MYKOLO ROMERIO UNIVERSITETO
TEISĖS FAKULTETO
BAUDŽIAMOSIOS TEISĖS IR PROCESO INSTITUTAS

VITALIJ MELNIKOV
(BAUDŽIAMOJI TEISĖ IR KRIMINOLOGIJA)

NETEISĖTAS POVEIKIS ELEKTRONINIAMS DUOMENIMS (BAUDŽIAMOJO KODEKSO 196 STRAIPSNIS)

Magistro baigiamasis darbas

Darbo vadovas –
Lektorė;
dr.
Renata Marcinauskaitė

Vilnius, 2016

TURINYS

ĮVADAS

Tiriama problema. Kaip atsižvelgiant į informacijos saugos srityje pateiktą aiškinimą būtų galima apibūdinti elektroninių duomenų integralumą ir prieinamumą kaip baudžiamojo įstatymo saugomą vertybę? Kokias Lietuvos Respublikos baudžiamojo kodekso (toliau – ir BK arba 2000 m. BK, arba naujasis baudžiamasis įstatymas)[1] 196 straipsnio įtvirtinimo, pakeitimų ir papildymų problemas atskleidžia neteisėto poveikio elektroniniams duomenims kriminalizavimo raida? Kas sudaro tiriamos nusikalstamos veikos kriminalizavimo kaip *delicta sui generis* pagrindą? Kokie neteisėto poveikio elektroniniams duomenims baudžiamojo teisinio reguliavimo ypatumai pasirinktose užsienio valstybėse? Kokia nusikalstamos veikos dalyko reikšmė BK 196 straipsnio ir BK straipsnių, kuriuose kriminalizuotos tradicinės nusikalstamos veikos, tarpusavio santykiui, kai nusikalstama veika padaroma elektroninėje erdvėje, turint omenyje ekvivalentiškumo principą? BK 196 straipsnyje vartojami terminai – „sugadinimas“, „sunaikinimas“, „pašalinimas“, „pakeitimas“, „naudojimosi apribojimas“ – apibūdina tik procesą, ar taip pat jo rezultatą – elektroninių duomenų integralumo ar prieinamumo pažeidimą? Ar konstatuojant tyčią būtina nustatyta, jog kaltininkas *inter alia* numatė elektroninių duomenų integralumo ar prieinamumo pažeidimo galimybę? Nusikalstamos veikos kvalifikavimui pagal BK 196 straipsnį svarbu nustatyti tai, kaip elektroniniai duomenys buvo paveikti (technologinis aspektas), ar tai, kad galiausiai tokie duomenys yra neteisėtai sunaikinti, sugadinti, pašalinti ar pakeisti arba naudojimasis tokiais duomenimis yra apribotas? Ar BK 196 straipsnyje įtvirtintos pavojingos veikos gali pasireikšti ir neveikimu? Ar iš dalies išlikę pradiniai elektroniniai duomenys, kurie dėl neteisėto poveikio prarado esminius kokybinius požymius, dėl ko prilygintini neegzistuojantiems, gali būti pripažinti sunaikintais? Visiškas (pilnas) (pavienių) elektroninių duomenų pakeitimas pripažintinas tokių duomenų pakeitimu ar sunaikinimu? Vienų elektroninių duomenų visiškas (pilnas) pakeitimas kitais (kaip visumos) pripažintinas tokių duomenų pakeitimu, sunaikinimu, ar prieinamumo pažeidimu? Koks yra elektroninių duomenų sugadinimo ir pakeitimo pavojingų veikų tarpusavio santykis? Ar elektroninių duomenų sunaikinimas gali būti pripažintas naudojimosi tokiais duomenimis apribojimu? Ar BK 197 straipsnyje kriminalizuotos pavojingos veikos – informacinės sistemos darbo sutrikdymas ar nutraukimas – apima neteisėtą poveikį elektroniniams duomenims? Ar BK 197 straipsnis apima naudojimosi elektroniniais duomenimis apribojimą, kurį sąlygoja neteisėtas poveikis informacinei sistemai? Koks yra

[1] “Lietuvos Respublikos baudžiamasis kodeksas,“ *Valstybės žinios* 89, 2741 (2000) (su vėlesniais pakeitimais ir papildymais).

elektroninių duomenų pašalinimo ir naudojimosi tokiais duomenimis apribojimo pavojingų veikų tarpusavio santykis? Ar neteisėto poveikio daugelio informacinių sistemų elektroniniams duomenims požymio aiškinimas pasirinkta formuluote susiaurintas iki tokių informacinių sistemų skaičiaus nustatymo, kuris atitinka apysunkiam nusikaltimui reikalingą pavojingumą? Ar neteisėtas poveikis elektroniniams duomenims pasinaudojant svetimais asmens duomenimis apima neteisėtą prisijungimą prie informacinės sistemos ar jos dalies pažeidžiant informacinės sistemos apsaugos priemones? Jeigu taip, kaip turėtų būti sprendžiama BK 196 straipsnio 2 dalies ir BK 198[1] straipsnio konkurencija, kai tokiu būdu padaromas neteisėtas poveikis elektroniniams duomenims?

Baigiamojo darbo aktualumas. Nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui mokslinio ištyrimo lygis nacionalinėje baudžiamosios teisės doktrinoje yra nedidelis. Ypatingai mažai mokslininkų tyrinėta elektroninių duomenų integralumą ir prieinamumą pažeidžianti nusikalstama veika. Tai žymi ir baigiamajame darbe tiriamų mokslinių problemų gausa. Mokslinių žinių trūkumas sąlygoja susiklosčiusios nacionalinės teismų praktikos nebuvimą, itin retą BK 196 straipsnio taikymą, nepakankamai argumentuotų teismų sprendimų priėmimą, diskutuotinus nusikalstamų veikų kvalifikavimo atvejus nacionalinėje teismų praktikoje. Mažiau negu prieš vienerius metus įsigaliojo nauja BK 196 straipsnio redakcija. Atliktų pakeitimų pagrindu, *inter alia* BK 196 straipsnio 2 dalis papildyta naujais nusikalstamą veiką kvalifikuojančiais požymiais, todėl atsirado jų mokslinio ištyrimo poreikis. Pagaliau, informacinei visuomenei būtina aiškiai suvokti neteisėto poveikio elektroniniams duomenims integralumo ir prieinamumo baudžiamosios teisinės apsaugos ribas.

Baigiamojo darbo mokslinis naujumas. Baigiamajame darbe nustatyta, kokią reikšmę nusikalstamos veikos dalykas turi BK 196 straipsnio ir BK straipsnių, kuriuose kriminalizuotos tradicinės nusikalstamos veikos, tarpusavio santykiui, kai nusikalstama veika padaroma elektroninėje erdvėje, turint omenyje ekvivalentiškumo principą. Atlikto tyrimo pagrindu pateiktos bendrosios BK 196 straipsnyje kriminalizuotų pavojingų veikų aiškinimo nuostatos, atskleisti skirtingi atskirų pavojingų veikų aspektai, pateikta ir įvertinta jų alternatyvaus aiškinimo galimybė, išspręstas jų tarpusavio santykis ir kt. Šiame kontekste paminėtina tai, kad baigiamajame darbe pateiktas galimas BK 196 ir 197 straipsnių tarpusavio santykio aiškinimas, sprendžiant, ar informacinės sistemos darbo sutrikdymo ar nutraukimo pavojingos veikos apima neteisėtą poveikį elektroniniams duomenims, taip pat tai, ar BK 197 straipsnis apima naudojimosi elektroniniais duomenimis apribojimą, kurį sąlygoja neteisėtas poveikis informacinei sistemai. Baigiamajame darbe įvertinta, ar neteisėto poveikio daugelio informacinių sistemų elektroniniams duomenims požymio aiškinimas pasirinkta formuluote

susiaurintas iki tokių informacinių sistemų skaičiaus nustatymo, kuris atitinka apysunkiam nusikaltimui reikalingą pavojingumą. Be to, nustatyta, ar pasinaudojant svetimais asmens duomenimis gali būti neteisėtai prisijungiama prie informacinės sistemos ar jos dalies pažeidžiant informacinės sistemos apsaugos priemones ir kaip turėtų būti sprendžiama BK 196 straipsnio 2 dalies ir BK 198[1] straipsnio konkurencija, kai tokiu būdu padaromas neteisėtas poveikis elektroniniams duomenims.

Tiriamų problemų ištyrimo lygis. Elektroninių duomenų integralumas ir prieinamumas plačiai nagrinėtas tiek Lietuvos (D. Štitilis, V. Klišauskas, A. Venčkauskas, S. Jastiuginas, E. Toldinas ir kt.), tiek užsienio valstybių (J. R. Vacca, M. E. Whitman, H. J. Mattord, M. Rhodes–Ousley, T. Mayfield, J. Graham, R. Howard, R. Olson, R. S. Sandhu ir kt.) autorių darbuose. Neteisėto poveikio elektroniniams duomenims nusikalstama veika nacionalinėje baudžiamosios teisės doktrinoje menkai nagrinėta. Tiriamos nusikalstamos veikos požymiai aptarti BK komentare[2], Lietuvos baudžiamosios teisės specialiosios dalies vadovėlyje[3]. Dalis BK 196 straipsnio dispozicijoje minimų požymių, t. y. elektroniniai duomenys, strateginę reikšmę nacionaliniam saugumui ar didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinti informacinė sistema, kurie atitinka įtvirtintus BK 198 ir 198[1] straipsniuose, taip pat BK 196, 198 ir 198[1] straipsnių tarpusavio santykis, išskyrus minėtą BK 196 straipsnio 2 dalies ir 198[1] straipsnio konkurenciją, išanalizuoti R. Marcinauskaitės daktaro disertacijoje[4]. Šio mokslinio darbo reikšmė aktuali ir kitų neteisėto poveikio elektroniniams duomenims požymių aiškinimui, pvz., pateiktas ekvivalentiškumo principo, elektroninių duomenų ir informacinių sistemų saugumo kaip baudžiamojo įstatymo saugomos vertybės ir kt. aiškinimas. Su tiriama nusikalstama veika susijęs viršnacionalinis teisinis reguliavimas, atskiri neteisėto poveikio elektroniniams duomenims nusikalstamos veikos aspektai bendrai aptariami mokomajame leidinyje „Elektroniniai nusikaltimai“[5], vadovėlyje „Teisės informatika ir informatikos teisė“[6], vadovėlyje „Informacinių technologijų teisė“[7], mokomojoje knygoje „Nusikaltimai elektroninėje erdvėje ir jų tyrimo metodikos“[8]. Pagaliau, neteisėto poveikio elektroniniams duomenims nusikalstamos veikos tyrimui reikšmingų aspektų galima rasti atskiruose R. Marcinauskaitės, D. Štitilio, D. Sauliūno, R.

---

[2] Armanas Abramavičius et. al., *Lietuvos Respublikos baudžiamojo kodekso komentaras. Specialioji dalis (99-212 straipsniai)* (Vilnius: VĮ Registrų centras, 2009).

[3] Aurelijus Gutauskas et. al., *Lietuvos baudžiamoji teisė. Specialioji dalis. Pirmoji knyga* (Vilnius: Justitia, 2013).

[4] Renata Marcinauskaitė, “Nusikalstamos veikos elektroninių duomenų ir informacinių sistemų konfidencialumui (Lietuvos Respublikos baudžiamojo kodekso 198 ir 198[1] straipsniai)“ (daktaro disertacija, Mykolo Romerio universitetas, 2013), http://vddb.library.lt/obj/LT-eLABa-0001:E.02~2014~D_20140124_091020-54546

[5] Darius Štitilis, *Elektroniniai nusikaltimai. Metodinė priemonė* (Vilnius: Mykolo Romerio universitetas, 2011), http://ebooks.mruni.eu/pdfreader/elektroniniai-nusikaltimai43253

[6] Darius Štitilis et. al., *Teisės informatika ir informatikos teisė* (Vilnius: Mykolo Romerio universitetas, 2006).

[7] Darius Sauliūnas et. al., *Informacinių technologijų teisė* (Vilnius: NVO Teisės Institutas, 2004).

[8] Nikolaj Goranin ir Dalius Mažeika, *Nusikaltimai elektroninėje erdvėje ir jų tyrimo metodikos: Mokomoji knyga* (Kaunas: TEV, 2011).

Petrausko, V. Klišausko ir kitų Lietuvos mokslininkų straipsniuose, publikacijose. Užsienio valstybių baudžiamosios teisės doktrinoje nusikalstama veika, kuria pažeidžiamas elektroninių duomenų integralumas ir prieinamumas, sulaukė didesnio mokslininkų dėmesio. Ypatingai reikšminga knyga „Computer crimes and digital investigations“[9], kurioje I. Walden nagrinėja tokius tiriamai nusikalstamai veikai svarbius aspektus kaip kompiuterinės programos problematika, neteisėtumo požymis, neteisėto poveikio elektroniniams duomenims kriminalizavimo kaip *delicta sui generis* pagrindimas ir kt. Taip pat paminėtinas J. Clough mokslinis veikalas „Principles of Cybercrime“[10], kuriame nagrinėjami tiriamos nusikalstamos veikos teisinio reguliavimo ypatumai atskirose užsienio valstybėse. Literatūroje rusų kalba skirtingų mokslininkų (S. Pashin, Ju. Gavrilin, I. Popov, J. Gulbin, I. Klepickij, V. Krylov, V. Golubev, V. Bechov, S. Boroin, S. Kochoi, D. Saveljev, T. Vaulina ir kt.) pateikti įvairūs kompiuterinės informacijos sunaikinimo, blokavimo, modifikavimo apibūdinimai, kuriuose galima įžvelgti atskirus šių požymių aiškinimui reikšmingus aspektus. Didelę reikšmę tiriamos nusikalstamos veikos nagrinėjimui turi 1989 m. Europos komiteto nusikaltimų problemoms tirti baigiamoji ataskaita (toliau – ir EKNPT baigiamoji ataskaita)[11], 2001 m. lapkričio 23 d. Europos Tarybos konvencijos dėl elektroninių nusikaltimų (toliau – ir Konvencija dėl elektroninių nusikaltimų arba Konvencija)[12] aiškinamoji ataskaita (toliau – ir Konvencijos aiškinamoji ataskaita)[13], dokumentai, kuriuose pateiktas oficialus autentiškas susijusių Europos Sąjungos teisės aktų nuostatų aiškinimas.

Baigiamojo daro reikšmė. Atlikto tyrimo ir jo pagrindu pateiktų išvadų reikšmė pasireiškia originaliu indėliu į besiformuojančią nacionalinės baudžiamosios teisės doktriną elektroninių duomenų integralumą ir prieinamumą pažeidžiančios nusikalstamos veikos srityje. BK 196 straipsnyje kriminalizuotos veikos požymių tyrimo pagrindu gali būti formuojamas ar keičiamas jų doktrininis ir teisminis aiškinimas. Tiriamos ir kitų susijusių nusikalstamų veikų tarpusavio santykio aiškinimo pagrindu gali būti formuojama ar keičiama teisės taikymo praktika. Pasinaudodami atlikto elektroninių duomenų integralumo ir prieinamumo, žalos padarymo, neteisėto poveikio daugelio informacinių sistemų elektroniniams duomenims, neteisėto poveikio elektroniniams duomenims

[9] Ian Walden, *Computer Crimes and Digital Investigations* (New York: Oxford University Press, 2007).
[10] Jonathan Clough, *Principles of Cybercrime* (New York: Cambridge University Press, 2010).
[11] Council of Europe, “Computer–Related Crime. Recommendation No. R (89) 9 on Computer–Related Crime and Final Report of the European Committee on Crime Problems,“ žiūrėta 2016 05 15, http://www.oas.org/juridico/english/89-9&final%20report.pdf
[12] “Konvencija dėl elektroninių nusikaltimų,“ *Valstybės žinios* 36, 1188 (2004).
[13] Committee of Ministers of the Council of Europe, “Explanatory Report to the Convention on Cybercrime,“ žiūrėta 2016 0515, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b

pasinaudojant svetimais asmens duomenimis požymių tyrimo rezultatais kiti mokslininkai galės nagrinėti BK 197 straipsnyje kriminalizuotą neteisėto poveikio informacinei sistemai veiką.

Tyrimo tikslas. Išsiaiškinti BK 196 straipsnyje įtvirtintos nusikalstamos veikos kriminalizavimo, aiškinimo ir taikymo problemas, taip pat santykį su kitomis susijusiomis nusikalstamomis veikomis, pateikti tiriamų problemų sprendimo būdus.

Tyrimo uždaviniai. *Pirma*, atskleisti elektroninių duomenų integralumą ir prieinamumą kaip baudžiamojo įstatymo saugomą vertybę. *Antra,* išsiaiškinti neteisėto poveikio elektroniniams duomenims kriminalizavimo raidą, pagrindimą, baudžiamojo teisinio reguliavimo ypatumus pasiriktose užsienio valstybėse. *Trečia,* nustatyti neteisėto poveikio elektroniniams duomenims nusikalstamos veikos sudėties požymių turinį. *Ketvirta*, atskleisti ir išspręsti BK 196 straipsnio ir kitų susijusių nusikalstamų veikų tarpusavio santykio problemą.

Tyrimo metodika. Pasitelkus *analizės* metodą tiriamos nusikalstamos veikos objektyvieji ir subjektyvieji sudėties požymiai atskirti ir analizuoti pavieniui. *Loginio–analitinio* metodo pagrindu atrinkta ir išanalizuota reikšminga Lietuvos ir užsienio valstybių baudžiamosios teisės doktrina, susiję nacionalinės, viršnacionalinės ir pasirinktų užsienio valstybių teisės aktai, nacionalinė teismų praktika, informacijos saugai skirta mokslinė literatūra. *Sisteminės analizės* metodo dėka tiriama nusikalstama veika analizuota nurodytos mokslinės literatūros, teisinio reguliavimo, teismų praktikos kontekste. *Loginis–analitinis* metodas pasitelktas atskleidžiant probleminius teisinio reguliavimo aspektus, aiškinant atskirų tiriamos nusikalstamos veikos sudėties požymių turinį, jų taikymą, apibendrinant tarpinius tyrimo duomenis, formuluojant atlikto tyrimo galutines išvadas. *Lyginamojo* metodo pagrindu sugretintos atskirų mokslininkų įžvalgos bei išvados. *Istorinio* metodo dėka nagrinėta neteisėto poveikio elektroniniams duomenims kriminalizavimo raida 2000 m. BK. *Teleologinio* metodo pagrindu atlikta BK 196 straipsnio pakeitimų ir papildymų projektų lydimųjų dokumentų analizė, kuri leido nustatyti atskiromis pataisomis siekiamus įstatymų leidėjo kėtinimus, kitus tiriamos nusikalstamos veikos požymių aiškinimui reikšmingus aspektus.

Tyrimo struktūra. *Pirmajame baigiamojo darbo skyriuje* analizuojamas elektroninių duomenų integralumas ir prieinamumas kaip baudžiamojo įstatymo saugoma vertybė, atsižvelgiant į informacijos saugos srityje pateiktą jų aiškinimą, taip pat pateikiamas galimas šių saugumo aspektų interpretavimas BK 196 straipsnio kontekste. *Antrajame baigiamojo darbo skyriuje* nagrinėjama neteisėto poveikio elektroniniams duomenims kriminalizavimo raida 2000 m. BK, atskleidžiami atliktų BK 196 straipsnio pataisų probleminiai aspektai. *Trečiajame baigiamojo darbo skyriuje* nagrinėjamas neteisėto poveikio elektroniniams duomenims kriminalizavimo kaip *delicta sui generis*

pagrindimas nacionalinėje ir užsienio baudžiamosios teisės doktrinoje, taip pat analizuojamas neteisėto poveikio elektroniniams duomenims teisinis reguliavimas pasirinktose užsienio valstybėse. *Ketvirtajame ir penktajame baigiamojo darbo skyriuose* tiriamas neteisėto poveikio elektroninių duomenų integralumui ir prieinamumui nusikalstamos veikos sudėties požymių turinys, BK 196 straipsnio ir kitų susijusių nusikalstamų veikų tarpusavio santykio problematika.

Ginamieji teiginiai. *Pirma,* neteisėto poveikio elektroniniams duomenims nusikalstamos veikos interpretavimui reikšmingos informacijos saugos, informacinių technologijų sritys, kuriose pateiktas aiškinimas turi būti adaptuotas baudžiamajai teisei. *Antra,* dalis BK 196 straipsnyje kriminalizuotos veikos požymių persidengia tarpusavyje, konkuruoja su kitų nusikalstamų veikų požymiais, kelia kitų interpretavimo problemų, kas sąlygoja neaiškumų inkriminuojant tiriamą nusikalstamą veiką. *Trečia*, neteisėto poveikio elektroniniams duomenims ir elektroninėje erdvėje padaromų tradicinių nusikalstamų veikų konkurencijos sprendimui reikšmingas ekvivalentiškumo principas. *Ketvirta,* dėl glaudaus BK XXX skyriuje įtvirtintų nusikalstamų veikų tarpusavio ryšio sudėtinga nustatyti, ar konkrečiu atveju inkriminuotina pavienė neteisėto poveikio elektroniniams duomenims veika, ar ji sudaro sutaptį su kitomis nusikalstamomis veikomis, ar apskritai neturi būti taikoma.

1. ELEKTRONINIŲ DUOMENŲ INTEGRALUMAS IR PRIEINAMUMAS KAIP BAUDŽIAMOJO ĮSTATYMO SAUGOMA VERTYBĖ

Pagrindą kalbėti apie elektroninių duomenų integralumą ir prieinamumą kaip baudžiamojo įstatymo saugomą vertybę sudarė neteisėto poveikio elektroniniams duomenims kriminalizavimas įsigaliojus naujajam baudžiamajam įstatymui. Reikalas tas, kad elektroninių duomenų ir informacinių sistemų saugumą pažeidžiančios veikos galiojant 1961 m. Baudžiamajam kodeksui[14] kaip *delicta sui generis* nebuvo kriminalizuotos. Todėl šių veikų saugomo teisinio gėrio įvairūs įvardijimo aspektai nacionalinėje baudžiamosios teisės doktrinoje nebuvo nagrinėti.[15]

Mokslinėje literatūroje teigiama, kad bendriausia prasme nusikalstamos veikos, įtvirtintos BK XXX skyriuje, kelia grėsmę elektroninėje erdvėje, jomis kėsinamasi į saugų duomenų apdorojimą, saugią informacinių sistemų veiklą. Tačiau rūšinės vertybės, įvardytos kaip elektroninių duomenų ir informacinių sistemų saugumas, turinio aiškinimui artimesnė Konvencijoje dėl elektroninių nusikaltimų minima kompiuterinių duomenų ir informacinių sistemų konfidencialumo, integralumo ir prieinamumo triada (II skyriaus 1 skirsnio 1 dalies pavadinimas). Tai pagrindžia vertybės pavadinime tiesiogiai minimo saugumo interpretavimas pasitelkus techninio kompiuterių saugumo sampratą, kurios pagrindą sudaro konfidencialumas, integralumas ir prieinamumas, t. y. klasikiniais pripažįstami elektroninių duomenų ir informacinių sistemų saugumo aspektai. Ši elektroninių duomenų ir informacinių sistemų trijų savybių visuma leidžia išskirti atskiras BK XXX skyriuje įtvirtintų nusikalstamų veikų grupes.[16] Atitinkamai, tai leidžia išskirti BK 196 straipsnyje kriminalizuotą veiką, kuria pažeidžiamas elektroninių duomenų integralumas ir prieinamumas. Minėta elektroninių duomenų ir informacinių sistemų saugumo aspektų triada paprastai siejama su informacijos sauga[17]. Todėl darbe elektroninių duomenų integralumas ir prieinamumas analizuojami pagrinde remiantis šios srities moksline literatūra.

Kaip pastebi T. Mayfield ir kiti, informacijos saugos bendruomenėje nėra sutariama dėl termino „integralumas“ vieningo apibrėžimo ar priimtinų apibrėžimų viseto. Teigiama, jog, būdamas

[14] "Lietuvos Tarybų Socialistinės Respublikos baudžiamasis kodeksas," *Vyriausybės žinios* 18, 147 (1961) (su vėlesniais pakeitimais ir papildymais).
[15] Renata Marcinauskaitė, *supra* note 4, p. 36.
[16] *Ibid.*, p. 41, 43-44.
[17] John Vacca, *Computer and Information Security Handbook* (Amsterdam: Elsiever, 2009), 256; Michael Whitman ir Herbert Mattord, *Principles of Information Security Fourth Edition* (Boston: Course Technology, 2012), 8-9; Mark Rhodes–Ousley, *Information Security: Second Edition* (New York: The McGraw–Hill, 2013), 85; Darius Štitilis ir Valdas Klišauskas, "Elektroninės informacijos saugos reglamentavimas Lietuvoje ir Rusijoje: lyginamieji aspektai," *Socialinės technologijos* 2, 2 (2012): 443; Saulius Jastiuginas, "Integralus informacijos saugumo valdymo modelis," *Informacijos mokslai* 61 (2012): 8; ir kt.

abstrakčiu daiktavardžiu, integralumas konkrečią prasmę įgauna iš terminų, su kuriais yra vartojamas, dėl jų tarpusavio santykio.[18] Informacijos saugos srityje integralumas paprastai siejamas su duomenimis[19], anot R. S. Sandhu – duomenimis *per se*, t. y. bitais ir baitais[20]. Tačiau, kaip pastebi S. Flowerday ir R. von Solms, kartais terminai „duomenys“ ir „informacija“ naudojami nepakankamai tiksliai, kai kas juos vartoja sinonimiškai. Autorių teigimu, tai lemia sutarimo dėl aptariamų terminų, ypač – termino „informacija“, apibrėžimo nebuvimas.[21] Todėl tinkamam elektroninių duomenų integralumo suvokimui pirmiausia turėtų būti nustatytas duomenų ir informacijos bei jų integralumo tarpusavio santykis[22].

Pasak S. Flowerday ir R. von Solms, informacinių sistemų ir informacinių technologijų srityje pripažįstama seka: įvestis (duomenys) – apdorojimas – išvestis (informacija). Kitaip tariant, apdoroti duomenys tampa informacija. Duomenys (terminas paprastai žymi tiek vienaskaitos (duomuo), tiek daugiskaitos (duomenys) formą) pripažįstami „žaliava“, naudojama „galutiniam produktui“, t. y. informacijai, sukurti. Sistema apdoroja duomenis ir juos paverčia informacija. Informacija gali tapti tiek pradiniai duomenys (po jų apdorojimo – *aut. pastaba*), tiek jų apdorojimo pagrindu gauti išsamesni duomenys. Autorių teigimu, terminas „informacijos integralumas“ pripažįstamas platesniu negu terminas „duomenų integralumas“: siekiant užtikrinti informacijos integralumą, ne tik duomenys, bet ir sistema, kurioje duomenys apdorojami, turi pasižymėti integralumu. Todėl informacijos integralumas negali būti geresnis negu sistemos, kuri apdoroja duomenis ar informaciją, integralumas, nors gali būti blogesnis. Iš kitos pusės, jeigu duomenys jų pateikimo sistemai metu stokos integralumo, tai, nepriklausomai nuo sistemos integralumo, po apdorojimo jie ir toliau gali išlikti neintegraliais.[23] Tai pagrindžia R. Christiaanse ir J. Hulstijn teiginį, kad informacijos integralumui reikalingas (be kita ko – *aut. pastaba*) duomenų integralumas[24].

Pasak A. Birgisson, A. Russo ir A. Sabelfeld, integralumas pasižymi daugiau negu vienu aspektu. Autorių teigimu, saugumui skirtose knygose sutariama dėl sudėtingumo pateikti apibrėžimą,

---

[18] Terry Mayfield et. al., “Integrity in Automated Information Systems,“ p. 5, žiūrėta 2016 05 15, https://www.cs.umd.edu/~waa/414-F11/C-TR-79-91.pdf

[19] James Graham, Richard Howard ir Ryan Olson, *Cyber Security Essentials* (Boca Raton: CRC Press, 2011), 4.

[20] Ravi Sandhu, “On Five Denitions of Data Integrity,“ p. 2, žiūrėta 2016 05 15, http://profsandhu.com/confrnc/ifip/i93int.pdf

[21] Stephen Flowerday ir Rossouw von Solms, “What constitutes information integrity?,” *SA Journal of Information Management* 9, 4 (2007): 2, http://dx.doi.org/10.4102/sajim.v9i4.201

[22] Apie terminų “duomenys” ir “informacija” tarpusavio santykį taip pat žr. šio darbo p. 29-30.

[23] Stephen Flowerday ir Rossouw von Solms, *op. cit.*, p. 2, 7-11.

[24] Rob Christiaanse ir Joris Hulstijn, “Neo–classical Principles for Information Integrity,“ p. 1, žiūrėta 2016 05 15, http://homepage.tudelft.nl/w98h5/Articles/integrity.pdf

atskleidžiantį duomenų integralumo esmę, be to, tyrimai ir mokomoji medžiaga nustato požiūrių į integralumą įvairovę (angl. *identify a range of integrity flavors*).[25]

Skirtingų autorių darbuose integralumas apibūdinamas kaip: elektroninių duomenų vidinės struktūros užbaigtumo bei vientisumo patvirtinimas[26]; savybė, pagrindžianti, kad duomenų saugojimo, apdorojimo ar siuntimo (angl. *in transit*) metu jie be atitinkamų teisėtų įgaliojimų nebuvo pakeisti[27]; galimybė garantuoti duomenų tikslumą ir nuoseklumą viso jų gyvavimo ciklo metu[28]; duomenų tikslumo ir prasmingumo garantija[29]; būklė, kuri egzistuoja, kai duomenys, lyginant su jų šaltiniu, yra nepakeisti ir nebuvo atsitiktinai ar piktavališkai modifikuoti, pakeisti ar sunaikinti[30]; būklė, kuriai esant duomenų turinys ir struktūra nustatyti ir keičiami tik turinčių atitinkamus teisėtus įgaliojimus asmenų ar procesų[31]; duomenų patikimumas[32], neiškreiptumas, pilnumas, adekvatumas[33], preciziškumas (angl. *precise*), tikslumas (angl. *accurate*), nuoseklumas, prasmingumas, teisingumas, modifikavimas tik priimtinu būdu, turinčių atitinkamus teisėtus įgaliojimus asmenų ar procesų[34], modifikacijų be atitinkamų teisėtų įgaliojimų nebuvimas[35] ir kt.

Daugelio autorių darbuose duomenų (informacijos) integralumas bendriausia prasme siejamas su apsauga nuo[36] jų modifikavimo (angl. *modify*)[37]. Dažnai, vietoje modifikavimo, nurodoma

---

[25] Arnar Birgisson, Alejandro Russo ir Andrei Sabelfeld, "Unifying Facets of Information Integrity," p. 1, žiūrėta 2016 05 15, http://www.cse.chalmers.se/~andrei/iciss10.pdf

[26] Renata Marcinauskaitė, "Nusikalstamomis veikomis elektroninėje erdvėje pažeidžiamos pagrindinės baudžiamojo įstatymo saugomos vertybės nustatymo problema," *Socialinių mokslų studijos* 3, 3 (2011): 909.

[27] Gary Stoneburner, "Computer Security: Underlying Technical Models for Information Technology Security: Recommendations of the National Institute of Standards and Technology," p. 2, žiūrėta 2016 05 15, http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf

[28] Fábio Buiati et al., "A Layered Trust Information Security Architecture," *Sensors* 14 (2014): 22759, http://dx.doi.org/10.3390/s141222754

[29] Arnar Birgisson, Alejandro Russo ir Andrei Sabelfeld, *op. cit.*, p. 1.

[30] Rob Christiaanse ir Joris Hulstijn, *supra* note 24, p. 1.

[31] Nikolaj Gajdamakin, *Teoreticheskie osnovy kompjuternoj bezopasnosti. Uchebnoe posobie* [Theoretical Foundations of Computer Security. Textbook] (Jekaterinburg, 2008), 10.

[32] Matt Bishop, *Introduction to Computer Security* (Boston: Addison–Wesley, 2004), 3; Renata Marcinauskaitė, *supra* note 4, p. 44.

[33] Nikolaj Gajdamakin, *op. cit.*, p. 10.

[34] Peng Li, Yun Mao ir Steve Zdancewic, "Information Integrity Policies," p. 1, žiūrėta 2016 05 15, http://www.cis.upenn.edu/~stevez/papers/LMZ03.pdf

[35] James Graham ir Richard Howard, ir Ryan Olson, *supra* note 19, p. 4.

[36] Pažymėtina, jog skirtingų autorių darbuose integralumas siejamas su poveikio duomenims „prevencija", „negalimumu", „apsauga nuo jo", „užtikrinimu, kad jis nebuvo atliktas" ir pan. Tiriamo elektroninių duomenų saugumo aspekto – integralumo – kontekste pasirinktas vartoti žodžių junginys „apsauga nuo".

[37] Abdellateef Muhsen, "Information Security Management in Palestinian Banking," p. 24, žiūrėta 2016 05 15, https://scholar.najah.edu/sites/default/files/Abdellateef%20Muhsen.pdf; Feruza Sattarova ir Kim Tao–hoon, "IT Security Review: Privacy, Protection, Access Control, Assurance and System Security," *International Journal of Multimedia and Ubiquitous Engineering* 2, 2 (2007): 19; Steve Winterfeld ir Jason Andress, *The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice* (Waltham: Elsevier Inc., 2013), 101, http://dx.doi.org/10.1016/B978-0-12-404737-2.00007-0; Per Oscarson, "Information Security Fundamentals: Graphical Conceptualisations for Understanding," iš *Security Education and Critical Infrastructures*, Cynthia Irvine ir Helen Armstrong (Eds.) (Monterey: Springer US, 2003), 98; Georgie Pender–Bey, "The Parkerian Hexad: The CIA Expanded,"

apsauga nuo jų pakeitimo (angl. *change, alter*)[38]. Išsamesniuose apibrėžimuose greta nurodytųjų taip pat minima apsauga nuo duomenų (informacijos) sunaikinimo (angl. *destroy*)[39], sugadinimo (angl. *corrupt, damage*)[40], ištrynimo (angl. *delete*)[41], rečiau – apsauga nuo duomenų (informacijos) sukūrimo[42], įvedimo (angl. *insert*), papildymo (angl. *add*)[43], atnaujinimo (angl. *update*)[44], manipuliavimo[45], kitokio „nagų prikišti prie“ (angl. *tamper with*)[46] duomenų (informacijos) ar kitokio žalingo poveikio jų autentiškai būklei (angl. *other disruption of authentic state*)[47] ir pan. Informacijos saugai skirtoje literatūroje pripažįstama, kad poveikis duomenų (informacijos) integralumui gali būti padarytas ne tik tyčia, bet ir neatsargiai (angl. *unintentionaly*)[48] ar atsitiktinai (angl. *accidental*)[49]. Aptariamas poveikis apima tiek saugomus, tiek apdorojamus, tiek siunčiamus duomenis (informaciją)[50], be to, turi būti neautorizuotas (angl. *unauthorised*)[51], netinkamas (angl. *improper*)[52] ar nepageidaujamas (angl. *undesirable*)[53], kitaip tariant – padarytas be duomenų (informacijos) savininko leidimo[54]. Netinkamas ir nepageidaujamas poveikis duomenų (informacijos) integralumui siejamas su autorizuotais vartotojais[55], kurie poveikį duomenims (informacijai) daro peržengdami suteiktų teisėtų įgaliojimų ribas[56].

---

p. 20, žiūrėta 2016 05 15, http://cs.lewisu.edu/mathcs/msisprojects/papers/georgiependerbey.pdf; Peng Li, Yun Mao ir Steve Zdancewic, *supra* note 34, p. 1.

[38] Mark Rhodes–Ousley, *supra* note 17, p. 86; Jason Andress, *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice 1st Edition* (Waltham: Syngress, 2011), 6; Saulius Jastiuginas, *supra* note 17, p. 8; Gary Stoneburner, *supra* note 27, p. 2; Matt Bishop, *supra* note 32, p. 3; Georgie Pender–Bey, *supra* note 37, p. 12.

[39] Darius Štitilis ir Valdas Klišauskas, *supra* note 17, p. 443; Fábio Buiati et al., *supra* note 28, p. 22759; Michael Whitman ir Herbert Mattord, *supra* note 17, p. 14; James Graham, Richard Howard ir Ryan Olson, *supra* note 19, p. 6.

[40] Michael Whitman ir Herbert Mattord, *op. cit.*, p. 14.

[41] Olga Laponina, *Osnovy setevoj bezopasnosti. Chast 1. Mezhsetevye ehkrany: Uchebnoe posobie* [Network Security Fundamentals. Part 1. Firewalls: Textbook] (Moskva: Nacionalnyj otkrytyj universitet „Intuit“, 2014), 20; Mark Rhodes–Ousley, *op. cit.*, p. 86; Jason Andress, *op. cit.*, p. 5; George Sadowsky et. al., *Information Technology Security Handbook* (Washington DC: O'Reilly Media, Inc., 2003), 102; Terry Mayfield et. al., *supra* note 18, p. 8.

[42] Olga Laponina, *op. cit.*, p. 20.

[43] Terry Mayfield et. al., *op. cit.*, p. 8.

[44] John Vacca, *supra* note 17, p. 256.

[45] Steve Winterfeld ir Jason Andress, *supra* note 37, p. 102.

[46] Fábio Buiati et al., *op. cit.*, p. 22759.

[47] Michael Whitman ir Herbert Mattord, *op. cit.*, p. 14.

[48] Abdellateef Muhsen, *supra* note 37, p. 25.

[49] Georgie Pender–Bey, *op. cit.*, p. 12; Feruza Sattarova ir Kim Tao–hoon, *supra* note 37, p. 19; Darius Štitilis et. al., *supra* note 6, 38.

[50] Michael Whitman ir Herbert Mattord, *op. cit.*, p. 14; Gary Stoneburner, *op. cit.*, p. 2.

[51] Fábio Buiati et al., *op. cit.*, p. 22759; Feruza Sattarova ir Kim Tao–hoon, *op. cit.*, p. 19; James Graham, Richard Howard ir Ryan Olson, *op. cit.*, p. 5; Steve Winterfeld ir Jason Andress, *op. cit.*, p. 101; Per Oscarson, *supra* note 37, p. 98; Mark Rhodes–Ousley, *op. cit.*, p. 86.

[52] Abdellateef Muhsen, *op. cit.*, p. 24; Matt Bishop, *op. cit.*, p. 3.

[53] Georgie Pender–Bey, *op. cit.*, p. 12; Jason Andress, *op. cit.*, p. 5.

[54] George Sadowsky et. al., *op. cit.*, p. 102.

[55] Georgie Pender–Bey, *op. cit.*, p. 12; Jason Andress, *op. cit.*, p. 5.

[56] Matt Bishop, *Computer Security: Art and Science* (Boston: Addison–Wesley, 2003), p. 27.

M. Bishop teigimu, integralumas apima duomenų integralumą (informacijos turinys) ir kilmės integralumą (duomenų šaltinis, dažnai vadinamas autentiškumo nustatymu)[57]. Tai pastebi ir S. Jastiuginas, kuris, apibūdindamas informacijos vientisumą, pažymėjo, kad *„[...] informacija ir jos šaltinis turi būti apsaugoti nuo bet kokio klaidingo ar nesankcionuoto pakeitimo, visi pakeitimai yra žinomi“*[58]. Pasak M. Bishop, duomenų kilmė (kaip ir iš kur jie buvo gauti), tai, kaip tinkamai duomenys buvo apsaugoti iki jų gavimo, pagaliau, tai, ar dabartinėje duomenų buvimo vietoje užtikrinta tinkama jų apsauga – visa tai daro įtaką duomenų integralumui[59].

Apibendrinant tai, kas išdėstyta, elektroninių duomenų integralumą kaip baudžiamojo įstatymo saugomą vertybę būtų galima apibūdinti kaip elektroninių duomenų saugumo aspektą, užtikrinantį, kad tokie duomenys yra nepaveikti arba poveikis, dėl kurio elektroniniai duomenys skiriasi nuo tų duomenų, kurie buvo prieš tokį poveikį, yra teisėtas.

Kalbant apie kitą elektroninių duomenų saugumo aspektą – jų prieinamumą – M. E. Whitman ir H. J. Mattord teigimu, prieinamumas atitinkamus teisėtus įgaliojimus turintiems vartotojams – asmenims ar informacinėms sistemoms – užtikrina galimybę pasiekti informaciją be trukdžių ar kliūčių ir gauti ją reikiamu formatu[60]. Kaip pastebi J. R. Vacca, kai pareikalaujama, informacija turi būti pasiekiama per priimtiną laiko tarpą[61]. C. Schou akcentuoja duomenų ar informacijos paslaugų pasiekiamumo autorizuotiems vartotojams patikimumą. A. P. Martin ir D. Khazanchi teigimu, prieinamumas susijęs su informacijos pasiekiamumu tiek, kiek reikia, kada reikia ir kur reikia.[62] Kaip pastebi M. E. Gladden, kai kurie prieinamumo apibrėžimai jungia du ar daugiau skirtingų tikslų teigiant, jog tikslas yra ne tik užtikrinti, kad duomenys visada būtų prieinami teisėtus įgaliojimus turintiems vartotojams teisėtiems tikslams, bet ir užtikrinti, kad jie visada būtų neprieinami bet kuriems asmenims ar procesams, kurie bando naudoti duomenis (ar didesnę sistemą) neautorizuotiems tikslams[63].

Pasak F. Buiati ir kitų, informacija yra neprieinama ne tik, kai ji prarandama ar sunaikinama, bet ir kai su ja neleidžiama susipažinti vartotojams, kurie turi atitinkamus teisėtus įgaliojimus, ar toks susipažinimas atidedamas[64]. S. Winterfeld teigimu, prieinamumo užtikrinimas reiškia atsparumą

[57] Matt Bishop, *supra* note 32, p. 3.
[58] Saulius Jastiuginas, *supra* note 17, p. 8.
[59] Matt Bishop, *supra* note 56, p. 26-27.
[60] Michael Whitman ir Herbert Mattord, *supra* note 17, p. 12.
[61] John Vacca, *supra* note 17, p. 256.
[62] Andrew Martin ir Deepak Khazanchi, "Information Availability and Security Policy," p. 1257, žiūrėta 2016 05 15, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.99.9445&rep=rep1&type=pdf
[63] Matthew Gladden, *The Handbook of Information Security for Advanced Neuroprosthetics* (Indianapolis: Synthypnion Academic, 2015), 134.
[64] Fábio Buiati et al., *supra* note 28, p. 22759.

atakoms, kurios gali sugadinti ar ištrinti duomenis arba lemti atsisakymą suteikti prieigą prie duomenų atakuojant aplinką, kurioje jie yra. Prieinamumas reikalauja turėti pakankamai atsparią aplinką tam, kad būtų galima susitvarkyti su sistemos trikdžiais (angl. *outages*), komunikacijos problemomis, energijos problemomis ir bet kokiu kitų problemų, kurios gali užkirsti kelią pasiekti duomenis, skaičiumi.[65]

Kaip pastebi M. E. Gladden, informacijos prieinamumo užtikrinimas apima duomenų ir sistemų, kuriose duomenys laikomi ir kuriomis jie pateikiami vartotojams, palaikymą (angl. *maintaining*)[66]. Pasak F. Buiati ir kitų, siekiant garantuoti informacijos prieinamumą nepriklausomai nuo to, kur ji bebūtų, tiek kompiuterinės sistemos, kuriose saugoma ar apdorojama informacija, tiek saugumo kontrolė, naudojama informacijos apsaugai, tiek komunikacijos kanalai, naudojami informacijai pasiekti, privalo funkcionuoti tinkamai ir pagal informacijos saugumo politiką[67]. Šiame kontekste paminėtini mokslinėje literatūroje skiriami informacijos prieinamumą sudarantys komponentai: patikimumas, pasiekiamumas ir savalaikiškumas. Patikimumas čia suprantamas kaip tikėtinumas, kad sistema pagal paskirtį adekvačiai veiks numatytą laiko tarpą tokiomis eksploatavimo sąlygomis, su kuriomis susidurs. Kitaip tariant, nepageidaujama pasikliauti sistema, kuria nepasitikima kaip galinčia nuosekliai vykdyti vartotojų užklausas. Pasiekiamumas žymi lygį, iki kurio sistema gali būti naudojama kiek įmanoma didesnio žmonių skaičiau be jos modifikavimo. Savalaikiškumas – tai galimybė laiku pasiekti informaciją ar tarnybas (angl. *services*). Savalaikiškumas žymi sistemos ar resursų reagavimą į vartotojo užklausas.[68]

Apibendrinant tai, kas išdėstyta, elektroninių duomenų prieinamumą kaip baudžiamojo įstatymo saugomą vertybę būtų galima apibūdinti kaip jų saugumo aspektą, užtikrinantį, kad sąlygos, kuriomis tokie duomenys įprastai gali būti teisėtai paveikti ar kitokiu būdu valdomi, naudojami ar jais disponuojama, nėra neteisėtai neigiamai paveiktos.

[65] Steve Winterfeld ir Jason Andress, *supra* note 37, p. 102.
[66] Matthew Gladden, *supra* note 63, p. 133.
[67] Fábio Buiati et al., *supra* note 28, p. 22759.
[68] Suhail Mir et al., "Information Availability: Components, Threats and Protection Mechanisms," *Journal of Global Research in Computer Science* 2, 3 (2011): 22, http://www.rroij.com/open-access/information-availability-components-threats-and-protection-mechanisms-21-26.pdf

2. NETEISĖTO POVEIKIO ELEKTRONINIAMS DUOMENIMS KRIMINALIZAVIMO RAIDA

Pasak D. Štitilio ir kitų, (2003 m. gegužės 1 d. įsigaliojus naujajam baudžiamajam įstatymui – *aut. pastaba*) Lietuva užtikrino formalią kompiuterinės informacijos ir kompiuterinių programų integralumo baudžiamąją teisinę apsaugą, nustatydama atsakomybę BK 196 ir 197 straipsniuose[69]. Reikalas tas, kad pirminėse šių straipsnių redakcijose atskirai kriminalizuotas kompiuterinės informacijos (BK 196 straipsnis) ir *inter alia*[70] kompiuteryje esančios programos (BK 197 straipsnis) sunaikinimas, sugadinimas ar pakeitimas padarant didelę žalą (toliau – ir BK 197 straipsnis aptariamoje dalyje). Dar iki 2000 m. BK įsigaliojimo G. Sabaliauskas pastebėjo, kad aptariami BK straipsniai dubliuoja vienas kitą[71]. Tam pritardamas D. Sauliūnas pažymėjo, jog kompiuterinė programa yra kompiuterinės informacijos rūšis[72], be to, sankcijos rodo, kad įstatymų leidėjas šias nusikalstamas veikas iš esmės laiko vienodai pavojingomis. Taigi įstatymų leidėjas vienodai vertina kompiuterinę informaciją ir kompiuteryje esančią programą. Todėl pasirinkimas šias nusikalstamas veikas išskirti į atskirus straipsnius atrodo keistas.[73]

R. Petrausko ir D. Štitilio teigimu, *„rengiant naująjį Kodeksą ir ypač jo normas, numatančias atsakomybę už kompiuterinius nusikaltimus internete, buvo atsižvelgta į Europos Tarybos rekomendaciją R 89(9) Europos Sąjungos šalių vyriausybėms, kurioje siūloma keičiant esamus arba kuriant naujus įstatymus atsižvelgti į Europos komiteto nusikaltimų problemoms tirti siūlomus minimalų ir neprivalomą sąrašus“*[74]. Tačiau EKNPT baigiamosios ataskaitos II skyriaus 2 dalies c punkte vienoje dispozicijoje įtvirtinta kompiuterinių programų ar duomenų sugadinimo (angl. *damage to computer data or programs*) veika rekomenduota kriminalizuoti, be kita ko, neteisėtą kompiuterinių duomenų ar kompiuterinių programų ištrynimą (angl. *erasure*), pabloginimą (angl. *deterioration*), prieigos prie jų apribojimą (angl. *suppression of*). Šiame kontekste atviru lieka klausimas, kodėl įstatymų leidėjas atsakomybę už poveikį kompiuterinei informacijai ir kompiuteryje esančiai programai kriminalizavo skirtinguose BK straipsniuose. Diskutuotina, dėl kokių priežasčių

[69] Darius Štitilis et. al., *supra* note 6, p. 264.
[70] Pirminėje BK 197 straipsnio redakcijoje taip pat kriminalizuotas programos, kuri sutrikdė ar pakeitė kompiuterinio tinklo, duomenų banko ar informacinės sistemos darbą, įdiegimas į kompiuterį ar kompiuterinį tinklą padarant didelės žalos.
[71] Giedrius Sabaliauskas, “Informacijos saugumas internete: teisininkų ir informatikų problema,“ *Justitia* 2, (2001): 26.
[72] Darius Sauliūnas, “Legislation on Cybercrime in Lithuania: Development and Legal Gaps in Comparison with the Convention on Cybercrime,“ *Jurisprudencija* 4, 122 (2010): 207.
[73] Darius Sauliūnas et. al., *supra* note 7, p. 533.
[74] Rimantas Petrauskas ir Darius Štitilis, “Lietuvos Respublikos baudžiamasis kodeksas nusikaltimų elektroninėje erdvėje konvencijos kontekste,“ *Jurisprudencija* 24, 16 (2002): 83.

pirminėje BK 196 straipsnio redakcijoje pasirinkta, lyginant su kompiuteriniais duomenimis, siauresnė[75] – kompiuterinės informacijos – integralumo baudžiamoji teisinė apsauga. Pagaliau, nėra aišku, kodėl apsiribota siauresniu kompiuterinės informacijos ir kompiuterinių programų integralumą pažeidžiančių pavojingų veikų spektru, neįtvirtintas šių veikų neteisėtumo reikalavimas, neužtikrinta kompiuterinės informacijos ir kompiuterinių programų prieinamumo baudžiamoji teisinė apsauga. Tai leidžia teigti, kad kriminalizuojant aptariamas veikas į EKNPT baigiamąją ataskaitą atsižvelgta tik iš dalies.

Pirmieji BK 196 straipsnio ir BK 197 straipsnio aptariamoje dalyje pakeitimai atlikti 2004 m. nacionalinę teisę derinant su Konvencijos dėl elektroninių nusikaltimų nuostatomis[76]. Atsižvelgiant į Konvencijos 4 straipsnyje įtvirtintą poveikio duomenims veiką, šiuose BK straipsniuose įtvirtintas pavojingų veikų neteisėtumo reikalavimas. Be to, kriminalizavus kompiuterinės informacijos ir kompiuteryje esančios programos neteisėtą pašalinimą, taip pat neteisėtą naudojimosi kompiuterine informacija apribojimą įrenginiais ar kompiuterinėmis programomis užtikrinta jų prieinamumo baudžiamoji teisinė apsauga. Paminėtina ir tai, kad įstatyme dėl Konvencijos dėl elektroninių nusikaltimų ratifikavimo Lietuva numatė išlygą, *„[...] kad už Konvencijos 4 straipsnyje nurodytų veikų padarymą baudžiamoji atsakomybė atsiranda padarius didelę žalą“*[77]. Tačiau kadangi šis pavojingų padarinių požymis buvo įtvirtintas aptariamų BK straipsnių pirminėse redakcijose, pakeitimai nurodytoje dalyje nebuvo reikalingi[78].

Kita vertus, neatsižvelgiant į Konvencijos 1 straipsnio b punkte pateiktą kompiuterinių duomenų apibrėžimą, taip pat jos 4 straipsnio 1 dalies dispozicijoje tiesiogiai minimus kompiuterinius duomenis, BK 196 straipsnyje kriminalizuotos veikos dalyku išliko siauresnė kompiuterinė informacija. Į tai dėmesį atkreipė D. Sauliūnas, kuris papildomai pažymėjo, kad *„[...] konvencija neskiria kompiuterinių duomenų ir kompiuterinės programos sąvokų, kaip tai yra padaryta Lietuvos BK XXX skyriuje. Konvencijoje kompiuterinės programos laikomos sudarytomis iš kompiuterinių duomenų ir todėl jų esmė nesikeičia“*[79]. Taigi atliktų pakeitimų pagrindu nebuvo išspręsta ir minėta

[75] Apie terminų “duomenys” ir “informacija” tarpusavio santykį plačiau žr. šio darbo p. 10, 29-30.
[76] “Lietuvos Respublikos baudžiamojo kodekso 13, 162, 191, 196, 197, 203, 206, 216, 219, 221, 309 straipsnių pakeitimo ir papildymo bei kodekso papildymo 198-1 ir 198-2 straipsniais įstatymas,“ *Valstybės žinios* 45, 760 (2004).
[77] “Lietuvos Respublikos įstatymas dėl Konvencijos dėl elektroninių nusikaltimų ratifikavimo,“ *Valstybės žinios* 36, 1178 (2004).
[78] Įdomu tai, kad svarstant *inter alia* BK 196 straipsnio pakeitimo įstatymo projektą Lietuvos Aukščiausiasis Teismas atkreipė dėmesį į didelės žalos požymio abstraktumą ir jo oficialaus autentiško aiškinimo poreikį. Tačiau tam nebuvo pritarta, argumentuojant tuo, kad, *„atsižvelgiant į BK struktūrą, netikslinga ir sudėtinga įstatymų leidėjui būtų detalizuoti vertinamąjį didelės žalos požymį. Šios sąvokos turinys turėtų būti atskleistas teismų praktikoje“.* Plačiau žr. “Komiteto išvada Baudžiamojo kodekso 13, 162, 191, 196, 197, 203, 206, 216, 219, 221, 309 straipsnių pakeitimo ir papildymo bei Kodekso papildymo 198(1) ir 198(2) straipsniais įstatymo projektui,“ (2004).
[79] Darius Sauliūnas et. al., *supra* note 7, p. 538.

BK 196 straipsnio ir BK 197 straipsnio aptariamoje dalyje persidengimo problema[80]. Be to, bent jau pasitelkus lingvistinį aiškinimą, nėra aišku, kuri iš šiuose BK straipsniuose įtvirtintų pavojingų veikų atitinka Konvencijos 4 straipsnyje įtvirtintas kompiuterinių duomenų neteisėto ištrynimo (angl. *deletion*), pabloginimo (angl. *deterioration*) pavojingas veikas. Pagaliau, BK 196 straipsnyje įtvirtinus baigtinį naudojimosi kompiuterine informacija apribojimo būdų sąrašą (įrenginius ar kompiuterines programas[81]) kompiuterinės informacijos prieinamumo baudžiamoji teisinė apsauga tapo siauresnė lyginant su reikalaujama Konvencijos 4 straipsnyje, kuriame kompiuterinių duomenų prieinamumo apsauga nėra ribojama pavojingos veikos padarymo būdais.

BK 196 ir 197 straipsniai baudžiamojo įstatymo lygiu atriboti tik 2007 m. nacionalinėje teisėje įgyvendinus[82] 2005 m. vasario 24 d. Tarybos pamatinio sprendimo 2005/222/TVR dėl atakų prieš informacines sistemas (toliau – ir Pamatinis sprendimas 2005/222/TVR)[83] nuostatas. Atsižvelgiant į Pamatinio sprendimo 2005/222/TVR 1 straipsnio b punkte suformuluotą kompiuterinių duomenų apibrėžimą, taip pat jo 4 straipsnyje įtvirtintos neteisėto įsikišimo į duomenis veikos dispozicijoje tiesiogiai minimus kompiuterinius duomenis, patikslintas BK 196 straipsnyje kriminalizuotos veikos dalykas – kompiuterinė informacija pakeista elektroniniais duomenimis. Tokiu būdu užtikrinta, R. Marcinauskaitės žodžiais, elektroninių duomenų, esančių iki informaciniame etape[84], baudžiamoji teisinė apsauga. Atitinkamai, senasis BK 196 straipsnio pavadinimas „kompiuterinės informacijos sunaikinimas ar pakeitimas“ pakeistas nauju – „neteisėtas poveikis elektroniniams duomenims“. Atsižvelgiant į Lietuvos Respublikos generalinės prokuratūros pastabą, jog *„[...] galimi atvejai, kuomet naudojimasis elektroniniais duomenimis bus apribotas ne*

[80] Įdomu tai, kad aptariamų pakeitimų svarstymo metu Lietuvos Aukščiausiasis Teismas siūlė apsvarstyti galimybę BK 196 straipsnį sujungti su 197 straipsniu dėl jų panašumo savo paskirtimi ir sankcijomis. Tačiau tam nebuvo pritarta, teigiant, jog nurodytuose straipsniuose įtvirtintas skirtingas nusikalstamos veikos dalykas. Beje, tai, kad įstatymo projekte siūloma BK 197 straipsnio redakcija ne visiškai atitinka Konvencijos 5 straipsnį pažymėjo Lietuvos teisės institutas ir Vilniaus universiteto Teisės fakultetas. Tačiau pastaruoju atveju problema įžvelgta tik didelės žalos kaip pavojingų padarinių požymio neatitikime Konvencijos 5 straipsnyje įtvirtintam dideliam kompiuterinės sistemos darbo trukdymui. Plačiau žr. "Komiteto išvada Baudžiamojo kodekso 13, 162, 191, 196, 197, 203, 206, 216, 219, 221, 309 straipsnių pakeitimo ir papildymo bei Kodekso papildymo 198(1) ir 198(2) straipsniais įstatymo projektui," (2004).

[81] Įdomu, jog tai padaryta atsižvelgus į Lietuvos Aukščiausiojo Teismo pastabą, kad *„[...] neaišku už kokio pobūdžio veiksmus bus nustatyta baudžiamoji atsakomybė. Juk apriboti naudojimąsi kompiuterine informacija galima tiek fizinės jėgos, tiek ir techninių priemonių pagalba. Akivaizdu, kad šiuo atveju kalbėti apie fizinės jėgos vartojimą netikslinga ir nelogiška. Dėl šios priežasties siūlome po žodžio „arba" įrašyti žodžius „kokių nors įrenginių ar kompiuterinių programų pagalba""*. Plačiau žr. *ibid*.

[82] "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* 81, 3309 (2007).

[83] "Tarybos pamatinis sprendimas 2005/222/TVR 2005 m. vasario 24 d. dėl atakų prieš informacines sistemas," *Oficialusis leidinys L* 69, 67 (2005).

[84] Renata Marcinauskaitė, *supra* note 4, 47.

tik įrenginiais ar programine įranga, bet kitais būdais (pvz., perpjovus kabelį, kuriuo perduodami elektroniniai duomenys), juo labiau, kad sparčiai vystantis technologijoms gali atsirasti nauji duomenų perdavimo sutrikdymo būdai, kurių neapimtų sąvokos „įrenginiai“ ar „programinė įranga““[85], BK 196 straipsnyje įtvirtintas nebaigtinis naudojimosi elektroniniais duomenimis apribojimo būdų sąrašas. Tokiu būdu elektroninių duomenų prieinamumo baudžiamosios teisinės apsaugos ribos išplėstos iki reikalaujamų minėtuose viršnacionalinės teisės aktuose. BK 196 straipsnis papildytas 2 dalimi, kurioje įtvirtintas nusikalstamą veiką kvalifikuojantis požymis: strateginę reikšmę nacionaliniam saugumui ar didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinčios informacinės sistemos elektroniniai duomenys[86]. Tokiu būdu įgyvendintas Pamatinio sprendimo 2005/222/TVR 7 straipsnio 2 dalyje įtvirtintas reikalavimas nustatyti griežtesnes sankcijas atvejams, kai nusikaltimas padarė poveikio esminiams interesams. Pagaliau, BK 196 straipsnis papildytas 3 dalimi, kurioje įtvirtintas nusikalstamą veiką privilegijuojantis požymis – nedidelė žala kaip pavojingi padariniai. Tokiu būdu BK 196 straipsnyje žala pagal dydį diferencijuota į nedidelę (3 dalis), ir didelę (1, 2 dalis).

Aptariamų BK 196 straipsnio pakeitimų svarstymo metu kilo abejonių dėl Pamatinio sprendimo 2005/222/TVR 4 straipsnyje įtvirtintų pavojingų veikų įgyvendinimo nacionalinėje teisėje tinkamumo. Europos teisės departamentas prie Teisingumo ministerijos pažymėjo, kad *„[...] turėtų būti perkeltos visos pamatinio sprendimo 4 straipsnyje minimos veikos, tai yra ištrynimas, sugadinimas, pažeidimas, pakeitimas, nuslėpimas ar prieigos užkirtimas“*[87]. Lietuvos Aukščiausiasis Teismas į tai dėmesį atkreipė kiek kitaip, nurodydamas, jog *„[...] keičiami BK XXX skyriaus straipsniai savo turiniu turi atitikti 2005 m. vasario 24 d. Tarybos pamatinio sprendimo 2005/222/TVR dėl atakų prieš informacines sistemas 4 straipsnyje minimas veikas“*[88]. Iš tiesų, bent jau pasitelkus lingvistinį aiškinimą, nėra aišku, kuri iš BK 196 straipsnyje įtvirtintų pavojingų veikų atitinka Pamatinio sprendimo 2005/222/TVR 4 straipsnyje įtvirtintas neteisėto kompiuterinių duomenų ištrynimo (angl. *deletion*), pabloginimo (angl. *deterioration*) pavojingas veikas. Pagaliau, BK 196 straipsnio 3 dalyje įtvirtinus nedidelės žalos požymį, išlygos, kurią Lietuva padarė

[85] "Komiteto išvada Baudžiamojo kodekso XXX skyriaus pavadinimo, 166, 167, 194, 196, 197, 198, 198(1), 198(2), 213, 214, 215, 262 straipsnių pakeitimo, Kodekso papildymo 257(1) straipsniu ir priedo papildymo įstatymo projektui," (2007).
[86] Įdomu, jog tai padaryta atsižvelgus į Lietuvos Respublikos teisingumo ministerijos pastabą, kad *„[...] svarbiau akcentuoti informacinės sistemos svarbą valstybės saugumui arba valstybės ūkiui ar finansinei sistemai, o ne įstaigos ar įmonės svarbą [...]“*, kaip, kad buvo siūloma pirmiau, bei šios biudžetinės įstaigos papildomam siūlymui *„[...] į šią kvalifikuotą nusikaltimo sudėtį įtraukti ne tik strateginę reikšmę turinčias įmones, bet ir valstybės ar savivaldybės įstaigas, kitas organizacijas“*. Plačiau žr. *ibid*.
[87] *Ibid*.
[88] *Ibid*.

ratifikuodama Konvenciją dėl elektroninių nusikaltimų, *„[...] kad už Konvencijos 4 straipsnyje nurodytų veikų padarymą baudžiamoji atsakomybė atsiranda padarius didelę žalą“*[89], atsisakyta tiek, kiek tai susiję su žalos dydžiu – didele žala – kaip baudžiamosios atsakomybės pagrindu, bet ne žalos kaip pavojingų padarinių požymio įtvirtinimu.

Paskutiniai BK 196 straipsnio pakeitimai siejami su 2013 m. rugpjūčio 12 d. Europos Parlamento ir Tarybos direktyvos 2013/40/ES dėl atakų prieš informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR (toliau – ir Direktyva 2013/40/ES)[90] įgyvendinimu nacionalinėje teisėje 2015 m.[91]. Atliktų pakeitimų pagrindu BK 196 straipsnio 2 dalyje įtvirtinti du nauji nusikalstamą veiką kvalifikuojantys požymiai: neteisėtas poveikis daugelio informacinių sistemų elektroniniams duomenims ir neteisėtas poveikis elektroniniams duomenims pasinaudojant svetimais asmens duomenimis. Šiais pakeitimais įgyvendintos Direktyvos 2013/40/ES preambulės 5, 13 punktų, 9 straipsnio 3, 5 dalių nuostatos, kuriose dėmesys skiriamas *inter alia* plataus masto elektroninėms atakoms prieš informacines sistemas, vadinamųjų „botnetų“ kūrimui ir naudojimui, neteisėtam įsikišimui į duomenis piktnaudžiaujant kito asmens duomenimis siekiant įgyti trečiosios šalies pasitikėjimą, tokiu būdu padarant žalą teisėtam tapatybės turėtojui. Kita vertus, dėl šių pataisų tapo neaiškiu pasinaudojimo svetimais asmens duomenimis ir informacinės sistemos apsaugos priemonių pažeidimo požymių tarpusavio santykis, kuris savo ruožtu iškėlė BK 196 straipsnio 2 dalies ir BK 198[1] straipsnio galimos konkurencijos klausimą[92]. Paminėtina ir tai, kad atliktų pakeitimų pagrindu BK 196 straipsnyje žala pagal dydį diferencijuota į nedidelę (3 dalis), vidutinę (1 dalis) bei didelę (2 dalis). Vis dėlto, bent jau pasitelkus lingvistinį aiškinimą, nėra aišku, kuri iš BK 196 straipsnyje įtvirtintų pavojingų veikų atitinka Direktyvos 2013/40/ES 5 straipsnyje įtvirtintas neteisėto kompiuterinių duomenų ištrynimo (angl. *deleting*), pabloginimo (angl. *deteriorating*) pavojingas veikas.

Neteisėto poveikio elektroniniams duomenims kriminalizavimo raida atskleidė, *pirma*, EKNPT baigiamosios ataskaitos, Konvencijos dėl elektroninių nusikaltimų, Pamatinio sprendimo 2005/222/TVR, Direktyvos 2013/40/ES ryšį su BK 196 straipsniu. Taigi analizuojant neteisėto poveikio elektroniniams duomenims sudėties požymius būtina atsižvelgti į nurodytuose

[89] “Lietuvos Respublikos įstatymas dėl Konvencijos dėl elektroninių nusikaltimų ratifikavimo,“ *Valstybės žinios* 36, 1178 (2004).
[90] “Europos Parlamento ir Tarybos direktyva 2013/40/ES dėl atakų prieš informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR,“ *Oficialusis leidinys L* 218, 8 (2013).
[91] “Lietuvos Respublikos baudžiamojo kodekso 7, 196, 197, 198-1, 198-2 straipsnių ir priedo pakeitimo ir Kodekso papildymo 270-3 straipsniu įstatymas,“ *Valstybės žinios* 2015-09697 (2015).
[92] Apie BK 196 straipsnio 2 dalies ir BK 198[1] straipsnio konkurenciją plačiau žr. šio darbo p. 75-77.

viršnacionalinės teisės aktuose suformuluotas nuostatas. Tačiau svarbu prisiminti rekomendacinį EKNPT ataskaitos pobūdį. Be to, kaip pastebi R. Marcinauskaitė, *„[...] analizuojant įvairius tarptautinių ir Europos Sąjungos teisės aktų reikalavimų įgyvendinimo aspektus pirmiausia pažymėtina, kad ne visos valstybės yra ratifikavusios Konvenciją dėl elektroninių nusikaltimų ir tik Europos Sąjungos valstybėms narėms privalomas Pamatinis sprendimas 2005/222/TVR* (taip pat Direktyva 2013/40/ES – *aut. pastaba*). *Antra, atkreiptinas dėmesys 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. [...] Į tai turėtų būti atsižvelgiama analizuojant įvairias mokslininkų išsakomas idėjas ir bandant spręsti nacionalinėje baudžiamojoje teisėje kylančias [...]* (neteisėto poveikio elektroniniams duomenims – *aut. pastaba*) *veikos inkriminavimo problemas“*[93]. *Antra*, neteisėto poveikio elektroniniams duomenims veikos atitikimas susijusių viršnacionalinės teisės aktų reikalavimams iš esmės užtikrintas tik 2007 m. nacionalinėje teisėje įgyvendinus Pamatinio sprendimo 2005/222/TVR nuostatas. Vis dėlto, bent jau pasitelkus lingvistinį aiškinimą, nėra aišku, kuri iš BK 196 straipsnyje įtvirtintų pavojingų veikų atitinka EKNPT baigiamosios ataskaitos II skyriaus 2 dalies c punkte, Konvencijos dėl elektroninių nusikaltimų 4 straipsnio 1 dalyje, Pamatinio sprendimo 2005/222/TVR 4 straipsnyje, Direktyvos 2013/40/ES 5 straipsnyje įtvirtintas neteisėto kompiuterinių duomenų (programų) ištrynimo (angl. *erasure* ar *deletion*), pabloginimo (angl. *deterioration*) pavojingas veikas. *Pagaliau*, 2015 m. atliktų pakeitimų pagrindu kriminalizavus neteisėtą poveikį elektroniniams duomenims pasinaudojant svetimais asmens duomenimis iškilo BK 196 straipsnio 2 dalies ir BK 198^1 straipsnio galimos konkurencijos klausimas.

[93] Renata Marcinauskaitė, *supra* note 4, p. 52.

3. NETEISĖTO POVEIKIO ELEKTRONINIAMS DUOMENIMS KRIMINALIZAVIMO PAGRINDIMAS, BAUDŽIAMASIS TEISINIS REGULIAVIMAS PASIRINKTOSE UŽSIENIO VALSTYBĖSE

Pasak R. Marcinauskaitės, *„neteisėto prisijungimo prie IS kaip nusikalstamos veikos įtvirtinimas Lietuvos BK sietinas su [...] ekvivalentaus elgesio fizinėje ir elektroninėje erdvėje vertinimo principo, o tiksliau su funkcinio ekvivalentiškumo įgyvendinimu. [...] sprendžiant CIA nusikalstamų veikų baudžiamojo teisinio vertinimo problemas, jos 2000 m. BK kriminalizuotos kaip delicta sui generis“*[94]. Tai leidžia teigti, kad neteisėto poveikio elektroniniams duomenims kriminalizavimas 2000 m. BK kaip *delicta sui generis* taip pat sietinas su ekvivalentiškumo principo įgyvendinimu. Tačiau žvelgiant istoriniu aspektu, mokslinėje literatūroje neteisėto poveikio elektroniniams duomenims kriminalizavimas kaip *delicta sui generis* grindžiamas šios veikos atribojimu nuo nusikalstamų veikų nuosavybei, o tiksliau – nuo turto sunaikinimo ar sugadinimo veikos.

Pasak J. Clough, praeityje neteisėtas poveikis elektroniniams duomenims, iš dalies sėkmingai, kvalifikuotas kaip turto sunaikinimo ar sugadinimo veika (angl. *criminal damage*)[95]. Pastaroji, I. Walden teigimu, gali būti reikšminga daugelyje situacijų, kuriose kompiuteris yra nusikalstamos veikos dalykas. Tačiau kompiuterinės sistemos vertė dažnai slypi ne fizinėje techninėje įrangoje, o joje saugomoje informacijoje, programinėje įrangoje ir duomenyse. Kokia apimtimi kompiuterinės informacijos neteisėtas ištrynimas ar modifikavimas lemia žalos turtui padarymą (angl. *damage to property*)? Šis klausimas spręstas *Cox v Riley* (1986) byloje, kurioje darbuotojas kaltintas tuo, kad iš plastikinės grandinės kortos (angl. *plastic circuit card*) ištrynė kompiuterinę programą, reikalingą kompiuterizuotam pjūklui veikti. Byloje teismas pažymėjo, kad programos ištrynimas turto – plastikinės grandinės kortos – sugadinimą lėmė tiek, kiek veika pakenkė kortos vertei ir naudingumui bei pareikalavo laiko, darbo ir pinigų jos veikimui atkurti. Pastaruoju aiškinimu buvo remtasi ir *R v Whiteley* (1991) byloje, kurioje teismas pažymėjo, kad 1971 m. Turto sunaikinimo ar sugadinimo aktas (angl. *Criminal Damage Act*) reikalauja įrodyti, jog buvo sužalotas materialus turtas, o ne būtinai materialų žalos pobūdį.[96] Kita vertus, kaip pastebi J. Clough, turto sunaikinimo ar sugadinimo veika apima ne visą neteisėto poveikio duomenims veikos spektrą ir yra pagrįsta nuosavybei būdingomis savybėmis, kurių taikymas duomenims buvo „labiau išradingas negu

[94] Renata Marcinauskaitė, *supra* note 4, p. 51.
[95] Jonathan Clough, *supra* note 10, p. 101.
[96] Ian Walden, *supra* note 9, p. 173.

praktiškas“[97]. Todėl, pasak I. Walden, nepaisant minėtų sėkmingų baudžiamųjų persekiojimų, išliko neapibrėžtumas netinkamo kompiuterių naudojimo veikas kvalifikuojant pagal 1971 m. Turto sunaikinimo ar sugadinimo aktą. Be to, susirūpinimą kėlė galimos situacijos, kuriose būtų sudėtinga nustatyti materialų turtą, kuriam padaryta žala, pvz., ištrynus viešuoju telefonų tinklu perduodamą informaciją. Kita problema susijusi su sunkumais praktikoje aiškinant teisėjams, magistratams ir prisiekusiesiems kaip faktai aptariamame kontekste dera su esamu turto sunaikinimo ar sugadinimo nusikalstamos veikos teisiniu reguliavimu. Dėl šių priežasčių Teisės komisija pasiūlė kriminalizuoti naują veiką 1990 m. Netinkamo kompiuterių naudojimo akte (angl. *Computer Misuse Act*). Šio akto 3 straipsniu[98] žalos koncepcija pagal 1971 m. Turto sunaikinimo ar sugadinimo aktą pakeista tokia apimtimi, jog kompiuterio turinio modifikavimas nepripažįstamas žala (angl. *damage*), todėl nekvalifikuojamas pagal 1971 m. Turto sunaikinimo ar sugadinimo aktą, nebent poveikis kompiuteriui ar kompiuterinei laikmenai pakenktų jų fizinei būklei.[99] Taigi kaip taikliai pastebi J. Clough, turi būti daromas skirtumas tarp kompiuterio fizinio sužalojimo (angl. *physical damage to a computer*) ir žalos, padarytos kompiuterio eksploatavimu (angl. *operation of a computer*)[100]. Šiame kontekste pažymėtina, jog EKNPT baigiamosios ataskaitos II skyriaus 2 dalies c punkte ir Konvencijos aiškinamosios ataskaitos 60 punkte nurodyta, kad, atitinkamai, kompiuterinių programų ar duomenų sugadinimo veika ir poveikio duomenims veika siekiama užtikrinti analogišką taikomai materialiems dalykams kompiuterinių duomenų ir kompiuterinių programų apsaugą nuo tyčinės žalos padarymo (angl. *damage*)[101]. Manytina, tai leidžia įžvelgti neteisėto poveikio elektroniniams duomenims kriminalizavimo kaip *delicta sui generis* pagrindimą poreikiu kriminalizuoti pavojingas veikas, kurioms kvalifikuoti yra nepakankamos tradicinių nusikalstamų veikų sudėtys.

Manytina, EKNPT baigiamosios ataskaitos II skyriaus 2 dalies c punkte aptiktinas kitas neteisėto poveikio elektroniniams duomenims veikos kriminalizavimo kaip *delicta sui generis* pagrindimo aspektas. Čia pažymėta, jog, siekiant užtikrinti efektyvią programinės įrangos ar duomenų apsaugą nuo piktavališko sužalojimo (angl. *damage*) ar trukdymo jais naudotis (angl. *interference*), pageidautina sukurti papildomas nuostatas, siejamas su veika ir jos neatidėliotinais padariniais (angl. *immediate effect*) programinei įrangai ar saugomiems duomenims, o ne nutolusiems padariniams visai

[97] Jonathan Clough, *supra* note 10, p. 101.
[98] Kuriame kriminalizuota kompiuterių darbo pabloginimo ir pan., ketinant tai padaryti arba padarant tai dėl neatsargumo (angl. *recklessness*), veika. Plačiau žr. Computer Misuse Act 1990, žiūrėta 2016 05 15, http://www.legislation.gov.uk/ukpga/1990/18/crossheading/computer-misuse-offences
[99] Ian Walden, *supra* note 9, p. 173-174.
[100] Jonathan Clough, *op. cit.*, 102.
[101] Council of Europe, *supra* note 11, p. 45; Committee of Ministers of the Council of Europe, *supra* note 13, p. 11.

sistemai[102]. Tai leidžia manyti, kad neteisėto poveikio elektroniniams duomenims veikos kriminalizavimas kaip *delicta sui generis* gali būti grindžiamas poreikiu baudžiamąją teisinę apsaugą užtikrinti anksčiau negu etape, kuriame prasideda ta, kurią teikia neteisėto poveikio informacinei sistemai nusikalstama veika. Paprasčiau tariant, tai gali būti grindžiama poreikiu kriminalizuoti veikas ankstyvajame etape, nelaukiant kol pasireikš neteisėtas poveikis informacinei sistemai.

Pasirinktų užsienio valstybių baudžiamojo teisinio reguliavimo analizė atskleidė skirtingus neteisėto poveikio elektroniniams duomenims kriminalizavimo variantus. Valstybių, kurios yra Konvencijos dėl elektroninių nusikaltimų dalyvės, baudžiamieji įstatymai skiriasi *inter alia* pagal tai, ar juose įtvirtintas didelės žalos požymis (atsižvelgiant į Konvencijos 4 straipsnio 2 dalyje numatytą išlygos galimybę).

Valstybėms, kurių baudžiamuosiuose įstatymuose nėra įtvirtintas didelės žalos požymis, priskirtina Kanada, kurios baudžiamojo kodekso 430 (1.1) straipsnyje kriminalizuota su kompiuteriniais duomenimis susijusi piktadarybė (angl. *mischief*) apibrėžta kaip *tyčinis kompiuterinių duomenų sunaikinimas, pakeitimas, pavertimas beprasmiais, nenaudotinais ar neefektyviais arba kliudymas, pertraukimas ar kišimasis į teisėtą kompiuterinių duomenų naudojimą, arba kliudymas, pertraukimas ar kišimasis prie asmens dėl teisėto kompiuterinių duomenų naudojimo* (angl. *in the lawful use of computer data*) *ar atsisakymas suteikti prieigą prie kompiuterinių duomenų asmeniui, turinčiam tam teisę*[103]. Albanijos Respublikos baudžiamojo kodekso 293/b straipsnyje, kuriame kriminalizuota kišimosi į kompiuterinius duomenis veika, didelės žalos požymis taip pat nėra įtvirtintas: *neteisėtas kompiuterinių duomenų sugadinimas, iškreipimas* (angl. *distorting*), *modifikavimas, ištrynimas ar prieigos prie jų apribojimas*. Šiame straipsnyje nusikalstamą veiką kvalifikuojančiais požymiais pripažįstami: kišimasis į karinius, nacionalinio saugumo, viešosios tvarkos, civilinės apsaugos, su sveikata susijusius kompiuterinius duomenis ar kitus kompiuterinius duomenis, turinčius visuomeninę reikšmę.[104]

Valstybėms, kurių baudžiamuosiuose įstatymuose įtvirtintas didelės žalos požymis, priskirtina Latvijos Respublika, kurios baudžiamojo kodekso 243 straipsnio 1 dalyje kriminalizuota kišimosi į automatinio duomenų apdorojimo sistemų veiklą ir neteisėtų veiksmų prieš tokiose sistemose esančią informaciją veika apibrėžta kaip *neteisėtas automatinio duomenų apdorojimo*

[102] Council of Europe, *supra* note 11, p. 43.
[103] Criminal Code of Canada, žiūrėta 2016 05 15, http://laws-lois.justice.gc.ca/eng/acts/c-46/page-88.html#h-116 Kanada Konvenciją dėl elektroninių nusikaltimų ratifikavo 2015 m. liepos 8 d.
[104] Criminal Code of the Republic of Albania, žiūrėta 2016 05 15, http://www.legislationline.org/download/action/download/id/5164/file/Albania_CC_am2013_en.pdf Albanija Konvenciją dėl elektroninių nusikaltimų ratifikavo 2002 m. birželio 20 d.

sistemoje laikomos informacijos modifikavimas, sugadinimas, sunaikinimas, pabloginimas (angl. *impairing*), *nuslėpimas ar sąmoningas neteisingos informacijos įvedimas* (angl. *entering*) *į automatinio duomenų apdorojimo sistemą, padarant didelę žalą* (angl. *substantial harm*). Nusikalstamą veiką kvalifikuojančiais požymiais šiame straipsnyje pripažįstami: veikos padarymas dėl savanaudiškų paskatų; veikos padarymas organizuotoje grupėje; veikos padarymas sukėlęs sunkius padarinius (angl. *serious consequences*); veikos padarymas prieš automatinio duomenų apdorojimo sistemą, kuri apdoroja duomenis, susijusius su valstybės politiniu, ekonominiu, kariniu, socialiniu ar kitu saugumu.[105]

Kai kurių valstybių baudžiamuosiuose įstatymuose didelės žalos (apskritai – žalos kaip pavojingų padarinių) požymis įtvirtintas tik atskiroje straipsnio dalyje. Štai Estijos Respublikos baudžiamojo kodekso 206 straipsnyje kriminalizuota kišimosi į kompiuterinius duomenis veika 1 dalyje apibrėžta kaip *neteisėtas duomenų, esančių kompiuterinėse sistemose, pakeitimas, ištrynimas, sugadinimas ar blokavimas* (angl. *blocking of*). Aptariamo straipsnio 2 dalyje nusikalstamą veiką kvalifikuojančiais požymiais pripažįstami: kišimasis į daugelio kompiuterinių sistemų duomenis, panaudojant baudžiamojo kodekso 216 straipsnyje numatytus prietaisus ar kompiuterines programas; kišimasis į kompiuterinius duomenis padarytas grupės asmenų; kišimasis į gyvybiškai svarbaus sektoriaus kompiuterinės sistemos duomenis; kišimasis į kompiuterinius duomenis padarant didelę žalą (angl. *significant damage*).[106] Šiame kontekste taip pat paminėtina Šveicarijos Konfederacijos baudžiamojo kodekso 144^1 straipsnio 1 dalyje kriminalizuota duomenų sugadinimo veika, kuri apibrėžta kaip *neteisėtas elektroniniu ar kitokiu panašiu būdu laikomų ar perduodamų duomenų pakeitimas, ištrynimas ar pavertimas nenaudotinais*. Nors ir toje pačioje straipsnio dalyje, tačiau atskirai, nusikalstamą veiką kvalifikuojančiu požymiu pripažįstamas didelės žalos padarymas.[107]

Pasirinktose bendrosios teisės tradicijos valstybėse, kurios yra Konvencijos dėl elektroninių nusikaltimų dalyvės, neteisėto poveikio elektroniniams duomenims veika apibrėžiama pakankamai abstrakčiai, nedetalizuojant šių veikų padarymo technologinių aspektų. Štai Jungtinės Didžiosios Britanijos ir Šiaurės Airijos Karalystės 1990 m. Netinkamo kompiuterių naudojimo akto 3 straipsnyje

---

[105] Criminal Code of the Republic of Latvia, žiūrėta 2016 05 15, http://www.vvc.gov.lv/export/sites/default/docs/LRTA/Likumi/The_Criminal_Law.doc Latvija Konvenciją dėl elektroninių nusikaltimų ratifikavo 2007 m. vasario 14 d.

[106] Criminal Code of the Republic of Estonia, žiūrėta 2016 05 15, https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/523122015005/consolide Estija Konvenciją dėl elektroninių nusikaltimų ratifikavo 2003 m. gegužės 12 d.

[107] Criminal Code of the Swiss Confederation, žiūrėta 2016 05 15, http://www.legislationline.org/download/action/download/id/5686/file/Swiss_CC_1937_am2014_en.pdf Šveicarijos Konfederacija Konvenciją dėl elektroninių nusikaltimų ratifikavo 2011 m. rugsėjo 21 d.

kriminalizuotos kompiuterių darbo pabloginimo ir pan., ketinant tai padaryti arba tai padarant dėl neatsargumo (angl. *recklessness*), veikos 1 dalyje, 2 dalies b, c, d, punktuose, 3 dalyje apibrėžta kaip *bet kokia neautorizuota veika, susijusi su kompiuteriu, žinant, kad ji neautorizuota, kurią darydamas asmuo ketino užkirsti ar apriboti prieigą prie bet kokios kompiuteryje laikomos programos ar duomenų, arba pakenkti bet kokios tokios programos veikimui ar bet kokių tokių duomenų patikimumui, arba sudaryti sąlygas padaryti bet kurią iš nurodytų veikų, arba, jeigu asmuo yra neatsargus dėl to* (angl. *is reckless as to*)*, ar jo veika lems bet kurios iš nurodytų veikų padarymą*. Aptariamo straipsnio 4 dalyje numatyta, kad ketinimas ar neatsargumas neprivalo būti susiję su konkrečiu kompiuteriu, konkrečia programa ar duomenimis, konkrečios rūšies programa ar duomenimis, o 5 dalyje nurodyta, jog veikos padarymas apima nulėmimą, kad veika būtų padaryta, terminas „veika“ apima eilę veikų, pagaliau, jog ko nors pabloginimas, prieigos užkirtimas ar apribojimas gali būti laikini.[108]

Jungtinių Amerikos Valstijų baudžiamojo kodekso 1030 straipsnyje kriminalizuota sukčiavimo ir kitų veikų, susijusių su kompiuteriais, veika, kuri a dalies 5 punkte apibrėžta kaip *sąmoningas programos, informacijos, kodo ar komandos perdavimas, kuriuo tyčia sukeliama neautorizuota žala* (angl. *damage*) *saugomam kompiuteriui, arba sąmoninga neautorizuota prieiga prie saugomo kompiuterio, kuria padaroma žala* (angl. *damage*) *dėl neatsargumo* (angl. *recklessly*), *arba sąmoninga neautorizuota prieiga prie saugomo kompiuterio, kuria sukeliame žala* (angl. *damage*) *ir nuostoliai (angl. loss*). Aptariamo baudžiamojo kodekso 1030 straipsnio e dalies 8 punkte terminas „žala“ apibrėžtas kaip bet koks duomenų, programos, sistemos ar informacijos integralumo ar prieinamumo pabloginimas, o 11 punkte terminas „nuostoliai“ apibrėžtas kaip bet kokie protingi praradimai, kuriuos patyrė bet kokia auka, įskaitant baudžiamojo persekiojimo, žalos įvertinimo, duomenų, programų, sistemos ar informacijos būklės, buvusios iki nusikaltimo padarymo, atkūrimo išlaidas, taip pat bet kokių pajamų praradimas, patirtos išlaidos ar kita susijusi žala, atsiradusi dėl aptarnavimo (angl. *service*) pertraukimo.[109] Atkreiptinas dėmesys į tai, kad Jungtinių Amerikos Valstijų baudžiamojo kodekso 1030 straipsnio a dalies 5 punkte duomenų, programos, sistemos ar informacijos integralumo ir prieinamumo pažeidimas iš dalies siejamas su prieš tai padaryta sąmoninga neautorizuota prieiga prie saugomo kompiuterio, t. y. su informacinių sistemų

[108] Computer Misuse Act 1990, žiūrėta 2016 05 15, http://www.legislation.gov.uk/ukpga/1990/18/crossheading/computer-misuse-offences Jungtinė Didžiosios Britanijos ir Šiaurės Airijos Karalystė Konvenciją dėl elektroninių nusikaltimų ratifikavo 2011 m. gegužės 25 d.

[109] US Code, žiūrėta 2016 05 15, http://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title18-section1030&num=0&edition=prelim Jungtinės Amerikos Valstijos Konvenciją dėl elektroninių nusikaltimų ratifikavo 2006 m. rugsėjo 29 d.

konfidencialumo pažeidimu. Toks neteisėto poveikio elektroniniams duomenims kriminalizavimo variantas aptiktinas rytų kaimynių valstybių baudžiamuosiuose įstatymuose.

Rusijos Federacijos baudžiamojo kodekso 272 straipsnyje kriminalizuota neteisėtos prieigos prie kompiuterinės informacijos veika 1 dalyje apibrėžta kaip *neteisėta prieiga prie įstatymu saugomos kompiuterinės informacijos, jeigu tai lėmė kompiuterinės informacijos sunaikinimą, blokavimą* (rus. *блокирование*), *modifikavimą arba kopijavimą*. Aptariamo straipsnio 2 dalyje nusikalstamą veiką kvalifikuojančiais požymiais pripažįstami veikos padarymas dėl savanaudiškų paskatų ar didelės žalos padarymas (rus. *крупный ущерб*). Aptariamo straipsnio 3 dalyje nusikalstamą veiką kvalifikuojančiais požymiais pripažįstami straipsnio 1 ar 2 dalyse numatytų veikų padarymas grupėje asmenų esant išankstiniam susitarimui arba organizuotoje grupėje, arba asmens, kuris pasinaudojo savo tarnybine padėtimi. Aptariamo straipsnio 4 dalyje nusikalstamą veiką kvalifikuojančiu požymiu pripažįstamas straipsnio 1, 2 ar 3 dalyse numatytų veikų padarymas, jeigu tai sukėlė sunkius padarinius (rus. *тяжкие последствия*) ar sukūrė tokių padarinių sukėlimo grėsmę. Be to, aptariamo straipsnio pabaigoje pažymėta, jog kompiuterinė informacija suvokiama kaip pranešimas, duomenys, esantys elektroninių signalų formoje, nepriklausomai nuo jų laikymo, apdorojimo ir perdavimo priemonių. Čia taip pat pateiktas didelės žalos apibrėžimas – vieną milijoną rublių viršijanti pinigų suma.[110]

Baltarusijos Respublikos baudžiamojo kodekso 350 straipsnyje, kuriame kriminalizuota kompiuterinės informacijos modifikavimo veika, kuri apibrėžta kaip *kompiuterinėje sistemoje laikomos informacijos pakeitimas ar žinomai neteisingos informacijos įvedimas* (rus. *внесение*), *padaręs didelės žalos* (rus. *существенный вред*)*, nesant nusikaltimų nuosavybei požymių (kompiuterinės informacijos modifikavimas)*. Nusikalstamą veiką kvalifikuojančiais požymiais pripažįstami avarijos, katastrofos, nelaimingų atsitikimų, susijusių su žmonėmis, neigiamų aplinkos pokyčių ar kitų sunkių padarinių sukėlimas arba kompiuterinės informacijos modifikavimas, susijęs su nesankcionuota prieiga prie kompiuterinės sistemos ar tinklo.[111] Taigi kompiuterinės sistemos ar tinklo konfidencialumo pažeidimas pripažįstamas nusikalstamą veiką kvalifikuojančiu požymiu.

Ukrainos baudžiamojo kodekso 361 straipsnyje kriminalizuota nesankcionuoto įsikišimo į elektroninės apdorojimo mašinos (kompiuterio), automatizuotų sistemų, kompiuterių tinklų arba elektroninių ryšio tinklų darbą veika apibrėžta kaip *nesankcionuotas įsikišimas į elektroninės*

[110] Ugolovnyj kodeks Rossijskoj Federacii [Criminal Code of the Russian Federation], žiūrėta 2016 05 15, http://www.uk-rf.com/ Rusijos Federacija nėra Konvencijos dėl elektroninių nusikaltimų dalyvė.

[111] Ugolovnyj kodeks Respubliki Belarus [Criminal Code of the Republic of Belarus], žiūrėta 2016 03 11, http://etalonline.by/?type=text&regnum=HK9900275#load_text_none_1_ Baltarusijos Respublika nėra Konvencijos dėl elektroninių nusikaltimų dalyvė.

apdorojimo mašinos (kompiuterio), automatizuotų sistemų, kompiuterių tinklų arba elektroninių ryšio tinklų darbą, kuris lėmė informacijos nutekinimą (rus. *утечке*), *praradimą*, *suklastojimą* (rus. *подделке*), *blokavimą arba informacijos apdorojimo proceso iškreipimą, arba nustatytos informacijos maršrutizavimo tvarkos pažeidimą*. Taigi aptariamame straipsnyje neteisėtas poveikis informacijai siejamas su prieš tai padarytu informacinės sistemos integralumo ar prieinamumo pažeidimu. Vien tik informacijos integralumo ir prieinamumo baudžiamoji teisinė apsauga užtikrinta Ukrainos baudžiamojo kodekso 362 straipsnyje, kuriame kriminalizuota nesankcionuotų veiksmų su informacija, apdorojama elektroninėse apdorojimo mašinose (kompiuteriuose), automatizuotose sistemose, kompiuterių tinkluose arba išsaugoma tokios informacijos laikmenose, kuriuos padarė asmuo, turintis prieigos teisę prie jos, veika apibrėžta kaip *nesankcionuotas informacijos, kuri apdorojama elektroninėse apdorojimo mašinose (kompiuteriuose), automatizuotose sistemose, kompiuterių tinkluose arba išsaugoma tokios informacijos laikmenose pakeitimas, sunaikinimas ar blokavimas*. Abiejų straipsnių kvalifikuotose dalyse nusikalstamą veiką kvalifikuojančiais požymiais pripažįstami veikos padarymas pakartotinai ar grupėje asmenų, arba didelės žalos padarymas (rus. *существенный вред*). Be to, Ukrainos baudžiamojo kodekso 361 straipsnio pabaigoje nurodoma, kad didelė žala (rus. *значительным ущербом*), jeigu ši pasireiškė kaip materialinės žalos padarymas, laikytina tokia žala, kuri šimtą ir daugiau kartų viršija neapmokestinamą piliečių darbo užmokesčio minimumą.[112]

Apibendrinant tai, kas išdėstyta, neteisėto poveikio elektroniniams duomenims kriminalizavimas naujajame baudžiamajame įstatyme kaip *delicta sui generis* sietinas su ekvivalentaus elgesio fizinėje ir elektroninėje erdvėje vertinimo principo įgyvendinimu. Žvelgiant istoriniu aspektu, mokslinėje literatūroje neteisėto poveikio elektroniniams duomenims kriminalizavimas kaip *delicta sui generis* grindžiamas šios veikos atribojimu nuo nusikalstamų veikų nuosavybei, o tiksliau – nuo turto sunaikinimo ar sugadinimo veikos. EKNPT baigiamosios ataskaitos II skyriaus 2 dalies c punkto nuostatos leidžia manyti, kad neteisėto poveikio elektroniniams duomenims veikos kriminalizavimas kaip *delicta sui generis* gali būti grindžiamas poreikiu baudžiamąją teisinę apsaugą užtikrinti anksčiau negu etape, kuriame prasideda ta, kurią teikia neteisėto poveikio informacinei sistemai nusikalstama veika. Pasirinktų užsienio valstybių baudžiamojo teisinio reguliavimo analizė atskleidė skirtingus neteisėto poveikio elektroniniams duomenims kriminalizavimo variantus. Valstybių, kurios yra Konvencijos dėl elektroninių

[112] Ugolovnyj kodeks Ukrainy [Criminal Code of Ukraine], žiūrėta 2016 05 15, http://meget.kiev.ua/kodeks/ugolovniy-kodeks/ Ukraina Konvenciją dėl elektroninių nusikaltimų ratifikavo 2006 m. kovo 10 d.

nusikaltimų dalyvės, baudžiamieji įstatymai skiriasi *inter alia* pagal tai, ar juose įtvirtintas didelės žalos požymis. Tokių valstybių, kuriose vyrauja bendrosios teisės tradicija, neteisėto poveikio elektroniniams duomenims veika apibrėžiama pakankamai abstrakčiai, nedetalizuojant šių veikų padarymo technologinių aspektų. Kai kurių užsienio valstybių baudžiamuosiuose įstatymuose neteisėto poveikio elektroniniams duomenims veika siejama su prieš tai padarytu informacinių sistemų integralumo ar prieinamumo arba konfidencialumo pažeidimu.

4. OBJEKTYVIEJI NETEISĖTO POVEIKIO ELEKTRONINIAMS DUOMENIMS SUDĖTIES POŽYMIAI

4.1. Elektroniniai duomenys kaip nusikalstamos veikos dalykas

BK 196 straipsnyje kriminalizuotos veikos dalykas yra elektroniniai duomenys[113]. Šio straipsnio kvalifikuotoje dalyje elektroniniai duomenys siejami su padidintos svarbos – turinčios strateginę reikšmę nacionaliniam saugumui ar didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai – informacine sistema, taip pat minimi daugelio informacinių sistemų kontekste. Mokslinėje literatūroje elektroninių duomenų problematika išsamiai nagrinėta R. Marcinauskaitės daktaro disertacijoje[114]. Siekiant nesikartoti, toliau darbe apibendrinamos mokslininkės padarytos įžvalgos bei išvados apie elektroninių duomenų sampratą ir ryšį su informacine sistema siejant tai su tiriama nusikalstama veika.

Visų pirma, būtina skirti duomenų ir informacijos sąvokas. Duomenys turi primityvią, vienetinę reikšmę ir, kitaip negu informacija, nėra siejami su jų galima reikšme adresatui. Duomenys virsta informacija kai tampa suprantami subjektui. Atsižvelgiant į tai, duomenų suvokimas, jų prasmė, nauda žmogui, duomenų formos bei turinio tinkamumas naudoti, kuris leidžia tenkinti žmonių informacinius poreikius, būdingi informacijai. Tuo tarpu duomenys yra tam tikra pradinė medžiaga informacijai gauti, t. y. potenciali informacija. Visa tai leidžia daryti išvadą, kad duomenų sąvoka yra platesne negu informacijos[115]. Todėl baudžiamajame įstatyme numačius duomenų, o ne informacijos terminą, konfidencialumo (teigtina – ir integralumo bei prieinamumo – *aut. pastaba*) prasme tiek duomenys, tiek ir informacija, kvalifikuojant kaltininko padarytas veikas pagal BK 198 straipsnį (teigtina – ir BK 196 straipsnį – *aut. pastaba*), turėtų būti laikomi lygiaverčiais. Antra, tam, kad duomenys būtų pripažinti elektroniniais duomenimis, jie turi būti sukurti arba perkelti į elektroninę formą. Kaip tokie, elektroniniai duomenys gali egzistuoti tik būdami informacinėje sistemoje, suvokiamoje pačia bendriausia prasme. Elektroninių duomenų apibūdinimui gali būti naudojami du – jų tinkamumo apdoroti informacinėje sistemoje ir elektroninių duomenų buvimo vietos – kriterijai. Pirmasis jų žymi elektroninių duomenų formą, kurią atpažįsta informacinė sistema, kuri dėl to su jais gali atlikti įvairius veiksmus. Antrasis kriterijus reikalauja nurodyti, kur konkrečiai informacinėje

[113] Be kita ko, mokslinėje literatūroje neteisėto poveikio elektroniniams duomenims kontekste vartojami skirtingi termino „elektroniniai duomenys“ atitikmenys, pvz., „kompiuteriniai duomenys“. Siekiant aiškumo, toliau darbe vartojamas terminas „elektroniniai duomenys“, išskyrus atvejus, kai šio termino atitikmens nurodymas tūrėtų reikšmę.
[114] Renata Marcinauskaitė, *supra* note 4, p. 106-122.
[115] Apie terminų “duomenys” ir “informacija” tarpusavio santykį taip pat žr. šio darbo p. 10.

sistemoje elektroniniai duomenys gali būti randami, taigi gali padėti juos apibūdinti. Abu kriterijai tarpusavyje glaudžiai susiję – elektroninė forma žymi galimybę apdoroti duomenis, kuri išlaikoma, jei duomenys yra įvedami į informacinę sistemą. Pagaliau, programinė įranga (programa), priklausomai nuo veikos pobūdžio, sukeltų pasekmių, kaltininko tyčios kryptingumo ir pan., gali būti suprantama kaip informacinės sistemos dalis, t. y. nuo elektroninių duomenų atskirta priemonė, padedanti apdoroti duomenis informacinėje sistemoje, arba kaip viena iš elektroninių duomenų formų.[116] *„Tai atspindi vieną iš klasikinių kompiuterių struktūros sudarymo idėjų, kad programą sudarančios komandos „užkoduojamos kaip ir apdorojamieji duomenys ir nesiskiria nuo kitos informacijos“*“[117].

Pasak R. Marcinauskaitės, *„dėl technologijų panaudojimo plėtros pakitus nusikalstamų veikų padarymo galimybėms, atsirado esminių tokių veikų kriminalizavimo pakankamumo problemų, kurios bandytos spręsti įvairiai; antai baudžiamajame įstatyme įtvirtintos naujos nusikalstamų veikų sudėtys, teismų praktikoje išplėstas senųjų sudėčių aiškinimas. Tačiau šie bandymai sukūrė ir visai kitų, t. y. baudžiamojo įstatymo normų tarpusavio santykio, problemų“*[118]. Šiame kontekste aktualu tai, kokia nusikalstamos veikos dalyko reikšmė BK 196 straipsnio ir BK straipsnių, kuriuose kriminalizuotos tradicinės nusikalstamos veikos, tarpusavio santykiui, kai nusikalstama veika padaroma elektroninėje erdvėje, turint omenyje ekvivalentiškumo principą? Mokslininkės teigimu, įsigaliojus 2000 m. BK *„[...] tradicinių nusikalstamų veikų, padarytų fizinėje ir virtualioje erdvėje, ekvivalentus vertinimas užtikrintas jų kvalifikavimui taikant tą patį BK straipsnį [...]“*[119]. Teismų praktikos analizė atskleidė diskutuotinus atvejus, kai veikų kvalifikavimą pagal BK 196 straipsnį, manytina, apsprendė elektroninė dokumentų forma, neatsižvelgiant į ekvivalentaus vertinimo principo reikalavimus.

Vilniaus miesto 2 apylinkės teismo 2009 m. gegužės 27 d. baudžiamuoju įsakymu V. Č. nuteistas *inter alia* pagal BK 196 straipsnio 3 dalį už tai, kad *elektroniniame dienyne sau ir savo broliui D. Č. pakeitė dėstytojo I. R. dėstomo dalyko pažymius iš „3“ (trejeto) į „5“ (penketą)*. Be to, V. Č. nuteistas už tai, kad *savo pažymį pakeitė elektroniniame dienyne dėstytojo I. B. pildomoje ataskaitoje*.[120] Tokia pati situacija įžvelgtina baudžiamojoje byloje, kurioje Vilniaus miesto apylinkės

[116] Renata Marcinauskaitė, *supra* note 4, p. 106-108, 113, 118.
[117] *Ibid.*, p. 117 (cituota iš: Pranas Kanapeckas, Egidijus Kazanavičius ir Antanas Mikuckas, *Kompiuterių elementai [elektroninis išteklius]: Vadovėlis* (Kaunas: Technologija, 2011), 475).
[118] Aurelijus Gutauskas et. al., *Baudžiamoji justicija ir verslas. Recenzuotų mokslinių straipsnių baudžiamosios teisės ir baudžiamojo proceso klausimais rinkinys* (Vilnius: Vilniaus universitetas, 2016): 277-278.
[119] Renata Marcinauskaitė, *op. cit.*, p. 22.
[120] "Vilniaus miesto 2 apylinkės teismo 2009 m. gegužės 27 d. baudžiamuoju įsakymu baudžiamojoje byloje Nr. 1-515-487/2009," prieiga per internetą: http://www.infolex.lt/tp/Default.aspx?id=20&item=doc&aktoid=278594&nr=1

teismo 2013 m. balandžio 4 d. baudžiamuoju įsakymu J. V. nuteistas *inter alia* pagal BK 196 straipsnio 1 dalį ir 196 straipsnio 1 dalį, ir 196 straipsnio 1 dalį, ir 196 straipsnio 1 dalį, ir 196 straipsnio 1 dalį, ir 196 straipsnio 1 dalį, ir 196 straipsnio 1 dalį, ir 196 straipsnio 1 dalį, ir 196 straipsnio 1 dalį už tai, kad *Vilniaus universiteto Informacinėje sistemoje neteisėtai pakeitė studijų vertinimų rezultatus sau ir E. K., D. L., L. V., M. Š., N. M., K. L., A. S., P. P., A. K., I. J., R. K.*[121]. Taigi šiose baudžiamosiose bylose asmenys buvo nuteisti pagal BK 196 straipsnį už tai, kad pakeitė elektroniniame dienyne esančius pažymius. Akivaizdu, kad dienyno forma gali būti ne tik elektroninė, bet ir fizinė. Fizinės formos dienynas galėtų būti pripažintas dokumentu BK 300 straipsnio kontekste, jeigu atitiktų dokumentų turiniui keliamus reikalavimus. Lietuvos Aukščiausiasis Teismas yra ne kartą pažymėjęs, 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). Tai įrašas, kurio panaudojimas gali sukelti fiziniam ar juridiniam asmeniui ar valstybei teisiškai reikšmingus padarinius (kasacinės nutartys baudžiamosiose bylose Nr. 2K-662/2000, 2K-775/2007, 2K-263/2010, 2K-57/2014)“*[122]. Fizinės formos dienynas paprastai turėtų atitikti nurodytus dokumentų turiniui keliamus reikalavimus. Taigi fizinės formos dienyne esančių pažymių pakeitimas turėtų būti kvalifikuojamas pagal BK 300 straipsnį kaip dokumentų suklastojimo veika. Vertinant ekvivalenčiai, pažymių pakeitimas elektroniniame dienyne turėtų būti kvalifikuojamas pagal BK straipsnį, kuris taikytinas pažymių pakeitimo fizinės formos dienyne atveju, t. y. pagal BK 300 straipsnį kaip dokumento suklastojimo veika. Štai Kauno apylinkės teismo 2015 m. lapkričio 26 d. baudžiamuoju įsakymu P. K. nuteistas *inter alia* pagal BK 300 straipsnio 1 dalį už tai, kad *išduotoje Lietuvos Respublikos LMSU studijų knygelėje įrašė melagingus duomenis – įskaitas, vertinimus, tokiu būdu suklastojo tikrą dokumentą*. Aprašomojoje teismo baudžiamojo įsakymo dalyje pažymėta, kad *P. K. suklastojo elektroniniuose pažangumo žurnaluose bei studijų knygelėje savo įvertinimo rezultatus*.[123] Pastarajam kvalifikavimo variantui pritartina.

[121] “Vilniaus miesto apylinkės teismo 2013 m. balandžio 4 d. baudžiamuoju įsakymu baudžiamojoje byloje Nr. 1-1471-716/2013,“ prieiga per internetą: http://www.infolex.lt/tp/Default.aspx?id=20&item=doc&aktoid=671988&nr=1
[122] “Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2015 m. sausio 27 d. nutartimi baudžiamojoje byloje Nr. 2K-32-696/2015,“ prieiga per internetą: http://www.infolex.lt/tp/Default.aspx?id=20&item=doc&aktoid=993262&nr=1
[123] “Kauno apylinkės teismo 2015 m. lapkričio 26 d. baudžiamuoju įsakymu baudžiamojoje byloje Nr. 1-2685-954/2015,“ prieiga per internetą: http://www.infolex.lt/tp/Default.aspx?id=20&item=doc&aktoid=1196012&nr=1

Tokia pati kvalifikavimo problema įžvelgtina baudžiamojoje byloje, kurioje Panevėžio apygardos teismo 2014 m. kovo 14 d. nuosprendžiu[124] R. P. nuteistas *inter alia* pagal BK 196 straipsnio 1 dalį už tai, kad *dirbdamas AB Šiaulių banko Anykščių klientų aptarnavimo skyriuje, buhalterio pareigose, pasinaudodamas AB Šiaulių banko jam suteiktais įgaliojimais vykdant savo darbines funkcijas, apgaule, be indėlininkų žinios ir sutikimo, prieš indėlio terminą, neteisėtai pakeisdamas elektroninius duomenis AB Šiaulių banko kompiuterinėje sistemoje BIS Forpost, naudodamas jam suteiktą identifikacinį kodą, nutraukė terminuotų indėlių sutartis, sudarytas su J. Ž., G. K., V. S., D. P., D. K., A. G., B. B., D. J., P. S., S. V.*. Teigtina, kad indėlių sutarčių nutraukimui pildytini dokumentai paprastai turėtų atitikti minėtus dokumentų turiniui keliamus reikalavimus. Todėl įrašų, kurie neatitinka tikrovės, juose atlikimas fizinėje erdvėje tūrėtų būti kvalifikuojamas kaip dokumentų suklastojimo veika. Vertinant ekvivalenčiai, terminuotų indėlių sutarčių nutraukimas atliekant atitinkamus pakeitimus kompiuterinėje sistemoje turėtų būti kvalifikuojamas pagal BK 300 straipsnį. Paminėtina, kad šioje baudžiamojoje byloje R. P. nuteistas *inter alia* pagal BK 300 straipsnio 1 dalį už tai, kad atlikdamas aukščiau nurodytus veiksmus papildomai *surašė susitarimus dėl terminuotų indėlių sutarčių nutraukimo, įrašydamas į juos tikrovės neatitinkančius duomenis apie tai, kad indėlininkų G. K., V. S., D. P., S. V. ir J. Ž. prašymu ir iniciatyva prieš terminą yra nutraukiamos terminuotų indėlių sutartys, ir už juos pasirašė sutarties skiltyje „Indėlininkas“, taip suklastodamas jų parašus*. Teigtina, kad abi R. P. padarytos veikos dėl aukščiau nurodytų priežasčių turėtų būti kvalifikuojamos pagal BK 300 straipsnį kaip dokumentų suklastojimo veika.

Panevėžio miesto apylinkės teismo 2011 m. gegužės 24 d. nuosprendžiu R. Š. nuteista *inter alia* pagal BK 196 straipsnio 1 dalį ir BK 196 straipsnio 1 dalį už tai, kad *41 atveju kuro pardavimą, už kurį klientai atsiskaitydavo grynais pinigais, kompiuterio programoje ir EKA kasos aparate fiksuodavo nurodydama mokėjimo rūšį „kreditas“ ir šiuos elektroninius duomenis perkėlė į buhalterinės apskaitos programą bei juos neteisėtai pakeitė, t. y. vietoje informacinėje sistemoje buvusių elektroninių duomenų patalpino kito turinio duomenis – „kredito“ mokėjimo rūšį pakeitė į „atsiskaitymą banko kortele“*. Be to, R. Š. nuteista už tai, kad *tam, jog 2000 litrų dyzelino trūkumas nepasimatytų mėnesio pabaigoje pildomose ataskaitose, neteisėtai pakeitė kompiuteryje esančius elektroninius duomenis, tai yra informacinę sistemą papildė naujais neegzistuojančiais elektroniniais duomenimis*.[125] Panaši situacija įžvelgtina baudžiamojoje byloje, kurioje Panevėžio miesto apylinkės

[124] "Panevėžio apygardos teismo 2014 m. kovo 14 d. nuosprendis baudžiamojoje byloje Nr. 1-35-366/2014," prieiga per internetą: http://www.infolex.lt/tp/875032?nr=2

[125] "Panevėžio miesto apylinkės teismo 2011 m. gegužės 24 d. nuosprendis baudžiamojoje byloje Nr. 1-187-389/2011," prieiga per internetą: http://www.infolex.lt

teismo 2013 m. balandžio 2 d. nuosprendžiu nuo baudžiamosios atsakomybės atleista E. K. pripažinta kalta padariusi *inter alia* BK 196 straipsnio 3 dalyje numatytą nusikalstamą veiką, o būtent: *bendrovės kompiuterio ir kasos aparato kompiuterinėje pardavimų programoje, esant užfiksuotiems prekių pardavimams pagal kasos tarnybinius kvitus, suformavo dienos prekių pardavimo vidinius dokumentus – PVM sąskaitas–faktūras – pardavimų operacinėje sistemoje (POS) į kompiuterio programą bei pardavimų operacinę sistemą įterpdama neparduotas prekes ir šiuos elektroninius duomenis perkėlė į pardavimų operacinės sistemos programą bei juos neteisėtai pakeitė, tai yra vietoje informacinėje sistemoje buvusių elektroninių duomenų pagal kasos tarnybinius kvitus, patalpino kito turinio duomenis – suformuodama tos dienos pardavimų vidinį dokumentą, parduotai prekei savo nuožiūra pritaikė nuolaidą, taip sumažindama realią parduotos prekės kainą, o susidariusiam kainų skirtumui tarp realios prekės kainos ir sumažintos prekės kainos, atlikdama kitų – tą dieną neparduotų prekių įterpimą į PVM sąskaitą–faktūrą POS, ir tokiu būdu pakeisdama elektroninius duomenis padarė neteisėtą poveikį UAB „D.“ elektroniniams duomenims. Tokiu būdu, formuodama vidinius dokumentus – pardavimų operacinės sistemos (POS) PVM sąskaitas–faktūras, neteisėtai pakeitė elektroninius duomenis, įterpdama į dokumentus neparduotas prekes, prieš tai neleistinai sumažindama realią parduotų prekių kainą ir suformuotus vidinius dokumentus, su žinomai neteisingais duomenimis, pateikė UAB „D.“ buhalterijai*.[126] Buhalterinės apskaitos programos duomenys nelaikytini buhalterinės apskaitos dokumentais[127]. Jeigu įmonės dokumentai, kuriuose atliekami įrašai apie įmonės pardavimus, prekes ir pan., atitiktų minėtus dokumentų turiniui keliamus reikalavimus, tokių įrašų, kurie neatitinka tikrovės, atlikimas tūrėtų būti kvalifikuojamas pagal BK 300 straipsnį. Vertinant ekvivalenčiai, atitinkamų įrašų atlikimas kompiuterinėje erdvėje turėtų būti kvalifikuojamas pagal BK 300 straipsnį.

Taigi vadovaujantis ekvivalentaus elgesio fizinėje ir elektroninėje erdvėje vertinimo principu, nusikalstama veika, padaryta elektroninėje erdvėje, kvalifikuotina pagal BK 196 straipsnį nustačius, kad elektroniniai duomenys, kuriems padarytas neteisėtas poveikis, nesudaro tradicinių nusikalstamų veikų dalyko. Nusikalstamos veikos dalyko atžvilgiu BK 196 straipsnis su BK straipsniais, kuriuose kriminalizuotos tradicinės nusikalstamos veikos, konkuruoja, atitinkamai, kaip

[126] “Panevėžio miesto apylinkės teismo 2013 m. balandžio 2 d. nuosprendis baudžiamojoje byloje Nr. 1-85-334/2013,“ prieiga per internetą: http://www.infolex.lt

[127] “*[...] buhalterinės apskaitos programos duomenys negali būti laikomi buhalterinės apskaitos dokumentais, nes jie neatitinka dokumentui keliamų reikalavimų [...]*,“ “Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2014 m. gruodžio 30 d. nutartis baudžiamojoje byloje Nr. 2K-580/2014,“ prieiga per internetą: http://www.infolex.lt/tp/Default.aspx?id=20&item=doc&aktoid=943727&nr=1

bendroji ir specialioji teisės norma. Baudžiamosios teisės teorijoje[128] tokia konkurencija sprendžiama taikant specialiąją teisės normą, t. y. nusikalstamą veiką kvalifikuojant pagal BK straipsnį, kuriame kriminalizuota tradicinė nusikalstama veika.

4.2. Pavojingos veikos

Nusikalstama neteisėto poveikio elektroniniams duomenims veika gali pasireikšti alternatyviomis elektroninių duomenų sunaikinimo, sugadinimo, pašalinimo ar pakeitimo arba naudojimosi tokiais duomenimis apribojimo veikomis. Pastaroji turi būti padaroma techninė įranga, programine įranga ar kitais būdais.

Pasak R. Mockevičiaus ir D. Valatkevičiaus, būtinas BK 196 straipsnyje kriminalizuotos *„[...] nusikalstamos veikos požymis yra padariniai. Jais laikomi sunaikinti, sugadinti, pašalinti ar pakeisti duomenys ar apribotas naudojimasis jais. Visi veiksmai, kuriais daromas poveikis elektroniniams duomenims, turi sukelti žalą“*[129]. Taigi BK 196 straipsnio 1 dalies dispozicijoje vartojami terminai – „sugadinimas“, „sunaikinimas“, „pašalinimas“, „pakeitimas“, „naudojimosi apribojimas“ – apibūdina tiek procesą, tiek jo rezultatą – elektroninių duomenų sunaikinimą, sugadinimą, pašalinimą ar pakeitimą arba naudojimosi tokiais duomenimis apribojimą, t. y. elektroninių duomenų integralumo ar prieinamumo pažeidimą.

Kaip pastebi R. Mockevičius ir D. Valatkevičius, *„elektroninių duomenų sunaikinimo, sugadinimo, pašalinimo ar pakeitimo padarymo būdai nėra numatyti šioje sudėtyje“*[130]. Taigi nurodytos pavojingos veikos gali būti padarytos bet kokiu būdu. Kita vertus, įstatymų leidėjui įtvirtinus pavyzdinį naudojimosi elektroniniais duomenimis apribojimo būdų sąrašą, teigtina, kad ši pavojinga veika gali būti padaryta bet kokiu būdu. Skirtumas tas, kad, pastarąjį požymį įtraukus į nusikalstamos veikos sudėtį, jis privalomai įrodinėtinas kiekvienoje byloje. Taigi nustačius kaltininko tyčia neteisėtai paveikti elektroninius duomenis nusikalstamos veikos kvalifikavimui pagal BK 196 straipsnį nėra svarbu kokiu būdu tai padaryta.

Pasak R. Mockevičiaus, D. Valatkevičiaus, pagal BK 196 straipsnį kvalifikuotini *„[...] ir tie veiksmai, kuriais fiziškai kenkiama informacinei sistemai ir jos komponentams [...], siekiant paveikti*

---

[128] Vladas Pavilonis, “Baudžiamosios teisės normų konkurencija,“ *Teisės problemos* 2, 12 (1996): 40; Vladas Pavilonis ir Egidijus Bieliūnas, *Nusikaltimų kvalifikavimas esant jų daugetui ir baudžiamosios teisės normų konkurencija* (Vilnius, 1984), 13; Alfonsas Klimka, *Nusikaltimų kvalifikavimas* (Vilnius, 1970), 75; Armanas Abramavičius et. al., *Baudžiamoji teisė. Trečiasis pataisytas ir papildytas leidimas* (Vilnius: Eugrimas, 2001), 338.
[129] Armanas Abramavičius et. al., *supra* note 2, p. 422.
[130] *Ibid*., p. 421.

šioje informacinėje sistemoje esančius elektroninius duomenis "[131]. Tą patį teigia ir M. Kuzminovas[132]. Kaip pastebi autoriai, kai tokia veika papildomai sudaro turto sunaikinimo ar sugadinimo sudėtį, nusikalstama veika kvalifikuotina pagal BK 196 ir 187 straipsnių sutaptį[133]. Pastaruoju atveju nusikalstamos veikos kvalifikavimą *inter alia* pagal BK 196 straipsnį apsprendžia kaltininko tyčios neteisėtai paveikti elektroninius duomenis nustatymas.

R. Mockevičiaus, D. Valatkevičiaus teigimu, *„sąvokos – pašalinimas, sunaikinimas, pakeitimas – tarpusavyje labai susijusios dėl to, kad fiziniame duomenų nešėjo lygmenyje [...] techniškai įmanomi tik trys veiksmai – skaitymas, įrašymas ir paties nešėjo suardymas. Nepaisant, koks veiksmas buvo atliktas, tokios pasekmės atsiranda, jeigu skaitymo/įrašymo metu duomenims yra padaromas koks nors poveikis. Tokio poveikio pasekmės atskiriamos pagal rezultatus [...]"*[134]. Manytina, tai, kokia iš aukščiau nurodytų pavojinga veika padaryta, apsprendžia neteisėto poveikio elektroniniams duomenims rezultatas. Kitaip tariant, nusikalstamos veikos kvalifikavimui svarbu nustatyti ne tai, kaip elektroniniai duomenys buvo paveikti (technologinis aspektas), o tai, kad galiausiai tokie duomenys yra neteisėtai pašalinti, sunaikinti, ar pakeisti. Turint omenyje tai, kad elektroninių duomenų sugadinimo pavojingos veikos pagrindą sudarą tokių duomenų pakeitimas[135], o elektroninių duomenų pašalinimo pavojinga veika yra vienas iš naudojimosi tokiais duomenimis apribojimo būdų[136], manytina, analogiškai, svarbu nustatyti ne tai, kaip elektroniniai duomenys buvo paveikti (technologinis aspektas), o tai, kad galiausiai elektroniniai duomenys yra neteisėtai sugadinti ar naudojimasis tokiais duomenimis yra apribotas (išskyrus kai toks naudojimasis apribojamas sunaikinant elektroninius duomenis)[137].

Remiantis Vilniaus apygardos teismo Baudžiamųjų bylų skyriaus 2014 m. balandžio 16 d. nutartimi, *„kompiuterinės informacijos sunaikinimas, sugadinimas, pašalinimas, pakeitimas, naudojimosi ja apribojimas tai tie negatyvūs nusikaltimo subjekto veiksmai, kuriais siekiama teisėtiems kompiuterinės informacijos vartotojams atimti galimybę tokią informaciją naudoti pagal paskirtį. Šiais veiksmais nusikaltimo subjektas pats neįgyja galimybės kad ir neteisėtai naudotis tokia informacija, informacijos neperima [...]"*[138]. Vis dėlto, toks aiškinimas kritikuotinas dėl termino

[131] Armanas Abramavičius et. al., *supra* note 2, p. 422.
[132] Aurelijus Gutauskas et. al., *supra* note 3, p. 466.
[133] Armanas Abramavičius et. al., *op. cit.*, p. 422; Aurelijus Gutauskas et. al., *op. cit.*, p. 460.
[134] Armanas Abramavičius et. al., *op. cit.*, p. 421.
[135] Apie tai plačiau žr. šio darbo p. 44-45.
[136] Apie tai plačiau žr. šio darbo p. 53.
[137] Apie tai plačiau žr. šio darbo p. 47-48.
[138] "Vilniaus apygardos teismo Baudžiamųjų bylų skyriaus 2014 m. balandžio 16 d. nutartis baudžiamojoje byloje Nr. 1A-303-256/2014," prieiga per internetą: http://www.infolex.lt/tp/821736?nr=1 Šioje baudžiamojoje byloje nagrinėtos nusikalstamos veikos padarymo laikas – 2012 ir 2013 m. Todėl teismo vartojamos terminijos priežastys nėra aiškios.

„kompiuterinė informacija“ vartojimo ir pavojingų veikų ribojimo aktyviais kaltininko veiksmais. Pastaruoju aspektu pažymėtina, jog mokslinėje literatūroje taip pat vyrauja pozicija, kad BK 196 straipsnyje kriminalizuota veika gali pasireikšti tik aktyviais veiksmais (veikimu) (R. Mockevičius, D. Valatkevičius, M. Kuzminovas)[139]. Tokia pozicija yra diskutuotina. Teoriškai, neteisėtas naudojimosi elektroniniais duomenims apribojimas gali pasireikšti ir tuo, kad turintis teisinę pareigą suteikti prieigą prie elektroninių duomenų ir galimybę tai padaryti asmuo, siekdamas apriboti naudojimąsi tokiais duomenimis, neveikia. Taip yra apribojama teisėto vartotojo galimybė naudotis elektroniniais duomenimis. Tokia veika yra kriminalizuota, pavyzdžiui, Kanados baudžiamojo kodekso 430 (1.1) straipsnyje, kuriame įtvirtinta su kompiuteriniais duomenimis susijusi piktadarybė (angl. *mischief*) apibrėžta *inter alia* kaip atsisakymas suteikti prieigą prie kompiuterinių duomenų asmeniui, turinčiam tam teisę[140]. Panaši neveikimo schema gali būti pritaikoma kalbant ir apie elektroninių duomenų pašalinimo pavojingą veiką, taip pat jų integralumą pažeidžiančias veikas.

Apibendrinant tai, kas išdėstyta, teigtina, kad nustačius kaltininko tyčia neteisėtai paveikti elektroninius duomenis nusikalstamos veikos kvalifikavimui pagal BK 196 straipsnį nėra svarbu kokiu būdu tai padaryta. Manytina, jog nusikalstamos veikos kvalifikavimui pagal BK 196 straipsnį svarbu nustatyti ne tai, kaip elektroniniai duomenys buvo paveikti (technologinis aspektas), o tai, kad galiausiai tokie duomenys yra neteisėtai sunaikinti, sugadinti, pašalinti ar pakeisti arba naudojimasis tokiais duomenimis yra apribotas (išskyrus kai toks naudojimasis apribojamas sunaikinant elektroninius duomenis). Turint tai omenyje, toliau nagrinėjamos atskiros pavojingos veikos, kuriomis pasireiškia neteisėtas poveikis elektroniniams duomenims.

4.2.1. Sunaikinimas

EKNPT baigiamosios ataskaitos II skyriaus 2 dalies c punkte ir Konvencijos aiškinamosios ataskaitos 61 punkte ištrynimo (angl. *erasure* ir *deletion*) pavojinga veika prilyginama materialaus daikto sunaikinimui (angl. *destruction*). Teigiama, jog ištrynimas sunaikina duomenis, padarydamas juos neatpažįstamais.[141] Tuo tarpu Lietuvos BK 196 straipsnyje elektroninių duomenų sunaikinimas kaip pavojinga veika įtvirtintas *expressis verbis*. Aptariamas požymis nacionalinėje baudžiamosios teisės doktrinoje aiškinamas kaip elektroninių duomenų ištrynimas (D. Sauliūnas, N. Goranin, D.

[139] Armanas Abramavičius et. al., *supra* note 2, p. 419; Aurelijus Gutauskas et. al., *supra* note 3, p. 459.
[140] Criminal Code of Canada, žiūrėta 2016 05 15, http://laws-lois.justice.gc.ca/eng/acts/c-46/page-88.html#h-116
[141] Council of Europe, *supra* note 11, p. 45; Committee of Ministers of the Council of Europe, *supra* note 13, p. 11.

Mažeika)[142], likvidavimas (R. Mockevičius, D. Valatkevičius, M. Kuzminovas)[143]. Šiame kontekste paminėtina, jog Rusijos Federacijos baudžiamojo kodekso 272 straipsnyje įtvirtinta kompiuterinės informacijos sunaikinimo (rus. *уничтожение*) pavojinga veika mokslinėje literatūroje aiškinama kaip jos ištrynimas (rus. *удаление*) (S. Pashin, Ju. Gavrilin, I. Popov, J. Gulbin, I. Klepickij ir kt.)[144], likvidavimas (rus. *ликвидация*) (V. Krylov, V. Golubev, V. Bechov)[145], praradimas (rus. *утрата*) (S. Boroin, S. Kochoi, D. Saveljev, T. Vaulina ir kt.)[146]. Taigi BK 196 straipsnyje įtvirtinta sunaikinimo pavojinga veika atitinka EKNPT baigiamosios ataskaitos II skyriaus 2 dalies c punkte, Konvencijos dėl elektroninių nusikaltimų 4 straipsnio 1 dalyje, Pamatinio sprendimo 2005/222/TVR 4 straipsnyje, Direktyvos 2013/40/ES 5 straipsnyje minimą ištrynimo pavojingą veiką.

EKNPT baigiamosios ataskaitos II skyriaus 2 dalies c punkte teigiama, jog duomenų ištrynimą gali lemti duomenų laikmenos sunaikinimas, magnetinės juostos perrašymas, duomenų „užtušavimas“ (angl. *blacking out of data*) ir būtinųjų jungčių ištrynimas[147]. Pasak R. Mockevičiaus, D. Valatkevičiaus, M. Kuzminovo, V. Golubev, elektroninių duomenų sunaikinimas reiškia jų likvidavimą bet kokiais būdais. M. Kuzminovas detalizuoja, kad ištrynimu elektroninių duomenų sunaikinimas pasireiškia paprastai.[148] Elektroninių duomenų neteisėto sunaikinimo ištrynimu atvejis aptiktinas Vilniaus apygardos teismo Baudžiamųjų bylų skyriaus 2014 m. balandžio 16 d. nutartyje, kuria paliktas galioti pirmos instancijos teismo nuosprendis, kuriuo V. S. nuteistas už tai, kad *inter alia neteisėtai prisijungė internetu iš kompiuterinės sistemos prie UAB „O“ internetinio puslapio administratoriaus teisėmis ir sunaikino ištrindamas iš šios sistemos standžiojo disko atminties įmonės klientų prisijungimo kodus, informaciją apie įmonėje siūlomus produktus ir jų aprašymus, informaciją apie įmonėje galiojančias akcijas bei pasiūlymus, padarydamas nedidelę žalą*[149]. Minėta, tai, kaip elektroniniai duomenys buvo paveikti (technologinis aspektas), nusikalstamos veikos kvalifikavimui

[142] Darius Sauliūnas et. al., *supra* note 7, p. 530; Nikolaj Goranin ir Dalius Mažeika, *supra* note 8, p. 25.
[143] Armanas Abramavičius et. al., *supra* note 2, p. 420; Aurelijus Gutauskas et. al., *supra* note 3, p. 464.
[144] Vitalij Vekhov ir Vladimir Golubev, *Rassledovanie kompjuternykh prestuplenij v stranakh SNG: Monografija* [Investigation of computer crimes in the CIS countries: Monograph], (Volgograd: Volgogradskaja akademija MVD Rossii, 2004), 78; Jurij Gavrilin et. al., *Prestuplenija v sfere kompjuternoj informacii: kvalifikacija i dokazyvanie* [Crimes in the sphere of computer information: qualification and proving] (Moskva: Knizhnyj mir, 2003), 22; Valerij Mazurov, *Kompjuternye prestuplenija: klassifikacija i sposoby protivodejstvija: Ychebno–prakticheskoe posobie* [Computer crimes: classification and methods of counteracting: Training and practical guide] (Moskva: Paleotip, Logos, 2002), 97.
[145] *Ibid*.; Vitalij Vekhov ir Vladimir Golubev, *op. cit.*, p. 79.
[146] Valerij Mazurov, *op. cit.*, p. 96.
[147] Council of Europe, *supra* note 11, p. 45; Committee of Ministers of the Council of Europe, *supra* note 13, p. 11.
[148] Armanas Abramavičius et. al., *op. cit.*, p. 420; Aurelijus Gutauskas et. al., *op. cit.*, p. 464; Vitalij Vekhov ir Vladimir Golubev, *op. cit.*, p. 79.
[149] "Vilniaus apygardos teismo Baudžiamųjų bylų skyriaus 2014 m. balandžio 16 d. nutartis baudžiamojoje byloje Nr. 1A-303-256/2014," prieiga per internetą: http://www.infolex.lt/tp/Default.aspx?id=20&item=doc&aktoid=821736&nr=1

pagal BK 196 straipsnį neturi reikšmės. Svarbu tai, kad galiausiai elektroniniai duomenys yra neteisėtai sunaikinti.

Mokslinėje literatūroje vyrauja skirtingos nuomonės dėl elektroninių duomenų sunaikinimo lygio. Vieni autoriai (D. Sauliūnas, N. Goranin, D. Mažeika, R. Mockevičius, D. Valatkevičius) elektroninių duomenų sunaikinimą sieja su jų visišku (pilnu) ištrynimu[150]. Kiti autoriai (Ju. Gavrilin, I. Popov) elektroninių duomenų sunaikinimą sieja su jų visišku ar daliniu ištrynimu, dėl kurio elektroniniai duomenys nustoja egzistuoti dėl esminių kokybinių požymių praradimo[151]. Manytina, pastaruoju atveju žodžių junginys „nustoja egzistuoti“ vartojamas perkeltine prasme, kadangi dalinis tokių duomenų ištrynimas objektyviai negali jų visiškai sunaikinti. Taigi pastaruoju atveju sunaikintais taip pat pripažįstami iš dalies išlikę pradiniai elektroniniai duomenys, kurie dėl neteisėto poveikio jiems prarado esminius kokybinius požymius, dėl ko prilygintini neegzistuojantiems (toliau – ir iš dalies išlikę pradiniai elektroniniai duomenys). Iš tiesų, įmanoma situacija, kai elektroniniai duomenys bus taip neteisėtai paveikti, kad išliks jų dalis, tačiau visumoje šie duomenys bus sunaikinti. Taip leidžia manyti ir EKNPT baigiamosios ataskaitos II skyriaus 2 dalies c punktas ir Konvencijos aiškinamosios ataskaitos 61 punktas, kuriuose pažymėta, jog ištrynimas sunaikina duomenis, padarydamas juos neatpažįstamais[152]. Akivaizdu, kad įmanomas tik iš dalies išlikusių pradinių elektroninių duomenų atpažinimo lygio vertinimas. Tačiau tokių duomenų pripažinimas sunaikintais lemia būtinumą šią pavojingą veiką atriboti nuo kitų elektroninių duomenų integralumą pažeidžiančių veikų, t. y. jų pakeitimo, sugadinimo. Tai savo ruožtu reikalauja nustatyti kriterijus, kurių pagrindu iš dalies išlikusius pradinius elektroninius duomenis būtų galima pripažinti dėl neteisėto poveikio praradusiais esminius kokybinius požymius, dėl ko tokie duomenys prilygintini neegzistuojantiems. Minėtas elektroninių duomenų atpažinimo lygio vertinimo kriterijus (EKNPT baigiamosios ataskaitos II skyriaus 2 dalies c punktas, Konvencijos aiškinamosios ataskaitos 61 punktas) kritikuotinas dėl pernelyg subjektyvaus pobūdžio. Atsižvelgiant į neteisėto poveikio elektroniniams duomenims ir turto sunaikinimo ar sugadinimo nusikalstamų veikų glaudų tarpusavio ryšį, šiame kontekste paminėtinas susijęs turto sunaikinimo ir sugadinimo nusikalstamos veikos aiškinimas. A. Drakšienės teigimu, *„turtas laikomas sunaikintu, kai jis netenka savo ekonominės ir ūkinės vertės bei jo nebegalima naudoti pagal funkcinę paskirtį. Turtas gali prarasti vertę, kai: [...] 2) turtas praranda savo vartojamąsias savybes bei ekonominę vertę ir nebegali būti panaudojamas pagal paskirtį [...]; 3) lieka*

[150] Darius Sauliūnas et. al., *supra* note 7, p. 530; Nikolaj Goranin ir Dalius Mažeika, *supra* note 8, p. 25; Armanas Abramavičius et. al., *supra* note 2, p. 420.
[151] Jurij Gavrilin et. al., *supra* note 144, p. 22; Vitalij Vekhov ir Vladimir Golubev, *supra* note 144, p. 78.
[152] Council of Europe, *supra* note 11, p. 45; Committee of Ministers of the Council of Europe, *supra* note 13, p. 11.

tik turto dalis, kurios atstatymui reikalingos lėšos, viršijančios pirminę to daikto vertę [...]; 4) nors ir nepažeidžiamas, tačiau nustoja egzistuoti kaip turtas“[153]. Taigi išlikusi turto dalis taip pat gali būti pripažinta sunaikinta. Tokiu turtas pripažįstamas, be kita ko, atsižvelgiant į jo vartojamųjų savybių bei ekonominės vertės praradimo lygį, galimumą naudoti pagal paskirtį, turto atstatymui reikalingų lėšų santykį su jo pirmine verte. Manytina, elektroninių duomenų specifika lemia tai, kad net ir menkiausias poveikis jiems gali sąlygoti visišką elektroninių duomenų vartojamųjų savybių bei ekonominės vertės praradimą ir padaryti juos visiškai nenaudotinais pagal paskirtį. Todėl pastarieji kriterijai nėra tinkami iš dalies išlikusius pradinius elektroninius duomenis pripažįstant sunaikintais. Vertinant atkūrimo kaštų ir pradinės vertės santykio kriterijaus pritaikomumą būtina turėti omenyje, jog elektroninių duomenų atkūrimas dažnai priklauso nuo techninių galimybių tai padaryti buvimo ar nebuvimo, kuriai esant, tam nebūtinai gali būti reikalingos lėšos ar šios lėšos nebūtinai gali būti proporcingos pradinių elektroninių duomenų vertei, pagaliau, elektroninių duomenų vertė dėl didelės jų įvairovės gali būti diskutuotina. Tačiau tai, manytina, nepaneigia atkūrimo kaštų ir pradinės vertės santykio kriterijaus taikymo galimybės iš dalies išlikusius pradinius elektroninius duomenis pripažįstant sunaikintais, jeigu tokių kaštų dydis *inter alia* priklauso nuo elektroninių duomenų sunaikinimo lygio. Taip pat šiuo atveju, manytina, aktualūs elektroninių duomenų atkūrimo galimumo, metodų ir pan. kriterijai, jeigu tai *inter alia* priklauso nuo elektroninių duomenų sunaikinimo lygio. Vis dėlto, būtina turėti omenyje, kad iš dalies išlikusius pradinius elektroninius duomenis pripažinti sunaikintais autoriai (Ju. Gavrilin, I. Popov) siūlo Rusijos Federacijos baudžiamojo kodekso 272 straipsnio kontekste, kuriame integralumo baudžiamoji teisinė apsauga siejama tik su kompiuterinės informacijos sunaikinimu, modifikavimu. Tuo tarpu BK 196 straipsnyje papildomai kriminalizuotas elektroninių duomenų sugadinimas, kuris mokslinėje literatūroje[154] siejamas su tokių duomenų pavertimu nenaudotinais ar beprasmiais, padarymu nesuprantamais, turinio tapimu nesuprantamu (naudotojui ar duomenis apdorojančiai sistemai), neįmanomumu identifikuoti elektroninius duomenis ir pan. Manytina, tai taip pat būdinga iš dalies išlikusiems pradiniams elektroniniams duomenims. Dėl šios priežasties, taip pat siekiant teisinio aiškumo, iš dalies išlikusių pradinių elektroninių duomenų pripažinimas sunaikintais ir išskyrimas greta elektroninių duomenų visiško sunaikinimo, sugadinimo ir pakeitimo pavojingų veikų BK 196 straipsnio kontekste pripažintinas pertekliniu.

[153] Armanas Abramavičius et. al., *supra* note 2, p. 370-371.
[154] Plačiau žr. šio darbo p. 44-45.

Mokslinėje literatūroje vieni autoriai elektroninių duomenų sunaikinimą sieja su jų panaudojimo pagal tikslinę paskirtį negalimumu (R. Mockevičius, D. Valatkevičius, M. Kuzminovas, V. Golubev)[155]. Tuo tarpu kiti autoriai elektroninių duomenų sunaikinimą sieja su jų pavertimu netinkamais naudoti pagal paskirtį (A. Popov, A. Pushkin, M. Dvoreckij, J. Liapunov, V. Maksimov, K. Skoromnikov, V. Komissarov, J. M. Tkachevskij ir kt.)[156]. Manytina, sunaikintų elektroninių duomenų netinkamumas naudoti pagal paskirtį tiksliau atspindi jų integralumo pažeidimo esmę, kadangi tokios galimybės nebuvimą gali lemti ir kitos, įskaitant elektroninių duomenų prieinamumo pažeidimą, priežastys.

R. Mockevičiaus, D. Valatkevičiaus, M. Kuzminovo, V. Golubev teigimu, elektroninių duomenų sunaikinimas nepriklauso nuo galimybės juos atstatyti (atkurti)[157]. Tuo tarpu A. Popov, A. Pushkin, M. Dvoreckij, K. Skoromnikov, V. Komissarov elektroninių duomenų sunaikinimą sieja su jos atstatymo (atkūrimo) negalimumu (rus. *когда она не может быть восстановлена*)[158]. Pasak M. Gercke, Konvencijos dėl elektroninių nusikaltimų rengėjai pateikdami ištrynimo apibrėžimą nedarė skirtumo tarp įvairių būdų, kuriais duomenys gali būti ištrinti. Duomenų perkėlimas į virtualią šiukšlių dėžę nepašalina (angl. *remove*) failo iš kietojo disko. Netgi šiukšlių dėžės „ištuštinimas“ nebūtinai pašaliną failą. Todėl nėra aišku, ar ištrintų duomenų atkūrimas užkertą kelią Konvencijos 4 straipsnio taikymui.[159] Vis dėlto, kaip teisingai pastebi A. Volevodz, informacijos ištrynimas, kurio pagrindu failas nėra sunaikinamas technine prasme, kelia didelę grėsmę informacijos prieinamumui ir saugumui (taigi – ir integralumui – *aut. pastaba*). Todėl vartotojo turimos galimybės atkurti sunaikintą informaciją pasitelkus specialią aparatinę–programinę įrangą ar gauti tokią informaciją iš kito vartotojo neatleidžia kaltininko nuo baudžiamosios atsakomybės.[160] Ju. Gavrilin teigimu, taip pat nėra svarbu, ar nukentėjęs asmuo turėjo kaltininko sunaikintų elektroninių duomenų kopiją[161]. Tą patį teigia R. Mockevičius ir D. Valatkevičius[162], taip pat M. Kuzminovas, kuris papildomai pažymi, kad *„[...] šiuo atveju galimas atleidimas nuo baudžiamosios atsakomybės dėl mažareikšmiškumo“*[163].

---

[155] Armanas Abramavičius et. al., *supra* note 2, p. 420; Aurelijus Gutauskas et. al., *supra* note 3, p. 416; Vitalij Vekhov ir Vladimir Golubev, *supra* note 144, p. 79.
[156] Valerij Mazurov, *supra* note 144, p. 96-97; Vitalij Vekhov ir Vladimir Golubev, *op. cit.*, p. 79.
[157] Armanas Abramavičius et. al., *op. cit.*, p. 420; Aurelijus Gutauskas et. al., *op. cit.*, p. 416; Vitalij Vekhov ir Vladimir Golubev, *op. cit.*, p. 79.
[158] *Ibid.*
[159] Marco Gercke, “Understanding cybercrime: Phenomena, challenges and legal response,“ p. 187, 296, žiūrėta 2016 05 15, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf
[160] Aleksandr Volevodz, *Protivodejstvie kompjuternym prestuplenijam: pravovye osnovy mezhdunarodnogo sotrudnichestva* [Combating computer crimes: the legal framework for international cooperation] (Moskva: Izdatelstvo „Jurlitinform“, 2002), 67-68.
[161] Jurij Gavrilin et. al., *supra* note 144, p. 22.
[162] Armanas Abramavičius et. al., *op. cit.*, p. 421.
[163] Aurelijus Gutauskas et. al., *op. cit.*, p. 465.

Toks aiškinimas aptiktinas teismų praktikoje. Štai Kauno apygardos teismo Baudžiamųjų bylų skyriaus 2012 m. spalio 22 d. nutartimi išnagrinėtas apeliacinis skundas, kuriuo A. A. ginčijo pirmos instancijos teismo nuosprendį *inter alia* dėl to, kad *jis sunaikino internetinėje svetainėje buvusius elektroninius duomenis. Apelianto manymu, nebuvo surinkta jokių objektyvių įrodymų, patvirtinančių, kad internetinės svetainės negalima buvo atstatyti iš kietojo kompiuterio disko arba kitais būdais*. Atmesdamas nuteistojo apeliacinį skundą aptariamoje dalyje Kauno apygardos teismas pažymėjo: *„Apelianto argumentas, jog internetinės svetainės atkūrimas iš kietojo disko yra labai nesudėtingas procesas bei kad civilinio ieškovo atstovas skirtingai nurodė aplinkybes apie internetinės svetainės atkūrimo galimybes niekaip nesusijęs su šios konkrečios nusikalstamos veikos kvalifikavimu. Atžymėtina ir tai, jog esanti galimybė specialios programinės įrangos pagalba atstatyti, atkurti sunaikintus, sugadintus, pakeistus ar pašalintus duomenis nepašalina baudžiamosios atsakomybės. Jos nepašalina ir tas faktas, kad nukentėjusysis turi tokių duomenų kopiją“*.[164] EKNPT baigiamosios ataskaitos II skyriaus 2 dalies c punkte ir Konvencijos aiškinamosios ataskaitos 60 punkte aptariamos nusikalstamos veikos kriminalizavimu saugomas teisinis interesas apibrėžtas kaip laikomų kompiuterinių duomenų ar kompiuterinių programų integralumas ir tinkamas funkcionavimas ar naudojimas. Aptariamame EKNPT baigiamosios ataskaitos punkte papildomai nurodyta, kad pavojingos veikos turi daryti neigiamą poveikį duomenų ar programų galimybei funkcionuoti pagal jais disponuojančio asmens priskirtą užduotį.[165] Teigtina, kad elektroninių duomenų integralumas, tinkamumas ir galimumas funkcionuoti pagal vartotojo priskirtą užduotį, taip pat elektroninių duomenų naudojimo galimybė jų sunaikinimu yra pažeidžiami. To nepaneigia elektroninių duomenų atstatymo galimybė. Todėl pritartina autorių pozicijai, kurios pagrindu galimybė atstatyti sunaikintus elektroninius duomenis nepaneigia jų sunaikinimo. Tuo tarpu elektroninių duomenų sunaikinimo konstatavimas tik tuomet, kai nėra galimybės jų atstatyti, neatitinka aptariama nusikalstama veika saugomo teisinio intereso.

Mokslinėje literatūroje vieni autoriai elektroninių duomenų sunaikinimą sieja su jų ištrynimu iš kompiuterio (elektroninės skaičiavimo mašinos) atminties (D. Sauliūnas, S. Pashin)[166], kiti su jų ištrynimu tiek iš informacinės sistemos standžiojo disko, tiek išorinių laikmenų (R. Mockevičius, M.

[164] "Kauno apygardos teismo Baudžiamųjų bylų skyriaus 2012 m. spalio 22 d. nutartis baudžiamojoje byloje Nr. 1A-94-175/2012," prieiga per internetą: http://www.infolex.lt/tp/Default.aspx?id=20&item=doc&aktoid=480057&nr=1
[165] Council of Europe, *supra* note 11, p. 45; Committee of Ministers of the Council of Europe, *supra* note 13, p. 11.
[166] Darius Sauliūnas et. al., *supra* note 7, p. 530; Vitalij Vekhov ir Vladimir Golubev, *supra* note 144, p. 78.

Kuzminovas)[167]. Pritartina tų autorių pozicijai, kurie elektroninių duomenų sunaikinimą sieja su jų ištrynimu iš bet kurių laikmenų (S. Nikulin, M. Karelina, A. Volevodz)[168].

Pagaliau, A. Volevodz teigimu, elektroninių duomenų sunaikinimu nepripažintinas failo, kuriame ši yra, pavadinimo pakeitimas[169]. Kaip pastebi V. Mazurov, tai nedaro įtakos šiuose failuose esančių elektroninių duomenų kokybei. Todėl tokie veiksmai turėtų būti vertinami kaip jų modifikavimas ar blokavimas (rus. *блокирование*), kadangi dėl to vartotojas gali laikinai ar visam laikui prarasti prieigą prie failo.[170] Anot A. Volevodz, informacijos sunaikinimu nepripažintinas failų senų versijų automatinis pakeitimas naujomis[171]. Pritartina nurodytiems autorių teiginiams.

4.2.2. Pakeitimas, sugadinimas

Kita BK 196 straipsnyje kriminalizuota pavojinga veika, kuria pasireiškia neteisėtas poveikis elektroniniams duomenims, yra jų pakeitimas. Konvencijos aiškinamosios ataskaitos 61 punkte duomenų pakeitimo pavojinga veika apibūdinama kaip esamų (angl. *existing*) duomenų modifikavimas[172]. EKNPT baigiamosios ataskaitos II skyriaus 2 dalies c punkte teigiama, jog aptariama pavojinga veika turi būti pakeista duomenų ar programų informacinė kokybė, paprastai – susijusio asmens nenaudai, pvz., teisės disponuoti duomenimis neautorizuotas pažeidimas ar kišimasis į ją, privatumo pažeidimas. Pakeitimo pavyzdžiais įvardijami papildymas naujais duomenimis ar sujungimas su kitais duomenimis.[173]

Pasak S. Borodin, modifikavimas – tai elektroninių duomenų turinio pakeitimas, lyginant su tuo, kurį savininkas ar teisėtas valdytojas turėjo iki nusikalstamos veikos padarymo[174]. D. Sauliūno teigimu, *„kompiuterinės informacijos pakeitimas – dalies failo turinio ištrynimas, kitų duomenų įrašymas ar kitoks poveikis turiniui, jeigu originalas yra modifikuojamas“*[175]. Anot N. Goranin ir D. Mažeikos, *„duomenų pakeitimas – tai duomenų turinio pakeitimas ar kitoks poveikis turiniui, modifikuojant originalą“*[176]. Apibendrinus, nurodyti autoriai pakeitimą sieja su pradinių elektroninių duomenų modifikavimu, kuris pasireiškia poveikiu jų turiniui. Pateikdami savo esme tapatų

[167] Armanas Abramavičius et. al., *supra* note 2, p. 420; Aurelijus Gutauskas et. al., *supra* note 3, p. 464.
[168] Aleksandr Volevodz, *supra* note 160, p. 67; Vitalij Vekhov ir Vladimir Golubev, *supra* note 144, p. 79.
[169] Aleksandr Volevodz, *op. cit.*, p. 68.
[170] Valerij Mazurov, *supra* note 144, p. 96-97.
[171] Aleksandr Volevodz, *op. cit.*, p. 68.
[172] Committee of Ministers of the Council of Europe, *supra* note 13, p. 11.
[173] Council of Europe, *supra* note 11, p. 34, 46, 60-61.
[174] Vitalij Vekhov ir Vladimir Golubev, *op. cit.*, p. 81.
[175] Darius Sauliūnas et. al., *supra* note 7, p. 531.
[176] Nikolaj Goranin ir Dalius Mažeika, *supra* note 8, p. 25.

apibrėžimą, Ju. Gavrilin ir I. Popov išskiria papildomą požymį: modifikavimas pasireiškia elektroninių duomenų pradinės būklės pakeitimu (pvz., duomenų bazės restruktūrizavimu ar reorganizavimu, jos failuose esančių įrašų ištrynimu ar papildymu, elektroninei skaičiavimo mašinai ar duomenų bazei skirtos programos išvertimu į kitą kalbą), nekeičiančiu objekto esmės (rus. *сущность*)[177]. Kaip pastebi J. Clough, Jungtinių Amerikos Valstijų statuto kontekste pakeitimo termino įprasta prasmė suprantama kaip kokios nors konkrečios savybės pasikeitimas, netampant kuo nors kitu[178]. Taigi neteisėtas poveikis elektroniniams duomenims dėl kurio „pasikeičia jų esmė“, elektroniniai duomenys tampa „kuo nors kitu“ nepripažįstamas jų pakeitimu. Manytina, tokį aiškinimą galima įžvelgti EKNPT baigiamosios ataskaitos II skyriaus 2 dalies c punkte, kuriame viena iš duomenų ištrynimo priežasčių įvardintas magnetinės juostos perrašymas (angl. *overprinting*)[179]. Manytina, pradinių elektroninių duomenų visiškas (pilnas) pakeitimas pripažintinas būdu, kuriuo jie sunaikinami. Kiek kitokios pozicijos yra R. Mockevičius ir D. Valatkevičius, kurie elektroninių duomenų pakeitimu pripažįsta *„[...] bet kokį duomenų modifikavimą: vietoje informacinėje sistemoje buvusių duomenų yra patalpinami kiti duomenys – kito turinio, formos, pobūdžio ar apimties, ištrinama dalis duomenų arba papildoma naujais duomenimis, pakeičiama esančių duomenų forma ar pobūdis. Duomenys gali būti pakeisti pilnai arba iš dalies. Pakeistos dalies dydis nėra svarbus nusikaltimo kvalifikavimui“*[180]. Tą patį teigia ir M. Kuzminovas[181]. Taigi šie autoriai elektroninių duomenų pakeitimu *inter alia* pripažįsta visišką (pilną) (pavienių) tokių duomenų pakeitimą, taip pat vienų elektroninių duomenų visišką (pilną) pakeitimą kitais (kaip visumos). Minėta, tai, kaip elektroniniai duomenys buvo paveikti (technologinis aspektas), nusikalstamos veikos kvalifikavimui neturi reikšmės. Svarbu nustatyti tai, kad galiausiai tokie duomenys yra neteisėtai *inter alia* sunaikinti, pakeisti. Visiškas (pilnas) (pavienių) elektroninių duomenų pakeitimas turėtų būti vertinamas kaip jų sunaikinimas, kadangi galiausiai pradinių elektroninių duomenų nelieka. Šiuo atveju neturi reikšmės tai, kad elektroniniai duomenys sunaikinami jų visiško pakeitimo būdu. Dėl tų pačių priežasčių sunaikinimu turėtų būti pripažįstamas vienų elektroninių duomenų visiškas (pilnas) pakeitimas kitais (kaip visumos), susijęs su pradinių elektroninių duomenų sunaikinimu. Tuo tarpu, vienų elektroninių duomenų visiškas (pilnas) pakeitimas kitais (kaip visumos), kuris nėra susijęs su pradinių elektroninių duomenų sunaikinimu, turėtų būti kvalifikuojamas kaip tokių duomenų prieinamumo pažeidimas, kadangi pradinių elektroninių duomenų integralumas nėra paveikiamas.

[177] Jurij Gavrilin et. al., *supra* note 144, p. 23; Vitalij Vekhov ir Vladimir Golubev, *supra* note 144, p. 81.
[178] Jonathan Clough, *supra* note 10, p. 111.
[179] Council of Europe, *supra* note 11, p. 45; Committee of Ministers of the Council of Europe, *supra* note 13, p. 11.
[180] Armanas Abramavičius et. al., *supra* note 2, p. 420-421.
[181] Aurelijus Gutauskas et. al., *supra* note 3, p. 464-465.

Pagaliau, S. Kazancev modifikavimą sieja su naujų nepageidautinų savybių atsiradimu[182]. V. Tkachenko teigimu, modifikavimas apsunkina elektroninių duomenų naudojimą[183]. Kaip pastebi M. Gercke, pakeitimas nebūtinai menkina galimumą naudoti tokius duomenis (angl. *serviceability*)[184]. Manytina, tarp nurodytų autorių pozicijų nėra esminių prieštaravimų, kadangi nepageidautinų savybių atsiradimas apima elektroninių duomenų naudojimo apsunkinimą, tokio naudojimo galimumo menkinimą, tuo tarpu elektroninių duomenų naudojimo apsunkinimas nebūtinai menkina galimumą naudoti tokius duomenis, t. y. naudojimo galimybė gali išlikti, nors ir būtų apsunkinta. M. Kuzminovo teigimu, „*nusikalstamos veikos kvalifikavimui, jei nustatyta žala, neturi reikšmės kaltininko aiškinimas, kad keisdamas jis norėjo patobulinti, pagerinti duomenis*“[185]. Tokiai pozicijai pritartina.

EKNPT baigiamojoje ataskaitoje pakeitimo pavojinga veika numatyta atskirai nuo kompiuterinių programų ar duomenų sugadinimo veikos – kaip savarankiška įtvirtinta neprivalomame sąraše (II skyriaus 3 dalies a punktas) tarp mažiau pavojingų veikų, kurios, D. Štitilio ir kitų žodžiais, *„[...] įtraukiamos į įstatymų leidybą, bet nėra privalomos“*[186]. Kita vertus, pabrėžtas kompiuterinių programų ar duomenų pakeitimo ir sugadinimo veikų glaudus ryšys, netgi dalinis sutapimas. Teigiama, jog ne iš karto aišku, kokie atvejai suprantami kaip kompiuterinių duomenų ar programų pakeitimas (ar modifikavimas) ir nepatenka į jų ištrynimo, sugadinimo, pabloginimo ar naudojimo apribojimo pavojingų veikų sritį. Pažymėta, kad savarankiška pakeitimo (ar modifikavimo) pavojingos veikos apimtis bet kuriuo atveju koreliuoja su, pvz., sugadinimo, pabloginimo pavojingų veikų aiškinimu.[187] Šiam ryšiui atskleisti toliau darbe analizuojamos elektroninių duomenų sugadinimo ir pabloginimo pavojingos veikos.

EKNPT baigiamosios ataskaitos II skyriaus 2 dalies c punkte ir Konvencijos aiškinamosios ataskaitos 61 punkte sugadinimo ir (kokybės) pabloginimo (pažeidimo) (angl. *deteriorating*, rus. *ухудшение качества*) pavojingos veikos apibūdinamos kaip persidengiančios bei pirmiausia susijusios su integralumo ar duomenų ir programų informacinio turinio neigiamu pakeitimu. Minėtame EKNPT baigiamosios ataskaitos punkte papildomai pažymėta, kad aptariamos pavojingos veikos taip pat apima atvejus, kurie Kanados teisėje apibūdinami kaip „pavertimas nenaudotinais ar beprasmiais“ (angl. *rendering useless or meaningless*).[188] Komentuodamas Kanados baudžiamojo

[182] Sergej Kazancev et. al., *Pravovoe obespechenie informacionnoj bezopasnosti: 2–e izdanie* [Legal protection of information security: 2nd Edition] (Moskva: Izdatelskij centr „Akademija“, 2007), 154.
[183] Valerij Mazurov, *supra* note 144, p. 100.
[184] Marco Gercke, *supra* note 159, p. 187, 297.
[185] Aurelijus Gutauskas et. al., *supra* note 3, p. 465.
[186] Darius Štitilis et. al., *supra* note 6, p. 251.
[187] Council of Europe, *supra* note 11, p. 34, 46, 60.
[188] *Ibid.*, p. 45; Committee of Ministers of the Council of Europe, *supra* note 13, p. 11.

kodekso 430 (1.1) straipsnį J. Clough pažymėjo, kad elektroninių duomenų pavertimą nenaudotinais, beprasmiais, neefektyviais gali lemti papildomų duomenų pridėjimas, kurie esamus duomenis padaro nesuprantamais (angl. *unintelligible*), ar klaidingų duomenų pridėjimas, o tai reiškia, kad originaliais duomenimis negalima pasitikėti[189]. Iš esmės taip pat nacionalinėje baudžiamosios teisės doktrinoje aiškinama BK 196 straipsnyje kriminalizuota elektroninių duomenų sugadinimo pavojinga veika.

Pasak D. Sauliūno, *„kompiuterinės informacijos sugadinimas – tai toks poveikis failui, kad jo turinys tampa nesuprantamas ir tik programavimo specialistai panaudodami nemažas laiko ir intelektines sąnaudas gali jį atstatyti“*[190]. Anot N. Goranin ir D. Mažeikos, *„sugadinimas – tai toks poveikis duomenims, kai jų turinys tampa nesuprantamas naudotojui ar duomenis apdorojančiai sistemai, o duomenų atstatymas reikalauja specialių informatikos žinių“*[191]. R. Mockevičiaus, D. Valatkevičiaus teigimu, *„elektroninių duomenų sugadinimas reiškia tokį poveikį duomenims, kai jų pobūdis ir esmė po nusikalstamos veikos subjekto veiksmų pasikeitė tiek, jog jų turinio neįmanoma suprasti arba jų neįmanoma identifikuoti, t. y. po veikos tik dalis duomenų išliko savo pirminėje būsenoje ir apimtyje. Sugadintų duomenų dalies dydis nėra svarbus nusikaltimo kvalifikavimui [...]“*[192]. Teigdamas tą patį, M. Kuzminovas akcentuoja, kad *„esminis dalykas yra duomenų pasikeitimo faktas, dėl ko buvo padaryta žalos“*[193].

Taigi EKNPT baigiamojoje ataskaitoje, Konvencijos aiškinamojoje ataskaitoje sugadinimo ir pabloginimo pavojingos veikos siejamos su pakeitimu. Teigtina, kad nacionalinėje baudžiamosios teisės doktrinoje minimas sugadintų elektroninių duomenų pasikeitimas yra ne kas kita kaip jų pakeitimo rezultatas. Tai leidžia teigti, kad elektroninių duomenų sugadinimo ir pabloginimo pavojingų veikų pagrindą sudaro pakeitimas. Taigi elektroninių duomenų sugadinimas, pabloginimas pripažintinas pakeitimo pavojingos veikos atmaina. Nuo elektroninių duomenų pakeitimo, sugadinimo ir pabloginimo pavojingos veikos skiriasi pakeistų elektroninių duomenų specialiais kokybiniais požymiais: integralumo ar informacinio turinio pasikeitimu, pavertimu nenaudotinais ar beprasmiais, padarymu nesuprantamais, turinio tapimu nesuprantamu (naudotojui ar duomenis apdorojančiai sistemai), neįmanomumu identifikuoti elektroninius duomenis ir pan. Todėl sugadinimo (pabloginimo) pavojinga veika pripažintina specialiu elektroninių duomenų pakeitimo atveju. Pasak R. Mockevičiaus ir D. Valatkevičiaus, *„kalbant apie pakeitimą, pabrėžtina, kad tai yra veikimas tam tikra kryptimi, t. y. siekiant pakeisti duomenų reikšmę ir turinį, todėl pagrindinis tokios veikos*

[189] Jonathan Clough, *supra* note 10, p. 114.
[190] Darius Sauliūnas et. al., *supra* note 7, p. 531.
[191] Nikolaj Goranin ir Dalius Mažeika, *supra* note 8, p. 25.
[192] Armanas Abramavičius et. al., *supra* note 2, p. 420.
[193] Aurelijus Gutauskas et. al., *supra* note 3, p. 464.

elementas yra duomenų pakeitimo kryptingumas. Jeigu tokio kryptingumo nėra, veika nelaikoma duomenų pakeitimu, o jos sunaikinimu ar sugadinimu“[194]. Tą patį teigia ir M. Kuzminovas[195]. Tokiai autorių pozicijai pritartina. Vis dėlto, įstatymų leidėjo sprendimas vienoje BK 196 straipsnio dalyje kriminalizuoti dvi – pakeitimo ir sugadinimo – pavojingas veikas, kurių abiejų pagrindą sudaro pakeitimas, o atribojimas pagrįstas specialiais pakeistų elektroninių duomenų kokybiniais požymiais, kurie priskirti tokių duomenų sugadinimo pavojingai veikai (nors dėl tapataus pagrindo juos taip pat gali sukelti pakeitimo pavojingos veikos padarymas), ir kaltininko tyčios kryptingumu, diskutuotinas.

4.2.3. Naudojimosi apribojimas technine įranga, programine įranga ar kitais būdais, pašalinimas

BK 196 straipsnyje elektroninių duomenų prieinamumo baudžiamoji teisinė apsauga užtikrinama naudojimosi tokiais duomenimis apribojimo technine įranga, programine įranga ar kitais būdais, taip pat elektroninių duomenų pašalinimo kriminalizavimu.

Remiantis EKNPT baigiamosios ataskaitos II skyriaus 2 dalies c punktu, naudojimasis duomenimis apribojamas kai kaltininkas juos pradangina (angl. *disappear*) ne ištrindamas, o duodamas atitinkamas instrukcijas. Tokiu būdu duomenys yra pašalinami (angl. *removed*) nuo autorizuotų vartotojų prieigos, dėl ko negali būti naudojami.[196] Konvencijos aiškinamosios ataskaitos 61 punkte naudojimosi kompiuteriniais duomenimis apribojimas apibūdinamas kaip bet kokie veiksmai, kuriais apribojamas (angl. *prevents*, rus. *ограничивающее*) ar nutraukiamas (angl. *terminates*, rus. *перекрывающее*) duomenų prieinamumas asmeniui, turinčiam prieigą prie kompiuterio ar duomenų laikmenos, kuriuose jie laikomi[197].

Mokslinėje literatūroje naudojimosi elektroniniais duomenimis apribojimas siejamas su negalėjimu gauti prieigą ar galimybės prieiti prie tokių duomenų nebuvimu (S. Kazancev, Kochoi, D. Saveljevo)[198], galimybės naudoti elektroninius duomenis nebuvimu ar panaikinimu (V. Kommissarov, J. Tkachevskij, M. Kuzminovas, R. Mockevičius, D. Valatkevičius, J. Gulbin)[199], prieigos prie informacinės sistemos ir jos teikiamų elektroninių duomenų resursų apribojimu, nutraukimu, dirbtiniu apsunkinimu (A. Volevodz, M. Karelina)[200], kliūčių laisvam elektroninių

[194] Armanas Abramavičius et. al., *supra* note 2, p. 420-421.
[195] Aurelijus Gutauskas et. al., *supra* note 3, p. 464-465.
[196] Council of Europe, *supra* note 11, p. 45.
[197] Committee of Ministers of the Council of Europe, *supra* note 13, p. 11.
[198] S. Ja. Kazancev et. al., *supra* note 182, p. 154; Valerij Mazurov, *supra* note 144, p. 99.
[199] *Ibid*., p. 98; Aurelijus Gutauskas et. al., *op. cit.*, p. 465; Armanas Abramavičius et. al., *op. cit.*, p. 422.
[200] Aleksandr Volevodz, *supra* note 160, p. 68; Vitalij Vekhov ir Vladimir Golubev, *supra* note 144, p. 79.

duomenų naudojimui sudarymu (S. Nikulin)[201], dirbtiniu vartotojų prieigos prie elektroninių duomenų apsunkinimu (J. Liapunov, V. Maksimov, T. Vaulina, S. Pashin, K. Skoromnikov, I. Klepickij, V. Tkachenko)[202]. Paminėtina ir tai, kad mokslinėje literatūroje naudojimosi elektroniniais duomenimis apribojimas siejamas su jų išsaugojimu (S. Nikulin, J. Tkachevskij, V. Kommissarov, A. Volevodz)[203], nesunaikinimu (J. Liapunov, V. Maksimov, T. Vaulina, S. Pashin, K. Skoromnikov, I. Klepickij, V. Tkachenko)[204].

Konvencijos dėl elektroninių nusikaltimų projektuose Nr. 19, 22, 24, 25[205] pažymėta būtinybė Konvencijos aiškinamojoje ataskaitoje išaiškinti, kad naudojimosi duomenimis apribojimo pavojinga veika turi dvi bendrai sutariamas prasmes: pirma, duomenų ištrynimo, kurio pagrindu duomenys nustoja fiziškai egzistuoti; antra, padarymo neprieinamais (angl. *render inaccessible*), t. y. prieigos prie duomenų užkirtimo juos išsaugant[206]. Tačiau šis išaiškinimas Konvencijos aiškinamosios ataskaitos 61 punkte nebuvo įtvirtintas *expressis verbis*. Naudojimosi kompiuteriniais duomenimis apribojimas čia siejamas su bet kokių veiksmų atlikimu.[207] Tai leidžia teigti, kad elektroninių duomenų sunaikinimas pripažintinas vienu iš naudojimosi tokiais duomenimis apribojimo būdų. Todėl aptariamos pavojingos veikos konkuruoja tarpusavyje. Kiekvienas elektroninių duomenų sunaikinimas apriboja naudojimąsi šiais duomenimis, tačiau ne kiekvienas naudojimosi elektroniniais duomenimis apribojimas pasireiškia tokių duomenų sunaikinimu. Elektroninių duomenų sunaikinimas yra ne tik naudojimosi tokiais duomenimis apribojimo būdas, bet ir tokio neteisėto poveikio rezultatas. Naudojimosi elektroniniais duomenimis apribojimas padarytą veiką atspindi tik iš dalies. Visumoje padaryta veika pasireiškia elektroninių duomenų sunaikinimu, dėl kurio naudojimasis tokiais duomenimis objektyviai nėra įmanomas. Atsižvelgiant į tai, aptariamu atveju kvalifikuojant nusikalstamą veiką prioritetas turėtų būti teikiamas išsamiau padarytą veiką

[201] Vitalij Vekhov ir Vladimir Golubev, *supra* note 144, p. 79.
[202] Valerij Mazurov, *supra* note 144, p. 98.
[203] *Ibid.*; Vitalij Vekhov ir Vladimir Golubev, *op. cit.*, p. 79-80; Aleksandr Volevodz, *supra* note 160, p. 68.
[204] Valerij Mazurov, *op. cit.*, p. 98.
[205] Darbo autoriui pavyko rasti šiuos ir paskutinįjį – Nr. 27 Konvencijos dėl elektroninių nusikaltimų projektą, kuris, bent jau aptariamoje dalyje atitinka priimtos Konvencijos ir jos aiškinamosios ataskaitos nuostatas.
[206] European Committee on crime problems, Committee of Experts on Crime in Cyber–space "Draft Convention on Cyber–crime (Draft N° 19)," žiūrėta 2016 05 15, http://www.politechbot.com/docs/treaty.html; European Committee on crime problems, Committee of Experts on Crime in Cyber–space "Draft Convention on Cyber–crime (Draft N° 22 REV 2)," žiūrėta 2016 05 15, http://www.iwar.org.uk/law/resources/eu/cybercrime.doc; European Committee on crime problems, Committee of Experts on Crime in Cyber–space "Draft Convention on Cyber–crime (Draft N° 24 REV. 2)," žiūrėta 2016 05 15, http://www.cyber-rights.org/documents/cybercrime24.htm; European Committee on crime problems, Committee of Experts on Crime in Cyber–space "Draft Convention on Cyber–crime (Draft N° 25 REV.)," žiūrėta 2016 05 15, http://www.interlex.it/testi/cybercr25.htm; European Committee on crime problems, Committee of Experts on Crime in Cyber–space "Draft Convention on Cyber–Crime and Explanatory Memorandum Related Thereto," žiūrėta 2016 05 15, http://www.statewatch.org/news/2001/may/cybercrime27.doc
[207] Committee of Ministers of the Council of Europe, *supra* note 13, p. 11.

atspindinčiam elektroninių duomenų sunaikinimui. Kitokia situacija susiklosto atvejais, kai elektroniniai duomenys, kurių naudojimasis apribojamas, nėra sunaikinami. Tokiu atveju poveikis elektroniniams duomenims yra tik naudojimosi tokiais duomenimis apribojimo būdas. Todėl nustačius tyčią apriboti naudojimąsi elektroniniais duomenimis inkriminuotinas šios pavojingos veikos padarymas.

Mokslinėje literatūroje nėra vieningos nuomonės dėl to, kokį laiko tarpą turi trūkti naudojimosi elektroniniais duomenimis apribojimas. S. Kochoi, D. Saveljeva nurodo reikšmingą (rus. *значимый*) laiko tarpą, pakankamą tam, kad pažeisti elektroninių duomenų vartotojų normalią veiklą ar sudaryti tokio pažeidimo grėsmę. O. Baev, V. Meshcheriakov teigimu, naudojimosi elektroniniais duomenimis apribojimas turi priklausyti nuo konkrečioje organizacinėje sistemoje esančių tokių duomenų paskirties, svarbos ir laiko tarpo, per kurį jie yra (įprastai – *aut. pastaba*) valdomi ar funkcionuoja.[208] Kiti autoriai teigia, kad naudojimosi elektroniniais duomenimis apribojimas gali būti nuolatinis ar laikinas (V. Krylov, V. Golubev, R. Mockevičius, D. Valatkevičius)[209]. Pasak M. Kuzminovo, *„nusikalstamos veikos kvalifikavimui neturi reikšmės, kiek laiko tai trunka“*[210]. Pritartina pastarųjų autorių pozicijai, kadangi kiekvienas naudojimosi elektroniniais duomenims apribojimas pažeidžia jų prieinamumą, nepriklausomai nuo tokio apribojimo trukmės.

BK 196 straipsnyje kriminalizuotas naudojimosi elektroniniais duomenimis apribojimas technine įranga, programine įranga ar kitais būdais. M. Britz teigimu, techninė įranga susijusi su fizinio ar materialaus pobūdžio komponentais[211]. Pasak R. Mockevičiaus, D. Valatkevičiaus, M. Kuzminovo, techninė įranga – tai įrengti sudėtingi mechanizmai, pvz., techninės užkardos, radijo trikdžių įrenginiai ir panašiai[212]. Techninės įrangos pavyzdys aptiktinas Vilkaviškio rajono apylinkės teismo 2013 m. lapkričio 4 d. baudžiamajame įsakyme, kuriuo V. M., G. D., A. K. ir R. V nuteisti *inter alia* pagal BK 197 straipsnio 3 dalį, t. y. pripažinti kalti padarę neteisėto poveikio informacinei sistemai nusikalstamą veiką, o būtent: *jie atgabeno judriojo radijo ryšių blokavimo prietaisą (slopintuvą) bei jį eksploatavo ir dėl šio prietaiso skleidžiamų radijo trikdžių realiai sutrikdė informacinės sistemos UAB „O“ bazinės stoties darbą – šie trikdžiai darė neigiamą įtaką ryšio kokybę – padarydami nedidelę žalą įmonės veiklai*[213]. Šioje byloje nusikalstamos veikos kvalifikavimą pagal

[208] Valerij Mazurov, *supra* note 144, p. 99.
[209] *Ibid*., p. 100; Vitalij Vekhov ir Vladimir Golubev, *supra* note 144, p. 80; Armanas Abramavičius et. al., *supra* note 2, p. 422.
[210] Aurelijus Gutauskas et. al., *supra* note 3, p. 465.
[211] Marjie Britz, *Computer Forensics and Cyber Crime: Third Edition* (United States: Prentice Hall, 2013), 29.
[212] Armanas Abramavičius et. al., *op. cit.*, p. 422; Aurelijus Gutauskas et. al., *op. cit.*, p. 465.
[213] "Vilkaviškio rajono apylinkės teismo 2013 m. lapkričio 4 d. įsakymas baudžiamojoje byloje Nr. 1-239-633/2013," prieiga per internetą: http://www.infolex.lt/tp/787150?nr=1

BK 197 straipsnio 3 dalį apsprendė UAB „O“ bazinės stoties pripažinimas informacine sistema. Manytina, atitinkamo neteisėto poveikio elektroniniams duomenims atveju kaltinamųjų panaudotas judriojo radijo ryšių blokavimo prietaisas (slopintuvas) atitiktų BK 196 straipsnyje įtvirtintą techninės įrangos požymį. M. Britz teigimu, programinės įrangos terminas siejamas su instrukcijų seka, skirta atlikti konkrečią užduotį. Konkrečiau tariant, programinė įranga yra dvejetainės bitų sekos, kurią sudaro instrukcijų procesoriui sąrašas, interpretavimas. Techninės įrangos parametrai apibrėžia komandas, kurias ši gali vykdyti, o instrukcijos nurodo, ką jai daryti. Be instrukcijų techninė įranga negali atlikti jokių užduočių, funkcijų, išnaudoti kitų galimybių. Programinė įranga taip pat reikalinga tam, kad sistemoje esantiems komponentams nurodyti, kaip sąveikauti su vartotojais.[214] Pasak R. Mockevičiaus, D. Valatkevičiaus, *„apriboti naudojimąsi duomenimis galima panaudojus tiek sisteminę ar taikomąją, tiek specialiai sukurtą ar pritaikytą kenkėjišką programinę įrangą“*[215]. Tą patį, tik trumpiau nurodo M. Kuzminovas[216]. M. Britz teigimu, skiriamos trys pagrindinės programinės įrangos ar instrukcijų rūšys: įkrovos seka, operacinė sistema ir taikomoji programinė įranga. Kompiuterio įkrovos seka susijusi su etapų seka, kuriuos kompiuteris atlieka iš karto po įjungimo, kurie būtini tam, kad šis taptų naudotinas. Operacinė sistema yra programinės įrangos dalis, kuri vykdo vartotojo užklausas ir pateikia sąsają su technine įranga. Taikomoji programinė įranga yra iš anksto supakuotos instrukcijos, kurios leidžia vartotojams atlikti įvairias funkcijas. Kenkėjiška programinė įranga siejama su kodais, kurie sukelia žalą kompiuterio sistemai. Pavyzdžiui, atgalinės durys (angl. *back door*) yra kodai, kurie leidžia vartotojams įeiti į sistemą be autorizacijos; Trojos arklys (angl. *Trojan horse*) yra programa, kuri išoriškai pasireiškia teisėta paskirtimi, tačiau kartu turi paslėptų savybių, kaip, pvz., atgalines duris ar paslėptą programą ir kita.[217] Pagaliau, naudojimasis elektroniniais duomenimis gali būti apribojamas bet kokiais kitais būdais, kurie nėra įvardinti BK 196 straipsnio 1 dalies dispozicijoje, tačiau, akivaizdu, nepriskiriami aukščiau aptartiems požymiams. Šiame kontekste paminėtina, jog nei viename susijusiame viršnacionalinės teisės akte naudojimosi elektroniniais duomenimis apribojimas nėra siejamas su techninės įrangos, programinės įrangos panaudojimu ar kitais apribojimo būdais.

Kaip pastebi R. Mockevičius ir D. Valatkevičius, *„sutrikdžius ar nutraukus informacinės sistemos darbą yra apribojamas naudojimasis joje esančiais duomenimis, ir atvirkščiai – elektroninių duomenų (ar programinės įrangos) sunaikinimas, sugadinimas, pašalinimas ar pakeitimas gali sukelti*

[214] Marjie Britz, *supra* note 211, p. 29, 31.
[215] Armanas Abramavičius et. al., *supra* note 2, p. 422.
[216] Aurelijus Gutauskas et. al., *supra* note 3, p. 465.
[217] Marjie Britz, *op. cit.*, p. 31-32, 38.

visos informacinės sistemos darbo sutrikimą ar nutraukimą. Šios veikos yra atribojamos pagal tikslą, kurio siekė nusikalstamos veikos subjektas, – jeigu veika nukreipta daugiau į informacinės sistemos formą (techninę ir programinę informacinių sistemų įrangą), jos funkcionavimą, darant poveikį duomenims ir programoms, tuo pačiu ir visai sistemai, tai ir mažos programinės įrangos nedidelės dalies sugadinimas, sukėlęs tokį poveikį, bus kvalifikuojamas pagal BK 197 str. Tačiau tais atvejais, kai nusikalstama veika nukreipta į informacinių sistemų turinį – elektroninius duomenis ir programinę įrangą, – taikytinas BK 196 str. Be to, ne visi programinės įrangos sutrikimai gali sukelti informacinės sistemos sutrikimą"[218]. Iš dalies sutinkant su autorių siūlomu veikos kvalifikavimo variantu, tai pagrindžiantiems argumentams pritartina tik dalinai dėl žemiau nurodytų priežasčių.

Remiantis EKNPT baigiamąja ataskaita, *pirma*, kompiuterinių duomenų ir programų sugadinimo bei kompiuterio sabotažo nusikalstamos veikos yra glaudžiai susijusios, netgi dalinai persidengia (II skyriaus 2 dalies c punktas). Kompiuterio sabotažo veika saugomas teisinis interesas – kompiuterio sistemos ar telekomunikacijų sistemos savininko ir (ar) naudotojo interesas, kad šie tinkamai funkcionuotų – yra labai panašus į kompiuterinių duomenų ar programų sugadinimo veika saugomą teisinį interesą (II skyriaus 2 dalies d punkte), t. y. (saugomų) kompiuterinių duomenų ar kompiuterinių programų integralumas ir tinkamas funkcionavimas ar naudojimas (II skyriaus 2 dalies c punkte). Tačiau esminė kompiuterio sabotažo veikos dalis yra ketinimas sutrikdyti kompiuterio ir (ar) telekomunikacijų sistemos funkcionavimą. Tai skiriasi nuo to, ką būtų galima pavadinti kompiuterinių duomenų sugadinimu (II skyriaus 2 dalies d punktas).[219] Šiame kontekste paminėtina, kad R. Mockevičiaus ir D. Valatkevičiaus teigimu, BK 197 straipsnyje kriminalizuotos veikos *„[...] objektas – informacinių sistemų tvarkingas funkcionavimas (bet kokio pobūdžio funkcijų atlikimas) ar valdymas. Šia veika pažeidžiami tiek informacinių sistemų savininkų, tiek jų naudotojų interesai"*[220]. *Antra,* kompiuterio sabotažo nusikalstamos veikos tikslas įvardijamas kaip kompiuterio ar telekomunikacijos sistemos darbo sutrikdymas (II skyriaus 2 dalies d punktas). Tuo tarpu tikslas, kurio siekiama kompiuterinių duomenų ar kompiuterinių programų sugadinimo veikos kriminalizavimu yra analogiškos taikomai materialiems dalykams kompiuterinių duomenų ir kompiuterinių programų apsaugos nuo tyčinės žalos padarymo užtikrinimas (II skyriaus 2 dalies c punktas).[221] *Trečia*, kompiuterio sabotažo nusikalstamos veikos padarymo būdai (angl. *the means*) gali būti bet kokios rūšies kišimasis į kompiuterių sistemą, o dispozicijoje kompiuterinių duomenų ar kompiuterinių

[218] Armanas Abramavičius et. al., *supra* note 2, p. 427-428.
[219] Council of Europe, *supra* note 11, p. 44-49. Beje, analogiškas saugomas teisinis interesas nurodytas Konvencijos aiškinamosios ataskaitos 65 punkte aiškinant kišimosi į sistemą nusikalstamą veiką.
[220] Armanas Abramavičius et. al., *op. cit.*, p. 426.
[221] Council of Europe, *op. cit.*, p. 44-49.

programų *inter alia* ištrynimas, pakeitimas, naudojimosi apribojimas įtvirtinti kaip pavyzdžiai. Šie pavyzdžiai didžiąją dalimi – tiek, kiek yra padaryti neteisėtai – sudaro kompiuterinių duomenų nusikalstamą veiką. Skirtumai išplaukia iš saugomų teisinių interesų skirtumų (angl. *protected objects*). Kompiuterio ir telekomunikacijų sistemų saugomas teisinis interesas skatina bendrai nustatyti įsikišimo veikas (angl. *calls for the general inclusion of acts of interference*), kurių pavyzdžiai pateikti, ir šiuo atžvilgiu siekia toliau (angl. *it goes further*), negu duomenų sugadinimo nuostatos (II skyriaus 2 dalies d punktas). Kompiuterinių duomenų ištrynimas, pakeitimas, naudojimosi tokiais duomenimis apribojimas taip pat minimi Konvencijos dėl elektroninių nusikaltimų 5 straipsnyje (poveikis sistemai), Pamatinio sprendimo 2005/222/TVR 3 straipsnyje (neteisėtas įsikišimas į sistemą), Direktyvos 2013/40/ES 4 straipsnyje (neteisėtas įsikišimas į sistemą). Šiuose viršnacionalinės teisės aktuose taip pat išskiriamas kompiuterinių duomenų sugadinimas, o Pamatinio sprendimo 2005/222/TVR 3 straipsnyje ir Direktyvos 2013/40/ES 4 straipsnyje – ir tokių duomenų pašalinimas (nuslėpimas). Konvencijos aiškinamosios ataskaitos 66 punkte pažymėta, kad terminas „sutrikdymas“ (angl. *hindering*) siejamas su veikomis, kuriomis įsikišama į kompiuterinės sistemos tinkamą funkcionavimą. Toks sutrikdymas turi būti padarytas įvedant, perduodant, sugadinant, ištrinant ar pakeičiant kompiuteriniais duomenis arba apribojant naudojimąsi tokiais duomenimis.[222] Pasak R. Mockevičiaus ir D. Valatkevičiaus, *„informacinės sistemos darbo sutrikdymas arba nutraukimas yra galimas sunaikinant, sugadinant, pašalinant ar pakeičiant informacinėje sistemoje esančią programą [...], blokuojant ar apkraunant [...] informacinės sistemos naudojamus resursus [...] ir pan.“*[223]. *Pagaliau*, R. Marcinauskaitės teigimu, *„[...] IS ir elektroninių duomenų atskyrimo problemos kyla dėl to, kad elektroniniais duomenimis pagal Konvencijos dėl elektroninių nusikaltimų ir Pamatinio sprendimo 2005/222/TVR* (taip pat Direktyvos 2013/40/ES – *aut. pastaba*) *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 (BK 198 straipsnis) ir IS konfidencialumo (BK 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“*[224]. Šiame

[222] Council of Europe, *supra* note 11, p. 44-49; Committee of Ministers of the Council of Europe, *supra* note 13, p. 12.
[223] Armanas Abramavičius et. al., *supra* note 2, p. 427.
[224] Renata Marcinauskaitė, *supra* note 4, p. 118.

kontekste paminėtina tai, kad Pamatinio sprendimo 2005/222/TVR aiškinamajame memorandume terminas „informacinė sistema“ interpretuojamas kaip apimantis tiek aparatinę (angl. *hardware*), tiek programinę (angl. *software*) sistemos įrangą, pabrėžiant – išskyrus pačios informacijos turinį (angl. *though not the content of the information itself*)[225].

Tai, kas išdėstyta, leidžia manyti, kad BK 197 straipsnyje nėra užtikrinta elektroninių duomenų, o BK 196 straipsnyje – informacinės sistemos integralumo ir prieinamumo baudžiamoji teisinė apsauga. Informacinės sistemos darbo neteisėtas sutrikdymas ar nutraukimas turėtų būti siejamas išimtinai su poveikiu programinei įrangai (programai), kuri BK 197 straipsnio kontekste konkrečiu atveju turėtų būti priemone, padedančia apdoroti duomenis informacinėje sistemoje. Tokiu būdu suprantama programinė įranga (programa) nenustoja būti elektroniniais duomenims. Todėl tokiai programinei įrangai (programai) daromą poveikį – elektroninių duomenų sunaikinimą, sugadinimą, pakeitimą, pašalinimą, naudojimosi apribojimą ar kt. – kaip informacinės sistemos darbo sutrikdymo ar nutraukimo padarymo būdą apima BK 197 straipsnyje įtvirtintos sutrikdymo ir nutraukimo pavojingos veikos. Šią išvadą pagrindžia tai, kad programinė įranga (programa) kaip priemonė, padedanti apdoroti duomenis informacinėje sistemoje, kartu su aparatine įranga užtikrina informacinės sistemos galimybes atlikti įvairius elektroninių duomenų apdorojimo veiksmus. Todėl apsauga nuo poveikio tokiu būdu suprantamai programinei įrangai (programai) kaip elektroniniams duomenims atitinka BK 197 straipsnyje saugomą teisinį interesą: informacinės sistemos savininko ir (ar) naudotojo interesą, kad ši tinkamai funkcionuotų, kuris siekia toliau, negu neteisėtas poveikis elektroniniams duomenims, kadangi neteisėtai paveikiama informacinė sistema. Taigi nustačius neteisėtą poveikį programinei įrangai (programai), kuri konkrečiu atveju yra priemonė, padedanti apdoroti duomenis informacinėje sistemoje, nusikalstama veika papildomai pagal BK 196 straipsnį nekvalifikuotina. Tačiau konstatavus, kad programinė įranga (programa) nėra tokia priemonė neteisėtas poveikis jai, jeigu tą apima kaltininko tyčia, kvalifikuotinas pagal BK 196 ir 197 straipsnių sutaptį.

Jeigu neteisėtas poveikis informacinei sistemai apriboja naudojimąsi programine įranga (programa), kuri pripažįstama priemone, padedančia apdoroti duomenis informacinėje sistemoje, padaryta veika kvalifikuotina pagal BK 197 straipsnį. Tokiais atvejais programinės įrangos (programos) naudojimosi apribojimas (kaip neteisėto poveikio informacinei sistemai padarinys) žymi informacinės sistemos darbo sutrikdymą ar nutraukimą. Ir atvirkščiai – jei poveikiu informacinei

[225] “Proposal for a Council Framework Decision on attacks against information systems /* COM/2002/0173 final - CNS 2002/0086 */,“ *Oficialusis leidinys* 203 *E* (2002).

sistemai apribotas naudojimasis kita programine įranga (programa) nusikalstama veika kvalifikuotina pagal BK 196 ir 197 straipsnių sutaptį.

BK 196 straipsnyje taip pat numatyta elektroninių duomenų pašalinimo pavojinga veika. Neteisėto poveikio elektroniniams duomenims veikos kriminalizavimo raida atskleidė, jog pašalinimo pavojinga veika BK 196 straipsnyje įtvirtinta nacionalinį teisinį reguliavimą derinant su Konvencijos dėl elektroninių nusikaltimų nuostatomis 2004 m.[226] Tačiau Konvencijos 4 straipsnio 1 dalyje pašalinimo pavojinga veika nėra įtvirtinta *expressis verbis*.

R. Mockevičiaus, D. Valatkevičiaus teigimu, *„elektroninių duomenų pašalinimas reiškia, kad sukuriamos tokios aplinkybės, kurioms esant neįmanomas priėjimas prie duomenų, nors patys duomenys ir nesunaikinami, t. y. duomenys yra išimti iš atitinkamos bylos, kompiuterio disko, išorinės atmintinės ar interneto tinklalapio, tačiau yra nesunaikinami, bet išsaugojami kitoje vietoje ar kitu būdu“*[227]. Iš esmės tą patį teigia M. Kuzminovas[228]. Pasak D. Sauliūno, *„kompiuterinės informacijos pašalinimas – tai failo perkėlimas į kitą kompiuterinę sistemą, t. y. nors iš pirminės sistemos failas gali būti ištrintas, jis gali būti išsaugotas kito kompiuterio kaupiklyje ar nešiojamoje laikmenoje“*[229]. Anot N. Goranin ir D. Mažeikos, *„duomenų pašalinimu laikomas veiksmas, kai duomenys perkeliami į kitą vietą, kitą kompiuterinę sistemą ar laikmeną“*[230]. Taigi elektroninių duomenų pašalinimo pavojinga veika nacionalinėje baudžiamosios teisės doktrinoje siejama su tokių duomenų vietos pakeitimu ar jų išsaugojimu kitu būdu, dėl ko prieiga prie elektroninių duomenų tampa neįmanoma, tačiau duomenys nėra sunaikinami. Taigi pašalinimo pavojinga veika apribojama teisėtų vartotojų prieiga prie elektroninių duomenų. Todėl šios pavojingos veikos kriminalizavimu BK 196 straipsnyje siekiama užtikrinti elektroninių duomenų prieinamumo baudžiamąją teisinę apsaugą.

Teisėtų vartotojų prieigos prie elektroninių duomenų apribojimas neišvengiamai lemia naudojimosi tokiais duomenimis apribojimą. Tai leidžia teigti, kad elektroninių duomenų pašalinimas yra būdas, kuriuo apribojamas naudojimasis tokiais duomenimis. Tačiau įstatymų leidėjui tokį būdą kriminalizavus kaip savarankišką pavojingą veiką, pašalinimo pavojinga veika pripažintina specialiu naudojimosi elektroniniais duomenimis apribojimo atveju. Šiame kontekste įstatymų leidėjo sprendimas vienoje BK 196 straipsnio dalyje kriminalizuoti dvi – pašalinimo ir naudojimosi apribojimo – pavojingas veikas, kurių abiejų pagrindą sudaro naudojimosi elektroniniais duomenimis

[226] "Lietuvos Respublikos baudžiamojo kodekso 13, 162, 191, 196, 197, 203, 206, 216, 219, 221, 309 straipsnių pakeitimo ir papildymo bei kodekso papildymo 198-1 ir 198-2 straipsniais įstatymas," *Valstybės žinios* 45, 760 (2004).
[227] Armanas Abramavičius et. al., *supra* note 2, p. 421-422.
[228] Aurelijus Gutauskas et. al., *supra* note 3, p. 465.
[229] Darius Sauliūnas et. al., *supra* note 7, p. 531.
[230] Nikolaj Goranin ir Dalius Mažeika, *supra* note 8, p. 25.

apribojimas, o atribojimas pagrįstas specialiu tokio apribojimo būdu, kuris priskirtas elektroninių duomenų pašalinimo pavojingai veikai (nors dėl tapataus pagrindo jis taip pat būdingas naudojimosi elektroniniais duomenimis apribojimo pavojingai veikai), diskutuotinas.

Minėta, Konvencijos aiškinamosios ataskaitos 61 punkte naudojimosi kompiuteriniais duomenimis apribojimas apibūdinamas kaip bet kokie veiksmai, kuriais apribojamas ar nutraukiamas duomenų prieinamumas asmeniui, turinčiam prieigą prie kompiuterio ar duomenų laikmenos, kuriuose jie laikomi[231]. Teigtina, kad vartojamas žodžių junginys „bet kokie veiksmai“ apima veiksmus, kuriais *inter alia* apribojama vartotojų prieiga prie elektroninių duomenų, t. y. jų pašalinimą. Tai leidžia manyti, kad dėl šios priežasties Konvencijos 4 straipsnio 1 dalyje pašalinimo pavojinga veika nėra įtvirtinta *expressis verbis*.

4.2.4. Pavojingų veikų neteisėtumo vertinimas

Elektroninių duomenų sunaikinimas, sugadinimas, pašalinimas ar pakeitimas arba naudojimosi tokiais duomenimis apribojimas techninė įranga, programine įranga ar kitais būdais tūri būti padaryti neteisėtai.

EKNPT baigiamosios ataskaitos II skyriaus 2 dalies c punkte neteisėtumo (angl. *without right*) požymio svarba siejama su tuo, kad vienas iš lygiagrečios (angl. *parallel*) – žalos nuosavybei (angl. *damaging property*) – nusikalstamos veikos požymių – daikto, kuriam padaryta žala, priklausymas kitam asmeniui – nėra įtvirtintas kompiuterinių programų ar duomenų sugadinimo veikos dispozicijoje. Pažymėta, kad pastarojo požymio funkciją perima terminas „neteisėtai“, kuris kompiuterinių duomenų ar programų sužalojimo veikos kontekste turi būti suprantamas plačiąja prasme kaip apimantis asmenis, kurie neturi teisės veikti taip, kaip pasielgė – savavališkai (angl. *in their own right*) ar įgalioti tų, kurie turi teisę.[232]

Neteisėtumo požymio oficialus autentiškas aiškinimas aptiktinas susijusiuose Europos Sąjungos teisės aktuose. Remiantis Pamatinio sprendimo 2005/222/TVR 1 straipsnio d punktu, *„neturint tam teisės“ – tai prieiga ar įsikišimas, kuriam nesuteikė leidimo sistemos ar jos dalies savininkas, kitas teisės turėtojas, arba kurio neleidžia nacionalinės teisės aktai“*. Toks pats, tik papildytas aspektais, susijusiais su duomenų perėmimu, neteisėtumo požymio interpretavimas įtvirtintas Direktyvos 2013/40/ES 2 straipsnio d punkte. Pamatinio sprendimo 2005/222/TVR

[231] Committee of Ministers of the Council of Europe, *supra* note 13, p. 11.
[232] Council of Europe, *supra* note 11, p. 46.

preambulės 13 punkte pažymėtas reikalingumas vengti bausti padarius nusikaltimą teisių turėtojus bei įgaliotuosius asmenis.

Nacionalinėje baudžiamosios teisės doktrinoje neteisėtumo požymis siejamas su teisėto duomenų savininko ar valdytojo leidimo naudotis ar dirbti su konkrečiais elektroniniais duomenimis neturėjimu, tokio naudojimosi ar darbo draudimu pagal teisės aktus, suteiktų įgaliojimų ar kompetencijos viršijimu, turint ribotą teisę naudotis ar dirbti su elektroniniais duomenimis (R. Mockevičius, D. Valatkevičius, M. Kuzminovas)[233].

Tiek susijusiuose viršnacionalinės teisės aktuose, tiek nacionalinėje baudžiamosios teisės doktrinoje aiškinant neteisėtumo požymį išskiriami atvejai, kuriais padaryta veika pripažįstama teisėta. Konvencijos aiškinamosios ataskaitos 62 punkte pažymėta, kad bendro pobūdžio veiksmai, susiję su kompiuterinių tinklų tvarkymu, kaip ir įprasti eksploatavimo ar komercinės praktikos metodai laikytini teisėtais ir negali būti pripažinti neteisėtais pagal poveikio duomenims veiką. Tokiems metodams priskiriami, pirmiausia, kompiuterinės sistemos testavimas ir saugumo užtikrinimas, turint jos savininko ar valdytojo sutikimą, ar kompiuterio operacinės sistemos nustatymų pakeitimas tuo atveju kai sistemos valdytojui reikalinga nauja programinė įranga (pvz., programinės įrangos, skirtos prieigai prie interneto, įdiegimas, kuris ištrina prieš tai įdiegtas atitinkamas programas).[234] Šiame kontekste paminėtina, kad, M. Kuzminovo teigimu, *„nebus laikoma neteisėtu duomenų sunaikinimu ir tinklalapio administratoriaus atliktas necenzūrinių komentarų, tautos, rasės, etninę, religinę ar kitokią nesantaiką kurstančios medžiagos, nelegalių programų pašalinimas, tinklo naudotojams taikomi draudimai prisijungti už tinklo taisyklių pažeidimą“*[235]. Konvencijos aiškinamosios ataskaitos 62 punkte nurodyta, jog srauto duomenų pakeitimas, siekiant užtikrinti informacijos apsikeitimo anonimiškumą (pvz., sistemų, kurios iš elektroninio laiško pašalina siuntėją identifikuojančius duomenis ir persiunčia tokį laišką adresatui, veikimas) ar duomenų pakeitimas, siekiant užtikrinti informacijos apsikeitimo anonimiškumą (pvz., šifravimas), turi būti vertinami kaip pagrįsta konfidencialumo apsauga ir pripažįstami teisėtais. Tačiau Šalys gali pripažinti neteisėtais tam tikrus piktnaudžiavimus, susijus su informacijos apsikeitimo anonimiškumu, pvz., kai paketų pavadinimai keičiami tam, kad nuslėpti nusikaltėlio asmenybę.[236] Pasak M. Kuzminovo, *„kai kuriose įstaigose yra draudžiama naudotis internetu, mobiliuoju ryšiu, todėl bausmės atlikimo įstaiga, panaudodama tokį ryšį blokuojančią įrangą, elgsis teisėtai. Jeigu dėl tokių veiksmų bus sutrikdyta*

[233] Armanas Abramavičius et. al., *supra* note 2, p. 419-420; Aurelijus Gutauskas et. al., *supra* note 3, p. 463-464.
[234] Committee of Ministers of the Council of Europe, *supra* note 13, p. 11.
[235] Aurelijus Gutauskas et. al., *supra* note 3, p. 464.
[236] Committee of Ministers of the Council of Europe, *op. cit.*, p. 11.

niekuo dėtų žmonių veikla, baudžiamoji atsakomybė negalima, nes kaltė nebus tyčinė, galimas tik žalos atlyginimas pagal CK. Nebus laikoma neteisėtu apribojimu naudotis duomenimis ir pagal baudžiamąjį procesą taikomos procesinės prievartos priemonės – juridiniams asmenims taikoma laikinoji procesinė prievartos priemonė, laikinas veiklos sustabdymas ar laikinas apribojimas, todėl, pavyzdžiui, gali būti sustabdyta ar nutraukta internetinė prekyba"[237]. Pagaliau, Pasiūlymo dėl Tarybos pamatinio sprendimo dėl atakų prieš informacines sistemas aiškinamajame memorandume pažymėta, jog ypatingai svarbu, kad baudžiamoji atsakomybė nebūtų taikoma už *inter alia* atgalinę inžineriją (angl. *reverse engineering*) 1991 m. gegužės 14 d. Tarybos direktyvos 91/250/EEB[238] dėl kompiuterinių programų teisinės apsaugos ribose; teisėtus mokslinius tyrimus[239].

Tai, kas išdėstyta, leidžia teigti, kad neteisėtumas konstatuotinas tuo atveju, jeigu darydamas poveikį elektroniniams duomenims asmuo tam neturi šių duomenų savininko ar teisėto valdytojo leidimo arba nors tokį leidimą turi, tačiau viršija suteiktų įgaliojimų ribas, arba toks poveikis elektroniniams duomenims draudžiamas teisės aktų.

4.3. Neteisėto poveikio elektroniniams duomenims pavojingi padariniai

Būtinas neteisėto poveikio elektroniniams duomenims nusikalstamos veikos požymis yra pavojingi padariniai. Pasak R. Mockevičiaus ir D. Valatkevičiaus, *„jais laikomi sunaikinti, sugadinti, pašalinti ar pakeisti duomenys ar apribotas naudojimasis jais. Visi veiksmai, kuriais daromas poveikis elektroniniams duomenims, turi sukelti žalą"*[240]. Taigi BK 196 straipsnio 1 dalies dispozicijoje vartojami terminai – „sugadinimas", „sunaikinimas", „pašalinimas", „pakeitimas", „naudojimosi apribojimas"[241] – apibūdina tiek procesą, tiek jo rezultatą – elektroninių duomenų sunaikinimą, sugadinimą, pašalinimą ar pakeitimą arba naudojimosi tokiais duomeninims apribojimą, t. y. elektroninių duomenų integralumo ar prieinamumo pažeidimą. Kartu dėl to turi būti padaryta žala. Pratęsiant R. Mockevičiaus ir D. Valatkevičiaus teiginį, *„jeigu kaltininkas savo veiksmais sunaikins, sugadins, pašalins ar pakeis arba apribos naudojimąsi nors ir nemaža elektroninių duomenų dalimi*

[237] Aurelijus Gutauskas et. al., *supra* note 3, p. 464.
[238] Šį Europos Sąjungos teisės aktą pakeitė: "Europos Parlamento ir Tarybos direktyva 2009/24/EB dėl kompiuterių programų teisinės apsaugos," *Oficialusis leidinys L* 111, 17 (2009).
[239] "Proposal for a Council Framework Decision on attacks against information systems /* COM/2002/0173 final - CNS 2002/0086 */," *Oficialusis leidinys* 203 *E* (2002).
[240] Armanas Abramavičius et. al., *supra* note 2, p. 422. Taip pat žr. Darius Štitilis ir Valdas Klišauskas, "Criminalization of dangerous acts in cyberspace in criminal codes of Lithuania and Russia: comparative aspects," *Matters of Russian and International Law* 3 (2013): 133.
[241] Neteisėtas elektroninių duomenų sunaikinimas, sugadinimas, pašalinimas ar pakeitimas arba naudojimosi tokiais duomenimis apribojimas išsamiai aptarti šio darbo 4.2 poskyryje, todėl plačiau neanalizuotini.

jų apimties požiūriu, tačiau tuo nesukels žalos, tokio asmens nebus galima traukti baudžiamojon atsakomybėn“[242].

Susijusiuose viršnacionalinės teisės aktuose oficialus autentiškas žalos požymio aiškinimas nėra pateiktas. Konvencijos dėl elektroninių nusikaltimų 4 straipsnio 2 dalyje Šalims numatyta teisė reikalauti, kad poveikio duomenims veika turi padaryti didelę žalą, tačiau pastarojo požymio interpretavimas paliktas nacionalinei teisėkūrai (Konvencijos aiškinamosios ataskaitos 64 punktas)[243]. Pamatinio sprendimo 2005/222/TVR preambulės 15 punkte, 7 straipsnio 2 dalyje minimi dideli nuostoliai (angl. *serious damages*), kurie vartojami sunkinančių aplinkybių ir griežtesnių bausmių numatymo tikslingumo kontekste. Nuostoliai yra piniginė žalos išraiška (Lietuvos Respublikos civilinio kodekso[244] 6.249 straipsnio 1 dalis), o *„nusikalstama veika padaryta žala – tai baudžiamojo įstatymo saugomų asmeninių ir turtinių vertybių sunaikinimas arba pakenkimas, sukėlęs neigiamų pasekmių, kurias galima įvertinti turtine išraiška. Žala padaroma baudžiamosios teisės ginamoms vertybėms“*[245]. Taigi nors nuostoliai yra tik žalos išraiškos forma, BK 196 straipsnio kontekste svarbu įvertinti ne tik ir ne tiek piniginę žalos išraišką, kiek aplinkybes, žyminčias turtinio ir neturtinio pobūdžio praradimus. Didelė žala minima Direktyvos 2013/40/ES preambulės 5 punkte. Tačiau ši vartojama didelės apimties kibernetinių atakų kontekste: didelės žalos nustatymas paliktas valstybėms narėms, pažymint, kad *„[...] tokia žala gali būti susijusi su visuomenei labai svarbių sisteminių paslaugų sutrikdymu ar patiriamomis didelėmis finansinėmis išlaidomis, arba asmens duomenų ar slapto pobūdžio informacijos praradimu“*. Didelė žala taip pat minima Direktyvos 2013/40/ES preambulės 11, 13 punktuose, 9 straipsnio 4 dalies b punkte, kuriuose vartojama mažareikšmiškumo bei sankcijų kontekste. Be to, Direktyvos 2013/40/ES preambulės 6 punkte didelės apimties kibernetinių atakų kontekste minima didžiulė ekonominė žala. Oficialus autentiškas žalos aiškinimas nėra pateiktas ir BK XXX skyriuje.

Mokslinėje literatūroje[246] ir teismų praktikoje pripažįstama, kad žala kaip pavojingi padariniai BK 196 straipsnio kontekste gali būti turtinė, neturtinė, socialinė, moralinė ir kitokio

[242] Armanas Abramavičius et. al., *supra* note 2, p. 422.
[243] Committee of Ministers of the Council of Europe, *supra* note 13, p. 11.
[244] “Lietuvos Respublikos civilinis kodeksas,“ *Valstybės žinios* 74, 2262 (2000).
[245] “Lietuvos Aukščiausiojo Teismo 2008 m. rugsėjo 21 d. teisės normų, reguliuojančių nusikalstama veika padarytos žalos atlyginimą, taikymo baudžiamosiose bylose apžvalga Nr. 29,“ prieiga per internetą: http://www.infolex.lt/tp/91332?nr=5
[246] Pasak P. Veršekio, didelės žalos požymio turinio atskleidimo kriterijai atskirų kategorijų bylose skiriasi iš esmės, todėl atskleidžiant aptariamo požymio turinį – itin svarbus analizuojamas kontekstas, t. y. visų pirma rūšinė nusikalstamos veikos sudėtis. Plačiau žr. Paulius Veršekys, “Vertinamieji nusikalstamos veikos sudėties požymiai“ (daktaro disertacija, Vilniaus universitetas, 2013), 206, http://vddb.laba.lt/obj/LT-eLABa-0001:E.02~2013~D_20131125_134053-73474 Atsižvelgiant į tai, analizuojant BK 196 straipsnyje įtvirtinto žalos kaip pavojingų padarinių požymio turinį taip pat atsižvelgtina į aptariamo požymio interpretavimą BK 197 straipsnio kontekste, kadangi juos vienija tapati rūšinė

pobūdžio[247]. R. Mockevičiaus ir D. Valatkevičiaus teigimu, tai priklauso nuo elektroninių duomenų, kurie buvo neteisėtai paveikti, pobūdžio[248]. Taigi kaip teisingai pastebi M. Kuzminovas, žala gali būti pripažįstami ne tik patirti nuostoliai, bet ir kritęs prestižas, klientų pasitikėjimas ir pan.[249]. Anot P. Veršekio, *„[...] nusikalstama veika padarytos žalos pobūdis gali būti labai įvairus, tačiau baudžiamajame procese esminę reikšmę turi žalos skirstymas į turtinę ir neturtinę žalą“*[250]. Šios žalos rūšys akcentuojamos susijusioje teismų praktikoje: *„Teisėjų kolegija pažymi, kad BK 197 straipsnyje nurodytos žalos (nepriklausomai nuo jos dydžio) turinį sudaro ne tik turtinė, bet ir neturtinė žala“*[251]. Šia *„[...] nusikalstama veika žala padaroma ne tik turtiniams, bet ir neturtiniams nukentėjusio asmens, t. y. informacinės sistemos savininko, interesams, be to, žala padaroma ir informacinės sistemos vartotojams, suvaržoma visuomenės teisė į nevaržomą informacijos sklaidą, informacijos prieinamumą, ribojama minties ir žodžio laisvė, pažeidžiamas elektroninės erdvės saugumas“*[252].

Kalbant apie žalos dydį, pažymėtina, jog BK 196 straipsnyje įtvirtintas, P. Veršekio žodžiais, vieno parametro trijų pakopų kiekybinis vertinimas: nedidelės žalos padarymas (3 dalis), (vidutinės) žalos padarymas (1 dalis), didelės žalos padarymas (2 dalis). Taigi BK 196 straipsnio struktūra nulemia, kad 1 dalyje įtvirtinta žala turi būti mažesnė už 2 dalyje įtvirtinta žalą, bet kartu didesnė nei žala pagal straipsnio 3 dalį. Mokslinėje literatūroje ir teismų praktikoje žalos dydis apibūdinamas kaip vertinamasis požymis, kurį lemia bendrieji baudžiamosios atsakomybės principai ir konkrečios nusikalstamos veikos aplinkybės: elektroninių duomenų pobūdis, jų statusas, nukentėjusiojo ypatybės, pažeistų interesų svarba, kiek ji reikšminga tokią žalą patyrusiam subjektui ir pan.[253]. Paminėtina, jog BK 197 straipsnio kontekste išskiriamos tokios aplinkybės kaip informacinės sistemos reikšmingumas (valstybinė, registras ar pan.), jos darbo sutrikdymo ar nutraukimo trukmė ir

baudžiamojo įstatymo saugoma vertybė, be to, abi nusikalstamos veikos skirtos užtikrinti integralumo ir prieinamumo baudžiamąją teisinę apsaugą.

[247] Armanas Abramavičius et. al., *supra* note 2, p. 422; Aurelijus Gutauskas et. al., *supra* note 3, p. 466; Darius Štitilis ir Valdas Klišauskas, *supra* note 240, p. 135; "Kauno apygardos teismas 2012 m. spalio 22 d. nutartis baudžiamojoje byloje Nr. 1A-94-175/2012," prieiga per internetą: http://www.infolex.lt/tp/Default.aspx?id=20&item=doc&aktoid=480057&nr=1

[248] Armanas Abramavičius et. al., *op. cit.*, p. 422.

[249] Aurelijus Gutauskas et. al., *op. cit.*, p. 466.

[250] Paulius Veršekys, *supra* note 246, p. 205.

[251] "Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2015 m. gegužės 12 d. nutartis baudžiamojoje byloje Nr. 2K-188-489/2015," prieiga per internetą: http://www.infolex.lt/tp/1048281?nr=1

[252] "Vilniaus apygardos teismo Baudžiamųjų bylų skyriaus 2013 m. birželio 20 d. nutartis baudžiamojoje byloje Nr. 1A-410-312/2013," prieiga per internetą: http://www.infolex.lt/tp/701867?nr=2#

[253] Armanas Abramavičius et. al., *op. cit.*, p. 422; Aurelijus Gutauskas et. al., *op. cit.*, p. 466; "Kauno apygardos teismas 2012 m. spalio 22 d. nutartis baudžiamojoje byloje Nr. 1A-94-175/2012," prieiga per internetą: http://www.infolex.lt/tp/Default.aspx?id=20&item=doc&aktoid=480057&nr=1; "Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2015 m. gegužės 12 d. nutartis baudžiamojoje byloje Nr. 2K-188-489/2015," prieiga per internetą: http://www.infolex.lt/tp/1048281?nr=1

pan.[254]. Manytina, elektroninių duomenų statusas žymį jų reikšmingumą (valstybinis, registras ir pan.), be to, nustatant padarytos žalos dydį taip pat svarbi elektroninių duomenų prieinamumo pažeidimo trukmė. M. Kuzminovas išskiria šiuos žalos dydžio vertinimui reikšmingus kriterijus: *„[...] kokia sugadintų ar prarastų duomenų ekonominė vertė; kokia žala įmonei ar fiziniam asmeniui atsirado dėl to, kad jie tam tikrą laiką negalėjo naudotis konkrečiais duomenimis (patirti nuostoliai, negautos pajamos); žalos santykis su įmonės vidutine dienos ar mėnesio apyvarta [...]; ar sugadintiems duomenims atkurti prireikė samdyti papildomų darbuotojų, kreiptis į kitų bendrovių ekspertus, ar tai padarė tos pačios įmonės darbuotojai, atlikdami savo darbines funkcijas, ir kiek darbo valandų užtruko incidentui pašalinti: ar bendrovė naudojo elementarias elektroninės informacijos apsaugos priemones (ugniasienė, kritinės informacijos atsarginės kopijos, skirtingi vaidmenys ir teisės tarp vartotojų grupės narių ir pan.) ir kt.“*[255]. Nurodytų aplinkybių kontekste nepritartina Kauno apygardos teismo Baudžiamųjų bylų skyriaus 2012 m. spalio 22 d. nutartyje padarytai išvadai, jog *„[...] sprendžiant apie padarytos žalos dydį [...] ne visais atvejais būtina remtis tik padarytos žalos pinigine išraiška“*[256]. Teigtina, kad sprendžiant apie padarytos žalos dydį visais atvejais būtina remtis ne tik padarytos žalos pinigine išraiška. Kokio dydžio žala padaryta kiekvienu konkrečiu atveju sprendžia teismas[257].

Pasak D. Sauliūno, *„jeigu žala yra turtinė, siekiant nuspręsti, ar ji yra didelė, logiška vadovautis didelės turtinės žalos sąvokos išaiškinimu pagal BK 212 straipsnį, kuris nustato, kad [...] didelė turtinė žala yra 150 MGL [...] dydžio sumą viršijanti žala. Be abejo, baudžiamojoje teisėje analogiją taikyti draudžiama, todėl teismui tai būtų tik orientacinė rekomendacija sprendžiant, ar žala yra didelė“*[258]. Vilniaus miesto apylinkės teismas 2013 m. kovo 25 d. nuosprendyje BK 197 straipsnio kontekste pažymėjo: *„BK 212 straipsnio 1 dalyje numatyta, kad didelė turtinė žala yra 150*

[254] Armanas Abramavičius et. al., *supra* note 2, p. 428; "Vilniaus apygardos teismo Baudžiamųjų bylų skyriaus 2013 m. birželio 20 d. nutartis baudžiamojoje byloje Nr. 1A-410-312/2013," prieiga per internetą: http://www.infolex.lt/tp/701867?nr=2#

[255] Aurelijus Gutauskas et. al., *supra* note 3, p. 466-467.

[256] "Kauno apygardos teismas 2012 m. spalio 22 d. nutartis baudžiamojoje byloje Nr. 1A-94-175/2012," prieiga per internetą: http://www.infolex.lt/tp/Default.aspx?id=20&item=doc&aktoid=480057&nr=1.

[257] Armanas Abramavičius et. al., *op. cit.*, p. 422; Aurelijus Gutauskas et. al., *op. cit.*, p. 466; "Kauno apygardos teismas 2012 m. spalio 22 d. nutartis baudžiamojoje byloje Nr. 1A-94-175/2012," prieiga per internetą: http://www.infolex.lt/tp/Default.aspx?id=20&item=doc&aktoid=480057&nr=1; "Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2015 m. gegužės 12 d. nutartis baudžiamojoje byloje Nr. 2K-188-489/2015," prieiga per internetą: http://www.infolex.lt/tp/1048281?nr=1; "Vilniaus apygardos teismo Baudžiamųjų bylų skyriaus 2013 m. birželio 20 d. nutartis baudžiamojoje byloje Nr. 1A-410-312/2013," prieiga per internetą: http://www.infolex.lt/tp/701867?nr=2#

[258] Darius Sauliūnas et. al., *supra* note 7, p. 531.

MGL dydžio sumą viršijanti žala“[259]. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2015 m. gegužės 12 d. nutartimi tokia įstatymo analogija pripažinta negalima: *„Teisėjų kolegija atkreipia dėmesį į svarbią aplinkybę, kad apeliacinės instancijos teismas, spręsdamas dėl patirtos turtinės žalos dydžio, klaidingai vadovavosi BK 212 straipsnio 1 dalimi, nepagrįstai didelę turtinę žalą siejo su 150 MGL dydžio sumą viršijančia žala. Šiame straipsnyje nurodytas 150 MGL dydžio kriterijus yra suformuluotas ir taikomas didelei turtinei žalai nustatyti nusikalstamose veikose ekonomikai ir verslo tvarkai. BK 212 straipsnio 1 dalyje tiesiogiai nurodyta, kad toks didelės turtinės žalos aiškinimas yra taikomas tik BK XXXI skyriuje nurodytai didelei žalai nustatyti“*[260].

Vilniaus apygardos teismo Baudžiamųjų bylų skyriaus 2013 m. birželio 20 d. nutartyje pažymėta: *„[...] 700,00 Lt dydžio turtinė žala neatitinka nedidelės turtinės žalos kriterijaus, kadangi viršija teismų praktikoje nustatytą 3 MGL dydžio sumą [...]“*[261]. Manytina, pastarąjį aiškinimą galėjo paskatinti turtinės žalos sutapatinimas su turto verte, kurios išaiškinimas pateiktas BK 190 straipsnio 1 dalyje[262]. Pasak P. Veršekio, *„[...] teismai praktikoje susiduria su tam tikromis didelės (nedidelės) turtinės žalos vertinamojo nusikalstamos veikos sudėties požymio inkriminavimo problemomis. Kaip pagrindinį trūkumą derėtų įvardinti netinkamą, BK 190 straipsnio sąvokų išaiškinimo analogija pagrįstą didelės (nedidelės) žalos vertinamojo požymio turinio atskleidimą. [...] absoliutus didelės turtinės žalos požymio sutapatinimas su formaliai išaiškintu didelės turtinės vertės dydžiu neatitinka įstatymų leidėjo ketinimų ir traktuotinas kaip nullum crimen sine lege principo draudžiama įstatymo analogija“*[263]. Taigi turtinės žalos dydis BK 196 straipsnio kontekste negali būti absoliučiai sutapatinamas su BK 190 straipsnio 1 dalyje pateiktu turto vertės išaiškinimu. Be to, kaip ir prieš tai minėtu BK 212 straipsnio atveju, BK 190 straipsnyje pateiktų sąvokų išaiškinimas siejamas su BK XXVIII skyriuje numatytais nusikaltimais ir baudžiamaisiais nusižengimais nuosavybei, turtinėms teisėms ir turtiniams interesams. Dar ir dėl to aptariama įstatymo analogija pripažinta negalima.

[259] “Vilniaus miesto apylinkės teismo 2013 m. kovo 25 d. nuosprendis baudžiamojoje byloje Nr. 1-455-655/2013,“ prieiga per internetą: http://www.infolex.lt/tp/932630?nr=1

[260] “Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2015 m. gegužės 12 d. nutartis baudžiamojoje byloje Nr. 2K-188-489/2015,“ prieiga per internetą: http://www.infolex.lt/tp/1048281?nr=1

[261] “Vilniaus apygardos teismo Baudžiamųjų bylų skyriaus 2013 m. birželio 20 d. nutartis baudžiamojoje byloje Nr. 1A-410-312/2013,“ prieiga per internetą: http://www.infolex.lt/tp/701867?nr=2#

[262] Pažymėtina, kad aptariamos nutarties priėmimo metu galiojusioje BK 190 straipsnio 1 dalies redakcijoje turtas pripažintas nedidelės vertės, kai jo vertė viršija 1 MGL, bet neviršija 3 MGL. Plačiau žr. “Lietuvos Respublikos baudžiamojo kodekso 139, 140, 176, 180, 181, 190, 201, 212, 249, 281 straipsnių pakeitimo ir papildymo įstatymas,“ *Valstybės žinios* 74, 3423 (2003).

[263] Paulius Veršekys, *supra* note 246, p. 207.

Teismų praktikos analizė atskleidė, kad teismai dažnai[264] nepateikia (išsamių) argumentų dėl nusikalstama veika padarytos žalos ir jos dydžio vertinimo. Dėl šios priežasties dažnai nėra aišku, kas sudarė padarytos veikos kvalifikavimo pagal atitinkamą BK 196 ar 197 straipsnio dalį pagrindą. Toliau pateikiami susijusios teismų praktikos[265] pavyzdžiai.

Kauno miesto apylinkės teismo 2011 m. spalio 25 d. nuosprendžiu A. A. nuteistas pagal BK 196 straipsnio 1 dalį už tai, kad *2010 m. rugpjūčio 10 d. neteisėtai sunaikino elektroninius duomenis, patalpintus internetinėje svetainėje, o 2010 m. rugpjūčio 11 d. pakeitė juos kitais, padarydamas Vilniaus V. S. vidurinei mokyklai didelę žalą*. Aprašomojoje nuosprendžio dalyje pasisakydamas dėl padarytos žalos ir jos dydžio vertinimo teismas pažymėjo, jog *„[...] kaltinamasis padarė Kodekso 196 str. 1 d. dispozicijoje nurodytą didelę (ji nėra apibrėžiama materialiniu dydžiu) žalą: iš civilinio ieškovo atstovų paaiškinimų matyti, kad sunaikintoji svetainė buvo sukurta dar 2004 metais, joje buvo daug informacijos, kurios atkurti nebėra galimybės“*. Taip pat paminėtina, jog *Vilniaus V. S. vidurinė mokykla baudžiamojoje byloje buvo pareiškusi 10000 litų dydžio civilinį ieškinį, kuriuo prašė atlyginti išlaidas, skirtas naujos svetainės sukūrimui, kuri pripažinęs pagrįstu ir įrodytu teismas tenkino*.[266] Remiantis baudžiamąją bylą apeliacine tvarka nagrinėjusio Kauno apygardos teismo Baudžiamųjų bylų skyriaus 2012 m. spalio 22 d. nutartimi: *„Nors ir sumažindamas civilinio ieškinio dydį* (nuo 10000 Lt iki 3000 Lt – *aut. pastaba*)*, teismas pažymi, kad civiliniam ieškovui buvo padaryta didelė žala. [...] Dėl konkrečios kaltininko veikos nebuvo sutrikdyta institucijos veikla, tačiau atsižvelgiant į civilinio ieškovo statusą, kad jis yra švietimo ir ugdymo įstaiga, kad internetinės svetainės*

[264] Žr., pvz., “Panevėžio miesto apylinkės teismo 2011 m. gegužės 24 d. nuosprendis baudžiamojoje byloje Nr. 1-187-389/2011,“ prieiga per internetą: http://www.infolex.lt; “Radviliškio rajono apylinkės teismo 2014 m. balandžio 15 d. nuosprendis baudžiamojoje byloje Nr. 1-104-632/2014,“ prieiga per internetą: http://www.infolex.lt/tp/916232?nr=1; “Telšių rajono apylinkės teismas 2012 m. liepos 27 d. baudžiamuoju įsakymu baudžiamojoje byloje Nr. 1-185-187/2012,“ prieiga per internetą: http://www.infolex.lt/tp/405719?nr=1; “Vilkaviškio rajono apylinkės teismo 2015 m. gegužės 22 d. nuosprendis baudžiamojoje byloje Nr. 1-111-633/2015,“ prieiga per internetą: http://www.infolex.lt/tp/Default.aspx?id=20&item=doc&aktoid=1068389&nr=1; “Panevėžio apygardos teismo 2014 m. kovo 14 d. nuosprendis baudžiamojoje byloje Nr. 1-35-366/2014,“ prieiga per internetą: http://www.infolex.lt/tp/875032?nr=2; “Vilniaus miesto apylinkės teismo 2015 m. vasario 10 d. baudžiamasis įsakymas baudžiamojoje byloje Nr. 1-844-276/2015,“ prieiga per internetą: http://www.infolex.lt/tp/1019539?nr=1

[265] Pažymėtina, jog visuose pateiktos teismų praktikos pavyzdžiuose nusikalstama veika padaryta iki 2015 m. birželio 19 d., kai įsigaliojo paskutiniai BK 196 ir 197 straipsnių pakeitimai, kurių pagrindu *inter alia* buvo įtvirtinta trijų dydžių žala: nedidelė, vidutinė, didelė. Plačiau žr. “Lietuvos Respublikos baudžiamojo kodekso 7, 196, 197, 198-1, 198-2 straipsnių ir priedo pakeitimo ir Kodekso papildymo 270-3 straipsniu įstatymas,“ *Valstybės žinios* 2015-09697 (2015). Taigi visuose pateiktos teismų praktikos pavyzdžiuose nusikalstamos veikos kvalifikavimo pagal konkrečią BK 196 ir 197 straipsnių dalį pagrindą žalos požymio atžvilgiu sudarė jos pripažinimas didele ar nedidele.

[266] “Kauno miesto apylinkės teismo 2011 m. spalio 25 d. nuosprendis baudžiamojoje byloje Nr. 1-2092-246/2011,“ prieiga per internetą: www.infolex.lt

sunaikinimas buvo padarytas prieš pat mokslo metų pradžią, kas sukėlė tam tikrų nepatogumų mokyklos bendruomenei, mokinių tėvams, konstatuotina, jog civilinis ieškovas patyrė didelę žalą“[267].

Vilniaus miesto apylinkės teismo 2013 m. kovo 25 d. nuosprendžiu A. V. nuteistas *inter alia* pagal 24 straipsnio 1 dalį ir 197 straipsnio 3 dalį, 24 straipsnio 4 dalį ir 197 straipsnio 1 dalį už tai, kad *organizavo elektroninės paslaugos trikdymo atakas prieš S. G. ir UAB „Tele–3” priklausančius tinklapius www.skundai.lt, www.tv3.lt ir www.tv3play.lt ir vadovavo jų vykdymui*. P. P nuteistas pagal 197 straipsnio 3 dalį ir 197 straipsnio 1 dalį už tai, kad, *vykdamas A. V. nurodymą, į minėtus tinklapius tyčia išsiuntė didelį užklausų kiekį. Dėl įvykdytos elektroninės paslaugos trikdymo atakos buvo sutrikdytas informacinės sistemos – tinklapio www.skundai.lt darbas ir padaryta 700 Lt turtinė žala tinklapio www.skundai.lt valdytojui S. G, taip pat sutrikdytas informacinių sistemų – tinklapių www.tv3.lt, www.tv3play.lt bei visos tarnybinės stoties darbas ir padaryta didelė – 52 809,56 Lt žala UAB „Tele–3“ ir 60 478 Lt žala Viasat Satellite Services AB*. Manytina, žalos ir jos dydžio vertinimui reikšmingi liudytojo S. G. parodymai, kuriuos apibendrinus paminėtina tai, kad *per atakas tinklapis krovėsi ilgiau nei įprastai arba visai neužsikraudavo ir tuomet kompiuterio ekrane atsirasdavo lentelė, kad trūksta atminties, todėl jis pasididino atminties resursus, per lapkričio mėnesį apie savaitę vyko atakos, vėliau jos irgi kartojosi, jam padaryta 668 Lt turtinė žala, kadangi norėdamas suvaldyti atakas, jis turėjo įdiegti programą, blokuojančią atakas, prašė priteisti 570 Lt neturtinę žalą, kadangi dėl internetinių atakų skyrė daug savo laisvo laiko*. Aprašomojoje nuosprendžio dalyje pasisakydamas dėl baudžiamojoje byloje pareikštų civilinių ieškinių teismas pažymėjo: *„Nekvestionuotina, jog UAB „Tele – 3“ patyrė neturtinės žalos dėl pablogėjusios reputacijos, kadangi vykdomų atakų dienomis, kai UAB „Tele – 3“ interneto puslapiai neveikė arba veikė itin blogai, kad galėjo sukelti TV3 televizijos žiūrovų pasipiktinimą, tačiau [...] Civilinis ieškovas nepateikė teismui neginčytinų įrodymų, kad dėl A. V. ir P. P. neteisėtų veikų ir jų vykdomų kibernetinių atakų TV3 televizija būtų patyrusi ilgalaikių pasekmių, būtų ženkliai sumažėjęs jos žiūrimumas. [...] Atsižvelgiant į tai, UAB „Tele – 3“ prašoma priteisti 50 000 Lt neturtinė žala mažintina iki 5000 Lt“*.[268] Ši baudžiamoji byla galutinai išspręsta Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2015 m. gegužės 12 d. nutartimi, kurioje pasisakydamas dėl padarytos žalos ir jos dydžio vertinimo teismas pažymėjo: *„Pagal nustatytas bylos aplinkybes UAB „T.“ padaryta 2809,56 Lt turtinė ir dėl televizijos kanalo reputacijos pablogėjimo – 5000 Lt neturtinė žala. Tačiau sprendžiant dėl padarytos žalos dydžio šioje byloje,*

[267] “Kauno apygardos teismas 2012 m. spalio 22 d. nutartis baudžiamojoje byloje Nr. 1A-94-175/2012,“ prieiga per internetą: http://www.infolex.lt/tp/Default.aspx?id=20&item=doc&aktoid=480057&nr=1

[268] “Vilniaus miesto apylinkės teismo 2013 m. kovo 25 d. nuosprendis baudžiamojoje byloje Nr. 1-455-655/2013,“ prieiga per internetą: http://www.infolex.lt/tp/932630?nr=1

atsižvelgtina į tai, kad: DDos atakomis buvo trikdomas tinklalapių, susijusių su visuomenės informavimu, darbas; šiomis atakomis sukelta problemų ne tik www.t.lt ir www.tv.lt, bet ir kitų tinklalapių funkcionavimui; intensyvi DDos ataka truko keletą dienų, jos padariniai likviduoti ne iš karto; panaudotos DDos atakos mechanizmas sudėtingas, atakos kompleksinės, kintančios; trikdymams sukelti naudotas didelis užkrėstų kompiuterių tinklas (botnet tinklas). Atsižvelgdama į šias aplinkybes, [...] UAB „T.“ padaryta žala yra didelė [...]“[269].

Vilniaus miesto apylinkės teismo 2013 m. balandžio 4 d. baudžiamuoju įsakymu J. V. nuteistas *inter alia* pagal BK 196 straipsnio 1 dalį ir 196 straipsnio 1 dalį, ir 196 straipsnio 1 dalį, ir 196 straipsnio 1 dalį, ir 196 straipsnio 1 dalį, ir 196 straipsnio 1 dalį, ir 196 straipsnio 1 dalį, ir 196 straipsnio 1 dalį, ir 196 straipsnio 1 dalį, ir 196 straipsnio 1 dalį už tai, kad *laikotarpiu nuo 2011 m. gegužės 26 d. iki 2011 m. sausio 5 d. Vilniaus universiteto Informacinėje sistemoje neteisėtai pakeitė studijų vertinimų rezultatus sau ir E. K., D. L., L. V., M. Š., N. M., K. L., A. S., P. P., A. K., I. J., R. K., dėl ko VĮ „Vilniaus universitetas“ buvo padaryta didelės žalos, kuri pasireiškė Vilniaus universiteto vardo ir garbės menkinimu, žalos padarymu studijų kokybei, sąžiningai studentų konkurencijai ir kitų Vilniaus universitete studijuojančių asmenų teisėtiems interesams gauti valstybės finansavimą studijoms.* Aprašomojoje baudžiamojo įsakymo dalyje teismas nepateikė argumentų dėl padarytos žalos ir jos dydžio vertinimo. Manytina, žalos ir jos dydžio vertinimui reikšminga tai, kad aptariamu baudžiamuoju įsakymu J. V. nuteistas *inter alia* pagal BK 182 straipsnio 1 dalį už tai, kad *pakeisdamas tikruosius elektroninius duomenis į netikrus, jis apgaule liko studijuoti valstybės finansuojamoje vietoje ir tuo apgaule išvengė pašalinimo iš universiteto už akademines skolas ir turtinės prievolės – sumokėti pirmosios pakopos (bakalauro) metinę studijų kainą 7 922,00 Lt, o pašalinimo iš VĮ „Vilniaus universitetas“ atveju - pareigos sumokėti į valstybės biudžetą 3 900 Lt studijų kainos skirtos valstybės finansuojamai vietai apmokėti, grąžinamos į valstybės biudžetą*.[270]

Prienų rajono apylinkės teismo 2012 m. gegužės 23 d. baudžiamuoju įsakymu R. B. nuteistas pagal BK 197 straipsnio 1 dalį už tai, kad *2012 m. kovo 1–3 d. prisijungė prie UAB „I. S.“ priklausančių internetinių svetainių www.infotour.lt, www.ieskok.eu, www.freeskelbimai.info, www.euros.lt, www.euroo.lt, www.vipskelbimai.eu, www.topskelbimai.info, www.talpink.eu, www.skelbiuonline.info, www.skelbimas.info, www.nemokanmi-skelbimai.info, www.ieskok.org, www.perka-parduota.lt ir, siųsdamas į jas didelį kiekį užklausų, tyčia sutrikdė UAB „I. S.“ serverių*

[269] “Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2015 m. gegužės 12 d. nutartis baudžiamojoje byloje Nr. 2K-188-489/2015,“ prieiga per internetą: http://www.infolex.lt/tp/1048281?nr=1

[270] “Vilniaus miesto apylinkės teismo 2013 m. balandžio 4 d. baudžiamasis įsakymas baudžiamojoje byloje Nr. 1-1471-716/2013,“ prieiga per internetą: http://www.infolex.lt/tp/Default.aspx?id=20&item=doc&aktoid=671988&nr=1

darbą, tuo padarydamas UAB „I. S.“ didelę 30 000 Lt žalą. Aprašomojoje baudžiamojo įsakymo dalyje pasisakydamas dėl padarytos žalos ir jos dydžio vertinimo teismas pažymėjo: *dėl kaltinamojo aktyvių neteisėtų veiksmų buvo sutrikdytas informacinės sistemos darbas, apribotas naudojimasis joje esančiais duomenimis ir padarytas poveikis visai informacinei sistemai*. Manytina, žalos ir jos dydžio vertinimui reikšmingi liudytojo R. J. parodymai, kuriuos apibendrinus paminėtina tai, kad *tris kartus buvo stabdomas ir iš naujo paleidžiamas serverio darbas, serveris negalėjo normaliai dirbti, strigo ir kitų svetainės lankytojų darbas, serveriu lankytojai naudotis praktiškai negalėjo, buvo neteisėtai pasisavinti svetainių administravimo slaptažodžiai, kurių pagalba buvo galima neteisėtai prisijungti prie svetainių, taip pat pasisavintas minėtų svetainių turinys ir duomenų bazės, iš jų įmonės buvo pavogta visa serveriuose saugota informacija, įmonės darbuotojai visą dieną bandė pertvarkyti sistemą, pakeitė administravimo slaptažodžius, interneto svetainės www.ieskok.org ir www.perka-parduoda.lt nefunkcionavo tol, kol jas atkūrė iš dienos archyvinės kopijos, tai truko keletą valandų, šios dvi interneto svetainės pagal lankytojų skaičių yra vienos iš populiariausių svetainių, dėl šių svetainių veiklos sutrikdymo, jų veiklos atkūrimo, duomenų vagystės, įmonė patyrė 30000 litų žalą.*[271]

Vilniaus miesto 2 apylinkės teismo 2009 m. gegužės 27 d. baudžiamuoju įsakymu V. Č. nuteistas *inter alia* pagal BK 196 straipsnio 3 dalį už tai, kad *2009 m. vasario 3 d. elektroniniame dienyne pakeitė dėstytojo I. R. dėstomo dalyko pažymius sau ir savo broliui D. Č. iš „3“ (trejeto) į „5“ (penketą)*, be to, *2009 m. vasario 4 d. elektroniniame dienyne dėstytojo I. B. pildomoje ataskaitoje pakeitė savo pažymį per abu kartus padarydamas VšĮ (duomenys neskelbtini) kolegija bendrai nedidelę neturtinę 5000 litų žalą*. Aprašomojoje baudžiamojo įsakymo dalyje pasisakydamas dėl baudžiamojoje byloje pareikšto civilinio ieškinio teismas pažymėjo: *atsižvelgiant į padarytų veiksmų pobūdį, pagrįstai darytina išvada, kad neteisėtais V. Č. veiksmais buvo pakenkta [...] kolegijos įvaizdžiui, kolegijos naudojamos duomenų bazės patikimumui bei buvo sukeltos duomenų baze besinaudojančių asmenų abejonės dėl jų duomenų, esančių kolegijos duomenų bazėje, teisingumo ir saugumo, todėl 5000 Lt prašomas žalos dydis yra laikytinas pagrįstu. Kaltinamasis sutinka atlyginti 5000 Lt žalą*.[272]

Vilniaus apygardos teismo Baudžiamųjų bylų skyriaus 2014 m. balandžio 16 d. nutartimi paliktas galioti apkaltinamasis nuosprendis, kuriuo V. S. nuteistas pagal BK 196 straipsnio 3 dalį už tai, kad *2012 m. gruodžio 21 d. neteisėtai prisijungė internetu iš kompiuterinės sistemos prie UAB*

[271] “Prienų rajono apylinkės teismo 2012 m. gegužės 23 d. baudžiamasis įsakymas baudžiamojoje byloje Nr. 1-122-805/2012,“ prieiga per internetą: http://www.infolex.lt/tp/473480?nr=1

[272] “Vilniaus miesto 2 apylinkės teismo 2009 m. gegužės 27 d. baudžiamasis įsakymas baudžiamojoje byloje Nr. 1-515-487/2009,“ prieiga per internetą: http://www.infolex.lt/tp/Default.aspx?id=20&item=doc&aktoid=278594&nr=1

„O“ kompiuterinės sistemos, t. y. prie minėtos įmonės internetinio puslapio administratoriaus teisėmis, ir sunaikino ištrindamas iš šios sistemos standžiojo disko atminties įmonės klientų prisijungimo kodus, informaciją apie įmonėje siūlomus produktus ir jų aprašymus, informaciją apie įmonėje galiojančias akcijas bei pasiūlymus, taip pat pakeitė informacinėje sistemoje buvusius duomenis apie siūlomas nuolaidas ir patalpino melagingą informaciją, tuo padarydamas UAB “O“ nedidelę 11 808,92 Lt žalą. Aprašomojoje nutarties dalyje teismas nepateikė argumentų dėl padarytos žalos ir jos dydžio vertinimo. Manytina, žalos ir jos dydžio vertinimui reikšmingi liudytojos Ž. B. parodymai, iš kurių paminėtina tai, kad buvo *„[...] sugadinta ir ištrinta įmonei svarbi informacija, paskelbta melaginga ir jų klientus klaidinanti medžiaga [...]“*.[273]

Vilkaviškio rajono apylinkės teismo 2013 m. lapkričio 4 d. baudžiamuoju įsakymu V. M., G. D., A. K. ir R. V nuteisti *inter alia* pagal BK 197 straipsnio 3 dalį už tai, kad, *laikotarpiu ne vėliau kaip nuo 2012 m. sausio 7 d. iki 2012 m. sausio 16 d., atgabeno judriojo radijo ryšių blokavimo prietaisą (slopintuvą) bei jį eksploatavo ir dėl šio prietaiso skleidžiamų radijo trikdžių realiai sutrikdė informacinės sistemos UAB „O“ bazinės stoties darbą – šie trikdžiai darė neigiamą įtaką ryšio kokybę – padarydami nedidelę žalą įmonės veiklai*. Aprašomojoje baudžiamojo įsakymo dalyje pasisakydamas dėl padarytos žalos ir jos dydžio vertinimo teismas pažymėjo: *inter alia* padarytos BK 197 straipsnio 3 dalyje įtvirtintos *veikos pobūdį ir pavojingumo visuomenei laipsnį teismas kvalifikuoja mažesniu nei jis apibrėžtas atitinkamoje rūšinėje baudžiamojo įstatymo dispozicijoje, kadangi informacinės sistemos trikdymas pagal bylos duomenis truko santykinai neilgai – apie 9 paras, jo trukmė ir mastas nebuvo tokie, kad būtų padarę ženklesnės turtinės ar kitokios žalos sistemos valdytojui (naudotojui)*.[274]

Remiantis moksline literatūra, kadangi neteisėto poveikio elektroniniams duomenims nusikalstamos veikos sudėtis materiali, kiekvienu atveju būtina nustatyti priežastinį ryšį tarp atliekamų veiksmų ir atsiradusių padarinių. Žalos atsiradimą turi lemti nusikalstamą veiką padariusio asmens veiksmai. Nusikalstama veika pripažįstama baigta nuo to momento, kai kyla žala. Jeigu kaltininkas siekia padaryti žalą, tačiau ji neatsiranda dėl nuo jo valios nepriklausančių aplinkybių, veika kvalifikuojama kaip pasikėsinimas.[275]

[273] “Vilniaus apygardos teismo Baudžiamųjų bylų skyriaus 2014 m. balandžio 16 d. nutartis baudžiamojoje byloje Nr. 1A-303-256/2014,“ prieiga per internetą: http://www.infolex.lt/tp/821736?nr=1

[274] “Vilkaviškio rajono apylinkės teismo 2013 m. lapkričio 4 d. įsakymas baudžiamojoje byloje Nr. 1-239-633/2013,“ prieiga per internetą: http://www.infolex.lt/tp/787150?nr=1

[275] Armanas Abramavičius et. al., *supra* note 2, p. 423; Aurelijus Gutauskas et. al., *supra* note 3, p. 467.

4.4. Nusikalstamą veiką kvalifikuojantys požymiai

BK 196 straipsnyje kriminalizuotą veiką kvalifikuojančiais požymiais pripažįstami neteisėtas poveikis daugelio informacinių sistemų elektroniniams duomenims arba strateginę reikšmę nacionaliniam saugumui ar didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinčios informacinės sistemos elektroniniams duomenims, arba nusikalstamos veikos padarymas pasinaudojant svetimais asmens duomenimis, arba padarant didelės žalos[276]. Dviejuose iš nurodytų požymių minima informacinė sistema. Todėl iš pradžių turėtų būti atskleistas jos turinys.

Remiantis R. Marcinauskaitės daktaro disertacija[277], komunikacijos ir informacijos mokslų srityje suformuluotos informacinės sistemos sąvokos atitinka bendrosios sistemų teorijos teiginius: sistema yra vienetas, kuris funkcionuoja aplinkoje, padeda siekti bendrų tikslų, yra sudarytas iš daugelio tarpusavyje sąveikaujančių dalių. Apibūdinant informacinę sistemą bendriausia prasme turimas mintyje technologijų, funkcijų ir šias technologijas naudojančių žmonių tarpusavio ryšys. Taigi informacinė sistema, be informacinių ir komunikacijos technologijų, komunikacijos ir informacijos mokslų srityje taip pat apima savo funkcionavimo kontekstą, susijusį su informacinės sistemos paskirtimi ir vartotojais. Vis dėlto, BK 198[1] straipsnyje (teigtina, ir BK 196 straipsnio 2 dalyje – *aut. pastaba*) minimos informacinės sistemos ištakų pirmiausia reikėtų ieškoti tiesiogiai tarptautiniuose ir Europos Sąjungos dokumentuose, kuriuose ji numatyta. Tiek Konvencijos dėl elektroninių nusikaltimų 1 straipsnio a punkte pateiktame kompiuterinės sistemos apibrėžime, tiek Pamatinio sprendimo 2005/222/TVR 1 straipsnio a punkte įtvirtintame informacinės sistemos apibrėžime aptariami išimtinai bendriausi technologiniai sistemų aspektai – aparatinė ir programinė įranga, sistemos atliekamos funkcijos. Į informacinės sistemos ir kompiuterinės sistemos turinį taip pat įtrauktos komunikacijos technologijos. Atsižvelgiant į tai, BK 198[1] straipsnyje (teigtina, ir BK 196 straipsnio 2 dalyje – *aut. pastaba*) vartojamas informacinės sistemos terminas turi būti suvokiamas be jos taikomojo aspekto – informacinės sistemos vartotojų ir aplinkos, kurioje ji funkcionuoja – ir bendriausia prasme galėtų būti laikoma informacinių technologijų (apimančių komunikacijos technologijas) sinonimu. BK 198[1] straipsnyje (teigtina, ir BK 196 straipsnio 2 dalyje – *aut. pastaba*) minima informacinė sistema turėtų būti siejama tik su kompiuterizuotomis informacinėmis sistemomis, kurios taiko informacines technologijas duomenų apdorojimo procesams realizuoti.

[276] Žalos kaip pavojingų padarinių požymis analizuotas darbo 4.3. poskyryje, todėl plačiau nebus nagrinėjamas.
[277] Mokslinėje literatūroje informacinės sistemos požymis išsamiai išnagrinėtas R. Marcinauskaitės daktaro disertacijoje. Plačiau žr. Renata Marcinauskaitė, *supra* note 4, p. 58-63. Siekiant nesikartoti, toliau darbe apibendrinamos mokslininkės padarytos įžvalgos bei išvados apie aptariamą nusikalstamos veikos sudėties požymį, siejant tai su tiriama nusikalstama veika.

Informacinės sistemos kaip neteisėto prisijungimo dalyko požymio (teigtina, ir BK 196 straipsnio 2 dalyje minimos informacinės sistemos – *aut. pastaba*) turinys apima tiek informacines technologijas, tiek komunikacijos technologijas. Kadangi informacinė sistema funkcionuoja kaip vienetas, kurį sudaro įvairus jos sudedamųjų dalių derinys, neteisėtas poveikis informacinės sistemos konfidencialumui gali būti padaromas tiesiogiai veikiant tik tam tikrus specifines funkcijas atliekančius jos komponentus.[278] Tai siejant su BK 196 straipsnio 2 dalimi, teigtina, kad šių informacinės sistemos komponentų elektroniniai duomenys atitinka BK 196 straipsnio 2 dalyje minimus informacinės sistemos elektroninius duomenis.

Neteisėto poveikio daugelio informacinių sistemų elektroniniams duomenims kriminalizavimas tiesiogiai susijęs su Direktyvos 2013/40/ES preambulės 13 punktu[279], 9 straipsnio 3 dalimi. Remiantis Direktyvos 2013/40/ES preambulės 13 punktu, *„tikslinga numatyti griežtesnes sankcijas tais atvejais, [...] kai elektroninė ataka vykdoma plačiu mastu ir todėl dėl jos daromas poveikis daugeliui informacinių sistemų, įskaitant tuos atvejus, kai ataka siekiama sukurti botnetą [...]“*. Direktyvos 2013/40/ES 9 straipsnio 3 dalyje valstybėms narėms numatyta pareiga užtikrinti, kad už *inter alia* neteisėto įsikišimo į duomenis nusikalstamą veiką, kai ji padaroma tyčia, būtų skiriama maksimali ne trumpesnė kaip trejų metų laisvės atėmimo bausmė, kai dėl 7 straipsnyje nurodytos, būtent tam tikslui skirtos arba pritaikytos priemonės[280] naudojimo nukenčia daug informacinių sistemų.

Pažymėtina, kad Direktyvoje 2013/40/ES greta „plačiu mastu vykdomos elektroninės atakos, dėl kurios daromas poveikis daugeliui informaciniu sistemų“ vartojami ir kiti žodžių junginiai: „didelės apimties atakos prieš informacines sistemas“ (Direktyvoje 2013/40/ES preambulės 5 punktas), „didelės apimties kibernetinėms atakoms“ (Direktyvoje 2013/40/ES preambulės 5, 6 punktai). Čia taip pat minima „per botnetą vykdoma ataka“ (Direktyvos 2013/40/ES preambulės 13

[278] Renata Marcinauskaitė, *supra* note 4, p. 59-63.

[279] Pažymėtina, jog Direktyvos 2013/40/ES oficialiame vertime lietuvių kalba preambulės 13 punkte padaryta klaida. Teigiama, kad „tikslinga numatyti griežtesnes sankcijas tais atvejais, [...] kai elektroninė ataka vykdoma plačiu mastu ir todėl dėl jos daromas poveikis daugeliui informacinių sistemų, įskaitant tuos atvejus, kai ataka siekiama sukurti botnetą *arba kai ji vykdoma naudojant botnetą ir tokiu būdu padaroma didelė žala*, įskaitant atvejus, kai ataka vykdoma per botnetą“. Tuo tarpu Direktyvos 2013/40/ES oficialiame vertime anglų kalba preambulės 13 punkte nurodyta: „It is appropriate to provide for more severe penalties [...] where a cyber attack is conducted on a large scale, thus affecting a significant number of information systems, including where it is intended to create a botnet, *or where a cyber attack causes serious damage, including where it is carried out through a botnet*“. Taigi Direktyvos 2013/40/ES oficialiu vertimu anglų kalba pabrėžiamas tikslingumas numatyti griežtesnes sankcijas tais atvejais *inter alia* kai elektronine ataka padaroma didelė žala, įskaitant atvejus, kai ataka vykdoma per botnetą. Atsižvelgiant į tai, baigiamajame darbe vadovaujamasi Direktyvos 2013/40/ES 13 punkto oficialiu vertimu anglų kalba.

[280] Direktyvos 2013/40/ES 7 straipsnyje minimos šios „būtent tam tikslui skirtos arba pritaikytos priemonės“ priemonės: *„[...] a) kompiuterinės programos, skirtos arba pritaikytos pirmiausia siekiant vykdyti bet kurią iš 3–6 straipsniuose nurodytų veikų‘ [...]“*.

punktas), kuri „gali būti naudojama didelės apimties kibernetinėms atakoms“ (Direktyvoje 2013/40/ES preambulės 5 punktas). Todėl pirmiausia turėtų būti aptarti elektroninę ataką apibūdinantys terminai „vykdoma plačiu mastu“ ir „didelės apimties“.

Direktyvos 2013/40/ES oficialių vertimų lietuvių ir anglų kalba palyginimas atskleidė, kad preambulės 5, 6 punktuose vartojamam terminui „didelė apimtis“ ir preambulės 13 punkte minimam terminui „platus mastas“ įvardyti vartojami skirtingi terminai anglų kalba. Didelės apimties atakos prieš informacines sistemas atitinka *large–scale attacks conducted against information systems* (preambulės 5 punktas), didelės apimties kibernetinės atakos atitinka *large–scale cyber attacks* (preambulės 5, 6 punktai). Tuo tarpu plačiu mastu vykdoma elektroninė ataka atitinka *a cyber attack conducted on a large scale* (preambulės 13 punktas). Tai leidžia manyti, jog Direktyvoje 2013/40/ES tokiu būdu elektroninės atakos atskiriamos pagal jų kokybinį ir kiekybinį pobūdį, t. y. kad, atitinkamai, didelės apimties elektroninės atakos žalingas potencialas nukreipiamas prieš atskiros (–ų) informacinės (–ių) sistemos (–ų) elektroninius duomenis, kai elektroninės atakos pobūdis neleidžia poveikio pripažinti daromu daugeliui jų. Tuo tarpu plačiu mastu vykdomos elektroninės atakos žalingas potencialas nukreipiamas prieš daugelio informacinių sistemų elektroninius duomenis[281].

Abiejų rūšių elektroninių atakų atribojimas įžvelgtinas Direktyvos 2013/40/ES preambulės 13 punkte: *„tikslinga numatyti griežtesnes sankcijas tais atvejais, [...] kai elektroninė ataka vykdoma plačiu mastu ir todėl dėl jos daromas poveikis daugeliui informacinių sistemų, įskaitant tuos atvejus, kai ataka siekiama sukurti botnetą, arba kai elektronine ataka padaroma didelė žala, įskaitant atvejus, kai ataka vykdoma per botnetą“*. Remiantis Direktyvos 2013/40/ES aiškinamuoju memorandumu, *„sąvoka „botnetas“ reiškia kompiuterių, kuriuose įdiegta kenkimo programinė įranga (kompiuterio virusai), tinklą. Toks užkrėstų kompiuterių („zombių“) tinklas gali būti naudojamas konkretiems veiksmams atlikti, pavyzdžiui, atakoms prieš informacines sistemas (t. y. kibernetinėms atakoms) rengti“*[282]. Per botnetą vykdomos elektroninės atakos gali būti tiek didelės apimties[283] (Direktyvos

[281] Vis dėlto, kategoriškos išvados dėl vartojamos terminijos neleidžia daryti *inter alia* Direktyvos 2013/40/ES aiškinamojo memorandumo oficialių vertimų lietuvių ir anglų kalba palyginimas, kuriuose minimiems „didelio masto atakos“, „didelio masto atakų“, „didelio masto atakoms“ terminams įvardyti *inter alia* vartojamas „*large–scale attacks*“ terminas anglų kalba, kuris sutampa su Direktyvos 2013/40/ES preambulės 5, 6 punktuose minimam terminui „didelė apimtis“ įvardyti vartojamu anglų kalbos žodžių junginiu. Paminėtina, jog „didelio masto“ terminui įvardyti Direktyvos 2013/40/ES aiškinamojo memorandumo oficialiame vertime anglų kalba taip pat vartojami šie atitikmenys: *executed on a large scale, size of the offences (cyber attacks), the large–scale aspect of the attacks, conducted on a large scale*.

[282] Europos Komisija, “Pasiūlymas dėl Europos Parlamento ir Tarybos direktyvos dėl atakų prieš informacines sistemas ir dėl Tarybos pamatinio sprendimo 2005/222/TVR panaikinimo, {SEC(2010) 1122 final} {SEC(2010) 1123 final} KOM (2010) 517 galutinis,“ p. 3, žiūrėta 2016 05 15, http://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:52010PC0517&from=EN

[283] Pvz., Telšių rajono apylinkės teismo 2012 m. liepos 27 d. baudžiamuoju įsakymu T. S. nuteistas pagal BK 197 straipsnio 3 dalį už tai, kad *panaudodamas DDoS atakas (didelis kiekis tinklo užklausų), neteisėtai sutrikdė UAB „ABG“ valdomos informacinės sistemos (tinklalapio www.streetracers.lt) darbą, tuo padarydamas bendrovei nedidelę 700 litų turtinę žalą*.

2013/40/ES preambulės 5 punktas), tiek didelio masto (Direktyvos 2013/40/ES aiškinamasis memorandumas). Tai leidžia teigti, kad Direktyvos 2013/40/ES preambulės 13 punkto kontekste per botnetą vykdomos elektroninės atakos, kuriomis daromas poveikis daugeliui informacinių sistemų, pripažįstamos vykdomomis plačiu mastu. Tuo tarpu per botnetą vykdomos didelės apimties elektroninės atakos, kuriomis nėra daromas poveikis daugeliui informacinių sistemų, pateisina griežtesnių sankcijų taikymą, jeigu elektronine ataka padaroma didelė žala.

Apibendrinus tai, kas išdėstyta, griežtesnės sankcijos pagal Direktyvą 2013/40/ES turi būti taikomos šiais atvejais: 1) plačiu mastu vykdoma elektroninė ataka, kuria daromas poveikis daugeliui informacinių sistemų, nesiekiant sukurti botnetą (Direktyvos 2013/40/ES preambulės 13 punktas); 2) plačiu mastu vykdoma elektroninė ataka, kuria daromas poveikis daugeliui informacinių sistemų, siekiant sukurti botnetą (Direktyvos 2013/40/ES preambulės 13 punktas); 3) per botnetą vykdoma elektroninė ataka, kuria nėra daromas poveikis daugeliui informacinių sistemų, tačiau padaroma didelė žala (Direktyvos 2013/40/ES preambulės 13 punktas); 4) dėl Direktyvos 2013/40/ES 7 straipsnyje nurodytos, būtent tam tikslui skirtos arba pritaikytos priemonės naudojimo nukenčia daug informacinių sistemų (Direktyvos 2013/40/ES 9 straipsnio 3 dalis). Kadangi išskirtas trečias atvejis nėra susijęs su poveikiu daugeliui informacinių sistemų – veikos kvalifikavimą čia apsprendžia didelės žalos padarymas – šis atvejis analizuojamo požymio kontekste nenagrinėtinas. Vis dėlto, išskirto trečio atvejo reikšmė pasireiškia tuo, kad, nenustačius neteisėto poveikio daugelio informacinių sistemų elektroniniams duomenims, turėtų būti vertinama, ar per botnetą vykdoma

---

Plačiau žr. "Telšių rajono apylinkės teismo 2012 m. liepos 27 d. baudžiamasis įsakymas baudžiamojoje byloje Nr. 1-185-187/2012," prieiga per internetą: http://www.infolex.lt/tp/405719?nr=1. Taip pat paminėtina Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2015 m. gegužės 12 d. nutartis, kuria *inter alia* paliktas galioti pirmos instancijos teismo nuosprendis, kuriuo A. V. nuteistas *inter alia* pagal BK 24 straipsnio 4 dalies ir 197 straipsnio 1 dalį, P. P. nuteistas pagal BK 197 straipsnio 1 dalį, už tai, kad *P. P., vykdamas A. V. nurodymą, laikotarpiu nuo 2011 m. spalio 19 d. iki 2011 spalio 21 d., pasinaudodamas kompiuterine technika ir programine įranga, skirta elektroninės paslaugos trikdymo atakai vykdyti, internetu iš Jungtinėse Amerikos Valstijose, Izraelyje, Vietname, Rusijos Federacijoje ir kitose pasaulio šalyse esančio kenkėjiškomis programomis užkrėsto kompiuterinio tinklo (naudojančio užkrėstus kompiuterius kaip tarpines tarnybines stotis siekiant nuslėpti realų naudotojo kompiuteriui priskirtą IP adresą), tyčia išsiuntė didelį užklausų kiekį į tinklapius www.tv3.lt ir www.tv3play.lt*. Aptariama nutartimi taip pat paliktas nepakeistu pirmos ir apeliacinės instancijos teismo nuosprendis dalyje, kuria A. V. nuteistas *inter alia* pagal BK 24 straipsnio 4 dalies ir 197 straipsnio 3 dalį, P. P. nuteistas pagal BK 197 straipsnio 3 dalį už tai, kad *P. P., vykdamas A. V. nurodymą, laikotarpiu nuo 2010 m. lapkričio 2 d. iki 2010 m. lapkričio 11 d., pasinaudodamas kompiuterine technika bei programine įranga, skirta elektroninės paslaugos trikdymo atakai vykdyti, internetu iš skirtingų Lietuvos Respublikos teritorijoje esančių kompiuterių, tyčia vienu metu išsiuntė didelį užklausų kiekį į tinklapį www.skundai.lt.* Tęsdamas nusikalstamą veiką *P. P., A. V. nurodymu, pasinaudodamas A kompiuterine technika ir programine įranga, skirta elektroninės paslaugos trikdymo atakai vykdyti, 2011 m. sausio 16 d., 2011 m. sausio 30 d. ir 2011 m. sausio 31 d., internetu, iš Lietuvos Respublikos teritorijoje esančių kompiuterių, bei 2011 m. vasario 5 d., vasario 10 d., spalio 21-22 d., iš užsienio šalyse (Tailande, Jungtinėse Amerikos Valstijose, Lenkijoje, Kolumbijoje ir kitose) esančių ir kenkėjišku programiniu kodu užkrėstu kompiuterinio tinklo (naudojančio užkrėstus kompiuterius kaip tarpines tarnybines stotis, siekiant nuslėpti realų naudotojo kompiuteriui priskirtą IP adresą), tyčia išsiuntė didelį užklausų kiekį į tinklapį www.skundai.lt.* Plačiau žr. "Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2015 m. gegužės 12 d. nutartis baudžiamojoje byloje Nr. 2K-188-489/2015," prieiga per internetą: http://www.infolex.lt/tp/1048281?nr=1

elektronine ataka padaryta didelė žala, kuri sudarytų pagrindą nusikalstamą veiką kvalifikuoti pagal BK 196 straipsnio 2 dalį.

Plačiu mastu vykdomų elektroninių atakų, kuriomis daromas poveikis daugeliui informacinių sistemų, nesiekiant sukurti botnetą, įtvirtinimo Direktyvos 2013/40/ES preambulės 13 punkte tikslas įžvelgtinas 2008 m. Europos Komisijos ataskaitoje Tarybai: *„Po to, kai priimtas Sprendimas* (Pamatinis sprendimas 2005/222/TVR – *aut. pastaba*)*, ne kartą prieš informacines sistemas įvykdytos nusikalstamos atakos parodė, kad, siekiant užkirsti joms kelią, šioje srityje reikia labiau derinti veiklą Europos lygmeniu. 2007 m. gegužės mėn. įvykdyta stambaus masto ataka prieš Estijos informacinę infrastruktūrą, per kurią ji išėjo iš rikiuotės [...]. [...] Po to, kai priimtas Sprendimas, visoje Europoje įvykdytos atakos parodė, kad kyla naujų pavojų: vienu metu įvykdytos itin didelio masto atakos prieš informacines sistemas ir padidėjo vadinamųjų „zombių“ tinklų naudojimas nusikalstamiems tikslams. [...] Atsižvelgdama į minėtuosius įvykius, Komisija apsvarstys veiksmus, kuriais būtų galima geriau reaguoti į „zombių“ tinklų keliamą grėsmę. Gali būti, kad bus numatyta konkrečiai laikyti nusikaltimu tam tikrus veiksmus, kurie palengvina nusikalstamą „zombių“ tinklų naudojimą, taip pat bus numatytos griežtesnės minimalios sankcijos už nusikalstamas stambaus masto ir itin pavojingas atakas prieš informacines sistemas“*[284]. Apie tai užsimenama ir Direktyvos 2013/40/ES aiškinamajame memorandume. Paminėtina, jog 2007 m. įvykdytos stambaus masto atakos prieš Estijos informacinę infrastruktūrą metu panaudotą botneto tinklą sudarė apie vienas milijonas kompiuterių[285], per tris savaites atakuojamų interneto tinklalapių skaičius išaugo iki šimtų, buvo sistemingai atakuojami ir išjungiami vyriausybės puslapiai, bankų sistemos, naujienų ir žiniasklaidos priemonės bei garsių Estijos universitetų svetainės[286]. Tai leidžia manyti, kad Direktyvos 2013/40/ES preambulės 13 punkte įtvirtinant aptariamą požymį omenyje turėtos akivaizdžiai plataus masto elektroninės atakos, kuriomis poveikis daromas neabejotinai dideliam informacinių sistemų skaičiui.

Direktyvos 2013/40/ES aiškinamajame memorandume aptiktinas didelio masto elektroninių atakų (bet ne daromo poveikio daugeliui informacinių sistemų) aiškinimas: *„Botneto pagalba rengiamos atakos dažnai būna didelio masto. Didelio masto atakos yra tokios atakos, kurios rengiamos pasitelkiant priemones, dėl kurių nukenčia daug informacinių sistemų (kompiuterių), arba tokios atakos, dėl kurių patiriama didelė žala, pvz., dėl sutrikusių sistemos paslaugų, finansinių*

[284] Europos Bendrijų Komisija, “Komisijos ataskaita Tarybai parengta pagal 2005 m. vasario 24 d. Tarybos pamatinio sprendimo dėl atakų prieš informacines sistemas 12 straipsnį, KOM (2008) 448 galutinis,“ p. 10, žiūrėta 2016 05 15, http://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:52008DC0448&from=EN

[285] Darius Štitilis, *supra* note 5, p. 16.

[286] Jason Richards “Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security,“ žiūrėta 2016 05 15, http://www.iar-gwu.org/node/65

išlaidų, prarastų asmens duomenų ir t. t. Šiame kontekste didelis botnetas yra laikomas tinklu, galinčiu padaryti didelę žalą“[287]. Taigi Direktyvos 2013/40/ES aiškinamajame memorandume išskiriami du kriterijai, kurie elektroninę ataką leidžia pripažinti vykdoma dideliu mastu: priemonių, dėl kurių nukenčia (angl. *affecting*) daug informacinių sistemų (kompiuterių), naudojimas ir didelės žalos padarymas. Dėl priemonių naudojimo elektroninė ataka pripažįstama vykdoma plačiu mastu tik kai nukenčia daug informacinių sistemų (kompiuterių). Tačiau tai, kiek informacinių sistemų (kompiuterių) dėl tokių priemonių naudojimo turi nukentėti, kad jų kiekį būtų galima pripažinti dideliu, nėra apibrėžta, taip pat nėra nurodyta pagal ką tai būtų galima nustatyti. Kalbant apie antrą kriterijų, paminėtina, jog didelės žalos ir didžiulės ekonominės žalos interpretavimas didelės apimties kibernetinių atakų kontekste aptiktinas Direktyvos 2013/40/ES preambulės 5, 6 punktuose, kur jų turinys aiškinamas panašiai kaip Direktyvos 2013/40/ES aiškinamajame memorandume: *„[...] užkrėstas kompiuterių tinklas, sudarantis botnetą, [...] gali būti naudojamas didelės apimties kibernetinėms atakoms, kurios paprastai gali sukelti didelę žalą [...]. [...] tokia žala gali būti susijusi su visuomenei labai svarbių sisteminių paslaugų sutrikdymu ar patiriamomis didelėmis finansinėmis išlaidomis, arba asmens duomenų ar slapto pobūdžio informacijos praradimu“* (Direktyvos 2013/40/ES preambulės 5 punktas); *„didelės apimties kibernetinės atakos gali sukelti didžiulę ekonominę žalą todėl, kad gali sutrikdyti informacinių sistemų veikimą ir komunikaciją, ir todėl, kad gali būti prarasta ar pakeista komerciniu požiūriu svarbi konfidenciali informacija ar kiti duomenys“* (Direktyvos 2013/40/ES preambulės 6 punktas). Taigi iš esmės skiriasi tik pavojingų padarinių požymio aiškinimo kontekstas: Direktyvos 2013/40/ES aiškinamajame memorandume minima didelio masto ataka, tuo tarpu Direktyvos 2013/40/ES preambulės 5, 6 punktuose – didelės apimties kibernetinė ataka. Tai leidžia manyti, kad šis didelės žalos požymio aiškinimas tinka tiek didelės apimties, tiek plačiu mastu vykdomoms elektroninėms atakoms apibūdinti – skiriasi tik šių pavojingų padarinių mastas, bet ne kokybė. Reikšminga tai, kad Direktyvos 2013/40/ES aiškinamajame memorandume nėra nurodyta, jog elektroninė ataka, kurios mastas didelis, kadangi padaroma didelė žala, turi būti padaromas poveikis daugeliui informacinių sistemų. Tai leidžia teigti, kad nenustačius neteisėto poveikio daugelio informacinių sistemų elektroniniams duomenims, turėtų būti vertinama, ar elektronine ataka *inter alia* dėl jos masto dydžio padaryta didelė žala, kuri sudarytų pagrindą nusikalstamą veiką kvalifikuoti pagal BK 196 straipsnio 2 dalį. Manytina, atsižvelgiant į kontekstą, aptariami terminai – „didelio masto elektroninė ataka“ ir „plačiu mastu vykdoma elektroninė ataka“ – vartojami sinonimiškai.

[287] Europos Komisija, *supra* note 281, p. 3-4, 6.

Plačiu mastu vykdomų elektroninių atakų, kuriomis daromas poveikis daugeliui informacinių sistemų, siekiant sukurti botnetą, įtvirtinimo tikslas *inter alia* įžvelgtinas Direktyvos 2013/40/ES preambulės 5 punkte: *„[...] direktyva siekiama, inter alia, nustatyti baudžiamąsias sankcijas už etapą, kuomet sukuriamas botnetas, būtent kai įgyjama nuotolinė daugelio kompiuterių kontrolė, pasitelkus prieš tuos kompiuterius nukreiptas kibernetines atakas ir juos užkrėtus žalinga programine įranga“*. BK 196 straipsnio kontekste aktualu tai, kad botneto kūrimas pasireiškia kenkėjiškos programinės įrangos įdiegimu užkrėstoje informacinėje sistemoje[288], todėl yra susijęs su neteisėtu poveikiu elektroniniams duomenims. Remiantis Direktyvos 2013/40/ES aiškinamuoju memorandumu: *„[...] didelis botnetas yra laikomas tinklu, galinčiu padaryti didelę žalą. Sunku nustatyti botnetų dydį, tačiau apskaičiuota, kad prisijungimų prie didžiausių nustatytų botnetų skaičius buvo nuo 40 000 iki 100 000 (t. y. užkrėstų kompiuterių) per 24 valandas. Prisijungimų skaičius per 24 valandas yra dažnai naudojamas matavimo vienetas botneto dydžiui nustatyti“*[289]. Pasak I. Walden, egzistuoja botnetų juodoji rinka, kur nusikalstamoms veikoms vykdyti gali būti samdomi šimtais, tūkstančiais ar netgi šimtais tūkstančių skaičiuojami kompiuteriai[290]. Tai leidžia manyti, kad elektroninės atakos, kuriomis siekiama sukurti botneta, vykdomos akivaizdžiai plačiu mastu, poveikis tokiomis atakomis daromas neabejotinai didelio skaičiaus informacinių sistemų elektroniniams duomenims. Manytina, tai turėta omenyje Direktyvos 2013/40/ES preambulės 13 punkte įtvirtinant aptariamą požymį.

Apibendrinant tai, kas išdėstyta, manytina, kad elektroninė ataka pripažįstama vykdoma plačiu mastu (didelio masto) tiek, kai ja daromas poveikis daugeliui informacinių sistemų, įskaitant atvejus, kai siekiama sukurti botnetą, tiek kai elektronine ataka, kurios mastas didelis, kadangi padaroma didelė žala, nėra padaromas poveikis daugeliui informacinių sistemų. Taigi terminai „didelio masto elektroninė ataka“, „plačiu mastu vykdoma elektroninė ataka“ nėra apriboti informacinių sistemų, kurioms daromas poveikis, skaičiaus nustatymu, bet taip pat priklauso nuo padarytos žalos ir jos dydžio vertinimo, sprendžiant, ar nusikalstama veika siekia pavojingumą, pateisinantį griežtesnių sankcijų taikymą. Tuo tarpu terminas „daromas poveikis daugeliui informacinių sistemų“ priklauso nuo informacinių sistemų, kurioms daromas poveikis, skaičiaus, kurio pakanka, siekiant elektroninę ataką (vien dėl to) pripažinti vykdoma plačiu mastu (didelio

[288] Moheeb Rajab et. al., “A Multifaceted Approach to Understanding the Botnet Phenomenon,“ p. 1-2, žiūrėta 2016 05 15, http://courses.isi.jhu.edu/netsec/papers/multifaceted.pdf; Kim–Kwang Choo, “Zombies and botnets,“ p. 2, žiūrėta 2016 05 15, http://aic.gov.au/media_library/publications/tandi_pdf/tandi333.pdf; David Barroso, “Botnets – The Silent Threat,“ p. 1, žiūrėta 2016 05 15, https://www.enisa.europa.eu/publications/archive/botnets-2013-the-silent-threat/at_download/fullReport

[289] Europos Komisija, *supra* note 282, p. 3.

[290] Ian Walden, *supra* note 9, p. 179.

masto) ir pateisinančiu griežtesnių sankcijų taikymą. Pastaruoju atveju reikšminga tai, kad elektroninės atakos pripažinimą vykdoma plačiu mastu (didelio masto) turi lemti ne didelės žalos padarymas (kuri taip pat gali kilti), o informacinių sistemų, kurioms daromas poveikis, skaičius. Taigi terminas „plačiu mastu vykdoma elektroninė ataka“ („didelio masto elektroninė ataka“) yra platesnis negu terminas „daromas poveikis daugeliui informacinių sistemų“. Todėl BK 196 straipsnio 2 dalyje įtvirtinto neteisėto poveikio daugelio informacinių sistemų elektroniniams duomenims požymio aiškinimas šia formuluote susiaurintas iki informacinių sistemų, kurių elektroniniai duomenys neteisėtai paveikiami, skaičiaus nustatymo, kuris atitinka apysunkiam nusikaltimui reikalingą pavojingumą. Sprendžiant tokio skaičiaus pripažinimo dideliu klausimą, reikšminga tai, kad šio požymio įtvirtinimą Direktyvos 2013/40/ES preambulės 13 punkte paskatino akivaizdžiai plataus masto elektroninės atakos, kuriomis poveikis daromas neabejotinai dideliam informacinių sistemų skaičiui, įskaitant atvejus, kuriais siekiama sukurti botnetą. Todėl ribiniais atvejais, kai poveikį negalima vienareikšmiškai pripažinti daromu daugelio informacinių sistemų elektroniniams duomenims, prioritetas turėtų būti teikiamas kitiems požymiams, pateisinantiems nusikalstamos veikos kvalifikavimą pagal BK 196 straipsnio 2 dalį, pvz., žalai, kuri vien dėl elektroninės atakos masto, paprastai tūrėtų būti didelė. Nenustačius tokių požymių, nusikalstama veika aptariamu ribiniu atveju pripažintina nesiekiančia pavojingumo, kuris pateisintų griežtesnių sankcijų taikymą.

Likusio aptarti požymio pagrindu griežtesnės sankcijos pagal Direktyvos 2013/40/ES 9 straipsnio 3 dalį turi būti taikomos kai dėl kompiuterinės programos, kuri skirta arba pritaikyta pirmiausia siekiant *inter alia* neteisėtai įsikišti į duomenis naudojimo nukenčia daug informacinių sistemų. Minėta, BK 196 straipsnio 2 dalyje įtvirtinto neteisėto poveikio daugelio informacinių sistemų elektroniniams duomenims požymio aiškinimas šia formuluote susiaurintas iki informacinių sistemų, kurių elektroniniai duomenys neteisėtai paveikiami, skaičiaus nustatymo, kuris atitinka apysunkiam nusikaltimui reikalingą pavojingumą. Todėl minėtos kompiuterinės programos naudojimas informacinių sistemų, kurių elektroniniai duomenys neteisėtai paveikiami, skaičiaus pripažinimui dideliu, manytina, neturi reikšmės.

Kitas BK 196 straipsnyje kriminalizuotą veiką kvalifikuojantis požymis – neteisėtas poveikis strateginę reikšmę nacionaliniam saugumui ar didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinčios (toliau – ir ypatingos reikšmės) informacinės sistemos elektroniniams duomenims. Šio padidintą informacinių sistemų reikšmę žyminčio požymio problematika išsamiai išnagrinėta R.

Marcinauskaitės daktaro disertacijoje[291]. Siekiant nesikartoti, toliau darbe apibendrinamos mokslininkės padarytos susijusios įžvalgos bei išvados, siejant tai su tiriama nusikalstama veika.

Viena iš infrastruktūros dalių yra informacinė sistema. Pastaroji rodo infrastruktūros sąsają su informacinėmis ir komunikacijos technologijomis. Informacinę infrastruktūrą gali sudaryti tiek viena informacinė sistema, tiek ir keletas jų. Sprendžiant, ar pati informacinė sistema yra ypatingos reikšmės, svarbu nustatyti, kad ji yra esminė užtikrinant pačios infrastruktūros funkcionavimą, sudaro pagrindą jos tinkamam veikimui. Ypatingos svarbos, valstybinės reikšmės ir strateginės bei didelės reikšmės tam tikriems sektoriams terminai baudžiamąja teisine prasme turėtų leisti įvardyti infrastruktūros, informacinės infrastruktūros išskirtinę, itin svarbią reikšmę. Strateginės reikšmės nacionaliniam saugumui arba didelės reikšmės valstybės valdymui, ūkiui ar finansų sistemai informacinės sistemos požymių nustatymui ir pagrindimui taikytini nukentėjusiųjų skaičiaus, poveikio ekonomikai ar visuomenei kriterijai. Tokiu atveju informacinės sistemos reikšmė atitinkamiems sektoriams būtų vertinama vertinant konkretaus sektoriaus, kuriame ji funkcionuoja, svarbą ir naudojant neigiamų padarinių masto kriterijus. Todėl aptariamas požymis būtų vertinamas kaskart atsižvelgiant į tai, ar buvo padaryta didelė žala ar kilo jos grėsmė nacionaliniam saugumui, valstybės valdymui, ūkiui ar finansų sistemai. Žalos mastui nustatyti gali būti taikomi nukentėjusiųjų, ekonominio poveikio ir poveikio visuomenei kriterijai. Neigiamų padarinių masto kriterijus turėtų būti taikomas atsižvelgiant į konkrečios srities – strateginės reikšmės nacionaliniam saugumui ar didelės reikšmės valstybės valdymui, ūkiui ar finansų sistemai – ir joje galinčios kilti didelės žalos ar jos grėsmės ypatumus.[292]

Neteisėto poveikio elektroniniams duomenims kriminalizavimo raida atskleidė, jog aptariamas požymis BK 196 straipsnio 2 dalyje kriminalizuotas įgyvendinant Pamatinio sprendimo 2005/222/TVR preambulės 15 punkte, 7 straipsnio 2 dalyje įtvirtintą galimybę nustatyti griežtesnes sankcijas, kai nusikaltimas padarė poveikio esminiams interesams. Jeigu dėl to būtų galima abejoti, kodėl BK 196 straipsnio kontekste ypatinga reikšmė siejama ne su elektroniniais duomenimis, o informacine sistema, tai tokias abejones pašalina Direktyvos 2013/40/ES 9 straipsnio 4 dalies c punktas. Čia valstybėms narėms įtvirtinta pareiga užtikrinti, kad už *inter alia* neteisėto įsikišimo į duomenis nusikalstamą veiką būtų nustatytos griežtesnės sankcijos tuo atveju, jei ji nukreipta prieš ypatingos svarbos infrastruktūros informacinę sistemą. Direktyvoje 2013/40/ES taip pat pažymėta, kad Sąjungoje yra ypatingos svarbos infrastruktūros objektų, kurių veiklos sutrikdymas arba

[291] Renata Marcinauskaitė, *supra* note 4, p. 89-95.
[292] *Ibid*., p. 94-95.

sunaikinimas padarytų didelį tarpvalstybinį poveikį (preambulės 4 punktas), nurodyta, kad vis didesnį susirūpinimą kelia galimi teroristų išpuoliai ar politiškai motyvuotos atakos prieš informacines sistemas, kurios yra valstybių narių ir Sąjungos ypatingos svarbos infrastruktūros dalis (preambulės 3 punktas). Tai leidžia manyti, kad griežtesnių sankcijų taikymą pateisintų neteisėtas poveikis ypatingos reikšmės informacinės sistemos elektroniniams duomenims, kuris kelia realų, o ne formalų pavojų. Tai, jog nusikalstama veika pagal BK 196 straipsnio 2 dalį nebūtų kvalifikuojama vien dėl to, kad elektroniniai duomenys yra ypatingos reikšmės informacinėje sistemoje, užtikrina reikalavimas nustatyti padarytą žalą.

Likęs aptarti BK 196 straipsnyje kriminalizuotą veiką kvalifikuojantis požymis – pasinaudojimas svetimais asmens duomenimis. Šio požymio kriminalizavimu įgyvendinta Direktyvos 2013/40/ES 9 straipsnio 5 dalis, kurioje valstybėms narėms nustatyta pareiga užtikrinti, kad sunkinančia aplinkybe būtų laikomas atvejis, kai *inter alia* neteisėto įsikišimo į duomenis nusikalstama veika įvykdoma piktnaudžiaujant kito asmens duomenimis siekiant įgyti trečiosios šalies pasitikėjimą, tokiu būdu padarant žalą teisėtam tapatybės turėtojui, išskyrus tuo atveju, jei ta aplinkybė jau yra taikoma kitai nusikalstamai veikai, už kurią baudžiama pagal nacionalinę teisę.

Asmens duomenų sąvoka pateikta Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo[293] 2 straipsnio 1 dalyje: *„bet kuri informacija, susijusi su fiziniu asmeniu – duomenų subjektu, kurio tapatybė yra žinoma arba gali būti tiesiogiai ar netiesiogiai nustatyta pasinaudojant tokiais duomenimis kaip asmens kodas, vienas arba keli asmeniui būdingi fizinio, fiziologinio, psichologinio, ekonominio, kultūrinio ar socialinio pobūdžio požymiai“*. Aptariamo įstatymo straipsnio 8 dalyje ypatingi asmens duomenys apibūdinami kaip *„duomenys, susiję su fizinio asmens rasine ar etnine kilme, politiniais, religiniais, filosofiniais ar kitais įsitikinimais, naryste profesinėse sąjungose, sveikata, lytiniu gyvenimu, taip pat informacija apie asmens teistumą“*. Nurodytų teisės normų analizė, M. Laurinaičio teigimu, *„[...] leidžia daryti išvadą, kad asmens duomenų sąvoka yra plati ir apima daug duomenų, kurie prima facie turi menką ryšį su konkrečiu asmeniu, tačiau kuriais remiantis gali būti nustatyta asmens tapatybė“*[294].

Pasak D. Štitilio ir M. Laurinaičio, tapatybės elektroninėje erdvėje nustatymas – tai vartotojo identifikavimo tam tikroje informacinėje sistemoje procesas, t. y. veiksmas kieno nors tapatybei nustatyti kompiuterių tinkle[295]. Anot M. Laurinaičio, vienas iš svarbiausių asmens identifikavimo

[293] "Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas," *Valstybės žinios* 22, 804 (2008).
[294] Darius Štitilis et. al., *Tapatybės vagystė elektroninėje erdvėje: socialiniai, elektroninio verslo ir teisinio reguliavimo aspektai* (Vilnius: Mykolo Romerio universitetas, 2011), 19.
[295] Darius Štitilis ir Marius Laurinaitis, "Tapatybės vagystė elektroninėje erdvėje," *Informacijos mokslai* 50 (2009): 246.

elektroninėje erdvėje elementų yra identifikavimas pagal tai, ką vartotojas turi žinoti. Autoriaus teigimu, *„[...] asmuo elektroninėje erdvėje gali būti identifikuojamas pagal unikalų pavadinimą (vardą) ir slaptažodį“*.[296] Pasak D. Štitilio ir M. Laurinaičio, *„[...] elektroninėje erdvėje tapatybė sutapatinama su prisijungimo vardu ir slaptažodžiu ir visos saugumo užtikrinimo priemonės [...] iš esmės atitinka asmens tapatybę elektroninėje erdvėje“*[297]. Kaip pastebi R. Marcinauskaitė, informacinių sistemų apsaugos priemonių pažeidimas tūrėtų būti konstatuotas *inter alia* kai pažeidžiami jų nustatyti apribojimai nesukeliant žalos pačioms apsaugos priemonėms, pvz., pažeidus autentifikavimo mechanizmų nustatytus prisijungimo prie IS apribojimus. Mokslininkės teigimu, *„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“*.[298]

Taigi pasinaudojant svetimais asmens duomenimis gali būti pažeidžiamos informacinės sistemos apsaugos priemonės. Tai yra vienas iš neteisėto prisijungimo prie informacinės sistemos ar jos dalies būdų[299]. Todėl BK 196 straipsnio 2 dalyje įtvirtintas pasinaudojimo svetimais asmens duomenimis požymis iš dalies apima neteisėtą prisijungimą prie informacinės sistemos ar jos dalies pažeidžiant informacinės sistemos apsaugos priemones. Baudžiamoji atsakomybė už tokią veiką taip pat numatyta BK 198^1 straipsnyje. Jeigu dėl to padaromas neteisėtas poveikis elektroniniams duomenims, padaryta veika atitinka tiek BK 198^1 straipsnio, tiek BK 196 straipsnio 2 dalies požymius, t. y. kyla šių nusikalstamų veikų konkurencija. BK 198^1 straipsnyje įtvirtinta veika apima tik neteisėtą prisijungimą prie informacinės sistemos ar jos dalies pažeidžiant informacinės sistemos apsaugos priemones pasinaudojant svetimais asmens duomenims. Tuo tarpu BK 196 straipsnio 2 dalis papildomai apima neteisėtą poveikį elektroniniams duomenims. Todėl teigtina, kad BK 196 straipsnio 2 dalis ir BK 198^1 straipsnis konkuruoja kaip, atitinkamai, visuma ir dalis. Vadovaujantis baudžiamosios teisės teorija[300], esant tokiai situacijai, taikytina BK 196 straipsnio 2 dalis, t. y. norma visuma, kadangi joje išsamiau aprašyti padarytos veikos požymiai, be to, į neteisėto poveikio

[296] Darius Štitilis et. al., *supra* note 294, p. 24.
[297] Darius Štitilis ir Marius Laurinaitis, *supra* note 295, p. 241.
[298] Renata Marcinauskaitė, *supra* note 4, p. 88.
[299] Kitas informacinės sistemos apsaugos priemonių pažeidimo būdas – žalos tokioms priemonėms padarymas. Plačiau žr. *ibid.*
[300] Vladas Pavilonis, *supra* note 128, p. 44. Vladas Pavilonis ir Egidijus Bieliūnas, *supra* note 128, p. 21; Alfonsas Klimka, *supra* note 128, p. 76, 90; Armanas Abramavičius et. al., *supra* note 128, p. 342; Tomas Girdenis, "Nusikalstamų veikų daugetas Lietuvos baudžiamojoje teisėje" (daktaro disertacija, Mykolo Romerio universitetas, 2010), 27, http://vddb.library.lt/obj/LT-eLABa-0001:E.02~2011~D_20101227_141843-98020

elektroniniams duomenims nusikalstama veiką, t. y. visumą (apysunkis nusikaltimas (BK 11 straipsnio 4 dalis)), įeinanti neteisėto prisijungimo prie informacinės sistemos nusikalstama veika, t. y. visumos dalis (nesunkus nusikaltimas (BK 11 straipsnio 3 dalis)), nėra pavojingesnė nei pati visuma, todėl neturi būti kvalifikuojama atskirai, t. y. pagal nusikalstamų veikų sutaptį.

Mokslinėje literatūroje teigiama, kad neviešų elektroninių duomenų (pvz., teisėto vartotojo prisijungimo vardo, slaptažodžio, kodo ar pan.) neteisėtu panaudojimu, kuriuo pasireiškia autentifikavimo procedūros apėjimas, yra suklaidinama informacinė sistema, kuri kaltininką identifikuoja kaip teisėtą sistemos vartotoja ir suteikia prie jos prieigą[301]. Tai leidžia teigti, kad tokiu prieigos kontrolės pažeidimu įgyjamas trečiosios šalies – informacinės sistemos – pasitikėjimas, padarant žalą teisėtam tapatybės turėtojui. Kadangi BK 196 straipsnio 2 dalyje įtvirtintas pasinaudojimo svetimais asmens duomenims požymis tiek, kiek jis susijęs su neteisėtu prisijungimu prie informacinės sistemos ar jos dalies pažeidžiant informacinės sistemos apsaugos priemones, Direktyvos 2013/40/ES 9 straipsnio 5 dalies žodžiais, jau yra taikomas *„[...] kitai nusikalstamai veikai, už kurią baudžiama pagal nacionalinę teisę“*, t. y. kriminalizuotas BK 198[1] straipsnyje, manytina, BK 196 straipsnio 2 dalyje įtvirtintas pasinaudojimo svetimais asmens duomenims požymis aptariamoje dalyje neatitinka Direktyvos 2013/40/ES 9 straipsnio 5 dalies reikalavimų.

[301] Renata Marcinauskaitė, *supra* note 4, p. 157.

5. SUBJEKTYVIEJI NETEISĖTO POVEIKIO ELEKTRONINIAMS DUOMENIMS SUDĖTIES POŽYMIAI

Kalbant apie subjektyviąją neteisėto poveikio elektroniniams duomenims pusę pagrindinis dėmesys skirtinas kaltės požymiui. Reikalas tas, kad įstatymų leidėjui BK 196 straipsnio dispozicijoje neįtvirtinus veikos padarymo tikslo ir motyvo, šie fakultatyvus sudėties požymiai veikos kvalifikavimui įtakos neturi[302]. Tuo tarpu pakaltinamumas, nors ir būdamas būtinuoju nusikalstamos veikos sudėties požymiu, preziumuojamas[303].

Kaltės nustatymo kiekvienoje byloje reikalavimas grindžiamas 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. Šios pagrindinės baudžiamosios atsakomybės nuostatos probleminiais informacinių ir komunikacijos technologijų panaudojimo atvejais, pvz., kilus neprognozuotam jų veiklos rezultatui, leidžia išvengti objektyvaus pakaltinimo, kai elektroninių duomenų konfidencialumo (teigtina – ir integralumo bei prieinamumo – *aut. pastaba*) pažeidimai padaryti be šių technologijų naudojo kaltės arba kita negu sudėtyje numatyta kaltės forma ir panašiai.[304]

BK 196 straipsnyje nesant nuorodos į veikos pripažinimą nusikalstama (ir tais atvejais), kai ji padaroma dėl neatsargumo, atsakomybė pagal baudžiamąjį įstatymą už neteisėtą poveikį elektroniniams duomenims galima esant tik tyčinei kaltės formai (BK 16 straipsnio 4 dalis). Tai atitinka susijusių viršnacionalinės teisės aktų nuostatas, kuriose aptariama nusikalstama veika siejama su tyčine kaltės forma (Konvencijos dėl elektroninių nusikaltimų 4 straipsnis, Pamatinio sprendimo 2005/222/TVR 4 straipsnis ir Direktyvos 2013/40/ES 5 straipsnis). Kaip pastebi R. Marcinauskaitė, *inter alia* subjektyvieji požymiai, konkrečiai – tyčinės kaltės nustatymo reikalavimas, rodo nusikalstamų veikų elektroninių duomenų informacinių sistemų saugumo inkriminavimo ribojimus. Mokslininkės teigimu, *„į tokio pobūdžio nusikalstamų veikų sudėtis įtraukus tik tyčinę kaltės formą išvengta jų, kaip „sugaunančių viską“ – nuo pavojingo iki bet kokio netinkamo elgesio su informacinėmis ir komunikacijos technologijomis – konstrukcijos“*.[305] Materiali sudėtis pagrindžia neteisėto poveikio elektroniniams duomenims veikos padarymo tiesiogine ir netiesiogine tyčia galimumą. Todėl konstatuojant tyčią būtina nustatyti, kad kaltininkas suvokė elektroninių duomenų

[302] Armanas Abramavičius et. al., *supra* note 2, p. 423; Aurelijus Gutauskas et. al., *supra* note 3, p. 460.
[303] Vytautas Piesliakas, *Lietuvos baudžiamoji teisė. Pirmoji knyga. Antroji pataisyta ir papildyta laida* (Vilnius: Justitia, 2009), 342.
[304] Renata Marcinauskaitė, *supra* note 4, p. 95, 153.
[305] *Ibid.*, 153.

neteisėto sunaikinimo, sugadinimo, pašalinimo ar pakeitimo arba naudojimosi tokiais duomenimis apribojimo techninę įrangą, programinę įrangą ar kitais būdais pavojingą pobūdį, numatė, kad dėl jo veikimo ar neveikimo gali būti pažeistas elektroninių duomenų integralumas ar prieinamumas ir gali būti padaryta žala, ir tokių padarinių norėjo arba nors jų nenorėjo, bet sąmoningai leido jiems atsirasti (BK 15 straipsnio 2 dalies 2 punktas, 3 dalis).

S. Bikelio teigimu, *„ [...] asmens, tyčia darančio nusikalstamą veiką, suvokimo dalykas yra (vien tiktai) visi baudžiamojo įstatymo specialiosios dalies straipsnio dispozicijoje įvardinti objektyvieji požymiai ir iš įstatymo išplaukiančios jų ypatybes [...] "*[306]. Taigi kaltininkas turi suvokti ne tik tai, kad jis daro poveikį elektroniniams duomenims, bet ir tai, jog tokie veiksmai yra neteisėti, kadangi šie objektyvieji požymiai tiesiogiai numatyti BK 196 straipsnio dispozicijoje. Pasak R. Marcinauskaitės, *„[...] jei nusikalstama veika padaroma elektroninėje erdvėje, toks suvokimas tūrėtų būti vertinamas atsižvelgiant į asmens patyrimą būtent šioje erdvėje. [...] 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, kada tam tikri jų veiksmai peržengia leidžiamas ribas. [...] šis aiškių ribų nustatymo poreikis aktualus visų CIA nusikalstamų veikų padarymo atvejais [...] "*[307]. Kaip pastebi I. Walden, kaltininko *inter alia* tyčia nebūtinai turi būti nukreipta į konkrečią programą, duomenis ar kompiuterį. Žinojimas yra susijęs tik su autorizacijos klausimu, bet ne daromos veikos mastu. Tokį teiginį autorius grindžia baudžiamųjų bylų pavyzdžiais, kuriose asmenys buvo nuteisti neatsižvelgiant į tai, kad jie nežinojo kokie kompiuteriai buvo paveikti dėl jų panaudotų virusų ir, nepriklausomai nuo to, jog atakos nebuvo nukreiptos prieš konkrečius kompiuterius.[308]

Kalbant apie kitą tyčios intelektinį momentą – galimybę numatyti pavojingų padarinių kilimą – pažymėtina, jog R. Mockevičius, D. Valatkevičius, M. Kuzminovas[309] apibrėždami aptariamos nusikalstamos veikos tyčios turinį neišskiria *elektroninių duomenų integralumo ar prieinamumo pažeidimo galimybės numatymą*, galimai sutapatindami tai su galimybe numatyti žalos kilimą. Tačiau elektroninių duomenų integralumo ir prieinamumo pažeidimas nebūtinai yra žala *per se*, pvz., trumpalaikis naudojimosi nenaudotinais elektroniniais duomenimis apribojimas, – tokiu atveju žalą gali sudaryti kitos su nusikalstama veika susijusios aplinkybės, pvz., prarasta reputacija. Todėl

[306] Skirmantas Bikelis, "Tyčinė kaltė baudžiamosios teisės teorijoje ir praktikoje" (daktaro disertacija, Mykolo Romerio universitetas, 2007), 56, http://vddb.library.lt/obj/LT-eLABa-0001:E.02~2007~D_20080111_173612-27751
[307] Renata Marcinauskaitė, *supra* note 4, p. 153-154.
[308] Ian Walden, *supra* note 9, p. 161, 176.
[309] Armanas Abramavičius et. al., *supra* note 2, p. 423; Aurelijus Gutauskas et. al., *supra* note 3, p. 459-460.

teigtina, jog kaltininkas turi numatyti tiek elektroninių duomenų integralumo ar prieinamumo pažeidimo, tiek žalos padarymo galimybę.

Apibendrinant tai, kas išdėstyta, neteisėto poveikio elektroniniams duomenims veika gali būti padaroma tiesiogine ir netiesiogine tyčia. Konstatuojant tyčią turėtų būti nustatoma, kad kaltininkas suvokė elektroninių duomenų neteisėto sunaikinimo, sugadinimo, pašalinimo ar pakeitimo arba naudojimosi tokiais duomenimis apribojimo technine įranga, programine įranga ar kitais būdais pavojingą pobūdį, numatė, kad dėl jo veikimo ar neveikimo gali būti pažeistas elektroninių duomenų integralumas ar prieinamumas ir gali būti padaryta žala, ir tokių padarinių norėjo arba nors jų nenorėjo, bet sąmoningai leido jiems atsirasti.

IŠVADOS

1. Baudžiamojo įstatymo saugomos vertybės kontekste elektroninių duomenų integralumas žymi, kad tokie duomenys yra nepaveikti arba paveikti teisėtai, o prieinamumas – jog sąlygos, kuriomis šie paprastai gali būti teisėtai valdomi, naudojami ar jais disponuojama, nėra neteisėtai paveiktos;
2. Neteisėto poveikio elektroniniams duomenims kriminalizavimas kaip *delicta sui generis* grindžiamas: jos atribojimu nuo turto sunaikinimo ar sugadinimo veikos; poreikiu kriminalizuoti pavojingas veikas, kurioms kvalifikuoti yra nepakankamos tradicinių nusikalstamų veikų sudėtys; ekvivalentiškumo principo įgyvendinimu ir kt.;
3. Aptariamos nusikalstamos veikos atžvilgiu valstybių, kurios yra Konvencijos dėl elektroninių nusikaltimų dalyvės, baudžiamieji įstatymai skiriasi pagal tai, ar juose įtvirtintas žalos požymis. Tokių valstybių, kuriose vyrauja bendrosios teisės tradicija, ši nusikalstama veika apibrėžta abstrakčiai, nedetalizuojant jos padarymo technologinių aspektų. Kai kurių kitų užsienio valstybių baudžiamuosiuose įstatymuose tokia nusikalstama veika siejama su prieš tai padarytu informacinių sistemų integralumo, prieinamumo ar konfidencialumo pažeidimu;
4. BK 196 straipsnyje kriminalizuotos veikos dalykas yra elektroniniai duomenys, kurie sudaro potencialią arba realią informaciją, pasižymi elektronine forma ir yra bendriausia prasme suvokiamoje informacinėje sistemoje. Programinė įranga (programa) gali būti suprantama kaip informacinės sistemos dalis arba kaip viena iš elektroninių duomenų formų;
5. Nusikalstamos veikos kvalifikavimui pagal BK 196 straipsnį svarbu nustatyti ne tai, kaip elektroniniai duomenys buvo paveikti (technologinis aspektas), o tai, kad tokie duomenys yra neteisėtai sunaikinti, sugadinti, pašalinti ar pakeisti arba naudojimasis jais yra apribotas;
6. Teoriškai, sunaikintais gali būti pripažinti iš dalies išlikę pradiniai elektroniniai duomenys, kurie dėl neteisėto poveikio prarado esminius kokybinius požymius, dėl ko prilygintini neegzistuojantiems, tačiau BK 196 straipsnio kontekste toks aiškinimas laikytinas pertekliniu;
7. Visiškas elektroninių duomenų pakeitimas vertintinas kaip jų sunaikinimas. Sunaikinimu taip pat pripažintinas vienų elektroninių duomenų visiškas pakeitimas kitais, jei tai susiję su pradinių elektroninių duomenų sunaikinimu. Jei tai nėra susiję su pradinių elektroninių duomenų sunaikinimu, padaryta veika kvalifikuotina kaip tokių duomenų prieinamumo pažeidimas;
8. Elektroninių duomenų sugadinimas yra speciali pakeitimo veikos atmaina, kuriai būdingi specifiniai pakeistų elektroninių duomenų kokybiniai požymiai. Pakeitimo ir sugadinimo pavojingos veikos atribojamos ir pagal kaltininko tyčios kryptingumą;

9. Elektroninių duomenų sunaikinimas padarytą veiką atspindi išsamiausiai, todėl tokiu būdu apribotas naudojimasis elektroniniais duomenimis kvalifikuotinas kaip jų sunaikinimas. Kai elektroniniai duomenys nėra sunaikinami, padarytas poveikis tokiems duomenims laikytinas tik naudojimosi jais apribojimo būdu. Todėl nustačius kaltininko tyčią apriboti naudojimąsi elektroniniais duomenimis inkriminuotinas šios pavojingos veikos padarymas;
10. Elektroninių duomenų pašalinimas yra būdas, kuriuo apribojamas naudojimasis tokiais duomenimis. Įstatymų leidėjui tokį būdą kriminalizavus savarankiškai, pašalinimo pavojinga veika pripažintina specialiu naudojimosi elektroniniais duomenimis apribojimo atveju;
11. Poveikis elektroniniams duomenims pripažintinas neteisėtu, jeigu asmuo tam neturi šių duomenų savininko ar teisėto valdytojo leidimo arba nors tokį leidimą turi, tačiau viršija suteiktų įgaliojimų ribas, arba toks poveikis elektroniniams duomenims draudžiamas teisės aktų;
12. Neteisėto poveikio elektroniniams duomenims pavojingais padariniais pripažintini elektroninių duomenų sunaikinimas, sugadinimas, pašalinimas ar pakeitimas arba naudojimosi tokiais duomenimis apribojimas, taip pat žalos padarymas;
13. Aptariama nusikalstama veika gali būti padaroma tiesiogine ir netiesiogine tyčia. Konstatuojant tyčią turėtų būti nustatoma, jog kaltininkas suvokė elektroninių duomenų neteisėto sunaikinimo, sugadinimo, pašalinimo ar pakeitimo arba naudojimosi tokiais duomenimis apribojimo technine įranga, programine įranga ar kitais būdais pavojingą pobūdį, numatė, kad dėl jo veikimo ar neveikimo gali būti pažeistas elektroninių duomenų integralumas ar prieinamumas ir gali būti padaryta žala, ir tokių padarinių norėjo arba nors jų nenorėjo, bet sąmoningai leido jiems atsirasti;
14. Neteisėto poveikio daugelio informacinių sistemų elektroniniams duomenims požymio aiškinimas šia formuluote susiaurintas iki informacinių sistemų, kurių elektroniniai duomenys neteisėtai paveikiami, skaičiaus nustatymo, kuris siekia apysunkio nusikaltimo pavojingumą;
15. Tai, kad nusikalstama veika pagal BK 196 straipsnio 2 dalį nebūtų kvalifikuojama vien dėl to, jog elektroniniai duomenys yra strateginę reikšmę nacionaliniam saugumui ar didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinčioje informacinėje sistemoje, užtikrina reikalavimas nustatyti padarytą žalą;
16. BK 196 straipsnio 2 dalyje įtvirtintas pasinaudojimo svetimais asmens duomenimis požymis iš dalies apima BK 198^1 straipsnyje numatytą neteisėto prisijungimo prie informacinės sistemos ar jos dalies pažeidžiant informacinės sistemos apsaugos priemones požymį. Jeigu dėl to padaromas neteisėtas poveikis elektroniniams duomenims, taikytina BK 196 straipsnio 2 dalis;

17. Sprendžiant apie padarytą žalą ir jos dydį visais atvejais būtina įvertinti turtinio ir neturtinio pobūdžio praradimus žyminčių aplinkybių visetą. Turtinės žalos dydžiui nustatyti negalima remtis BK 212 ir 190 straipsniuose pateiktu didelės turtinės žalos ir turto vertės aiškinimu;
18. Vadovaujantis ekvivalentiškumo principu, nusikalstama veika, padaryta elektroninėje erdvėje, kvalifikuotina pagal BK 196 straipsnį nustačius, kad elektroniniai duomenys, kuriems padarytas neteisėtas poveikis, nesudaro tradicinių nusikalstamų veikų dalyko;
19. Veika kvalifikuotina pagal BK 196 ir 187 straipsnių sutaptį nustačius kaltininko tyčią fiziniu poveikiu informacinei sistemai ar jos komponentams neteisėtai paveikti elektroninius duomenis;
20. Neteisėtas poveikis programinei įrangai (programai), kuri yra priemonė, padedanti apdoroti duomenis informacinėje sistemoje, kvalifikuotinas pagal BK 197 straipsnį. Papildomai nustačius neteisėtą poveikį programinei įrangai (programai) kaip elektroniniams duomenims, kuri konkrečiu atveju nėra tokia priemone, ar (ir) kitiems tokiems duomenims, jeigu tai apima kaltininko tyčia, nusikalstama veika kvalifikuotina pagal BK 196 ir 197 straipsnių sutaptį;
21. Jeigu neteisėtas poveikis informacinei sistemai apriboja naudojimąsi programine įranga (programa), kuri yra priemonė, padedanti apdoroti duomenis informacinėje sistemoje, padaryta veika kvalifikuotina pagal BK 197 straipsnį. Jei poveikiu informacinei sistemai buvo apribotas naudojimasis programine įranga (programa), kuri neatitinka minėtų požymių, padaryta veika kvalifikuotina pagal BK 196 ir 197 straipsnių sutaptį.

LITERATŪRA

Knygos, moksliniai straipsniai, daktaro disertacijos:

1. Abramavičius, Armanas, et. al. *Baudžiamoji teisė. Trečiasis pataisytas ir papildytas leidimas*. Vilnius: Eugrimas, 2001;
2. Abramavičius, Armanas, et. al. *Lietuvos Respublikos baudžiamojo kodekso komentaras. Specialioji dalis (99-212 straipsniai)*. Vilnius: VĮ Registrų centras, 2009;
3. Andress, Jason. *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice 1st Edition*. Waltham: Syngress, 2011;
4. Bikelis, Skirmantas. "Tyčinė kaltė baudžiamosios teisės teorijoje ir praktikoje." Daktaro disertacija, Mykolo Romerio universitetas, 2007. http://vddb.library.lt/obj/LT-eLABa-0001:E.02~2007~D_20080111_173612-27751;
5. Bishop, Matt. *Computer Security: Art and Science*. Boston: Addison–Wesley, 2003;
6. Bishop, Matt. *Introduction to Computer Security*. Boston: Addison–Wesley, 2004;
7. Britz, Marjie. *Computer Forensics and Cyber Crime: Third Edition*. United States: Prentice Hall, 2013;
8. Clough, Jonathan. *Principles of Cybercrime*. New York: Cambridge University Press, 2010;
9. Gajdamakin, Nikolaj. *Teoreticheskie osnovy kompjuternoj bezopasnosti. Uchebnoe posobie* [Theoretical Foundations of Computer Security. Textbook]. Jekaterinburg, 2008;
10. Gavrilin, Jurij, et. al. *Prestuplenija v sfere kompjuternoj informacii: kvalifikacija i dokazyvanie* [Crimes in the sphere of computer information: qualification and proving]. Moskva: Knizhnyj mir, 2003;
11. Girdenis, Tomas. "Nusikalstamų veikų daugetas Lietuvos baudžiamojoje teisėje." Daktaro disertacija, Mykolo Romerio universitetas, 2010. http://vddb.library.lt/obj/LT-eLABa-0001:E.02~2011~D_20101227_141843-98020;
12. Gladden, Matthew. *The Handbook of Information Security for Advanced Neuroprosthetics*. Indianapolis: Synthypnion Academic, 2015;
13. Goranin, Nikolaj, ir Dalius Mažeika. *Nusikaltimai elektroninėje erdvėje ir jų tyrimo metodikos: Mokomoji knyga*. Kaunas: TEV, 2011;
14. Graham, James, Richard Howard ir Ryan Olson. *Cyber Security Essentials*. Boca Raton: CRC Press, 2011;

15. Gutauskas, Aurelijus, et. al. *Baudžiamoji justicija ir verslas. Recenzuotų mokslinių straipsnių baudžiamosios teisės ir baudžiamojo proceso klausimais rinkinys*. Vilnius: Vilniaus universitetas, 2016;
16. Gutauskas, Aurelijus, et. al. *Lietuvos baudžiamoji teisė. Specialioji dalis. Pirmoji knyga*. Vilnius: Justitia, 2013;
17. Jastiuginas, Saulius. "Integralus informacijos saugumo valdymo modelis." *Informacijos mokslai* 61 (2012): 8;
18. Kanapeckas, Pranas, Egidijus Kazanavičius ir Antanas Mikuckas. *Kompiuterių elementai [elektroninis išteklius]: Vadovėlis*. Kaunas: Technologija, 2011;
19. Kazancev, Sergej, et. al. *Pravovoe obespechenie informacionnoj bezopasnosti: 2–e izdanie* [Legal protection of information security: 2nd Edition]. Moskva: Izdatelskij centr „Akademija", 2007;
20. Klimka, Alfonsas. *Nusikaltimų kvalifikavimas*. Vilnius, 1970;
21. Laponina, Olga. *Osnovy setevoj bezopasnosti. Chast 1. Mezhsetevye ehkrany: Uchebnoe posobie* [Network Security Fundamentals. Part 1. Firewalls: Textbook]. Moskva: Nacionalnyj otkrytyj universitet „Intuit", 2014;
22. Marcinauskaitė, Renata. "Nusikalstamomis veikomis elektroninėje erdvėje pažeidžiamos pagrindinės baudžiamojo įstatymo saugomos vertybės nustatymo problema." *Socialinių mokslų studijos* 3, 3 (2011): 909;
23. Marcinauskaitė, Renata. "Nusikalstamos veikos elektroninių duomenų ir informacinių sistemų konfidencialumui (Lietuvos Respublikos baudžiamojo kodekso 198 ir 198^1 straipsniai)." Daktaro disertacija, Mykolo Romerio universitetas, 2013. http://vddb.library.lt/obj/LT-eLABa-0001:E.02~2014~D_20140124_091020-54546;
24. Mazurov, Valerij. *Kompjuternye prestuplenija: klassifikacija i sposoby protivodejstvija: Ychebno–prakticheskoe posobie* [Computer crimes: classification and methods of counteracting: Training and practical guide]. Moskva: Paleotip, Logos, 2002;
25. Oscarson, Per. "Information Security Fundamentals: Graphical Conceptualisations for Understanding." Iš *Security Education and Critical Infrastructures*, Cynthia Irvine, Helen Armstrong (Eds.), 98. Monterey: Springer US, 2003;
26. Pavilonis, Vladas, ir Egidijus Bieliūnas. *Nusikaltimų kvalifikavimas esant jų daugetui ir baudžiamosios teisės normų konkurencija*. Vilnius, 1984;

27. Pavilonis, Vladas. “Baudžiamosios teisės normų konkurencija.“ *Teisės problemos* 2, 12 (1996): 40;
28. Petrauskas, Rimantas, ir Darius Štitilis. “Lietuvos Respublikos baudžiamasis kodeksas nusikaltimų elektroninėje erdvėje konvencijos kontekste.“ *Jurisprudencija* 24, 16 (2002): 83;
29. Piesliakas, Vytautas. *Lietuvos baudžiamoji teisė. Pirmoji knyga. Antroji pataisyta ir papildyta* laida. Vilnius: Justitia, 2009;
30. Rhodes–Ousley, Mark. *Information Security: Second Edition*. New York: The McGraw–Hill, 2013;
31. Sabaliauskas, Giedrius. “Informacijos saugumas internete: teisininkų ir informatikų problema.“ *Justitia* 2, (2001): 26;
32. Sadowsky, George, et. al. *Information Technology Security* Handbook. Washington DC: O‘Reilly Media, Inc., 2003;
33. Sattarova, Feruza, ir Kim Tao–hoon. “IT Security Review: Privacy, Protection, Access Control, Assurance and System Security.“ *International Journal of Multimedia and Ubiquitous Engineering* 2, 2 (2007): 19;
34. Sauliūnas, Darius, et. al. *Informacinių technologijų teisė*. Vilnius: NVO Teisės Institutas, 2004.
35. Sauliūnas, Darius. “Legislation on Cybercrime in Lithuania: Development and Legal Gaps in Comparison with the Convention on Cybercrime.“ *Jurisprudencija* 4, 122 (2010): 207;
36. Štitilis, Darius, et. al. *Tapatybės vagystė elektroninėje erdvėje: socialiniai, elektroninio verslo ir teisinio reguliavimo aspektai*. Vilnius: Mykolo Romerio universitetas, 2011;
37. Štitilis, Darius, et. al. *Teisės informatika ir informatikos teisė*. Vilnius: Mykolo Romerio universitetas, 2006;
38. Štitilis, Darius, ir Marius Laurinaitis. “Tapatybės vagystė elektroninėje erdvėje.“ *Informacijos mokslai* 50 (2009): 246;
39. Štitilis, Darius, ir Valdas Klišauskas. “Criminalization of dangerous acts in cyberspace in criminal codes of Lithuania and Russia: comparative aspects.“ *Matters of Russian and International Law* 3 (2013): 133;
40. Štitilis, Darius, ir Valdas Klišauskas. “Elektroninės informacijos saugos reglamentavimas Lietuvoje ir Rusijoje: lyginamieji aspektai.“ *Socialinės technologijos* 2, 2 (2012): 443;
41. Vacca, John. *Computer and Information Security Handbook*. Amsterdam: Elsiever, 2009;

42. Vekhov, Vitalij, ir Vladimir Golubev. *Rassledovanie kompjuternykh prestuplenij v stranakh SNG: Monografija* [Investigation of computer crimes in the CIS countries: Monograph]. Volgograd: Volgogradskaja akademija MVD Rossii, 2004;
43. Veršekys, Paulius. "Vertinamieji nusikalstamos veikos sudėties požymiai." Daktaro disertacija, Vilniaus universitetas, 2013. http://vddb.laba.lt/obj/LT-eLABa-0001:E.02~2013~D_20131125_134053-73474;
44. Volevodz, Aleksandr. *Protivodejstvie kompjuternym prestuplenijam: pravovye osnovy mezhdunarodnogo sotrudnichestva* [Combating computer crimes: the legal framework for international cooperation]. Moskva: Izdatelstvo „Jurlitinform", 2002;
45. Walden, Ian. *Computer Crimes and Digital Investigations*. New York: Oxford University Press, 2007;
46. Whitman, Michael, ir Herbert Mattord. *Principles of Information Security Fourth Edition*. Boston: Course Technology, 2012.

Elektroniniai leidiniai:

1. Barroso, David. "Botnets – The Silent Threat." Žiūrėta 2016 05 15. https://www.enisa.europa.eu/publications/archive/botnets-2013-the-silent-threat/at_download/fullReport;
2. Birgisson, Arnar, Alejandro Russo ir Andrei Sabelfeld. "Unifying Facets of Information Integrity." Žiūrėta 2016 05 15. http://www.cse.chalmers.se/~andrei/iciss10.pdf;
3. Buiati, Fábio, et al. "A Layered Trust Information Security Architecture." *Sensors* 14 (2014): 22759. http://dx.doi.org/10.3390/s141222754;
4. Christiaanse, Rob, ir Joris Hulstijn. "Neo–classical Principles for Information Integrity." Žiūrėta 2016 05 15. http://homepage.tudelft.nl/w98h5/Articles/integrity.pdf;
5. Committee of Ministers of the Council of Europe. "Explanatory Report to the Convention on Cybercrime." Žiūrėta 2016 05 15. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b;
6. Computer Misuse Act 1990. Žiūrėta 2016 05 15. http://www.legislation.gov.uk/ukpga/1990/18/crossheading/computer-misuse-offences;

7. Council of Europe. “Computer–Related Crime. Recommendation No. R (89) 9 on Computer–Related Crime and Final Report of the European Committee on Crime Problems.“ Žiūrėta 2016 05 15. http://www.oas.org/juridico/english/89-9&final%20report.pdf;
8. Criminal Code of Canada. Žiūrėta 2016 05 15. http://laws-lois.justice.gc.ca/eng/acts/c-46/page-88.html#h-116;
9. Criminal Code of the Republic of Albania. Žiūrėta 2016 05 15. http://www.legislationline.org/download/action/download/id/5164/file/Albania_CC_am2013_en.pdf;
10. Criminal Code of the Republic of Estonia. Žiūrėta 2016 05 15. https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/523122015005/consolide;
11. Criminal Code of the Republic of Latvia. Žiūrėta 2016 05 15. http://www.vvc.gov.lv/export/sites/default/docs/LRTA/Likumi/The_Criminal_Law.doc;
12. Criminal Code of the Swiss Confederation. Žiūrėta 2016 05 15. http://www.legislationline.org/download/action/download/id/5686/file/Swiss_CC_1937_am2014_en.pdf;
13. European Committee on crime problems, Committee of Experts on Crime in Cyber–space “Draft Convention on Cyber–crime (Draft N° 19).“ Žiūrėta 2016 05 15. http://www.politechbot.com/docs/treaty.html;
14. European Committee on crime problems, Committee of Experts on Crime in Cyber–space “Draft Convention on Cyber–crime (Draft N° 22 REV 2).“ Žiūrėta 2016 05 15. http://www.iwar.org.uk/law/resources/eu/cybercrime.doc;
15. European Committee on crime problems, Committee of Experts on Crime in Cyber–space “Draft Convention on Cyber–crime (Draft N° 24 REV. 2).“ Žiūrėta 2016 05 15. http://www.cyber-rights.org/documents/cybercrime24.htm;
16. European Committee on crime problems, Committee of Experts on Crime in Cyber–space “Draft Convention on Cyber–crime (Draft N° 25 REV.).“ Žiūrėta 2016 05 15. http://www.interlex.it/testi/cybercr25.htm;
17. European Committee on crime problems, Committee of Experts on Crime in Cyber–space “Draft Convention on Cyber–Crime and Explanatory Memorandum Related Thereto.“ Žiūrėta 2016 05 15. http://www.statewatch.org/news/2001/may/cybercrime27.doc;
18. Europos Bendrijų Komisija. “Komisijos ataskaita Tarybai parengta pagal 2005 m. vasario 24 d. Tarybos pamatinio sprendimo dėl atakų prieš informacines sistemas 12 straipsnį, KOM (2008)

448 galutinis.“ Žiūrėta 2016 05 15. http://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:52008DC0448&from=EN;

19. Europos Komisija. “Pasiūlymas dėl Europos Parlamento ir Tarybos direktyvos dėl atakų prieš informacines sistemas ir dėl Tarybos pamatinio sprendimo 2005/222/TVR panaikinimo, {SEC(2010) 1122 final} {SEC(2010) 1123 final} KOM (2010) 517 galutinis.“ Žiūrėta 2016 05 15. http://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:52010PC0517&from=EN;
20. Flowerday, Stephen, ir Rossouw von Solms. “What constitutes information integrity?” *SA Journal of Information Management* 9, 4 (2007): 2. http://dx.doi.org/10.4102/sajim.v9i4.201;
21. Gercke, Marco. “Understanding cybercrime: Phenomena, challenges and legal response.“ Žiūrėta 2016 05 15. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf;
22. Kim–Kwang Choo. “Zombies and botnets.“ Žiūrėta 2016 05 15. http://aic.gov.au/media_library/publications/tandi_pdf/tandi333.pdf;
23. Li, Peng, Yun Mao ir Steve Zdancewic. “Information Integrity Policies.“ Žiūrėta 2016 05 15. http://www.cis.upenn.edu/~stevez/papers/LMZ03.pdf;
24. Martin, Andrew, ir Deepak Khazanchi. “Information Availability and Security Policy.“ Žiūrėta 2016 05 15. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.99.9445&rep=rep1&type=pdf;
25. Mayfield, Terry, et. al. “Integrity in Automated Information Systems.“ Žiūrėta 2016 05 15. https://www.cs.umd.edu/~waa/414-F11/C-TR-79-91.pdf;
26. Mir, Suhail, et al. “Information Availability: Components, Threats and Protection Mechanisms.” *Journal of Global Research in Computer Science* 2, 3 (2011): 22. http://www.rroij.com/open-access/information-availability-components-threats-and-protection-mechanisms-21-26.pdf;
27. Muhsen, Abdellateef. “Information Security Management in Palestinian Banking.” Žiūrėta 2016 05 15. https://scholar.najah.edu/sites/default/files/Abdellateef%20Muhsen.pdf;
28. Pender–Bey, Georgie. “The Parkerian Hexad: The CIA Expanded.“ Žiūrėta 2016 05 15. http://cs.lewisu.edu/mathcs/msisprojects/papers/georgiependerbey.pdf;
29. Rajab, Moheeb, et. al. “A Multifaceted Approach to Understanding the Botnet Phenomenon.“ Žiūrėta 2016 05 15. http://courses.isi.jhu.edu/netsec/papers/multifaceted.pdf;
30. Richards, Jason. “Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security.“ Žiūrėta 2016 05 15. http://www.iar-gwu.org/node/65;

31. Sandhu, Ravi. “On Five Denitions of Data Integrity.“ Žiūrėta 2016 05 15. http://profsandhu.com/confrnc/ifip/i93int.pdf;
32. Štitilis, Darius. *Elektroniniai nusikaltimai. Metodinė priemonė*. Vilnius: Mykolo Romerio universitetas, 2011. http://ebooks.mruni.eu/pdfreader/elektroniniai-nusikaltimai43253;
33. Stoneburner, Gary. “Computer Security: Underlying Technical Models for Information Technology Security: Recommendations of the National Institute of Standards and Technology.“ Žiūrėta 2016 05 15. http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf
34. Ugolovnyj kodeks Respubliki Belarus [Criminal Code of the Republic of Belarus]. Žiūrėta 2016 03 11. http://etalonline.by/?type=text&regnum=HK9900275#load_text_none_1_;
35. Ugolovnyj kodeks Rossijskoj Federacii [Criminal Code of the Russian Federation]. Žiūrėta 2016 05 15. http://www.uk-rf.com/;
36. Ugolovnyj kodeks Ukrainy [Criminal Code of Ukraine]. Žiūrėta 2016 05 15. http://meget.kiev.ua/kodeks/ugolovniy-kodeks/;
37. US Code. Žiūrėta 2016 05 15. http://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title18-section1030&num=0&edition=prelim;
38. Winterfeld, Steve, ir Jason Andress. *The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice*. Waltham: Elsevier Inc., 2013. http://dx.doi.org/10.1016/B978-0-12-404737-2.00007-0.

Teisės aktai:

1. “Europos Parlamento ir Tarybos direktyva 2009/24/EB dėl kompiuterių programų teisinės apsaugos.“ *Oficialusis leidinys L* 111, 17 (2009).
2. “Europos Parlamento ir Tarybos direktyva 2013/40/ES dėl atakų prieš informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR.“ *Oficialusis leidinys L* 218, 8 (2013);
3. “Komiteto išvada Baudžiamojo kodekso 13, 162, 191, 196, 197, 203, 206, 216, 219, 221, 309 straipsnių pakeitimo ir papildymo bei Kodekso papildymo 198(1) ir 198(2) straipsniais įstatymo projektui.“ (2004);
4. “Komiteto išvada Baudžiamojo kodekso XXX skyriaus pavadinimo, 166, 167, 194, 196, 197, 198, 198(1), 198(2), 213, 214, 215, 262 straipsnių pakeitimo, Kodekso papildymo 257(1) straipsniu ir priedo papildymo įstatymo projektui.“ (2007);

5. “Konvencija dėl elektroninių nusikaltimų.“ *Valstybės žinios* 36, 1188 (2004);
6. “Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas.“ *Valstybės žinios* 22, 804 (2008);
7. “Lietuvos Respublikos baudžiamasis kodeksas.“ *Valstybės žinios* 89, 2741 (2000);
8. “Lietuvos Respublikos baudžiamojo kodekso 13, 162, 191, 196, 197, 203, 206, 216, 219, 221, 309 straipsnių pakeitimo ir papildymo bei kodekso papildymo 198-1 ir 198-2 straipsniais įstatymas.“ *Valstybės žinios* 45, 760 (2004);
9. “Lietuvos Respublikos baudžiamojo kodekso 139, 140, 176, 180, 181, 190, 201, 212, 249, 281 straipsnių pakeitimo ir papildymo įstatymas.“ *Valstybės žinios* 74, 3423 (2003);
10. “Lietuvos Respublikos baudžiamojo kodekso 7, 196, 197, 198-1, 198-2 straipsnių ir priedo pakeitimo ir Kodekso papildymo 270-3 straipsniu įstatymas.“ *Valstybės žinios* 2015, 09697 (2015);
11. “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* 81, 3309 (2007);
12. “Lietuvos Respublikos civilinis kodeksas.“ *Valstybės žinios* 74, 2262 (2000);
13. “Lietuvos Respublikos įstatymas dėl Konvencijos dėl elektroninių nusikaltimų ratifikavimo.“ *Valstybės žinios* 36, 1178 (2004);
14. “Lietuvos Tarybų Socialistinės Respublikos baudžiamasis kodeksas.“ *Vyriausybės žinios* 18, 147 (1961);
15. “Proposal for a Council Framework Decision on attacks against information systems /* COM/2002/0173 final - CNS 2002/0086 */.“ *Oficialusis leidinys* 203 *E* (2002);
16. “Tarybos pamatinis sprendimas 2005/222/TVR 2005 m. vasario 24 d. dėl atakų prieš informacines sistemas.“ *Oficialusis leidinys L* 69, 67 (2005).

Lietuvos Respublikos teismų praktika:

1. “Kauno apygardos teismo Baudžiamųjų bylų skyriaus 2012 m. spalio 22 d. nutartis baudžiamojoje byloje Nr. 1A-94-175/2012.“ Prieiga per internetą: http://www.infolex.lt/tp/Default.aspx?id=20&item=doc&aktoid=480057&nr=1;

2. “Kauno apylinkės teismo 2015 m. lapkričio 26 d. baudžiamuoju įsakymu baudžiamojoje byloje Nr. 1-2685-954/2015.“ Prieiga per internetą: http://www.infolex.lt/tp/Default.aspx?id=20&item=doc&aktoid=1196012&nr=1;
3. “Kauno miesto apylinkės teismo 2011 m. spalio 25 d. nuosprendis baudžiamojoje byloje Nr. 1-2092-246/2011.“ Prieiga per internetą: www.infolex.lt;
4. “Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2014 m. gruodžio 30 d. nutartis baudžiamojoje byloje Nr. 2K-580/2014.“ Prieiga per internetą: http://www.infolex.lt/tp/Default.aspx?id=20&item=doc&aktoid=943727&nr=1;
5. “Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2015 m. gegužės 12 d. nutartis baudžiamojoje byloje Nr. 2K-188-489/2015.“ Prieiga per internetą: http://www.infolex.lt/tp/1048281?nr=1;
6. “Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2015 m. sausio 27 d. nutartimi baudžiamojoje byloje Nr. 2K-32-696/2015.“ Prieiga per internetą: http://www.infolex.lt/tp/Default.aspx?id=20&item=doc&aktoid=993262&nr=1;
7. “Lietuvos Aukščiausiojo Teismo 2008 m. rugsėjo 21 d. teisės normų, reguliuojančių nusikalstama veika padarytos žalos atlyginimą, taikymo baudžiamosiose bylose apžvalga Nr. 29.“ Prieiga per internetą: http://www.infolex.lt/tp/91332?nr=5;
8. “Panevėžio apygardos teismo 2014 m. kovo 14 d. nuosprendis baudžiamojoje byloje Nr. 1-35-366/2014.“ Prieiga per internetą: http://www.infolex.lt/tp/875032?nr=2;
9. “Panevėžio miesto apylinkės teismo 2011 m. gegužės 24 d. nuosprendis baudžiamojoje byloje Nr. 1-187-389/2011.“ Prieiga per internetą: http://www.infolex.lt;
10. “Panevėžio miesto apylinkės teismo 2013 m. balandžio 2 d. nuosprendis baudžiamojoje byloje Nr. 1-85-334/2013.“ Prieiga per internetą: http://www.infolex.lt;
11. “Prienų rajono apylinkės teismo 2012 m. gegužės 23 d. baudžiamasis įsakymas baudžiamojoje byloje Nr. 1-122-805/2012.“ Prieiga per internetą: http://www.infolex.lt/tp/473480?nr=1;
12. “Radviliškio rajono apylinkės teismo 2014 m. balandžio 15 d. nuosprendis baudžiamojoje byloje Nr. 1-104-632/2014.“ Prieiga per internetą: http://www.infolex.lt/tp/916232?nr=1;
13. “Telšių rajono apylinkės teismas 2012 m. liepos 27 d. baudžiamuoju įsakymu baudžiamojoje byloje Nr. 1-185-187/2012.“ Prieiga per internetą: http://www.infolex.lt/tp/405719?nr=1;
14. “Vilkaviškio rajono apylinkės teismo 2013 m. lapkričio 4 d. įsakymas baudžiamojoje byloje Nr. 1-239-633/2013.“ Prieiga per internetą: http://www.infolex.lt/tp/787150?nr=1;

15. “Vilkaviškio rajono apylinkės teismo 2015 m. gegužės 22 d. nuosprendis baudžiamojoje byloje Nr. 1-111-633/2015.“ Prieiga per internetą: http://www.infolex.lt/tp/Default.aspx?id=20&item=doc&aktoid=1068389&nr=1;
16. “Vilniaus apygardos teismo Baudžiamųjų bylų skyriaus 2013 m. birželio 20 d. nutartis baudžiamojoje byloje Nr. 1A-410-312/2013.“ Prieiga per internetą: http://www.infolex.lt/tp/701867?nr=2#;
17. “Vilniaus apygardos teismo Baudžiamųjų bylų skyriaus 2014 m. balandžio 16 d. nutartis baudžiamojoje byloje Nr. 1A-303-256/2014.“ Prieiga per internetą: http://www.infolex.lt/tp/821736?nr=1;
18. “Vilniaus miesto 2 apylinkės teismo 2009 m. gegužės 27 d. baudžiamuoju įsakymu baudžiamojoje byloje Nr. 1-515-487/2009.“ Prieiga per internetą: http://www.infolex.lt/tp/Default.aspx?id=20&item=doc&aktoid=278594&nr=1;
19. “Vilniaus miesto apylinkės teismo 2013 m. balandžio 4 d. baudžiamuoju įsakymu baudžiamojoje byloje Nr. 1-1471-716/2013.“ Prieiga per internetą: http://www.infolex.lt/tp/Default.aspx?id=20&item=doc&aktoid=671988&nr=1;
20. “Vilniaus miesto apylinkės teismo 2013 m. kovo 25 d. nuosprendis baudžiamojoje byloje Nr. 1-455-655/2013.“ Prieiga per internetą: http://www.infolex.lt/tp/932630?nr=1;
21. “Vilniaus miesto apylinkės teismo 2015 m. vasario 10 d. baudžiamasis įsakymas baudžiamojoje byloje Nr. 1-844-276/2015.“ Prieiga per internetą: http://www.infolex.lt/tp/1019539?nr=1.

ANOTACIJA LIETUVIŲ IR ANGLŲ KALBOMIS

Baigiamajame darbe tiriama viena iš kompiuterinių nusikalstamų veikų, suvokiamų siaurąja prasme, – neteisėtas poveikis elektroniniams duomenims. Šios veikos kriminalizavimu Lietuvos Respublikos baudžiamojo kodekso 196 straipsnyje siekiama užtikrinti elektroninių duomenų integralumo ir prieinamumo kaip jų saugumo aspektų baudžiamąją teisinę apsaugą. Tyrimu siekiama išsiaiškinti neteisėto poveikio elektroniniams duomenims nusikalstamos veikos kriminalizavimo, aiškinimo ir taikymo problemas, taip pat santykį su kitomis susijusiomis nusikalstamomis veikomis, pateikti nagrinėjamų problemų sprendimo būdus. Atlikto tyrimo pagrindu gauti rezultatai suteikia žinių apie Lietuvos Respublikos baudžiamojo kodekso 196 straipsnyje įtvirtintos nusikalstamos veikos kriminalizavimo esmę, teikiamą baudžiamąją teisinę apsaugą, atskirų sudėties požymių turinį, santykį su kitomis susijusiomis nusikalstamomis veikomis ir su tuo susijusią problematiką.

Reikšminiai žodžiai: poveikis, elektroniniams, duomenims, integralumas, prieinamumas.

Thesis examines one of the computer crimes, understood in the narrow sense, – illegal data interference. The purpose of criminalization of this offence under Article 196 of the Criminal Code of the Republic of Lithuania is the need to ensure criminal legal protection of integrity and availability as the aspects of security of electronic data. The study aims to find out the problems of criminalization, interpretation and application of illegal data interference offence, as well as its relationship with other related offenses and to provide the relevant solutions. The results of the study provide knowledge about the essence of the criminalization, the provided criminal legal protection, contents of the individual constituent elements, the relationship with other related offenses and the related issues of the offence established in Article 196 of the Criminal Code of the Republic of Lithuania.

Kywords: illegal, data, interference, integrity, availability.

SANTRAUKA LIETUVIŲ KALBA

Baigiamojo darbo temos pavadinimas – „Neteisėtas poveikis elektroniniams duomenims (Baudžiamojo kodekso 196 straipsnis)“. Tai viena iš kompiuterinių nusikalstamų veikų, suvokiamų siaurąja prasme, kurios kriminalizavimu Lietuvos Respublikos baudžiamojo kodekso 196 straipsnyje siekiama užtikrinti elektroninių duomenų integralumo ir prieinamumo kaip jų saugumo aspektų baudžiamąją teisinę apsaugą. Tyrimu siekiama išsiaiškinti neteisėto poveikio elektroniniams duomenims nusikalstamos veikos kriminalizavimo, aiškinimo ir taikymo problemas, taip pat santykį su kitomis susijusiomis nusikalstamomis veikomis, pateikti nagrinėjamų problemų sprendimo būdus. Siekiant visapusiško supratimo, baigiamajame darbe analizuojami ne tik Lietuvos Respublikos baudžiamojo kodekso 196 straipsnyje kriminalizuotos nusikalstamos veikos atskiri sudėties požymiai, santykis su kitomis susijusiomis nusikalstamomis veikomis, bet ir informacijos saugos srityje pateiktas elektroninių duomenų integralumo ir prieinamumo aiškinimas, neteisėto poveikio elektroniniams duomenims kriminalizavimo raida, pagrindimas, baudžiamasis teisinis reguliavimas pasirinktose užsienio valstybėse. Atliktas tyrimas struktūrizuotas į viena kitą nuosekliai keičiančias dalis: iš pradžių analizuojamas elektroninių duomenų integralumas ir prieinamumas kaip baudžiamojo įstatymo saugoma vertybė, tuomet nagrinėjama neteisėto poveikio elektroniniams duomenims kriminalizavimo raida, pagrindimas, baudžiamasis teisinis reguliavimas pasirinktose užsienio valstybėse, pagaliau, šiame kontekste tiriamas atskirų Lietuvos Respublikos baudžiamojo kodekso 196 straipsnyje kriminalizuotos nusikalstamos veikos sudėties požymių turinys, santykis su kitomis susijusiomis nusikalstamomis veikomis ir su tuo susijusi problematika. Tyrimas pagrįstas informacijos saugai skirtos mokslinės literatūros, nacionalinės ir užsienio valstybių baudžiamosios teisės doktrinos, nacionalinės teismų praktikos, susijusių nacionalinės ir viršnacionalinės teisės aktų, taip pat dokumentų, kuriuose pateiktas jų nuostatų oficialus autentiškas aiškinimas, analize. Atlikto tyrimo pagrindu gauti rezultatai suteikia žinių apie Lietuvos Respublikos baudžiamojo kodekso 196 straipsnyje įtvirtintos nusikalstamos veikos kriminalizavimo esmę, teikiamą baudžiamąją teisinę apsaugą, atskirų sudėties požymių turinį, santykį su kitomis susijusiomis nusikalstamomis veikomis ir su tuo susijusią problematiką.

SANTRAUKA ANGLŲ KALBA

The topic of master‘s thesis is „Illegal data interference (Article 196 of the Criminal Code of the Republic of Lithuania)”. It is one of the computer crimes, understood in the narrow sense. The purpose of criminalization of this offence under Article 196 of the Criminal Code of the Republic of Lithuania is the need to ensure criminal legal protection of integrity and availability as the aspects of security of electronic data. The study aims to find out the problems of criminalization, interpretation and application of illegal data interference offence, as well as its relationship with other related offenses and to provide the relevant solutions. For a comprehensive understanding, thesis analyzed not only individual constituent elements, relationship with other related offenses of the offence established in Article 196 of the Criminal Code of the Republic of Lithuania, but also the interpretation of the electronic data integrity and availability set out in the field of information security, the evolution ant justification of criminalization, criminal legal regulation in selected foreign countries of illegal data interference. A study conducted structured into following parts: at first analyzed the integrity and availability of the electronic data as the values protected by the criminal law, then examined the evolution ant justification of criminalization, criminal legal regulation in selected foreign countries of illegal data interference, finally, in this context analyzed individual constituent elements, relationship with other related offenses and the related issues of the offence set out in Article 196 of the Criminal Code of the Republic of Lithuania. The study based on analysis of scientific literature on information security, national and foreign criminal law doctrine, national case law, the relevant national and supranational legislation, as well as documents containing official authentic interpretation of their provided provisions. The results of the study provide knowledge about the essence of the criminalization, the provided criminal legal protection, contents of the individual constituent elements, the relationship with other related offenses and the related issues of the offence established in Article 196 of the Criminal Code of the Republic of Lithuania.

PATVIRTINIMAS APIE ATLIKTO DARBO SAVARANKIŠKUMĄ

20 - -
Vilnius

Aš, Mykolo Romerio universiteto (toliau – Universitetas),

_____

(fakulteto / instituto, programos pavadinimas)

Studentas (-ė)_____,
(vardas, pavardė)

patvirtinu, kad šis rašto darbas / bakalauro / magistro baigiamasis darbas

„_____

_____“:

1. Yra atliktas savarankiškai ir sąžiningai;
2. Nebuvo pristatytas ir gintas kitoje mokslo įstaigoje Lietuvoje ar užsienyje;
3. Yra parašytas remiantis akademinio rašymo principais ir susipažinus su rašto darbų metodiniais nurodymais.

Man žinoma, kad už sąžiningos konkurencijos principo pažeidimą – plagijavimą studentas gali būti šalinamas iš Universiteto kaip už akademinės etikos pažeidimą.

_____ _____
(parašas) *(vardas, pavardė)*