online and Offline Equivalence: Aspiration and Achievement. *International Journal of Law and Information Technology*. 2010, 18 (3).
157. Reed, C. Taking Sides on Technology Neutrality. *SCRIPTed*. 2007, 4(3).
158. Reed, D. Should the English Legal System adopt the US Law of Cyber – Trespass? *SCRIPTed*. 2011, 8(1).
159. Reed, C. *Internet: law text and materials*. Cambridge: Cambridge University Press, 2004.
160. *Regulating Technologies*. Brownsword, R.; Yeung, K. (eds). Oxford; Portland (Or.): Hart Publishing, 2008.
161. Reidenberg, J. R. Lex Informatica: The Formulation of Information Policy Rules through Technology. *Texas Law Review*. 1998, 76 (3).
162. *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.
163. Rowland, D.; Macdonald, E. Information Technology Law. 3-iasis leidimas. Sydney; Portland (Or.): Cavendish Publishing, 2005.
164. Sauliūnas, D. Legislation on Cybercrime in Lithuania: Development and Legal Gaps in Comparison with the Convention on Cybercrime. *Jurisprudencija* 2010, 4 (122).
165. Saulis, A.; Vasilecas, O. *Informacinių sistemų projektavimo metodai: mokomoji knyga*. Vilnius: Technika, 2008.
166. Schauer, F. Free Speech and the Demise of the Soapbox. *Columbia Law Review*, 1984, 84 (2).
167. Schellekens, M. What holds Off – Line, also holds On-Line? [interaktyvus], [žiūrėta 2012-09-29]. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=952275>.
168. *Seeds of Disaster, Roots of Response: How Private Actions Can Reduce Public Vulnerability*. Auerswald, P. E., *et al* (eds). Cambridge: Cambridge University Press, 2006.
169. Sinkevičius, E. *Neteisėtas banko kredito gavimas arba panaudojimas ir jų kvalifikavimas*. Vilnius: Lietuvos teisės universiteto Leidybos centras, 2002.
170. Skersys, G. *Informacijos sauga*. Mokomoji knyga. Kaunas: TEV [i.e. Technologija], 2011.
171. Skyrius, R.; Mikalauskienė, A.; Zalieckaitė, L. *Informacijos ir komunikacijos technologijos*. Vilnius: UAB „Vilniaus spauda", 2008.

172. Smith, R. G., Grabosky, P., Urbas, G. *Cyber Criminals on Trial.* Cambridge: Cambridge University Press, 2004.
173. Spinello, R. A. *Cyberethics: Morality and Law in Cyberspace*. Jones and Bartlett Publishers, Inc. 2000.
174. Strawbridge, M. *Netiquette: Internet Etiquette in the Age of the Blog*. Software Reference Ltd. 2006.
175. Stoneburner, G. *Underlying Technical Models for Information Technology Security: recomendations of the National Institute of Standards and Technology* [interaktyvus], [žiūrėta 2010-09-27]. <http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf>
176. Sumit, K.; Nishit, N.; Sumita, N. *Communication networks: principles and practice*. New York: McGraw-Hill, 2007.
177. Štitilis, D. *Elektroniniai nusikaltimai*. Vilnius: Mykolo Romerio universitetas, 2011.
178. Štitilis, D., *et al. Tapatybės vagystė elektroninėje erdvėje: socialiniai, elektroninio verslo ir teisinio reguliavimo aspektai*. Vilnius: Mykolo Romerio universitetas, 2011.
179. Štitilis, D.; Laurinaitis, M. Tapatybės vagystė elektroninėje erdvėje. *Informacijos mokslai*. 2009, 50.
180. Štitilis, D. Teisinės atsakomybės pagrindų nustatymo už neteisėtas veikas elektroninėje erdvėje problemos: daktaro disertacija: socialiniai mokslai, teisė (01 S). – Vilnius: LTU, 2002.
181. Štitilis, D. Kai kurie neteisėtos prieigos prie kompiuterinės informacijos kriminalizavimo aspektai. *Jurisprudencija*. 2003, 47(39)
182. Švedas, G. Veikos kriminalizavimo kriterijai: teorija ir praktika. *Teisė*. 2012, 82.
183. Švedas, G. *Baudžiamosios politikos pagrindai ir tendencijos Lietuvos Respublikoje*. Vilnius: Teisinės informacijos centras, 2006
184. *Tarptautinių žodžių žodynas*. Sudarytojai Bendorienė, A., *et al*. Atsakomasis redaktorius Kinderys, A. Vilnius: Alma litera, 2001.
185. *Technikos enciklopedija*. II tomas. Redaktorių taryba: pirmininkas Zavadskas, E. K. *et al*. Vilnius: Mokslo ir enciklopedijų leidybos inst., 2003.
186. *The History of Information Security: A Comprehensive Handbook*. Leeuw, D. K., Bergstra, J. (eds). Amsterdam, *et al.*: Elsevier, 2007.
187. *The Internet Encyclopedia*. Bidgoli, H. (ed.). John Wiley and Sons, Inc. 2004.
188. Thornton, G. Unauthorised Access (hacking). [interaktyvus], [žiūrėta 2012-11-26] <http://ebookbrowse.com/grant-thornton-unauthorised-access-pdf-d18884414>.
189. *Ugolovnoe pravo Rossii. Osobennaja chast: uchebnik* [Russian criminal law. Special Part: The textbook]. Borzenkova, G. N.; Komissarova, V. S. (red.), Moskva: Zercalo – M, 2005.
190. *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.
191. *Ugolovnoe pravo Rossii. Osobennaja chast: uchebnik* [Russian criminal law. Special Part: The textbook]. Rarog, A. I. (red.). Moskva: Ehksmo, 2010
192. *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
193. Vaitkevičiūtė, V. *Tarptautinių žodžių žodynas*. 4-asis pataisytas ir papildytas leidimas. Vilnius: Žodynas, 2007.

194. Valauskas, E. J. Lex Networkia: Understanding the Internet Community. *First Monday*. 1996.
195. Van der Haar, I. M. Technological Neutrality: What Does It Entail? [interaktyvus], [žiūrėta 2013-06-01] <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=985260>.
196. Venčkauskas, A.; Toldinas, E. *Kompiuterių ir operacinių sistemų sauga*. Kaunas: Vitae Litera, 2008.
197. Volevodz, A. G. *Protivodeistvie kompiuternym prestuplenijam* [Counteraction to computer crime]. Moskva: Izdatelstvo «Jurlitinform», 2002.
198. Vetrov, N. I. *Ugolovnoe pravo. Osobenaja chast: uchebnik* [Criminal law. Special Part: Textbook]. 2-asis leidimas. Moskva: JUNITI-DANA: Zakon i pravo, 2002
199. Žilinskas, A.; Leonavičius, G.; Valavičius, E. *Informatika*. Vilnius: „Aldorija", 2000.
200. Žėkas, T. Vaiko išnaudojimas pornografijai: baudžiamieji teisiniai ir kriminologiniai aspektai: daktaro disertacija: socialiniai mokslai, teisė (01 S). – Vilnius: Vilniaus universitetas, 2011
201. Wacks, P., *Personal Information: Privacy and the Law*. Oxford: Clarendon Press, 1989.
202. Walden, I. *Computer Crimes and Digital Investigations*. Oxford: Oxford University Press, 2007.
203. Webster, M. *Data protection in the financial services industry*. Aldershot; Burlington (Vt.): Gower, 2006.
204. Wessel, J. *Baudžiamoji teisė. Bendroji dalis: baudžiamoji veikla ir jos struktūra*. Vilnius: Eugrimas, 2003.
205. Whitman, M. E., *et al*. *Principles of information security*. 3–ioji laida. Boston: Thomson: Course Technology, 2009.
206. 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).
207. 2009 m. kovo 16 d. Lietuvos Respublikos valstybės kontrolės išankstinio tyrimo ataskaita Nr. IT-P-900-1-3 Strateginės informacijos sauga. [interaktyvus], [žiūrėta 2013-08-29]. <http://www.vkontrole.lt/audito_ataskaitos.aspx?tipas=7>.

V. Lietuvos teismų praktika

208. Lietuvos Respublikos Konstitucinio Teismo 2006 m. sausio 16 d. nutarimas.
209. Lietuvos Respublikos Konstitucinio Teismo 2005 m. rugsėjo 29 d. nutarimas.
210. Lietuvos Respublikos Konstitucinio Teismo 2004 m. gruodžio 29 d. nutarimas.
211. Lietuvos Respublikos Konstitucinio Teismo 2004 m. gruodžio 13 d. nutarimas.
212. Lietuvos Respublikos Konstitucinio Teismo 2003 m. kovo 24 d. nutarimas.
213. Lietuvos Respublikos Konstitucinio Teismo 2003 m. gegužės 30 d. nutarimas.
214. Lietuvos Respublikos Konstitucinio Teismo 2002 m. rugsėjo 19 d. nutarimas
215. Lietuvos Respublikos Konstitucinio Teismo 2002 m. spalio 23 d. nutarimas.
216. Lietuvos Respublikos Konstitucinio Teismo 2001 m. liepos 12 d. nutarimas.
217. Lietuvos Respublikos Konstitucinio Teismo 2000 m. gegužės 8 d. nutarimas.
218. Lietuvos Respublikos Konstitucinio Teismo 1999 m. spalio 21 d. nutarimas.
219. Teismų praktikos sukčiavimo baudžiamosiose bylose (Baudžiamojo kodekso 182 straipsnis) apžvalga. *Teismų praktika*. 2012, Nr. 36.

220. Teismų praktikos taikant turto konfiskavimą (BK 72 straipsnis) apžvalga. *Teismų praktika*. 2010, Nr. 32.
221. 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.
222. 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.
223. Lietuvos Aukščiausiojo Teismo teisėjų senato 2002 m. birželio 21 d. nutarimas Nr. 37 „Dėl teismų praktikos nagrinėjant psichotropinių ar narkotinių medžiagų grobimo, neteisėto šių medžiagų ir jų pirmos kategorijos pirmtakų (prekursorių) gaminimo, įgijimo, laikymo, gabenimo, siuntimo, pardavimo ar kitokio platinimo baudžiamąsias bylas“. *Teismų praktika*. 2002, Nr. 17.
224. Lietuvos Aukščiausiojo Teismo senato 1998 m. gruodžio 22 d. nutarimas Nr. 8 „Dėl teismų praktikos sukčiavimo ir turto pasisavinimo arba iššvaistymo baudžiamosiose bylose (BK 274–275 straipsniai)“. *Teismų praktika*. 1998, Nr. 10.
225. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2012 m. birželio 26 d. nutartis baudžiamojoje byloje (bylos Nr. 2K-375/2012).
226. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2011 m. balandžio 5 d. nutartis baudžiamojoje byloje (bylos Nr. 2K-159/2011).
227. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2011 m. balandžio 19 d. nutartis baudžiamojoje byloje (bylos Nr. 2K-162/2011)
228. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2011 m. gruodžio 6 d. nutartis baudžiamojoje byloje (bylos Nr. 2K-482/2011).
229. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2010 m. kovo 23 d. baudžiamojoje byloje (bylos Nr. 2K-198/2010).
230. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2010 m. gegužės 11 d. nutartis baudžiamojoje byloje (bylos Nr. 2K-185/2010).
231. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2010 m. spalio 12 d. nutartis baudžiamojoje byloje (bylos Nr. 2K-448/2010).
232. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2010 m. gruodžio 7 d. nutartis baudžiamojoje byloje (bylos Nr. 2K-555/2010).
233. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2010 m. gruodžio 21 d. nutartis kasacinėje byloje (bylos Nr. 2K-560/2010).
234. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2009 m. kovo 31 d. nutartis baudžiamojoje byloje (bylos Nr. 2K-76/2009).
235. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2009 m. balandžio 28 d. nutartis baudžiamojoje byloje (bylos Nr. 2K-90/2009).
236. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2009 m. gegužės 5 d. nutartis baudžiamojoje byloje (bylos Nr. 2K-104/2009).
237. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus plenarinės sesijos 2009 m. spalio 20 d. nutartis baudžiamojoje byloje (bylos Nr. 2K-P-218/2009).
238. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2007 m. kovo 20 d. nutartis baudžiamojoje byloje (bylos Nr. 2K-123/2007).

239. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2007 m. lapkričio 27 d. baudžiamojoje byloje (bylos Nr. 2K-733/2007).
240. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2006 m. balandžio 25 d. baudžiamojoje byloje (bylos Nr. 2K-396/2006).
241. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2006 m. gegužės 30 d. baudžiamojoje byloje (bylos Nr. 2K-330/2006).
242. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2008 m. gruodžio 9 d. nutartis baudžiamojoje byloje (bylos Nr. 2K-368/2008).
243. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2006 m. sausio 24 d. nutartis kasacinėje byloje (bylos Nr. 2K-86/2006).
244. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2006 m. balandžio 11 d. baudžiamojoje byloje (bylos Nr. 2K-213/2006).
245. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2006 m. balandžio 25 d. nutartis baudžiamojoje byloje (bylos Nr. 2K-396/2006).
246. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2006 m. birželio 27 d. baudžiamojoje byloje (bylos Nr. 2K-467/2006).
247. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2005 m. vasario 22 d. nutartis baudžiamojoje byloje (bylos Nr. 2K-187/2005).
248. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2001 m. spalio 9 d. nutartis baudžiamojoje byloje (bylos Nr. 2K-682/2001).
249. Vilniaus apygardos teismo 2013 m. gegužės 29 d. nutartis baudžiamojoje byloje (bylos Nr. 1A-294-166/2013).
250. Vilniaus apygardos teismo 2011 m. gruodžio 23 d. nuosprendis baudžiamojoje byloje (bylos Nr. 1A-977/2011).
251. Vilniaus miesto apylinkės teismo 2013 m. sausio 25 d. nuosprendis baudžiamojoje byloje (bylos Nr. 1-258-716/2013).
252. Vilniaus miesto 1 apylinkės teismo 2011 m. kovo 25 d. nuosprendyje baudžiamojoje byloje (bylos Nr. 1-68-203/2011).
253. Vilniaus miesto 1 apylinkės teismo 2011 m. gruodžio 6 d. nuosprendis baudžiamojoje byloje (bylos Nr. 1-1430-276/2011).
254. Vilniaus miesto 1 apylinkės teismo 2010 m. kovo 5 d. teismo baudžiamasis įsakymas baudžiamojoje byloje (bylos Nr. N1-724-276/2010).
255. Vilniaus miesto 1 apylinkės teismo 2009 m. rugsėjo 14 d. teismo baudžiamasis įsakymas baudžiamojoje byloje (bylos Nr. N1-1470-88/2009).
256. Vilniaus miesto 1 apylinkės teismo 2008 m. rugsėjo 5 d. nuosprendis baudžiamojoje byloje (bylos Nr. 1-17-296/2008).
257. Vilniaus miesto 2 apylinkės teismo 2011 m. liepos 1 d. nuosprendis baudžiamojoje byloje (bylos Nr. 1-188-387/2011).
258. Vilniaus miesto 2 apylinkės teismo 2009 m. gegužės 27 d. teismo baudžiamasis įsakymas baudžiamojoje byloje (bylos Nr. 1-515-487/2009).
259. Vilniaus miesto 2 apylinkės teismo 2008 m. liepos 2 d. nuosprendis baudžiamojoje byloje (bylos Nr. 1-5-655/2008).
260. Vilniaus miesto 3 apylinkės teismo 2010 m. sausio 27 d. nuosprendis baudžiamojoje byloje (bylos Nr. 1-182-498/10).

261. Vilniaus miesto 4 apylinkės teismo 2010 m. gegužės 17 d. nuosprendis baudžiamojoje byloje (bylos Nr. 1-106-816/2010).
262. Vilniaus rajono apylinkės teismo 2009 m. rugsėjo 8 d. nuosprendis baudžiamojoje byloje (bylos Nr. 1-278-298/2009).
263. Kauno apylinkės teismo 2013 m. birželio 7 d. nuosprendis baudžiamojoje byloje (bylos Nr. 1-680-530/2013).
264. Klaipėdos miesto apylinkės teismo 2009 m. liepos 1 d. teismo baudžiamasis įsakymas baudžiamojoje byloje (bylos Nr. 1-770-795/2009).
265. Klaipėdos miesto apylinkės teismo 2009 m. birželio 29 d. teismo baudžiamasis įsakymas baudžiamojoje byloje (bylos Nr. 1-740-93/2009).
266. Kupiškio rajono apylinkės teismo 2009 m. rugsėjo 2 d. nuosprendį baudžiamojoje byloje (bylos Nr. 1-53-100/2009).
267. Lazdijų rajono apylinkės teismo 2012 m. lapkričio 5 d. nuosprendis baudžiamojoje byloje (bylos Nr. 1-40-743/2012).
268. Mažeikių rajono apylinkės teismo 2009 m. rugpjūčio 12 d. nuosprendis baudžiamojoje byloje (bylos Nr. 1-188-785/2009).
269. Radviliškio rajono apylinkės teismo 2010 m. kovo 22 d. teismo baudžiamasis įsakymas baudžiamojoje byloje (byloje Nr. 1-116-632/2010).
270. Šiaulių miesto apylinkės teismo 2011 m. liepos 18 d. teismo baudžiamasis įsakyme baudžiamojoje byloje (bylos Nr. 1-617-885/2011).
271. Šiaulių rajono apylinkės teismo 2010 m. liepos 19 d. teismo baudžiamasis įsakymas baudžiamojoje byloje (bylos Nr. 1-199-776/2010).
272. Šilalės rajono apylinkės teismo 2010 m. lapkričio 4 d. teismo baudžiamasis įsakymas baudžiamojoje byloje (bylos Nr. 1-121-799/2010).
273. Šilutės rajono apylinkės teismo 2006 m. birželio 28 d. nuosprendis baudžiamojoje byloje (bylos N1-249-299/2005).
274. Ukmergės rajono apylinkės teismo 2012 m. gruodžio 17 d. teismo baudžiamasis įsakymas baudžiamojoje byloje (bylos Nr. 1-312-627/2012).

VI. Europos Žmogaus Teisių Teismo praktika

275. *Custers, Deveaux and Turk v. Denmark*, no. 11843/03, 11847/03, 11849/03, ECHR 2007.
276. *Dragotoniu and Militaru-Pidhorni v. Romania*, no. 77193/01, 77196/01, ECHR 2007.
277. *Niemietz v. Germany*, no. 13710/88, ECHR 1992.

VII. Užsienio valstybių teismų praktika

278. *United States v. Mitra*, no. 04–2328, US 7th Cir., 2005. [interaktyvus], [žiūrėta 2012-09-04]. <http://caselaw.findlaw.com/us-7th-circuit/1031818.html>.
279. *United States v. Bradford C. Councilman*, no. 03–1383, United States Court of Appeals, 1st Circuit, 2005 [interaktyvus], [žiūrėta 2013-06-02]. <http://media.ca1.uscourts.gov/cgi-bin/getopn.pl?OPINION=03-1383EB.01A>.
280. *Briggs v. State of Maryland*, no. 24, Court of Appeals of Maryland, 1997. [interaktyvus], [žiūrėta 2013-06-02] <http://law.justia.com/cases/maryland/court-of-appeals/1998/24a97-2.html>.
281. *State of Kansas v. Anthony A. Allen*, no. 74,639, Soupreme Court of Kansas, 1996. [Interaktyvus]. [žiūrėta 2013-06-02]. <http://files.grimmelmann.net/cases/Allen.pdf>.

282. *United States v. Morris*, no. 774, United States Court of Appeals, 2 nd Circuit, 1991 [interaktyvus], [žiūrėta 2012-12-03] <http://www.loundy.com/CASES/US_v_Morris2.html>.

VIII. Kiti šaltiniai

283. ISO/IEC 2382-1:1996 *Informacijos technologijos. Terminai ir apibrėžimai. 1-oji laida. Pagrindiniai terminai.*

284. LST ISO/IEC 27001:2006 *Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai*

Lietuvos Respublikos baudžiamojo kodekso 166, 168, 198, 198[2], 214 ir 215 straipsniuose numatytos alternatyvios veikos

Pavojingos veikos	Baudžiamojo įstatymo straipsnis
Stebėjimas, fiksavimas, perėmimas	**BK 166 straipsnis** „Tas, kas <...> perėmė, fiksavo ar stebėjo asmens elektroninių ryšių tinklais siunčiamus pranešimus, arba neteisėtai fiksavo, klausėsi ar stebėjo asmens pokalbius elektroninių ryšių tinklais <...>“. **BK 198 straipsnis** „Tas, kas <...> stebėjo, fiksavo, perėmė, <...> neviešus elektroninius duomenis“.
Įgijimas, laikymas	**BK 166 straipsnis** „Tas, kas <...> kitaip pažeidė asmens susižinojimo neliečiamumą“. **BK 198 straipsnis** „Tas, kas <...> įgijo, laikė, pasisavino <...> neviešus elektroninius duomenis“. **BK 198[2] straipsnis** „Tas, kas <...> slaptažodžius, prisijungimo kodus ar kitokius panašius duomenis, tiesiogiai skirtus daryti nusikalstamas veikas, <...> tuo pačiu tikslu juos įgijo ar laikė“. **BK 214 straipsnis** „Tas, kas <...> įgijo, laikė, <...> vienos ar daugiau svetimų elektroninių mokėjimo priemonių ar jų naudotojo tapatybės patvirtinimo priemonių duomenis, pakankamus finansinei operacijai inicijuoti <...>“.
Paskleidimas, platinimas	**BK 168 straipsnis** „Tas, kas <...> viešai paskelbė <...> informaciją apie kito žmogaus privatų gyvenimą, jeigu tą informaciją jis sužinojo dėl savo tarnybos ar profesijos arba atlikdamas laikiną užduotį, arba ją surinko darydamas šio kodekso 165–167 straipsniuose numatytą veiką“. **BK 198 straipsnis.** „Tas, kas <...> paskleidė <...> neviešus elektroninius duomenis“. **BK 198[2] straipsnis.** „Tas, kas <...> pardavė ar kitaip platino <...> programinę įrangą, taip pat slaptažodžius, prisijungimo kodus ar kitokius panašius duomenis, tiesiogiai skirtus daryti nusikalstamas veikas <...>“. **BK 214 straipsnis** „Tas, kas <...> perdavė ar realizavo vienos ar daugiau svetimų elektroninių mokėjimo priemonių ar jų naudotojo tapatybės patvirtinimo priemonių duomenis, pakankamus finansinei operacijai inicijuoti <...>“.

Pavojingos veikos	Baudžiamojo įstatymo straipsnis
Panaudojimas	**BK 168 straipsnis** „Tas, kas <...> pasinaudojo ar kitų asmenų labui panaudojo informaciją apie kito žmogaus privatų gyvenimą, jeigu tą informaciją jis sužinojo dėl savo tarnybos ar profesijos arba atlikdamas laikiną užduotį, arba ją surinko darydamas šio kodekso 165–167 straipsniuose numatytą veiką“. **BK 198 straipsnis** „Tas, kas <...> kitaip panaudojo <...> neviešus elektroninius duomenis“. **BK 198^2 straipsnis** Tokios veikos nenumato. **BK 215 straipsnis** „Tas, kas neteisėtai inicijavo ar atliko vieną ar daugiau finansinių operacijų <...> neteisėtai panaudodamas vieną ar daugiau svetimų elektroninių mokėjimo priemonių ar jų naudotojo tapatybės patvirtinimo priemonių duomenis <...>“.

MYKOLO ROMERIO UNIVERSITETAS

Renata Marcinauskaitė

NUSIKALSTAMOS VEIKOS ELEKTRONINIŲ DUOMENŲ IR INFORMACINIŲ SISTEMŲ KONFIDENCIALUMUI (LIETUVOS RESPUBLIKOS BAUDŽIAMOJO KODEKSO 198 IR 198^1 STRAIPSNIAI)

Daktaro disertacijos santrauka
Socialiniai mokslai, teisė (01 S)

Vilnius, 2013

Disertacija rengta 2009–2013 metais Mykolo Romerio universitete, Teisės fakultete.

Moksliniai vadovai:

prof. dr. Olegas Fedosiukas (Mykolo Romerio universitetas, socialiniai mokslai, teisė – 01 S), 2012–2013 metai;

doc. dr. Agnė Baranskaitė (Mykolo Romerio universitetas, socialiniai mokslai, teisė – 01 S), 2009–2012 metai.

Disertacija ginama Mykolo Romerio universiteto Teisės mokslo krypties taryboje:

Pirmininkas:

prof. dr. Rima Ažubalytė (Mykolo Romerio universitetas, socialiniai mokslai, teisė – 01 S).

Nariai:

prof. dr. Edita Gruodytė (Vytauto Didžiojo universitetas, socialiniai mokslai, teisė – 01 S);

prof. dr. Raimundas Jurka (Mykolo Romerio universitetas, socialiniai mokslai, teisė – 01 S);

prof. dr. Jonas Prapiestis (Vilniaus universitetas, socialiniai mokslai, teisė – 01 S);

prof. dr. Darius Štitilis (Mykolo Romerio universitetas, socialiniai mokslai, teisė – 01 S).

Oponentai:

prof. dr. Armanas Abramavičius (Vilniaus universitetas, socialiniai mokslai, teisė – 01 S);

dr. Algimantas Čepas (Lietuvos teisės institutas, socialiniai mokslai, teisė – 01 S).

Disertacija bus ginama viešame Teisės mokslo krypties tarybos posėdyje 2014 m. sausio 10 d. 13.00 val. Mykolo Romerio universiteto I-414 auditorijoje.

Adresas: Ateities g. 20, LT-08303, Vilnius, Lietuva.

Disertacijos santrauka išsiųsta 2013 m. gruodžio 10 d.

Su disertacija galima susipažinti Mykolo Romerio universiteto (Ateities g. 20, Vilnius) ir Lietuvos nacionalinėje Martyno Mažvydo (Gedimino pr. 51, Vilnius) bibliotekose.

Renata Marcinauskaitė

NUSIKALSTAMOS VEIKOS ELEKTRONINIŲ DUOMENŲ IR INFORMACINIŲ SISTEMŲ KONFIDENCIALUMUI (LIETUVOS RESPUBLIKOS BAUDŽIAMOJO KODEKSO 198 IR 198[1] STRAIPSNIAI)

Santrauka

Tiriamoji problema. Kompiuterinių informacinių technologijų ir elektroninių ryšių raida sudarė prielaidas didelės apimties įvairaus pobūdžio informacijos sklaidai, naujoms prieigos prie informacijos, taip pat jos apsikeitimo galimybėms atsirasti nacionaliniu ir tarptautiniu lygiu. Šis vienas iš globalinės transformacijos aspektų atskleidė ne tik elektroninėje terpėje vykstančius teigiamus pokyčius, lemiančius ir skatinančius elektroninės erdvės naudotojų sąsają ir sąveiką, bet taip pat parodė informacinės visuomenės pažeidžiamumo problemą – viena iš elektroninėje erdvėje atsiradusių grėsmių yra joje padaromos nusikalstamos veikos. Į tokių veikų sąrašą patenka ne tik dėl naujųjų technologijų panaudojimo pakitusios tradicinės veikos, bet ir tos, kurios atsirado išimtinai kaip šių technologijų vystymosi rezultatas. Prie pastarųjų priskirtinos Lietuvos Respublikos baudžiamojo kodekso (toliau – BK) XXX skyriuje aprašytos nusikalstamos veikos elektroninių duomenų ir informacinių sistemų saugumui. Šiame darbe tiriama vienos iš jų rūšies – nusikalstamų veikų elektroninių duomenų ir informacinių sistemų konfidencialumui, numatytų BK 198 ir 198[1] straipsniuose, problematika. Ši rūšis išskirta struktūrizavus BK XXX skyriuje esančias nusikalstamas veikas: pasitelkus *CIA triadą* į jas pažvelgta kaip į konfidencialumo, integralumo ir prieinamumo pažeidimus.

Technologijų pažangos ir nusikalstamų veikų padarymo galimybių sintezė rodo kiekybiškai daug ir kokybiškai naujas baudžiamosios teisės problemas saugant visuomenės, kurioje pagrindinis galios ir produktyvumo šaltinis yra susijęs su sparčiu technologijomis pagrįstu informacijos apdorojimu, interesus elektroninėje erdvėje. Naujų pagal savo pobūdį diskusinių klausimų gausa lėmė, kad tiriant pasirinktų nusikalstamų veikų problematiką neapsiribota vien jų sudėties požymių turinio analize – į elektroninių duomenų ir informacinių sistemų konfidencialumo pažeidimus iš baudžiamosios teisės pozicijų pažvelgta plačiau. Darbe ieškota tokio pobūdžio nusikalstamų veikų ištakų, kriminalizavimo pateisinimo, galimo jų ryšio su tradicinėmis veikomis, atskyrimo nuo kitų panašių nusikalstamų veikų kriterijų. Taip pat formuluojant principines šių veikų aiškinimo pozicijas ne kartą kelti technologijų ir joms baudžiamajame įstatyme įvardyti vartojamos terminologijos suderinimo bei principų, suformuluotų ne baudžiamosios teisės srityje, pritaikomumo klausimai.

Darbo aktualumas, naujumas ir tyrimų rezultatų reikšmė. Sąlygos analizuoti nusikalstamas veikas elektroninių duomenų ir informacinių sistemų konfidencialumui nacionaliniu lygiu buvo sudarytos įsigaliojus 2000 metų BK, kai dėl technologijų pokyčių atsiradusios naujos veikos kriminalizuotos *sui generis* ir nebelaikomos kitų veikų sudedamąja dalimi. Tokių nusikalstamų veikų atsiradimas sukėlė fundamentalias teisėkūros bei baudžiamojo įstatymo normų taikymo (atitinkamai jų aiškinimo) problemas, į kurias jau atkreiptas dėmesys priėmus, bet dar neįsigaliojus 2000 metų BK. „Nors užsienio valstybių

mokslininkai jau keletą metų diskutuoja apie <...> teisines problemas, susijusias su elektroninės erdvės panaudojimu, Lietuvoje pastebimos tik pradinių diskusijų apraiškos. Veikų elektroninėje erdvėje teisinio reglamentavimo ir atsakomybės pagrindų už neteisėtas veikas nustatymo (Lietuvos kontekste) klausimais nebuvo gilesnių studijų"[1] teigta tuometinėje mokslinėje literatūroje. Reikėtų pripažinti, kad praėjus bene dešimčiai metų šis teiginys tam tikra prasme išlieka vis dar aktualus – net ir sukūrus teisinius pagrindus baudžiamajai atsakomybei už tokias veikas kilti, gilesnių diskusijų dėl šių pagrindų tinkamumo praktiškai nėra. Be to, po 2000 metų baudžiamojo įstatymo įsigaliojimo praėjęs laiko tarpas 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 pakankamos, suprantamos, ar jomis buvo pasiekti norimi tikslai, koks realus jų taikymo rezultatas. Juo labiau kad teismų praktika šios kategorijos baudžiamosiose bylose yra gana chaotiška, dažni atvejai, kai konfidencialumą pažeidžiančios veikos yra neatpažįstamos, šių veikų sudėties požymiai inkriminuojami intuityviai be tvirtesnio teorinio pagrindimo. Be abejo, tokiai situacijai formuotis sąlygas sudaro *inter alia* ir nepakankama nusikalstamų veikų elektroninių duomenų ir informacinių sistemų konfidencialumui analizė doktrinos lygmeniu, diskusijų trūkumas.

Šio darbo mokslinis naujumas yra tai, kad pirmą kartą Lietuvoje disertacijos lygiu išsamiai išnagrinėtos nusikalstamos veikos elektroninių duomenų ir informacinių sistemų konfidencialumui. Darbe atskleisti Lietuvos baudžiamosios teisės doktrinoje dar nenagrinėti šių veikų sudėties požymių aspektai, pasisakyta dėl technologinių – teisinių problemų įtakos veikų aiškinimui ir inkriminavimui, sistemiškai analizuotos tarptautiniu ir Europos Sąjungos lygiu priimtų teisės aktų, užsienio valstybių bei Lietuvos baudžiamojo įstatymo normos. Vadovaujantis šių nusikalstamų veikų sudėties požymių analize suformuluoti nusikalstamų veikų elektroninių duomenų ir informacinių sistemų konfidencialumui atskyrimo nuo panašių nusikalstamų veikų kriterijai. Atkreiptas dėmesys į technologinio neutralumo ir ekvivalentinio vertinimo principų taikymo galimybes ir problemas baudžiamosios teisės kontekste. Tyrimas neapribotas tik teoriniu lygmeniu – pirmą kartą šių nusikalstamų veikų analizei pasitelkta teismų praktika, ją apibendrinus iškeltos konkrečios kvalifikavimo problemos ir pateikti galimi jų sprendimo variantai. Be to, darbe atrinkta ir reikšminga užsienio valstybių teismų praktika – nagrinėtos bylos padėjo nustatyti Lietuvoje dar nepasitaikiusius probleminius nusikalstamų veikų elektroninių duomenų ir informacinių sistemų konfidencialumui aspektus.

Atsižvelgiant į tai, kad darbe pateikti moksliškai pagrįsti nusikalstamų veikų elektroninių duomenų ir informacinių sistemų konfidencialumui aiškinimo ir inkriminavimo problemų sprendimo variantai, ši medžiaga galės būti naudinga besiformuojančiai elektroninių nusikalstamų veikų doktrinai, taip pat naudojama praktiniu baudžiamojo įstatymo taikymo lygmeniu sprendžiant kylančius tokių nusikalstamų veikų kvalifikavimo klausimus.

Disertacijos tyrimo objektas. Šio disertacinio tyrimo objektas yra viena iš nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui rūšių – nusikalstamos veikos elektroninių duomenų ir informacinių sistemų konfidencialumui, numatytos BK 198 ir 198[1] straipsniuose, ir jų baudžiamojo teisinio vertinimo problemos.

[1] Štitilis, D. Teisinės atsakomybės pagrindų nustatymo už neteisėtas veikas elektroninėje erdvėje problemos: daktaro disertacija: socialiniai mokslai, teisė (01 S). – Vilnius: LTU, 2002, p. 7.

Darbo tikslas ir uždaviniai. *Disertacinio darbo tikslas* – nustatyti nusikalstamų veikų, kuriomis pažeidžiamas elektroninių duomenų ir informacinių sistemų konfidencialumas, aiškinimui svarbias principines nuostatas, kuo išsamiau paaiškinti šių veikų sudėties požymius, identifikuoti jų baudžiamojo teisinio vertinimo problemas, taip pat nustačius esamo teisinio reguliavimo trūkumus, pateikti galimas jo tobulinimo ar šių veikų požymių aiškinimo kryptis.

Disertacinio darbo uždaviniai:

1. Analizuojant ekvivalentinio vertinimo ir technologinio neutralumo principus baudžiamosios teisės kontekste, atskleisti esminius nusikalstamų veikų, padaromų elektroninėje erdvėje, kriminalizavimo ir šių veikų požymių aiškinimo probleminius aspektus.

2. Baudžiamojo įstatymo saugomos vertybės pagrindu struktūrizavus BK XXX skyriuje esančias nusikalstamas veikas, identifikuoti tas, kurios pažeidžia elektroninių duomenų ir informacinių sistemų konfidencialumą, atskleisti, kaip ši vertybė interpretuotina elektroninių duomenų ir informacinių sistemų saugumo kontekste.

3. Kuo išsamiau atskleisti neteisėto prisijungimo prie informacinės sistemos nusikalstamos veikos (BK 198[1] straipsnis) sudėties požymius, nustatyti esamo teisinio reguliavimo ar sudėties požymių aiškinimo trūkumus, pateikti galimas teisinio reguliavimo tobulinimo ar šios veikos požymių aiškinimo kryptis.

4. Kuo išsamiau atskleisti neteisėto elektroninių duomenų perėmimo ir panaudojimo nusikalstamos veikos (BK 198 straipsnis) sudėties požymius, nustatyti esamo teisinio reguliavimo ar sudėties požymių aiškinimo trūkumus, pateikti galimas teisinio reguliavimo tobulinimo ar šios veikos požymių aiškinimo kryptis.

5. Išanalizuoti nusikalstamų veikų elektroninių duomenų ir informacinių sistemų konfidencialumui santykį su panašiomis nusikalstamomis veikomis, suformuluoti šių nusikalstamų veikų atskyrimo kriterijus.

Ginamieji disertacijos teiginiai:

1. Nusikalstamų veikų elektroninėje erdvėje kriminalizavimui ir sudėties požymių aiškinimui yra aktualūs ekvivalentinio vertinimo ir technologinio neutralumo principai.

2. Elektroninių duomenų ir informacinių sistemų saugumo interpretavimui pasitelkus *CIA triados* saugumo modelį, BK XXX skyriuje esančios veikos struktūrizuojamos į elektroninių duomenų ir informacinių sistemų konfidencialumo, integralumo bei prieinamumo pažeidimus.

3. Pasirinkta neteisėto prisijungimo prie informacinės sistemos nusikalstamos veikos koncepcija BK kelia šios veikos požymių aiškinimo, taigi ir šios veikos inkriminavimo problemų.

4. Neteisėto elektroninių duomenų perėmimo ir panaudojimo nusikalstamos veikos aprašymas BK kelia šios veikos sudėties požymių aiškinimo, jų tarpusavio santykio nustatymo, taigi ir šios veikos inkriminavimo sunkumų.

5. Nusikalstamų veikų elektroninių duomenų ir informacinių sistemų konfidencialumui atskyrimas nuo kitų veikų elektroninių duomenų ir informacinių sistemų saugumui, nusikalstamų veikų finansų sistemai ir nusikalstamų veikų privataus gyvenimo neliečiamumui yra probleminis.

Tyrimų apžvalga. Lietuvoje nusikalstamos veikos elektroninių duomenų ir informacinių sistemų konfidencialumui nebuvo plačiai nagrinėtos, praktiškai neanalizuoti ir šių nusikalstamų veikų sudėties požymiai. Bendrai veikų elektroninėje erdvėje tematika tiek galiojant 1961 m., tiek 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 skirta bendriems tokių veikų aiškinimo klausimams. Atskirais aspektais jas nagrinėjo ir R. Petrauskas, tiesa, dar galiojant 1961 m. baudžiamajam įstatymui. Jau įsigaliojus 2000 m. BK, pavieniai veikų elektroninėje erdvėje aiškinimo atvejai paprastai sutinkami mokomuosiuose leidiniuose, pavyzdžiui, 2006 metų vadovėlyje „Teisės informatika ir informatikos teisė" ir 2004 metų leidinyje „Informacinių technologijų teisė". Dėl baudžiamojo įstatymo ir tarptautinių teisės aktų suderinamumo elektroninių nusikalstamų veikų reglamentavimo srityje yra pasisakęs D. Sauliūnas. Kai kurie šių veikų aspektai jų tyrimo metodikos kontekste aptariami ir N. Goranin bei D. Mažeikos. Paminėtinas ir baudžiamojo įstatymo komentaras, kuriame matyti glaustas teorinis elektroninių duomenų ir informacinių sistemų konfidencialumą pažeidžiančių veikų aiškinimas. Pastaruoju metu mokslinėje literatūroje daugiau dėmesio pradėta skirti tapatybės vagystės (angl. *identity theft*) elektroninėje erdvėje kriminalizavimo klausimams, kuriais domisi D. Štitilis, P. Pakutinskas, M. Laurinaitis ir I. Dauparaitė.

Kiek kitokia situacija yra užsienio valstybių baudžiamosios teisės moksle, kuriame įvairiems nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui bei apskritai nusikalstamų veikų elektroninėje erdvėje aspektams teikiamas didesnis dėmesys. Bendro pobūdžio elektroninių veikų kriminalizavimo ir aiškinimo, elgesio elektroninėje erdvėje vertinimo problemas savo darbuose nagrinėjo J. Clough, I. Walden, C. Reed, U. Kohl, S. W. Brenner, M. Schellekens, R. Ali, I. M. van der Haar, J.–B. Koops, R. W. Downing, P. Ohm, C. A. Kirby ir kt. Neteisėtos prieigos prie informacinės sistemos ar elektroninių duomenų kriminalizavimo, inkriminavimo *iner alia* ir tokių nusikalstamų veikų požymių aiškinimo klausimais yra pasisakę O. S. Kerr, M. W. S. Wong, M. J. Madison, I. Walden, D. Bainbridge, J. Angel, G. Thornton, J. Clough, B. A. Howell, A. S. Blunn, D. Rowland, E. Macdonald. Taip pat paminėtini ir Rusijos baudžiamosios teisės mokslininkai N. I. Vetrov, V. A. Mazurov, A. V. Naumov, A. G. Volevodz, V. E. Kozlov, O. Ja. Baev ir V. A. Meshherkov, S. A. Pashin ir kt.

Darbo metodologija. Plačiausiai disertaciniame tyrime, aiškinant nusikalstamas veikas elektroninių duomenų ir informacinių sistemų konfidencialumui, naudoti metodai – *analizė* ir *sintezė*. *Analizės metodas* taikytas šių veikų struktūrą skaidant dalimis ir aiškinant atskirus objektyviuosius bei subjektyviuosius požymius. Be to, šis metodas leido atskleisti ir atskirų požymių, tiesiogiai susijusių su informacinėmis ir komunikacijos technologijomis, turinį – atskyrus teisinę ir technologinę požymių pusę spręstas jų suderinimo klausimas. Siekiant visapusio veikų pažinimo, neapsieita ir be *sintezės metodo*, kuris naudotas analizės metu dėl atskirų požymių gautas įžvalgas jungiant į vieną visumą. Būtent ši visuma sudarė sąlygas nustatyti, kokia šių veikų koncepcija vadovautasi jas apibrėžiant baudžiamajame įstatyme, kokios yra šių nusikalstamų veikų ribos.

Disertaciniame tyrime taip pat dažnai naudotas ir *sisteminės analizės metodas*, kurio parinkimą lėmė pačių nusikalstamų veikų elektroninių duomenų ir informacinių sistemų

konfidencialumui specifika: įvairūs šių veikų aspektai sutinkami tarptautiniu ir Europos Sąjungos lygiu priimtuose teisės aktuose, aiškinant šias veikas būtina sieti skirtingose mokslo šakose suformuluotas teorijas. Šis metodas leido nustatyti nagrinėjamų nusikalstamų veikų vietą elektroninių nusikalstamų veikų ir nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui visete. Taikant jį spręstos kompleksinės technologinį aspektą turinčios problemos, tiesiogiai susijusios su disertaciniame tyrime keltu technologijų ir terminologijos klausimu. Sisteminės analizės metodas sudarė galimybes analizuoti veikų sudėties požymių tarpusavio ryšį, atskleisti šių veikų santykį su panašiomis baudžiamajame įstatyme numatytomis veikomis, ieškoti jų atskyrimo kriterijų.

Nagrinėjamų problemų kompleksiškumas lėmė, kad disertaciniame tyrime buvo būtina susieti baudžiamosios teisės ir informacinių bei komunikacijos technologijų sritis. Siekiant atskleisti technologinį – teisinį nusikalstamų veikų aspektą, taikytas *apibendrinimo metodas.* Išskyrus bendriausius, esminius technologijų srityje analizuojamų objektų požymius, jie derinti su sudėties požymių baudžiamaisiais teisiniais aspektais. Taip tyrime buvo sprendžiama technologijų ir joms įvardyti naudojamos terminologijos pritaikomumo baudžiamosios teisės srityje problema, pateiktas 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 Europos Sąjungos teisės aktais, skirtais kovai su veikomis elektroninėje erdvėje. Jų įtaka matyti ne tik Lietuvos, bet ir užsienio valstybių baudžiamojo įstatymo nuostatoms. Pasirinktas skirtingas minėtų teisės aktų reikalavimų įgyvendinimo būdas sudaro sąlygas formuotis ir skirtingoms tokio pobūdžio veikų koncepcijoms. Šių skirtumų identifikavimui ir analizei pasitelktas *lyginamasis metodas* leido sugretinti skirtingas veikų koncepcijas, įvairių mokslininkų nuomones, nustatyti veikų inkriminavimo problemas, suformuluoti galimus jų sprendimo variantus ir pan.

Atskleidžiant nusikalstamų veikų elektroninių duomenų ir informacinių sistemų konfidencialumui požymių turinį naudotas ir *lingvistinis metodas.* Atliekant disertacinį tyrimą buvo nustatytas įvairių sąvokų interpretavimo trūkumas, todėl šis metodas tapo aktualus bandant suformuluoti galimas jų aiškinimo kryptis. Tačiau taikant lingvistinį metodą pastebėta, kad baudžiamosios teisės srityje vartojamoms sąvokoms yra būdingas specifinis nuo kasdieninės kalbos besiskiriantis turinys, kuris dar daugiau savitumo įgyja informacinių ir komunikacijos technologijų kontekste.

Disertaciniame tyrime pasitelktas taip pat empirinis *dokumentų analizės metodas.* Jis taikytas apibendrinant besiklostančią teismų praktiką nusikalstamų veikų elektroninių duomenų ir informacinių sistemų konfidencialumui bylose, naudojant teismų sprendimus išryškinant kylančias veikų inkriminavimo problemas, pagrindžiant galimus jų sprendimo variantus. Tyrime analizuoti ir užsienio valstybių teismų reikšmingiausi sprendimai, leidę kelti naujas, Lietuvoje kol kas dar nežinomas problemas, pateikiant jų sprendimo siūlymus.

Disertacijos struktūra. Disertaciją sudaro įvadas, dėstomoji dalis, išvados, naudotų šaltinių ir literatūros sąrašas bei priedas. Dėstomąją dalį sudaro penki skyriai, apimantys įvairius nusikalstamų veikų elektroninių duomenų ir informacinių sistemų konfidencialumui tyrimo aspektus.

Pirmajame disertacijos skyriuje „**Esminiai nusikalstamų veikų, padaromų elektroninėje erdvėje, baudžiamieji teisiniai aspektai**“ analizuojami elektroninėje erdvėje padaromų nusikalstamų veikų kriminalizavimui ir šių veikų sudėties požymių aiškinimui svarbūs technologinio neutralumo ir ekvivalentinio vertinimo principai. Baudžiamosios teisės kontekste aptariant įvairius minėtų principų aspektus atkreiptas dėmesys į tai, kad šių principų ištakos nėra tiesiogiai siejamos su baudžiamosios teisės šaka. Tačiau kaip vieną iš pavojingų veikų reguliavimo elektroninėje erdvėje priemonių pasirinkus baudžiamąjį teisinį reguliavimą, jie tampa aktualūs ir šioje srityje. Šiame skyriuje prieita prie išvados, kad technologinio neutralumo principas leidžia išvengti baudžiamosios teisės normų taikymo apribojimų, galinčių kilti dėl jose naudojamų su technologijomis susijusių požymių. Tačiau kartu pabrėžta, kad toks požymių aiškinimas turi būti suderintas su baudžiamojoje teisėje svarbiais legalumo ir teisinio tikrumo principais. Kito – ekvivalentinio vertinimo principo – analizė leido nustatyti, kad nusikalstamos veikos elektroninių duomenų ir informacinių sistemų konfidencialumui Lietuvos BK yra kriminalizuotos įgyvendinant funkcinio ekvivalentiškumo reikalavimus.

Antrajame disertacijos skyriuje „**Elektroninių duomenų ir informacinių sistemų konfidencialumas kaip baudžiamojo įstatymo saugoma vertybė**“ aptarti rūšinės baudžiamojo įstatymo saugomos vertybės, nurodytos BK XXX skyriaus pavadinime, pokyčiai, taip pat pritarta dabartiniam teisinio gėrio pavadinimui – elektroninių duomenų ir informacinių sistemų saugumas. Šios vertybės turiniui atskleisti disertacijoje siūloma pasitelkti klasikinę *CIA triadą* ir apie elektroninių duomenų ir informacinių sistemų saugumą kalbėti kaip apie jų konfidencialumo, integralumo ir prieinamumo užtikrinimą. Toks vertybės turinys sudarė galimybes iš BK XXX skyriuje aprašytų nusikalstamų veikų išskirti tas, kuriomis yra pažeidžiamas elektroninių duomenų ir informacinių sistemų konfidencialumas – tai neteisėtas elektroninių duomenų perėmimas ir panaudojimas (BK 198 straipsnis) bei neteisėtas prisijungimas prie informacinės sistemos (BK 198[1] straipsnis). Šiame disertacijos skyriuje taip pat atskirai aptarti įvairūs konfidencialumo aspektai šį teisinį gėrį analizuojant informacinių sistemų ir elektroninių duomenų kontekste.

Trečiajame disertacijos skyriuje „**Neteisėtas prisijungimas prie informacinės sistemos (BK 198[1] straipsnis)**“ analizuojama informacinės sistemos konfidencialumą pažeidžianti nusikalstama veika. Disertacijoje atkreipiamas dėmesys į tai, kad ši veika BK yra kriminalizuota *per se* be tiesioginio ryšio su tolimesniais kaltininko veiksmais jau pačioje sistemoje. Tačiau baudžiamajai atsakomybei pagal BK 198[1] straipsnį kilti yra būtina nustatyti ne tik neteisėto prisijungimo prie informacinės sistemos faktą, bet taip pat ir informacinės sistemos apsaugos priemonių pažeidimą. Šiame skyriuje, atskleidžiant nusikalstamos veikos sudėties požymius, analizuotos skirtingos elektroninės erdvės vertinimo pozicijos – *išorinė* ir *vidinė perspektyvos*. Būtent *vidinė perspektyva*, sudariusi galimybes į elektroninę erdvę pažvelgti kaip virtualią realybę, leido pastebėti tradicinės neteisėto įsibrovimo į svetimą valdą doktrinos vystymąsi. Ši doktrina laikyta logišku atspirties tašku aiškinant neteisėto prisijungimo prie IS veiką ir vadinta elektroniniu įsibrovimu į svetimą elektroninę erdvę.

Ketvirtajame disertacijos skyriuje „**Neteisėtas elektroninių duomenų perėmimas ir panaudojimas (BK 198 straipsnis)**“ aptarta neviešų elektroninių duomenų konfidencialumą pažeidžianti nusikalstama veika. Jos sudėties požymių analizė parodė, kad BK 198 straipsnyje yra kriminalizuotas tiek informacinėje sistemoje perduodamų duomenų perėmimas, tiek ir tokioje sistemoje laikomų (saugomų), t. y. „*nejudamų*“ elektroninių

duomenų neteisėtas įgijimas. Disertacijoje pastebėta, kad pasirinktas toks neviešų elektroninių duomenų konfidencialumo pažeidimo kriminalizavimo būdas kelia šios nusikalstamos veikos *perkriminalizavimo*, jos sudėties požymių tarpusavio suderinamumo ir panašių nusikalstamų veikų atskyrimo problemų.

Penktajame disertacijos skyriuje „**Nusikalstamų veikų elektroninių duomenų ir informacinių sistemų konfidencialumui atskyrimas nuo panašių nusikalstamų veikų**“ analizuojamos nusikalstamų veikų elektroninių duomenų ir informacinių sistemų konfidencialumui atskyrimo nuo nusikalstamų veikų finansų sistemai (BK 214, 215 straipsniai), nusikaltimų privataus gyvenimo neliečiamumui (BK XXIV skyrius) ir kitų nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui problemos. Šiame skyriuje pateikti galimi tokių nusikalstamų veikų atribojimo kriterijai ir kylančių atribojimo problemų sprendimo variantai.

IŠVADOS

1. Ekvivalentinio vertinimo principas bendriausia prasme atspindi idėją, kad baudžiamojo įstatymo normos turi užtikrinti vienodą vertybių apsaugos lygį fizinėje ir elektroninėje erdvėse. Praktiškai įgyvendinant lygiavertį veikų vertinimą Lietuvos baudžiamajame įstatyme, tradicinėms veikoms, padarytoms elektroninėje erdvėje, kvalifikuoti taikomas tas pats BK straipsnis, pagal kurį kvalifikuojamos analogiškos veikos fizinėje erdvėje. Įgyvendinant funkcinį ekvivalentiškumą *CIA nusikalstamoms veikoms* kvalifikuoti baudžiamajame įstatyme įtvirtintos savarankiškos normos (BK 196–198[2] straipsniai).

2. Technologinio neutralumo principas yra aktualus siekiant išvengti baudžiamojo įstatymo normų taikymo apribojimų, galinčių kilti dėl jose naudojamų su technologijomis susijusių požymių. Tačiau šį principą pasitelkiant baudžiamojoje teisėje, jo apimtis neišvengiamai siaurina baudžiamosios teisės principai, leidžiantys išvengti pernelyg plataus ir nepagrįsto veikų kriminalizavimo, atitinkamai ir nepagrįsto baudžiamosios atsakomybės ribų išplėtimo.

3. Elektroninių duomenų ir informacinių sistemų saugumo turiniui atskleisti taikytina ne abstrakti saugumo samprata, o klasikinis *CIA triados* saugumo modelis, leidžiantis nustatyti trijų elektroninių duomenų ir informacinių sistemų savybių – konfidencialumo, integralumo ir prieinamumo – išsaugojimo poreikį. Šio modelio pagrindu BK XXX skyriuje esančios veikos gali būti grupuojamos į konfidencialumo, integralumo ar prieinamumo pažeidimus.

Tiek neviešų elektroninių duomenų, tiek informacinių sistemų konfidencialumas rodo prieigos prie jų apribojimus, t. y. duomenys ar sistemos, atliekančios duomenų apdorojimo funkcijas, yra prieinamos tik vartotojams, turintiems prieigos prie jų teisę, ir tik ta apimtimi, kuria jiems ši teisė buvo suteikta.

4. Neteisėto prisijungimo prie informacinės sistemos nusikalstama veika yra kriminalizuota *per se* be tiesioginės sąsajos su kitomis elektroninių duomenų ir informacinių sistemų saugumą pažeidžiančiomis veikomis. Kadangi paprastai galimybes atlikti bet kokias veikas pačioje sistemoje sudaro pirminiai kaltininko neteisėto prisijungimo veiksmai, tai neturėtų stebinti dažni BK 198[1] straipsnyje numatytos veikos inkriminavimo atvejai.

5. Siekiant išvengti akivaizdžiai nepavojingų veikų kriminalizavimo, neteisėto prisijungimo prie IS apibrėžtis susiaurinta į šios veikos sudėtį įtraukus veikos padarymo būdą – IS apsaugos priemonių pažeidimą. Šioms priemonėms aiškinti taikytina technologinė IS

apsaugos priemonių koncepcija. Platesnis šių priemonių interpretavimas galimas tik tuo atveju, jei prieš tai įvertinama neteisėto prisijungimo prie IS *perkriminalizavimo* grėsmė.

IS apsaugos priemonių pažeidimas interpretuotinas ne tik kaip žalos apsaugos priemonėms padarymas, bet ir kaip tokių priemonių nustatytų apribojimų (reikalavimų) pažeidimas, kai žala pačioms apsaugos priemonėms gali būti ir nesukeliama.

6. Neteisėtą prisijungimą prie IS kriminalizavus *per se* sudarytos ribotos galimybės prieigos neteisėtumu pripažinti ir teisėtumo ribas peržengiančią prieigą. Siauresnis aiškinimas leidžia išvengti baudžiamajai atsakomybei kilti būtino pavojingumo lygio nesiekiančių veiksmų kriminalizavimo.

Prisijungimo prie IS neteisėtumas konstatuotinas nustačius tiek autentifikavimo procedūros pažeidimo, tiek ir IS apsaugos silpnų vietų išnaudojimo faktą.

7. Prisijungimo aiškinimui taikytinas *vidinės perspektyvos* požiūris, kuris elektroninę erdvę apibūdina kaip virtualią realybę. Todėl, nepriklausomai nuo to, ar prisijungimas yra suvokiamas kaip komanda, kuria pradedamas darbo seansas su IS, ar jis suprantamas kaip galimybė prieiti prie IS išteklių, prisijungimas būtų metaforiškai prilyginamas *virtualiam įėjimui* į sistemą. Toks aiškinimas reikštų, kad prisijungimo veiksmui konstatuoti nepakanka tik sąveikos su IS.

Nors galimybės prieiti prie IS išteklių kriterijus padeda aiškiau suvokti prisijungimo veiką, tačiau jos baigtumo momentui neturi būti svarbi kaltininko reali galimybė atlikti tolesnius veiksmus IS.

8. BK 198[1] straipsnyje numatytas nusikalstamos veikos dalykas – IS – baudžiamosios teisės kontekste turėtų būti suvokiamas be jos funkcionavimo konteksto ir bendriausia prasme laikomas IT (apimančių ir komunikavimo technologijas) arba kompiuterinės sistemos sinonimu.

Strateginę reikšmę nacionaliniam saugumui arba didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinti IS yra neteisėto prisijungimo prie IS veiką kvalifikuojanti aplinkybė. Ypatingai IS svarbai BK 198[1] straipsnio 2 dalyje nurodytoms sritims konstatuoti taikytini *nukentėjusiųjų*, *ekonominio poveikio* ir *poveikio visuomenei* kriterijai.

9. Pagrindžiant tyčinę kaltę svarbus *vidinės perspektyvos* požiūris į elektroninę erdvę, kuris sudaro galimybes į ribų ir jų peržengimo neteisėtumo suvokimą pažvelgti iš elektroninės erdvės vartotojo pozicijos. Todėl šioje erdvėje nustatytų apribojimų suvokimui vertinti taikytinas tokių apribojimų ir jų pažeidimo *numatomumo kriterijus* – jis leidžia atsižvelgti į asmens patyrimą elektroninėje erdvėje kaip *vietoje*.

10. Neteisėtas elektroninių duomenų perėmimas ir panaudojimas BK 198 straipsnyje kriminalizuotas plačiai – į vieną nusikalstamą veiką sujungti tiek *duomenų, perduodamų IS* (angl. *data in transmission*), tiek ir *duomenų, laikomų joje* (angl. *data „in rest"*), konfidencialumo pažeidimai. Ši veika taip pat nėra susieta su papildomais požymiais (pavyzdžiui, techninių priemonių panaudojimu, kaltininko nusikalstamais ketinimais), galinčiais padėti išvengti jos „perkriminalizavimo" problemų.

11. Apibūdinant neteisėto elektroninių duomenų perėmimo ir panaudojimo nusikalstamos veikos dalyką, būtina išskiti du – *teisinį* ir *technologinį* – jo aspektus. Teisinis aspektas siejamas su elektroninių duomenų neviešumu, o technologinis – su tokių duomenų elektronine forma.

Elektroninių duomenų neviešumas rodo, kad jie priklauso duomenų, kuriems taikomas tam tikras apsaugos lygis – atitinkami konfidencialumo apsaugos reikalavimai, rūšiai.

Neviešumo pagrindai gali būti kildinami tiek iš įstatymų ar kitų teisės aktų (objektyvūs), tiek ir asmenų susitarimų, privačių tikslų ir pan. (subjektyvūs).

Duomenų elektroninei formai konstatuoti taikytini jų *tinkamumo apdoroti IS* arba tokių *duomenų buvimo IS (tam tikroje jos dalyje ar išorinėje laikmenoje)* 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 pasitelktini *nukentėjusiųjų*, *ekonominio poveikio* ir *poveikio visuomenei* kriterijai. Ypatingą elektroninių duomenų svarbą *inter alia* gali rodyti ne tik duomenų turinys, bet ir itin didelis jų kiekis. Tokiais atvejais pavieniai duomenys, kurie dėl savo turinio nėra laikomi ypatingos svarbos, šią savybę gali įgyti dėl neteisėto disponavimo tokiais duomenimis kiekio.

12. BK 198 straipsnyje nusikalstamos veikos dalykas – nevieši elektroniniai duomenys nėra konkretizuoti iki *IS laikomų* ir *IS perduodamų duomenų*, todėl minėto straipsnio dispozicija nesuteikia galimybių alternatyvias veikas susieti tik su viena iš šių duomenų rūšių.

12.1. Stebėjimo, fiksavimo ir perėmimo veikų atskyrimo problemos kyla šias alternatyvas analizuojant *IS perduodamų duomenų* kontekste. Stebėjimas paprastai neatsiejamas nuo prieš tai atlikto ar stebėjimo metu vykdomo perduodamų duomenų fiksavimo; pats neteisėtas programinės įrangos veikimas tinkle fiksuojant duomenis gali būti prilyginamas tinklo srauto stebėjimui; fiksavimas bendriausia prasme gali būti laikomas tuo pačiu elektroninių duomenų perėmimu. Bandant atrasti šių alternatyvų skirtumus siūlytina skirti neteisėtą srauto ir turinio duomenų gavimą – fiksavimo veiką susieti su srauto duomenų, o perėmimo su turinio duomenų neteisėtu gavimu.

Atsižvelgiant į tokio pobūdžio veikų padarymo mechanizmą, kaltininkui dažnai teks inkriminuoti ne tik perėmimo, bet ir fiksavimo bei stebėjimo veikas.

12.2. Fiksavimo ir įgijimo santykio problemos kyla šias veikas susiejus su *IS laikomais duomenimis*, nes joms suteiktas bene analogiškas turinys. BK 198 straipsnyje tokias veikas atskyrus, tenka ieškoti galimų šių alternatyvų atribojimo kriterijų. Diskutuotina, ar jais negali būti laikomi skirtingas fiksavimo ir įgijimo veikų baigtumo momentas arba galimybė veikos metu keisti elektroninių duomenų formą iš elektroninės į materialią.

12.3. Elektroninių duomenų perėmimas ir įgijimas yra pagal savo prasmę artimos veikos, tačiau jas abi įtvirtinus BK 198 straipsnyje neišvengiamai tenka atskirti *IS laikomus* ir *IS perduodamus* duomenis. Perėmimo veika išimtinai sietina su neteisėtu *IS perduodamų* duomenų gavimu. Vengiant dubliavimo, apie įgijimą galėtų būti kalbama tik tais atvejais, kai neteisėtai gaunami *IS laikomi* elektroniniai duomenys.

12.4. Stebėjimo veiką numačius kaip savarankišką alternatyvą, vien šio veiksmo su *IS laikomais duomenimis* pakanka baudžiamajai atsakomybei pagal BK 198 straipsnį kilti. Tokiais atvejais siekiant užtikrinti pakankamą veikos pavojingumą svarbu nustatyti ne tik patį stebėjimo faktą, bet ir kitas aplinkybes, liudijančias žalos baudžiamojo įstatymo saugomiems teisiniams gėriams kilimą. Siūlytina atsižvelgti į kaltininko ketinimus gavus duomenis padaryti kitas nusikalstamas veikas, duomenų apsaugos priemonių pažeidimus, įvairių techninių priemonių, skirtų duomenims gauti, panaudojimu, kaltininko neteisėtus veiksmus prisijungiant prie IS ir taip gaunant prieigą prie duomenų, stebėjimo veiksmų pastovumą, stebėtų duomenų kiekį, jų reikšmę, žalos sukėlimą ir pan.

12.5. Elektroninių duomenų laikymu pripažįstamas šių duomenų buvimas kaltininko žinioje – jo kontroliuojamose materialiose priemonėse, kuriose yra elektroniniai duome-

nys, arba jam prieinamoje vietoje elektroninėje erdvėje (pavyzdžiui, elektroninio pašto serveryje).

Konstatuojant laikymą būtina nustatyti kaltininko galimybę prieiti prie elektroninių duomenų, daryti jiems poveikį.

12.6. Elektroninių duomenų pasisavinimo aiškinimui aktualūs kai kurie tradicinio turto pasisavinimo aspektai. Tačiau, atsižvelgiant į turto pasisavinimo specifiką ir pernelyg didelę jo sąsają su turtinių nusikalstamų veikų doktrina, aiškinant elektroninių duomenų pasisavinimą siūlytina atsisakyti elektroninės erdvės kontekste sunkiai pritaikomų kriterijų ir apie elektroninių duomenų pasisavinimą kalbėti kaip apie neteisėtą kaltininko tapimą faktiniu elektroninių duomenų turėtoju. Tai yra, kai kaltininkui konkrečiomis sąlygomis buvo suteikta prieigos prie duomenų teisė, tačiau jis peržengė jos teisėtumo ribas ir elektroniniais duomenimis disponavo pažeisdamas nustatytus apribojimus.

12.7. Elektroninių duomenų neteisėto paskleidimo veika sietina ne tik su aktyviais veiksmais perduodant duomenis tretiesiems asmenims, bet ir su sąlygų prieiti prie duomenų sudarymu. Tokiu atveju paskleidimui konstatuoti tai, kieno iniciatyva – siuntėjo ar gavėjo – duomenų perdavimo procesas buvo inicijuotas, neturės reikšmės.

12.8. Kitokio elektroninių duomenų panaudojimo požymis rodo nebaigtinį neteisėto disponavimo elektroniniais duomenimis veikų sąrašą. Šios veikos formuluotė leidžia teigti, kad tokia veika dažnai yra kitų nusiklastamų veikų padarymo būdas – vienas dažnesnių atvejų yra neviešų elektroninių duomenų neteisėtas panaudojimas prisijungiant prie IS.

13. Disponavimo neviešais elektroniais duomenimis neteisėtumas reiškia, kad asmuo gaudamas prieigą arba atlikdamas kitas veikas su neviešais elektroniniais duomenimis neturi teisėto leidimo tokiems veiksmams arba nors toks leidimas yra suteiktas, tačiau veiksmus jis padaro pažeisdamas nustatytą neviešų elektroninių duomenų disponavimo tvarką (įpareigojimus).

14. Konstatuojant tyčinę kaltę *inter alia* elektroninių duomenų konfidencialumo pažeidimo suvokimą, apribojimai elektroninėje erdvėje vertinti iš *vidinės perspektyvos pozicijos*, sudarančios galimybę atsižvelgti į elektroninės erdvės vartotojo patirtį šioje erdvėje. Apribojimų vertinimui taikytinas jų *numatomumo kriterijus*, leidžiantis pagrįsti, kad asmuo suvokė nustatytas ribas, jų nesilaikydamas pažeidė elektroninių duomenų konfidencialumą.

15. Nustačius, kad neteisėtai prisijungiant prie IS panaudoti nevieši elektroniniai duomenys arba padarytas neteisėtas poveikis elektroniniams duomenims, spręstina, ar, be BK 198^1 straipsnyje aprašytos veikos, inkriminuotinos ir BK 196 ar 198 straipsnyje numatytos veikos. BK 198^1 straipsnyje esančią normą laikant *norma visuma*, o BK 196 ir 198 straipsnių normas – jos dalimi, neteisėtas prisijungimas prie IS, priklausomai nuo apsaugos priemonių pažeidimo būdo, kvalifikuotinas pagal nusikalstamų veikų sutaptį, t. y. BK 198^1 ir 196 ar 198 straipsnius. Šiuo metu už minėtų veikų padarymą nustatytos sankcijos lemia, kad IS konfidencialumą pažeidžianti norma niekada neapims *normos dalies* – neteisėto poveikio elektroniniams duomenims (BK 196 straipsnis) ar neteisėto elektroninių duomenų perėmimo ar panaudojimo (BK 198 straipsnis).

16. Baudžiamoji atsakomybė už įvairaus pobūdžio neteisėto disponavimo elektroniniais duomenimis veiksmus numatyta ne tik BK 198 straipsnyje, bet tam tikra dalimi ir BK 198^2 bei 214, 215 straipsniuose. Nustačius, kad kaltininkas įgijo visus BK 214 straipsnyje nurodytus požymius turinčius duomenis, jo veikai kvalifikuoti taikytinos ne BK 198 ar 198^2 straipsniuose numatytos normos, o specialioji, esanti BK 214 straipsnyje.

Pavojinga veika, pasireiškusi neteisėtu finansinės operacijos inicijavimu panaudojant elektroninės mokėjimo priemonės naudotojo tapatybės patvirtinimo priemonių duomenis, kvalifikuojama taikant ne BK 198, o 215 straipsnį.

17. BK XXIV skyriuje kriminalizuotos įvairios asmens privatumo pažeidimo apraiškos *inter alia* ir elektroninėje erdvėje, o tai kelia BK 198 straipsnyje ir šiame skyriuje aprašytų nusikalstamų veikų atskyrimo problemų. Nustačius, kad padaryti neteisėti įsikišimo į privatumo sritį veiksmai, jie kvalifikuotini pagal BK 166, 167 ar 168 straipsnius. Šiuose straipsniuose esančios normos yra specialios normai, esančiai BK 198 straipsnyje.

PASIŪLYMAI

Atsižvelgiant į disertacijoje iškeltas problemas ir pateiktus galimus jų sprendimo variantus siūlytini tokie BK 198 ir 198[1] straipsnių pakeitimai:

1. Pakeisti BK 198 straipsnį ir jį išdėstyti taip:

198 straipsnis. ~~Neteisėtas elektroninių duomenų perėmimas ir panaudojimas~~ Neteisėtas disponavimas neviešais elektroniniais duomenimis

1. Tas, kas neteisėtai stebėjo, fiksavo, perėmė~~,~~ **elektroninių ryšių tinklais siunčiamus neviešus elektroninius duomenis arba neteisėtai** įgijo, laikė, pasisavino, paskleidė ar kitaip panaudojo neviešus elektroninius duomenis arba **materialų objektą, kurio turinys yra** ~~neviešus elektroninius duomenis~~ **tokie duomenys**,

baudžiamas bauda **arba laisvės apribojimu, arba areštu, arba** laisvės atėmimu iki ~~ketverių metų~~ **dvejų metų**.

2. Tas, kas **padarė šio straipsnio 1 dalyje numatytus veiksmus neteisėtai prisijungęs prie informacinės sistemos arba neteisėtai** stebėjo, fiksavo, perėmė~~,~~ **ryšių tinklais siunčiamus strateginę reikšmę nacionaliniam saugumui arba didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinčius neviešus elektroninius duomenis arba neteisėtai** įgijo, laikė, pasisavino, paskleidė ar kitaip panaudojo ~~strateginę reikšmę nacionaliniam saugumui arba didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinčius neviešus elektroninius duomenis,~~ **tokius elektroninius duomenis arba materialų objektą, kurio turinys yra tokie duomenys,**

baudžiamas **bauda arba** laisvės atėmimu iki ~~šešerių metų~~ **ketverių metų**.

3. Už šiame straipsnyje numatytas veikas atsako ir juridinis asmuo.

2. Pakeisti BK 198[1] straipsnį ir jį išdėstyti taip:

198[1] straipsnis. Neteisėtas prisijungimas prie informacinės sistemos

1. Tas, kas neteisėtai prisijungė prie informacinės sistemos pažeisdamas **arba apeidamas** informacinės sistemos apsaugos priemones,

baudžiamas viešaisiais darbais arba bauda, **arba laisvės apribojimu,** arba areštu, arba laisvės atėmimu iki vienerių metų.

2. Tas, kas neteisėtai prisijungė prie strateginę reikšmę nacionaliniam saugumui arba didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinčios informacinės sistemos,

baudžiamas bauda arba areštu, arba laisvės atėmimu iki trejų metų.

3. Už šiame straipsnyje numatytas veikas atsako ir juridinis asmuo.

MOKSLINIŲ PUBLIKACIJŲ SĄRAŠAS

Mokslinių publikacijų disertacijos tema sąrašas:

1. Marcinauskaitė, R. Nusikalstamomis veikomis elektroninėje erdvėje pažeidžiamos pagrindinės baudžiamojo įstatymo saugomos vertybės nustatymo problema. *Socialinių mokslų studijos*. 2011, Nr. 3(3): 897–914.
2. Kalpokas, V.; Marcinauskaitė, R. Tapatybės vagystė elektroninėje erdvėje: technologiniai aspektai ir baudžiamasis teisinis vertinimas. *Teisės problemos*. 2012, Nr. 3(77): 30–52.
3. Marcinauskaitė, R. Technologinio neutralumo principo taikymo problemos aiškinant nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui sudėties požymius. *Socialinių mokslų studijos.* 2013, Nr. 5(1): 367–379.
4. Fedosiuk, O.; Marcinauskaitė, R. Criminalization of Cybercrime and Principle of Equivalence. *Administratīvā un kriminālā justīcija.* 2013, No. 2(63): 8–13.

Kitų mokslinių publikacijų sąrašas:

1. Marcinauskaitė, R. Psichinės bei fizinės prievartos sąsajos probleminiai aspektai baudžiamosios teisės doktrinoje ir teismų praktikoje. *Jurisprudencija.* 2008. Nr. 11(113): 42–49.
2. Šukytė, J.; Marcinauskaitė, R. Kai kurie psichinės prievartos doktrinos probleminiai aspektai. *Socialinių mokslų studijos*. 2012, Nr. 4(2): 685–695.

PRANEŠIMAI DISERTACIJOS TEMA MOKSLINĖSE KONFERENCIJOSE

1. Marcinauskaitė, R. Cybercrime: The Main Threats and their development in the Modern Society (tarptautinė konferencija „International Conference of Young Scientists – 2012“. Šiauliai, Šiaulių universitetas, 2012 m. gegužės 10–11 d.).
2. Marcinauskaitė, R. Sukčiavimo elektroninėje erdvėje baudžiamasis teisinis vertinimas (Moksliniame seminaras „Sukčiavimas elektroninėje erdvėje: technologiniai aspektai ir teisinis vertinimas“. Vilnius, Teisingumo ministerija, 2012 m. gegužės 25 d.).

MOKSLINIAI TYRIMAI DISERTACIJOS TEMA STAŽUOTĖSE

1. 2012 m. rugsėjo 3 d.–2012 m. spalio 3 d. mokslinė stažuotė Lietuvos Respublikos generalinės prokuratūros Baudžiamojo persekiojimo departamente.

GYVENIMO APRAŠYMAS

Asmeninė informacija

Gimimo data:	1982 m. sausio 1 d.
Kontaktinė informacija:	renata.marcinauskaite@gmail.com

Aukštasis išsilavinimas

2009–2013	Teisės (01 S) doktorantūra, Mykolo Romerio universitetas
2005–2007	Teisės magistras, Mykolo Romerio universitetas
2001–2005	Teisės bakalauras, Mykolo Romerio universitetas

Pedagoginio darbo patirtis

2007–2011	Mykolo Romerio universiteto Teisės fakulteto Baudžiamosios teisės ir kriminologijos katedros lektorė

Darbo patirtis:

2010–iki dabar	Lietuvos Aukščiausiojo Teismo Teisės tyrimų ir apibendrinimo departamento Baudžiamosios teisės grupės konsultantė
2008–2010	Lietuvos Respublikos teisingumo ministerijos Administracinės ir baudžiamosios justicijos departamento Baudžiamosios justicijos skyriaus vyriausioji specialistė

MYKOLAS ROMERIS UNIVERSITY

Renata Marcinauskaitė

CRIMINAL OFFENCES AGAINST THE CONFIDENTIALITY OF ELECTRONIC DATA AND INFORMATION SYSTEMS (CRIMINAL CODE OF THE REPUBLIC OF LITHUANIA ARTICLES 198 AND 198[1])

Summary of the Doctoral Dissertation
Social Sciences, Law (01 S)

Vilnius, 2013

The dissertation was written during the period of 2009–2013 at Mykolas Romeris University, Faculty of Law.

Academic supervisors:

prof. dr. Olegas Fedosiukas (Mykolas Romeris University, Social Sciences, Law – 01 S), year 2012–2013;

doc. dr. Agnė Baranskaitė (Mykolas Romeris University, Social Sciences, Law – 01 S), year 2009–2012.

The doctoral dissertation will be defended at the Law Research Council of Mykolas Romeris University:

Chairman:

prof. dr. Rima Ažubalytė (Mykolas Romeris University, Social Sciences, Law – 01 S).

Members:

prof. dr. Edita Gruodytė (Vytautas Magnus University, Social Sciences, Law – 01 S);

prof. dr. Raimundas Jurka (Mykolas Romeris University, Social Sciences, Law – 01 S);

prof. dr. Jonas Prapiestis (Vilnius University, Social Sciences, Law – 01 S);

prof. dr. Darius Štitilis (Mykolas Romeris University, Social Sciences, Law – 01 S).

Opponents:

prof. dr. Armanas Abramavičius (Vilnius University, Social Sciences, Law – 01 S);

dr. Algimantas Čepas (The Law Institute of Lithuania, Social Sciences, Law – 01 S).

The public defense of the Doctoral Dissertation will take place at the Law Research Council at Mykolas Romeris University on the 10th of January, 2014, 1:00 PM, at the Mykolas Romeris University, auditorium I-414.

Address: Ateities str. 20, LT-08303, Vilnius, Lithuania.

The summary of the Doctoral Dissertation was send out on the 10th of December, 2013.

The Doctoral Dissertation is available at the library of the Mykolas Romeris University (Ateities g. 20, Vilnius) and Lithuanian National Library of Martynas Mazvydas (Gedimino ave. 51, Vilnius).

Renata Marcinauskaitė

CRIMINAL OFFENCES AGAINST THE CONFIDENTIALITY OF ELECTRONIC DATA AND INFORMATION SYSTEMS (CRIMINAL CODE OF THE REPUBLIC OF LITHUANIA ARTICLES 198 AND 198[1])

Summary

Research problem. The development of information technologies and electronic networks created preconditions for different types of large-scale dissemination of information, new accesses to information, and information exchange at the national and international levels. This one aspect of global transformation revealed not only positive changes that influenced and encouraged interface and interaction of cyber users in the cyberspace, but also showed that information society is vulnerable – one of many threats in the cyberspace are criminal offences, that can be committed there. The list of such offences includes not only traditional crimes that have changed due to new technologies, but also crimes that are solely the result of development of these technologies. Criminal offences, described in the chapter XXX of the Criminal Code (hereinafter – CC) of the Republic of Lithuania and committed against security of electronic data and information systems, should be also attributed to the latter. This thesis analyses one type of such crimes: problems of criminal acts against confidentiality of electronic data and information systems provided in the CC Articles 198 and 198[1]. This type was distinguished by structuring criminal offences in the chapter XXX of CC; they were reviewed through the *CIA triad* as violations of confidentiality, integrity and availability.

The synthesis of technological progress and criminal offences shows quantitatively more and qualitatively new problems of criminal law in protecting interests of society, where the main source of power and productivity is related to a rapid information processing based on technologies in the cyberspace. The abundance of new questions for discussion determined that the study of problems of chosen criminal offences is not limited to the content analysis of their constituent elements. Confidentiality violations of electronic data and information systems were reviewed more broadly from the criminal law perspective. The thesis analysed the source of such criminal acts, justification for criminalization, potential connection with traditional crimes, and separation from other similar criminal acts. Also, it provides principal positions for interpreting these crimes and analyses issues of technologies and terminology, principles that were formulated not in the field of criminal law, as well as issues of their applicability.

Relevance and novelty of the thesis, significance of the research results. Conditions for analysing criminal offences against the confidentiality of electronic data and information systems at the national level were created in 2000 after adopting CC, when new crimes that occurred due to technology changes were criminalized and no longer considered as integral part of other crimes. The occurrence of such criminal offences caused fundamental problems of law and criminal law application (and their interpretation). These problems were noticed

after the adoption of CC of 2000, but before it enter into force. Although foreign scholars have been discussing about legal problems related to the use of cyberspace for several years, Lithuanian scholars are only at the initial stage of discussions. There were no further studies regarding the regulation of offences in the cyberspace and determination of liabilities for illegal acts (in the context of Lithuania), states scholarly literature of that time. It should be acknowledged that almost ten years later in a certain way, this statement remains relevant. Even after creating legal basics of criminal liability for such crimes, there are no further discussions on the suitability of these basics. Furthermore, the period after CC of 2000 entered into force is more than sufficient to analyse the effectiveness of legal regulation, discuss whether the norms that regulate liability for criminal offences against confidentiality of electronic data and information systems are sufficient, understandable, whether they helped to achieve desired goals, and what is the real outcome of their application. Especially, when court practice, regarding criminal cases of this category, is quite chaotic, and there are several cases, when crimes against confidentiality remains unacknowledged, constituent elements of such crimes are incriminated intuitively without sufficient theoretical justification. There is no doubt that *inter alia* insufficient analysis of criminal offences against the confidentiality of electronic data and information systems at the level of doctrine, the lack of discussions creates conditions for formation of such situation.

Scholarly novelty of this thesis manifests in the fact that for the first time in Lithuania, a dissertation analyses criminal offences against the confidentiality of electronic data and information systems in details. The thesis reveals aspects of constituent elements of such crimes in the Lithuanian doctrine of criminal law, explains technological-legal problems, systematically analyses international and the European Union's legal acts, as well as legal norms of the criminal law applied in foreign countries and Lithuania. According to analysis of constituent elements of criminal offences, criteria to separate criminal acts against confidentiality of electronic data and information systems from other similar crimes were formed. The thesis highlights possibilities to apply the principles of technological neutrality and equivalence in the context of criminal law. The study is not limited only to the theoretical level. For the first time, the analysis of these crimes includes court practice, specific qualification problems were formulated after summarizing the court practice, and recommendations are provided. Also, the thesis chose significant court practice of foreign countries. Cases that were analysed helped to determine problematic aspects of criminal offences against confidentiality of electronic data and information systems that have not occurred in Lithuania yet.

Considering the fact that this thesis provides scholarly-based recommendations for interpreting and incriminating criminal offences against confidentiality of electronic data and information systems, this material can be useful to the doctrine of cybercrimes, and also can be used at the practical level of the criminal law in solving issues related to qualification of such crimes.

Object of the dissertation. The object of this dissertation is one type of criminal offences against the security of electronic data and information systems, which is criminal offences against the confidentiality of electronic data and information systems, provided in the Articles 198 and 198[1] of the CC, and issues of their criminal legal assessment.

Goal and tasks. *Goal of the dissertation:* to determine principal provisions of criminal offences that are committed against confidentiality of electronic data and information systems, explain constituent elements of these crimes as detailed as possible, identify problems of their criminal legal assessment, determine weaknesses of legal regulation and also provide recommendations for improvement of legal regulation or feature interpretation.

Tasks of the dissertation:

1. To reveal essential problematic aspects of criminal offences committed in the cyberspace, criminalization, and interpretation of their elements, while analysing principles of equivalent assessment and technological neutrality in the context of criminal law.

2. To identify criminal offences that violate confidentiality of electronic data and information systems based on values protected by the criminal law and after structuring criminal offences provided in the chapter XXX of the CC, to reveal how this legal value should be interpreted in the context of security of electronic data and information systems.

3. To reveal constituent elements of unlawful connection to an information system (CC Article 198[1]), determine weaknesses of the current legal regulation or interpretation of constituent elements, provide potential solutions for improving legal regulation or interpretation of constituent elements.

4. To reveal constituent elements of unlawful interception and use of electronic data (CC Article 198), determine weaknesses of the current legal regulation or interpretation of constituent elements, provide potential solutions for improving legal regulation or interpretation of constituent elements.

5. To analyse the correlation between criminal offences against confidentiality of electronic data and information systems and similar criminal offences, form criteria for separating these offences.

Defended statements of the dissertation:

1. The principles of equivalent assessment and technological neutrality are relevant for criminalization of dangerous acts in the cyberspace and interpreting constituent elements.

2. Crimes provided in the chapter XXX of the CC are structured into violations of confidentiality, integrity, and availability of electronic data and information systems by using *CIA triad* security model, used for interpreting security of electronic data and information systems.

3. A chosen concept of unlawful connection to an information system in the CC causes problems for incrimination and interpretation of this criminal offence.

4. A chosen concept of unlawful interception and use of electronic data in the CC causes problems for incrimination and interpretation of this criminal offence, as well as the determination of correlation between them.

5. Separation of criminal offences against confidentiality of electronic data and information systems from similar criminal offences against security of electronic data and information systems, criminal offences against the financial system and crimes against inviolability of a person's private life is problematic.

Review of the researches. In Lithuania, the topic of criminal offences against confidentiality of electronic data and information systems was researched very poorly, and constituent elements of these crimes were barely analysed at all. In general, only D. Štitilis

was interested in the topic of crimes in the cyberspace during the period when the CC of 1961 was applied, and later when the CC of 2000 entered into force. This author's dissertation of 2002 "Problems of determining legal liability basics for unlawful acts in the cyberspace" and subsequent articles focused on general issues of interpreting such crimes. R. Petrauskas analysed them in separate aspects, but only at the time, when the CC of 1961 was still applicable. After the CC of 2000 entered into force, individual articles on crimes in the cyberspace were found in educational publications, for example, in the textbook of 2006 "Informatics of Law and the Law of Informatics" and the publication of 2004 "The Law of Information Technologies". Also, D. Sauliūnas expressed his opinion on compatibility of CC and international legal instruments in the field of cybercrime regulation. Some aspects of these crimes were analysed by N. Goranin and D. Mažeikos in the context of their investigation methods. It should be noted that a commentary of the CC provides a brief theoretical interpretation of crimes against confidentiality of electronic data and information systems. Recently, scholarly literature pays more attention to criminalization issues of identity theft in the cyberspace, and D. Štitilis, P. Pakutinskas, M. Laurinaitis and I. Dauparaitė show their interest in this topic.

The science of criminal law in foreign countries, where various crimes against security of electronic data and information systems and cybercrimes in general get far more attention, present a bit different situation. Issues of general criminalization and interpretation of cybercrimes and assessment of behaviour in the cyberspace were analysed by J. Clough, I. Walden, C. Reed, U. Kohl, S. W. Brenner, M. Schellekens, R. Ali, I. M. van der Haar, J.–B. Koops, R. W. Downing, P. Ohm, C. A. Kirby, and others. Issues of unlawful access to an information system or electronic data were analysed by O. S. Kerr, M. W. S. Wong, M. J. Madison, I. Walden, D. Bainbridge, J. Angel, G. Thornton, J. Clough, B. A. Howell, A. S. Blunn, D. Rowland, E. Macdonald. Also, Russian scholars of the criminal law, such as N. I. Vetrov, V. A. Mazurov, A. V. Naumov, A. G. Volevodz, V. E. Kozlov, O. Ja. Baev and V. A. Meshherkov, S. A. Pashin, and others, should be also mentioned.

Methodology. Methods of *analysis* and *synthesis* were two the most broadly used methods in the dissertation research, explaining criminal offences against confidentiality of electronic data and information systems. The method of *analysis* was applied to separate the structure of these crimes and interpret individual objective or subjective elements. Also, this method allowed to reveal the content of individual elements that are directly related to information and communication technologies. The question of compatibility was managed after separating legal and technological elements. In order to acquire full knowledge of the crimes, *the method of synthesis* was applied to combine individual elements that were discovered during the analysis. The completeness helped to determine what kind of conception defined these crimes in the CC and what the limits of these criminal offences are.

The dissertation research also used *the method of systematic analysis*, which was chosen due to particularity of criminal offences against electronic data and information systems: various aspects of these crimes can be found in international and the European Union legal acts, and it is necessary to relate theories that were formed in various fields of science to interpret these crimes. This method allowed to determine the place of criminal offences against security of electronic data and information systems in the cybercrime field totality.

It helped to solve complex problems with the technological aspect and directly related to the issue of technologies and terminology. The method of systematic analysis allowed to analyse the correlation between constituent elements of crimes, reveal their relationship with similar crimes defined in the CC, and find a criterion to separate them.

The complexity of analysed problems determined that it was necessary to relate the field of criminal law and information and communication technologies in the dissertation research. *The method of generalization* was used in order to reveal the technological – legal aspect of criminal offences. Distinguished general and essential elements in the field of technologies, they were related to the criminal legal aspect of constituent elements. Such method of the research helped to solve the issue of compatibility between technologies and terminology used in the CC and provide the interpretation of technology – related elements.

It would not be a mistake to claim that currently, the origins of regulating criminal offences against confidentiality of electronic data and information systems are associated with the international and the European Union legal acts that are aimed at fighting against crimes in the cyberspace. Their influence is seen not only in provisions of the CC in Lithuania, but also in foreign countries. Different implementation method of the mentioned legal acts allows to form different concepts of such crimes. *The comparison method* was chosen for identification and analysis, allowed to compare different concepts of the crimes, opinion of various scholars, determine problems of incrimination, form potential recommendations, etc.

The linguistic method was used to reveal the content of elements of criminal offences against confidentiality of electronic data and information systems. The dissertation research helped to determine weaknesses of interpreting various concepts, therefore, this method became relevant in trying to form potential interpretation directions. However, while applying the linguistic method, it was noticed that concepts used in the CC have specific content, which is different from the daily language, and this content acquires even more individuality in the context of information and communication technologies.

The dissertation research also uses the empirical *method of document analysis*. It was applied for summarizing the court practice in the cases of criminal offences against confidentiality of electronic data and information systems, using court decisions that highlighted incrimination problems, and justifying potential suggestions. The study also analysed the most significant court decisions in foreign countries, which allowed to raise new issues that were unknown in Lithuania, and provided suggestions.

Structure. The dissertation consists of an introduction, main section, conclusions, list of references, and annex. The main section consists of five chapters covering various research aspects of criminal offences against confidentiality of electronic data and information systems.

The first chapter of the dissertation "**Essential Criminal Legal Aspects of Criminal Offences in the Cyberspace"** analyses the principles of technological neutrality and equivalent assessment that are important for criminalization of criminal acts in the cyberspace and interpretation of constituent elements of these crimes. While analysing the aspects of these principles in the context of the criminal law, the chapter focuses on the fact that the origins of these principles are not directly related to the field of criminal law. However, they become very relevant in this field as well, when the criminal legal regulation

is used as a measure to regulate crimes in the cyberspace. This chapter concludes that the principle of technological neutrality allows avoiding restrictions of the criminal law standards that may arise due to the use of technology – related elements. However, it also emphasizes that such interpretation of elements has to comply with important principles of legality and legal certainty in the criminal law. The analysis of the principle of equivalent assessment allowed to determine that criminal offences against confidentiality of electronic data and information systems in the Lithuanian CC are criminalized by implementing requirements of functional equivalency.

The second chapter of the dissertation "**Confidentiality of Electronic Data and Information Systems as Protected Value of the Criminal Law"** analyses changes of a value protected by the criminal law and specified in the title of the CC chapter XXX, and also, supports the current title of the legal good – security of electronic data and information systems. The dissertation suggests to use the classical *CIA triad* to reveal the content of the value and talk about security of electronic data and information systems like it was the security of confidentiality, integrity, and availability. Such content of the value allowed to distinguish criminal offences that violate confidentiality of electronic data and information systems, such as unlawful interception and use of electronic data (CC Article 198) and unlawful connection to an information system (CC Article 198[1]). This chapter also talks about various aspects of confidentiality by analysing this legal good in the context of electronic data and information systems.

The third chapter of the dissertation "**Unlawful Connection to an Information System (CC Article 198[1])**" analyses criminal offence against confidentiality of information system. The dissertation focuses on the fact that this crime in the CC is criminalized through *per se* without any direct connection with further actions of a perpetrator in the same system. However, it is necessary to determine not only the fact of unlawful connection to an information system, but also to determine the violation of security measures, in order to apply criminal liability according to the CC Article 198[1]. This chapter reveals constituent elements of the criminal act and analyses different positions of assessing the cyberspace: *internal* and *external perspectives*. The *internal perspective*, allowed to look into the cyberspace as the virtual reality and notice the development of traditional trespass doctrine. This doctrine was considered to be a logical starting point for interpreting unlawful connection to an information system and was called a *cybertrespass*.

The fourth chapter of the dissertation "**Unlawful Interception and Use of Electronic Data (CC Article 198)**" analyses the criminal offence against confidentiality of electronic data. The analysis of its constituent elements showed that the CC Article 198 criminalizes both the interception of data transferred in the information system and the unlawful acquisition of data stored in the system, i.e. *data "in rest"*. It was observed that the chosen method of criminalizing the criminal offence against confidentiality of electronic data raises problems of *overcriminalization*, compatibility of constituent elements, and separation of similar offences.

The fifth chapter of the dissertation "**Separation of Criminal Offences against Confidentiality of Electronic Data and Information Systems from Similar Criminal Offences"** analyses the issue of separating criminal offences against confidentiality of electronic data and information systems from criminal offences against financial system (CC Articles 214, 215), crimes against inviolability of a person's private life (CC chapter

XXIV), and other criminal offences against security of electronic data and information systems. This chapter provides potential criteria for separating these offences and suggestions how to solve problems of restriction.

CONCLUSIONS

1. In the most general sense, the principles of equivalent assessment reflects an idea that the standards of the criminal law has to ensure the same protection of values in the physical space and cyberspace. While practically implementing the equivalent assessment of criminal offences in the Lithuanian CC, traditional criminal offences committed in the cyberspace are qualified by using a CC article, which is used to qualify similar offences in the physical space. The CC embedded independent norms to implement functional equivalence for qualification of *CIA criminal offences* (CC Articles 196–198[2]).

2. The principles of technological neutrality is relevant in order to avoid restrictions of the CC application that may arise due to the use of technology – related elements. However, the principles of the criminal law inevitably narrow the extent of this principle, allowing to avoid *overcriminalization* and unjustified extension of criminal liability.

3. The classical security model of *CIA triad* was used instead of an abstract concept of security in order to reveal the content of security of electronic data and information systems. This model allowed to determine the need of preserving three elements of electronic data and information systems: confidentiality, integrity, and availability. Based on this model, the criminal acts in the CC chapter XXX can be grouped into violations of confidentiality, integrity, and availability.

Confidentiality of both electronic data and information systems proves restrictions to their access, i.e., data or systems that process information are available only to the users, who have the access rights and only to a certain extent.

4. Unlawful connection to an information system is criminalized through *per se* without any direct connection with other criminal offences against security of electronic data and information systems. Since the initial actions of a perpetrator to connect unlawfully provide further opportunities to commit any other crimes in the same system, therefore, frequent incrimination of such offence should not come as a surprise.

5. In order to avoid criminalization of obviously innocuous offences, the definition of unlawful connection to an information system narrows the composition of this crime, when the method of this crime is specified – violation of security measures of the information system. The technological concept of these security measures are used to interpret these measures. Broader interpretation of these measures might be possible if the threat of *overcriminalization* is acknowledged.

Violation of security measures should be interpreted not only as the damage to security measures, but also as a violation of determined restriction (requirements), when damage for these security measures was not caused.

6. When unlawful connection to an information system would be criminalized *per se*, it would create limited options to recognize unlawful access and access exceeding legality limits. The narrower interpretation allows avoiding criminalization of obviously innocuous crimes.

Unlawful connection to an information system should be recognized only after determining the violation of authentication procedure and the fact of exploiting security weaknesses.

7. The approach of *internal perspective* was applied to interpret the connection, and it defines the cyberspace as a virtual reality. Therefore, despite the fact whether the connection is perceived as a command, which starts the session with IS, or whether it is perceived as an opportunity to access resources of an information system, metaphorically, the connection would be equal to a *virtual entry* into the system.

Although the criterion of accessing resources of an IS helps understanding the crime of connection, but a real possibility of the perpetrator to perform further actions in an information system should not be significantly important to the moment of its finality.

8. The object of criminal offence provided in the CC article 198^1 is an information system, which, in the context of the criminal law, should be perceived without its context of functionality and in general sense, should be considered as a synonymous of information technologies (including communication technologies) or computer systems.

An information system, which is significantly meaningful to the national security or the state government, economy, or financial system, is a circumstance, which qualifies unlawful connection to an information system. Criteria of *victims, economic effect*, and *effect on society* are applied to state the importance of an information system provided in the CC article 198^1 section 2 to the mentioned fields.

9. The approach of *internal perspectives* towards the cyberspace are very important in justifying intentional guilt and provide an opportunity to see the boundaries of their legality from the perspective of the cyberspace user. Therefore, in order to assess the perception of determined restrictions, a *foreseeability criterion* of such restrictions and their violations should be applied. It allows to consider a personal experience in the cyberspace as in a *place*.

10. Unlawful interception and the use of electronic data provided in the CC Article 198 is criminalized broadly. One criminal act includes crimes against confidentiality of *data in transmission* and *data "in rest"*. This crime is not associated with additional elements (for example, the use of technical measures, criminal intent of the perpetrator) that might help to avoid problems of *overcriminalization*.

11. While describing the object of unlawful interception and the use of electronic data, it is necessary to distinguish two aspects – *legal* and *technological*. The legal aspect is related to the confidentiality of electronic data, and the technological one to an electronic form of such data.

The confidentiality of electronic data shows that it belongs to the data type, which has a certain security level, appropriate security requirements are applied. The basics of confidentiality may derive from laws or other legal acts (objective), personal agreements, private goals, etc. (subjective).

Criteria of *suitability to process in an information system* or *existence of such data in an information system (in a certain area or external media)* are applied to state the electronic form of data.

Electronic data that are strategically important to the national security or the state government, economy, or financial system, is a circumstance, which qualifies unlawful interception or the use of electronic data. Criteria of *victims, economic effect*, and *effect*

on society are applied to determine this fact. Not only can the content of data show the significance of electronic data, but also their significant quantity. In such cases, individual data that are considered to be strategically unimportant, can acquire this element due to unlawful disposition of quantity of such data.

12. The object of a criminal act in the CC Article 198 – confidential electronic data – is not specified to the categories of *data that are stored in an information system* and *data in transmission*; therefore, disposition of this article does not provide an opportunity to related alternative acts with only one type of these data.

12.1. Problems of separating observation, recording, and interception crimes arise while analysing data in transmission. Observation is usually associated with the previous data recording or recording during data transmission; unlawful operation of the software in a network might be compared to the monitoring of network traffic; in general sense, recording might be considered as an interception of electronic data. By searching for differences of these alternatives, it is suggested to relate unlawful receipt of traffic data with unlawful record, and the interception of the content with unlawful interception. Considering the mechanism of committing these crimes, the perpetrator will frequently be incriminated with interception, recording, and observation crimes.

12.2. Problems of correlation between the recording and acquisition arise when these crimes are related to *data "in rest"*, because they have the most similar content. When these crimes in the CC Article 198 are separated, it is required to search for criteria of demarcation of these alternatives. It is debatable, whether they could be considered as different finality moments of recording and acquisition or a possibility to change the form of electronic data into material data during the act of crime.

12.3. Interception and the acquisition of electronic data are similar crimes, but both in the CC Article 198 should be inevitably separated into receipt of *data in transmission* and *data "in rest"*. Interception is solely related to unlawful acquisition of *data in transmission*. To avoid duplication, it is necessary to relate the acquisition of electronic data only when it is associated with unlawful receipt of *data "in rest"*.

12.4. When observation act will be determined as an independent alternative, the combination of this action and *data "in rest"* would be enough to apply criminal liability according to the CC Article 198. In such cases, to ensure sufficient threat of the act, it is important to determine the fact of observation and other circumstances proving the threat to legal goods protected by the criminal law. It is suggested to consider the perpetrator's intentions, when the data is acquired to commit other crimes; violations of data security measures; the use of various technological measures for the acquisition and the use of data; relate illegal actions of the perpetrator to an information system in order to acquire access to data; stability of observation actions; quantity of observed data, their meaning, damage, etc.

12.5. Storing of electronic data shall be considered when the perpetrator has data: possesses electronic data in controlled material media or accessible location in the cyberspace (for example, e-mail server). When storing is recognized, it is required to determine the perpetrator's possibility to access electronic data and affect them.

12.6. Some of traditional property appropriation aspects are relevant to the interpretation of electronic data appropriation. However, considering the particularity of property appropriation and its connection to the doctrine of crimes against property, it is suggested to abandon criteria that are difficultly applied in the cyberspace context,

while interpreting the appropriation of electronic data, and consider the appropriation of electronic data as an unlawful act of becoming the actual holder of electronic data. It means that the perpetrator gained the legal access to the data on particular circumstances, but went beyond the boundaries of legality and disposed electronic data, while violating specific restrictions.

12.7. Unlawful distribution of electronic data is related not only to the active actions in transferring data to the third parties, but also with the access to the data. In this case, it will not matter who – the sender or the receiver – initiated the process of transferring data.

12.8. The feature of otherwise use the electronic data shows a non-exhaustive list of unlawful disposal of electronic data. The wording of this crime allows to argue that such crime is usually the method for committing other criminal acts; one of the most common cases is the unlawful use of confidential electronic data connecting to an information system.

13. The unlawfulness of using confidential electronic data means that a person gained the access or performed other crimes with confidential electronic data, but did not have a lawful permission to perform these actions or although, this permission was given, but these actions violated the procedure (obligations) for using confidential electronic data.

14. When stating intentional fault *inter alia*, the perception of violating confidentiality of electronic data and restrictions in the cyberspace should be assessed from the *internal perspective*, which allows to consider the user's experience in the cyberspace. The criteria of foreseeability applied to assess restriction allows justification that a person realized the limits, but still violated the confidentiality of electronic data.

15. After determining that during the unlawful connection to an information system, confidential electronic data were used or electronic data was unlawfully affected, it should be judged, whether criminal acts described in the CC Article 198^1, 196 or 198 were incriminated. When the norm in the CC Article 198^1 is considered to the *completeness* of the norms, and the CC Articles 196 and 198 are considered to be the parts of it, the unlawful connection to an information system, depending on how security measures were breached, should be qualified according to the coincidence of criminal acts, i.e., CC Article 198^1 and 196 or 198. Currently the sanctions for these crimes influence that the norm in CC Article 198^1 will never cover the other part of the norm: the unlawful influence on electronic data (CC Article 196) or the unlawful interception and the use of electronic data (CC article 198).

16. The CC Article 198, certain part of the Articles 198^2 and 214, 215 determine criminal liability for the various unlawful disposal of electronic data. After determining that the perpetrator acquired all data that have the elements provided in the CC Article 214, a special norm provided in the CC Article 214 shall be applied to qualify the perpetrator's crime, rather than the norms in the CC Articles 198 or 198^2.

A dangerous act, featuring the initiation of illegal transaction, using data for verification of consumer's identity for online payment measures, should be qualified by applying the CC Article 215, rather than the Article 198

17. The CC chapter XXIV criminalizes various crimes against inviolability of a person's private life *inter alia* in the cyberspace, which causes problems to separate criminal acts described in the CC chapter XXIV and Article 198. After determining the unlawful interference with privacy sphere, it should be qualified according to the CC Articles 166, 167, or 168. The norms in these articles are special to the norm in the CC Article 198.

RECOMMENDATIONS

Considering the issues described in the dissertation and after providing potential recommendations, it is suggested to make the following changes of the CC Articles 198 and 198[1]:

1. To change the CC Article 198 and arrange it as follows:

Article 198. ~~Unlawful Interception and Use of Electronic Data~~ Unlawful Disposal of Non-Public Electronic Data

1. A person who unlawfully observes, records, intercepts~~,~~ **non-public electronic data transmitted through the electronic communications networks or unlawfully** acquires, stores, appropriates, distributes or otherwise uses the electronic data which may not be made public**, or material item whose content is such data,**

shall be punished by a fine **or restriction of liberty or arrest** or by imprisonment for a term of up to ~~four~~ **two** years.

2. A person who **commits the acts provided for in paragraph 1 of this Article unlawfully connected to an information system or** unlawfully observes, records, intercepts~~,~~ **electronic data transmitted through the electronic communications networks which may not be made public and which are of strategic importance for national security or of major importance for state government, the economy or the financial system, or unlawfully** acquires, stores, appropriates, distributes or otherwise uses ~~the electronic data which may not be made public and which are of strategic importance for national security or of major importance for state government, the economy or the financial system~~ **such electronic data or material item whose content is such data**

shall be punished by **a fine or** imprisonment for a term of up to ~~six~~ **four** years.

3. A legal entity shall also be held liable for the acts provided for in this Article.

2. To change the CC Article 198[1] and arrange it as follows:

Article 198[1]. Unlawful Connection to an Information System

1. A person who unlawfully connects to an information system by damaging **or circumventing** the protection means of the information system

shall be punished by community service or by a fine **or restriction of liberty** or by arrest or by imprisonment for a term of up to one year.

2. A person who unlawfully connects to an information system of strategic importance for national security or of major importance for state government, the economy or the financial system

shall be punished by a fine or by arrest or by imprisonment for a term of up to three years.

3. A legal entity shall also be held liable for the acts provided for in this Article.

LIST OF ACADEMIC PUBLICATIONS

Academic publications related to the dissertation:

1. Marcinauskaitė, R. The Problems of Identification of the Main Object of the Cyber offences. *Social Science Studies*. 2011, No. 3(3), p. 897–914.
2. Kalpokas, V.; Marcinauskaitė, R. Identity Theft in Cyberspace: Technological aspects and Criminal Legal Assessment. *Law Problems*. 2012, No. 3(77), p. 30–52.
3. Marcinauskaitė, R. The Technological Neutrality Principle and Its Significance in Formulating and Explaining the Offences against the Security of Electronic Data and Information Systems. *Social Science Studies.* 2013, No. 5(1), p. 367–379.
4. Fedosiuk, O.; Marcinauskaitė, R. Criminalization of Cybercrime and Principle of Equivalence. *Administratīvā un krimināla justīcija*. 2013, No. 2(63), p. 8–13.

Other academic publications:

1. Marcinauskaitė, R. The Problematic Aspects of the Interrelation between Physical and Mental Violence in the Doctrine and Practice of Criminal Law. *Jurisprudencija*. 2008. No. 11(113), p. 42–49.
2. Šukytė, J.; Marcinauskaitė, R. Some Problematic Aspects of the Doctrine of Mental Violence. *Social Science Studies*. 2012, No. 4(2), p. 685–695.

ANNOUNCEMENTS IN SCIENTIFIC CONFERENCES ON THE THEME OF DISSERTATION

1. Marcinauskaitė, R. Cybercrime: The Main Threats and their development in the Modern Society („International Conference of Young Scientists – 2012". Šiauliai, The Univesity of Šiauliai, 10–11th May, 2012).
2. Marcinauskaitė, R. The Criminal Law Evaluation of Computer – related froud (Scientific Seminar „Computer – related froud: Technological aspects and Legal Assessment". Vilnius, Ministry of Justice of the Republic of Lithuania, 25th of May, 2012).

SCIENTIFIC RESEARCHES ON THE THEME OF DISSERTATION IN INTERNSHIPS

1. 3rd September–3rd October, 2012 internship at the Department of Criminal Prosecution, Prosecution Service of the Republic of Lithuania.

CURRICULUM VITAE

Personal Information

Date of birth:	The 1st of January 1982
Contacts:	renata.marcinauskaite@gmail.com

Higher Education

2009–2013	Law PhD, Mykolas Romeris University
2005–2007	Master of Law, Mykolas Romeris University
2001–2005	Bachelor of Law, Mykolas Romeris University

Lecturing Experience

2007–2011	*Lecturer* at the Department of Criminal Law and Criminology, Faculty of Law, Mykolas Romeris University

Work Experience

2010–till now	*Adviser* at the Criminal Law group, Department of Legal Analysis and Review, Supreme Court of Lithuania
2008–2010	*Chief Specialist* at the Division of Criminal Justice, Administrative and Criminal Justice Department, Ministry of Justice of the Republic of Lithuania

Marcinauskaitė, Renata

NUSIKALSTAMOS VEIKOS ELEKTRONINIŲ DUOMENŲ IR INFORMACINIŲ SISTEMŲ KONFIDENCIALUMUI (LIETUVOS RESPUBLIKOS BAUDŽIAMOJO KODEKSO 198 IR 198[1] STRAIPSNIAI): daktaro disertacija. – Vilnius: Mykolo Romerio universitetas, 2013. 220 p.
Bibliogr. 173–186 p.
ISBN 978-9955-19-599-3

Šio disertacinio tyrimo objektas yra viena iš nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui rūšių – nusikalstamos veikos elektroninių duomenų ir informacinių sistemų konfidencialumui, numatytos Lietuvos Respublikos baudžiamojo kodekso 198 ir 198[1] straipsniuose, ir jų baudžiamojo teisinio vertinimo problemos. Disertacijoje aptartas baudžiamojo įstatymo saugomo teisinio gėrio turinys, atskleista kaip konfidencialumas interpretuotinas elektroninių duomenų ir informacinių sistemų saugumo kontekste. Analizuoti neteisėto prisijungimo prie informacinės sistemos (Baudžiamojo kodekso 198[1] straipsnis) ir neteisėto elektroninių duomenų perėmimo ir panaudojimo (Baudžiamojo kodekso 198 straipsnis) sudėties požymiai, pateiktos galimos teisinio reguliavimo tobulinimo ir šių veikų požymių aiškinimo kryptys. Šiai analizei pasitelkti ekvivalentinio vertinimo ir technologinio neutralumo principai leido spręsti tokių veikų kriminalizavimo ir jų požymių aiškinimo sunkumus. Disertacijoje taip pat aptartas nusikalstamų veikų elektroninių duomenų ir informacinių sistemų konfidencialumui santykis su panašiomis nusikalstamomis veikomis finansų sistemai, asmens privataus gyvenimo neliečiamumui, kitomis nusikalstamomis veikomis elektroninių duomenų ir informacinių sistemų saugumui, suformuluoti jų atskyrimo kriterijai.

The object of this dissertation is one type of criminal offences against the security of electronic data and information systems, which is criminal offences against the confidentiality of electronic data and information systems, provided in the Articles 198 and 198[1] of the Criminal Code of the Republic of Lithuania, and issues of their criminal legal assessment. The dissertation discussed the content of the main value protected by the criminal law, revealed how confidentiality should be interpreted in the context of security of electronic data and information systems. The analysis of unlawful connection to an information system (CC Article 198[1]) and unlawful interception and use of electronic data (CC article 198) constituent elements is presented in the dissertation; also it provides potential solutions for improving legal regulation and interpretation of constituent elements of such offences. The principles of equivalent assessment and technological neutrality invoked for this analysis allowed to solve criminalization and interpretation problems of such offences. In the dissertation author also discussed the correlation between criminal offences against confidentiality of electronic data and information systems and similar criminal offences against financial system, crimes against inviolability of a person's life and other criminal offences against security of electronic data and information systems, formed criteria for separating these offences.

Renata Marcinauskaitė

CRIMINAL OFFENCES AGAINST THE CONFIDENTIALITY OF ELECTRONIC DATA AND INFORMATION SYSTEMS (CRIMINAL CODE OF THE REPUBLIC OF LITHUANIA ARTICLES 198 AND 198[1])

Doctoral Dissertation

Maketavo *Birutė Bilotienė*

SL 585. 2013 11 20. 19,2 leidyb. apsk. l.
Tiražas 20 egz. Užsakymas 20 935
Mykolo Romerio universitetas
Ateities g. 20, Vilnius
Puslapis internete www.mruni.eu
El. paštas leidyba@mruni.eu

Parengė spaudai UAB „Baltijos kopija“
Kareivių g. 13B, Vilnius
Puslapis internete www.kopija.lt
El. paštas info@kopija.lt
Spausdino UAB „Vitae Litera“
Kurpių g. 5–3, Kaunas
Puslapis internete www.bpg.lt
El. paštas info@bpg.lt

ISBN 978-9955-19-599-3

