MYKOLO ROMERIO UNIVERSITETO
TEISĖS FAKULTETO
BAUDŽIAMOSIOS TEISĖS IR PROCESO INSTITUTAS

MANTAS MICKEVIČIUS
(BAUDŽIAMOSIOS TEISĖS IR KRIMINOLOGIJOS STUDIJŲ PROGRAMA)
Programos valstybinis kodas 621M90011

NUSIKALSTAMOS VEIKOS ELEKTRONINIŲ DUOMENŲ IR INFORMACINIŲ SISTEMŲ SAUGUMUI

Magistro baigiamasis darbas

Darbo vadovas –
Lektorė, Jolita Šukytė

Vilnius, 2015

TURINYS

ĮVADAS 3
1. NETEISĖTAS POVEIKIS ELEKTRONINIAMS DUOMENIMS (BK 196 str.) 8
1.1. Objektyvieji neteisėto poveikio elektroniniams duomenims sudėties požymiai. 8
1.1.1 Elektroninių duomenų saugumas kaip saugoma vertybė. 8
1.1.2 Elektroniniai duomenys kaip nusikalstamos veikos dalykas. 10
1.1.3 Neteisėtas elektroninių duomenų sunaikinimas, sugadinimas, pašalinimas, pakeitimas ar naudojimosi apribojimas kaip pavojingos veikos. 14
1.1.4 Neteisėto poveikio elektroniniams duomenims baigtumo momentas ir padariniai. 21
1.1.5 Elektroniniai duomenys, esantys strateginę reikšmę nacionaliniam saugumui ar didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinčiuose informacinėse sistemose kaip kvalifikuojantis sudėties požymis. 25
1.2 Subjektyvieji neteisėto poveikio elektroniniams duomenims sudėties požymiai. 28
2. NETEISĖTAS ELEKTRONINIŲ DUOMENŲ PERĖMIMAS IR PANAUDOJIMAS (BK 198 str.) 29
2.1 Objektyvieji neteisėto elektroninių duomenų perėmimo ir panaudojimo sudėties požymiai. 29
2.1.1 Elektroninių duomenų konfidencialumas kaip saugoma vertybė. 29
2.1.2 Nevieši elektroniniai duomenys kaip nusikalstamos veikos dalykas. 31
2.1.3 Neteisėtas stebėjimas, fiksavimas, perėmimas, įgijimas, laikymas, pasisavinimas, paskleidimas ar kitoks panaudojimas kaip pavojingos veikos 33
2.1.4 Neteisėtas perėmimas ir panaudojimas neviešų elektroninių duomenų, kurie turi strateginę reikšmę nacionaliniam saugumui ar didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai kaip kvalifikuojantis sudėties požymis. 41
2.2. Subjektyvieji neteisėto elektroninių duomenų perėmimo ir panaudojimo sudėties požymiai 42
3. NUSIKALSTAMŲ VEIKŲ ELEKTRONINIŲ DUOMENŲ SAUGUMUI ATRIBOJIMAS NUO PANAŠIŲ VEIKŲ. 44
3.1 Nusikalstamos veikos elektroninių duomenų saugumui (BK 196 straipsnis) bei nusikalstamų veikų intelektinei ir pramoninei nuosavybei (BK 193 straipsnis) santykis. 44
3.2 Baudžiamosios ir administracinės atsakomybės už neteisėtą informacinių sistemų duomenų rinkimą, kaupimą, saugojimą, sunaikinimą ir asmens duomenų tvarkymo ir privatumo taisyklių pažeidimą atribojimas (ATPK 214[15]). 48
Išvados 53
Pasiūlymai 55
LITERATŪROS SĄRAŠAS 56
ANOTACIJA LIETUVIŲ IR ANGLŲ KALBOMIS 63
SANTRAUKA LIETUVIŲ KALBA 64
SANTRAUKA ANGLŲ KALBA 66
PATVIRTINIMAS APIE ATLIKTO DARBO SAVARANKIŠKUMĄ 68

ĮVADAS

Naujų technologijų atsiradimas bei vystymasis turėjo įtakos naujų nusikalstamo elgesio formų atsiradimui.[1] Neišvengiamai buvo susidurta su tokio pobūdžio nusikalstamų veikų darymu, dėl ko atsirado poreikis kriminalizuoti nusikalstamas veikas elektroninių duomenų ir informacinių sistemų saugumui. Šioms nusikalstamoms veikoms yra skirtas Lietuvos Respublikos baudžiamojo kodekso (toliau – BK) specialus XXX skyrius „Nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui“. Šis skyrius jau buvo keistas kelis kartus išplečiant ir patikslinant nusikalstamų veikų sudėtis taip pat jas papildant kvalifikuotomis sudėtimis.[2]

Tiriama problema. Sparti technologijų raida bei jų panaudojimas mūsų kasdieniniame gyvenime neišvengiamai sudarė galimybes atsirasti naujoms nusikalstamoms veikoms. Informacijos ištrynimas, sunaikinimas, perėmimas ar kitoks poveikis gali sukelti neigiamas pasekmes. Tokios nusikalstamos veikos numatytos BK XXX „Nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui“ skyriuje. Minėtame skyriuje išdėstytas nusikalstamas veikas, pagal nusikalstamos veikos dalyką, galima suskirstyti į kelias rūšis:

1) Elektroniniai duomenys (BK 196 ir 198 str.);

2) Informacinės sistemos (BK 197 ir 198[1] str.);

3) Įrenginiai ar programinė įranga, slaptažodžiai, prisijungimo kodai ar kitokie panašūs duomenys skirti tiesiogiai daryti nusikalstamas veikas (BK198[2] str.):

Pasitelkus tokį nusikalstamų veikų skirstymą, išskiriant nusikalstamas veikas pagal dalyką, kuriuos veikiant yra pažeidžiamos baudžiamojo įstatymo saugomos vertybės, šiame darbe tiriama pirmosios rūšies, nusikalstamos veikos elektroninių duomenų saugumui (BK 196 ir 198 str.), problematika.

Besivystančios naujosios technologijos leido tradicinėms nusikalstamoms veikoms persikelti į elektroninę erdvę, kas lėmė netinkamą baudžiamojo įstatymo nuostatų taikymą, kadangi baudžiamajame kodekse yra gausybė straipsnių, kuriuose yra numatyta baudžiamoji atsakomybė už panašius ar net tapačius nusikalstamos veikos sudėties požymius. Taip pat nagrinėjant teismų praktiką, susijusią su nusikalstamomis veikomis elektroninių duomenų saugumui, matoma, kad nėra nusistovėjusios nuoseklios praktikos, todėl teismai kartais netinkamai inkriminuoja tam tikrus sudėties požymius. Todėl šiame darbe yra nagrinėjami nusikalstamų veikų elektroninių duomenų

[1] Higgins, G. E., Cybercrime: An introduction to an Emerging phenomenon: New York: McGraw-Hill, 2010, p. 1.
[2] Kuzminovas, M., Nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui. *Lietuvos baudžiamoji teisė. Specialioji dalis.* Pirmoji knyga: vadovėlis. Vilnius: Justitia, 2013, p. 457.

saugumui (BK 196 ir 198 straipsniai) sudėties požymiai bei jų taikymo problemos. Be to, darbe ieškoma jų ryšio su kitomis nusikalstamomis veikomis ir atribojimo kriterijų, siekiant nustatyti optimalų baudžiamojo įstatymo nuostatų taikymą tokio tipo bylose. Taip pat nagrinėjamas baudžiamosios ir administracinės atsakomybės atribojimas, kadangi tiek baudžiamosios atsakomybės kilimui pagal BK 198 straipsnio 2 dalį, tiek administracinės atsakomybės kilimui pagal ATPK 214[15] straipsnį nereikalaujama, kad dėl padarytos veikos atsirastų kokie nors padariniai.

Baigiamojo darbo aktualumas. Nusikalstamų veikų elektroninių duomenų saugumui skaičius auga kartu su besivystančia bei tobulėjančia technologija, tai lemia nusikalstamų veikų didėjimą elektroninėje erdvėje. Tokio pobūdžio nusikalstamų veikų didėjimą parodo ir prokuratūros ataskaita[3].

Nusikalstamos veikos elektroninių duomenų saugumui buvo kriminalizuotos nuo naujojo BK įsigaliojimo ir nebėra laikomi kitų nusikalstamų veikų sudedamąją dalimi. Šioms nusikalstamoms veikoms tapus savarankiškomis iki šiol galima įžvelgti kylančias problemas dėl jų taikymo, kadangi nėra vienodos teismų praktikos, ji yra tebeformuojama.

Baigiamojo darbo mokslinis naujumas pasireiškia tuo, kad iki šiol galima atrasti problemų taikant šias normas. Kol kas yra parašyta nedaug mokslinių darbų, kuriuose yra neišsamiai nagrinėjami šių nusikalstamų veikų sudėties požymiai arba detalizuojamos tik kelios BK XXX skyriuje esančios nusikalstamos veikos. Taip pat dar iki šiol nebuvo specialiai skirtas dėmesys baudžiamosios ir administracinės atsakomybės atribojimo kriterijų paieškai, todėl šiame darbe ir stengiamasi šiuos kriterijus atrasti.

Baigiamajame darbe tiriamos problemos ištyrimo lygis. Nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui ilgą laiką nesusilaukė ypatingo dėmesio, galima įžvelgti pavienius bandymus aiškinti šių nusikalstamų veikų sudėties požymius. R. Marcinauskaitė 2013 metais apsigintoje disertacijoje „Nusikalstamos veikos elektroninių duomenų ir informacinių sistemų konfidencialumui (Lietuvos Respublikos baudžiamojo kodekso 198 ir 198[1] straipsniai)“ skyrė didelį dėmesį BK XXX skyriaus straipsniuose (198 ir 198[1] str.) numatytų nusikalstamų veikų sudėties požymiams, straipsnių tarpusavio santykiui, atribojimui nuo nusikalstamų veikų finansų sistemai bei nusikalstamų veikų privataus gyvenimo neliečiamumui ir kitas jų baudžiamojo teisinio vertinimo problemas[4]. Be to šioms nusikalstamoms veikoms dėmesį buvo skyręs ir D. Štitilis 2002 metais apsigintoje disertacijoje „Teisinės atsakomybės pagrindų nustatymo už neteisėtas veikas elektroninėje

[3] Plačiau žr. Lietuvos Respublikos Prokuratūros veiklos 2013 metais ataskaita. [interaktyvus], [žiūrėta 2015-02-13], <http://www.prokuraturos.lt/LinkClick.aspx?fileticket=3I95v%2Bn6dGs%3D&tabid=515>.

[4] Marcinauskaitė, R., *Nusikalstamos veikos elektroninių duomenų ir informacinių sistemų konfidencialumui (Lietuvos Respublikos baudžiamojo kodekso 198 str. ir 198[1] straipsniai).* Daktaro disertacija. Socialiniai mokslai, teisė (01S). Vilnius: Mykolo Romerio Universitetas, 2013.

erdvėje problemos“. Vėlesniuose jo darbuose buvo analizuojami bendri šių nusikalstamų veikų aiškinimo klausimai bei analizuojamos teisinės atsakomybės nustatymo už neteisėtas veikas elektroninėje erdvėje problemos[5]. Bendrus šių nusikalstamų veikų aiškinimo atvejus galima rasti ir metodinėse knygose, vadovėliuose, tokiuose kaip „Informacinių technologijų teisė“[6], „Elektroniniai nusikaltimai“[7], „Teisės informatika ir informatikos teisė“[8]. Taip pat paminėtini ir baudžiamojo įstatymo komentarai, kuriuose, kuriose matomas teorinis nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui normų aiškinimas.

Priešingai yra užsienio valstybėse, kuriose skiriamas didesnis dėmesys šioms nusikalstamoms veikoms. Apie elektroninių duomenų saugumo problemas tam tikrais aspektais yra pasisakę Susan W. Brenner, P. Grabosky, M. Williams, G. E. Higgins, I. Walden, M. T. Britz, J.T. Wells, G. L. Kovacich, W. C. Boni ir kt.

Baigiamojo darbo reikšmė. Gauti magistrinio darbo rezultatai bus naudingi tiek teoriniu, tiek praktiniu aspektu. Šie rezultatai gali būti naudingi teisės mokslininkams, tiriantiems nusikalstamas veikas elektroninių duomenų saugumui. Taip pat tyrimo rezultatai gali būti įdomūs, aktualūs ir naudingi kitiems asmenims, kurie siektų pagilinti žinias šia tema.

Tyrimo objektas. Šio magistro baigiamojo darbo objektas yra nusikalstamų veikų elektroninių duomenų saugumui numatytos BK 196 ir 198 straipsniuose, šių nusikalstamų veikų sudėties požymiai bei su jais susijusios problemos.

Tyrimo dalykas. Tyrimo dalyką sudaro įstatymų normos, reglamentuojančios nusikalstamas veikas elektroninių duomenų saugumui, poįstatyminiai teisės aktai, ES ir tarptautiniai teisės aktai, moksliniai darbai ir teismų praktika.

Tyrimo tikslai ir uždaviniai. Magistro baigiamojo darbo tyrimo tikslas yra išanalizuoti nusikalstamų veikų elektroninių duomenų saugumui (BK 196 ir 198 str.) sudėties požymius bei kylančias problemas juos inkriminuojant teismų praktikoje. Siekiant šių tikslų yra keliami šie uždaviniai:

1) Atskleisti nusikalstamos veikos elektroninių duomenų saugumui (BK 196 ir 198 str.) sudėties požymius bei identifikuoti kylančias problemas.

[5] Štitilis, D., *Teisinės atsakomybės pagrindų nustatymo už neteisėtas veikalas elektroninėje erdvėje problemos*. Daktaro disertacija. Socialiniai mokslai, teisė (01 S). Vilnius: 2002.
[6] Civilka M., *et al. Informacinių technologijų teisė*. Vilnius: NVO Teisės institutas, 2004.
[7] Štitilis, D., *Elektroniniai nusikaltimai*. Metodinė priemonė. Vilnius: Mykolo Romerio universitetas, 2011.
[8] Kiškis, M., *et al*., *Teisės informatika ir informatikos teisė*. Vadovėlis. Vilnius: Mykolo Romerio universitetas, 2006.

2) Nustatyti nusikalstamų veikų elektroninių duomenų saugumui santykį su panašiomis nusikalstamomis veikomis bei suformuluoti atribojimo kriterijus nuo administracinės teisės pažeidimų.
3) Ištirti šių nusikalstamų veikų reglamentavimo problemas remiantis teismų praktika bei moksliniais darbais.

Tyrimo metodika. Tam, kad būtų pasiekti tyrimo tikslai ir uždaviniai bei pagrįsti ginamieji teiginiai, tiriamajame darbe naudoti tiek teoriniai tiek empiriniai tyrimo metodai.

1) *Analizės* metodas taikytas nustatant bei aiškinant atskirus objektyviuosius ir subjektyviuosius nusikalstamos veikos sudėties požymius.
2) *Sisteminės analizės* metodas taikytas analizuojant Lietuvos Respublikos teismų praktiką, kurioje buvo nagrinėjami nusikalstamų veikų elektroninių duomenų saugumui atvejai, siekiant atrasti esminius skirtumus ir panašumus.
3) *Aprašomasis-lyginamasis* metodas taikytas aprašant Lietuvos ir užsienio šalių mokslininkų nuomones apie nusikalstamas veikas elektroninių duomenų saugumui. Taip pat taikant šį metodą buvo lyginamos tiek Lietuvos Respublikos įstatymuose, tiek tarptautiniuose teisės aktuose reglamentuotos teisės normos, susijusios su nusikalstamomis veikomis elektroninių duomenų saugumui bei kt.
4) *Apibendrinimo metodas* taikytas siekiant apibendrinti visą išanalizuotą ir panaudotą literatūrą, gautus empirinio tyrimo rezultatus, taip pat darant galutines išvadas.
5) *Dokumentų analizės* metodas taikytas analizuojant baudžiamąsias bylas dėl nusikalstamų veikų elektroninių duomenų saugumui.

Tyrimo struktūra. Magistro baigiamasis darbas susideda iš: įvado, trijų dėstomųjų dalių, išvadų, santraukos lietuvių kalba, santraukos anglų kalba, literatūros sąrašo, anotacijos lietuvių ir anglų kalbomis.

Pirmojoje dalyje analizuojami neteisėto poveikio elektroniniams duomenims (BK 196 str.) sudėties požymiai, tačiau esant ribotai šio darbo apimčiai ne visi sudėties požymiai bus išsamiai nagrinėjami.

Antrojoje dalyje analizuojami neteisėto elektroninių duomenų perėmimo ir panaudojimo (BK 198 str.) sudėties požymiai, tačiau esant ribotai šio darbo apimčiai ne visi sudėties požymiai bus išsamiai nagrinėjami.

Trečioje dalyje nustatinėjami pagrindiniai nusikalstamų veikų elektroninių duomenų saugumui atribojimo kriterijai nuo panašių nusikalstamų veikų bei baudžiamosios atsakomybės nuo administracinės atsakomybės atribojimo kriterijai.

Ginamasis teiginys. Nusikalstamų veikų elektroninių duomenų saugumui įstatyminis reglamentavimas, atsižvelgiant į teismų praktiką bei mokslinę literatūrą, reikalauja tikslinimo, kadangi kyla problemos atribojant nuo kitų nusikalstamų veikų bei inkriminuojant sudėties požymius.

1. NETEISĖTAS POVEIKIS ELEKTRONINIAMS DUOMENIMS (BK 196 str.)

1.1. Objektyvieji neteisėto poveikio elektroniniams duomenims sudėties požymiai.

1.1.1 Elektroninių duomenų saugumas kaip saugoma vertybė.

BK 196 straipsnyje numatytos nusikalstamos veikos pagrindinė saugoma vertybė yra laikomas elektroninių duomenų saugumas. Aiškinant elektroninių duomenų saugumą yra pasitelkiamos suformuluotos koncepcijos, kurios padeda atskleisti elektroninių duomenų saugumo turinį. Egzistuojant įvairioms elektroninių duomenų saugumo koncepcijoms, kai kurioms esant iš esmės panašioms, galima išskirti dvi pagrindinės koncepcijas: 1) techninis kompiuterių saugumas (angl. *Technical Computer Security*); 2) elektroninės erdvės saugumas (angl. *Cybersecurity).* Pirmoji koncepcija yra siejama su trimis elektroninių duomenų saugumą apibūdinančiomis savybėmis: elektroninių duomenų konfidencialumas, integralumas, prieinamumas. Antrajai koncepcijai apibūdinti yra vartojamos ganėtinai įvairios definicijos, kurias sieja tai, kad siekiama apsaugoti įvairias elektroninėje erdvėje kylančias grėsmes kaip neleistinu elektroninių duomenų naudojimu, prie tokių duomenų priėjimui ir pan.

Toliau bus nagrinėjama pirmoji koncepcija, kuri leido tarpusavyje į vieną savarankišką rūšį sujungti BK XXX skyriuje kriminalizuotas nusikalstamas veikas. Taip pat pažymėtina ir tai, kad techninis kompiuterių saugumas gali būti laikomas elektroninių duomenų saugumo sinonimu[9]. Taigi, elektroninių duomenų saugumas, kaip anksčiau minėta, remiasi trimis aspektais: konfidencialumu, vientisumu ir prieinamumu (dar vadinama *CIA Triad*)[10]. Lygiai tokie pat elektroninių duomenų saugumo aspektai įvardinti Konvencijoje dėl elektroninių nusikaltimų II skyriaus 1 skirsnio 1 dalyje „Nusikaltimai kompiuterinių duomenų ir sistemų konfidencialumui, vientisumui, prieinamumui“[11]. Šie suformuluoti aspektai yra laikomi klasikiniais, kurie yra pripažįstami daugumos mokslininkų, tačiau yra mokslininkų, kurie savaip papildo šiuos klasikinius aspektus. Pavyzdžiui išskirdami elektroninių duomenų autentiškumą kaip savybę, kuri garantuoja duomenų neiškraipymą jų saugojimo, kaupimo, apdorojimo ir perdavimo metu[12]. Taip pat aptinkamas ir skirtingai vertinamas Donn B. Parker skirstymas, dar vadinamas *The Parker Hexad.* Jis elektroninių duomenų saugumą

[9] Marcinauskaitė, R. Nusikalstamomis veikomis elektroninėje erdvėje pažeidžiamos pagrindinės baudžiamojo įstatymo saugomos vertybės nustatymo problema. *Socialinių mokslų studijos.* Mokslo darbai. 2011, 3 (3), p. 912.
[10] Jason, A. *The basics of information security: understanding the fundamentals of InfoSec in theory and practice*. Antrasis leidimas. Waltham, MA: Syngress, 2014, p. 5.
[11] Europos Tarybos konvencija dėl elektroninių nusikaltimų. *Valstybės žinios.* 2004, Nr. 36-1188.
[12] Kuzminovas, M., *supra* note 2, p. 417.

sudarančius aspektus praplėtė ir išskyrė tokius kriterijus kaip elektroninių duomenų konfidencialumą, vientisumą, prieinamumą, naudingumą, autentiškumą, laikymą ir valdymą. Toks Donn B. Parker skirstymas susilaukė tiek kritikos, tiek ir palaikymo, pastarieji tokį skirstymą laikė labiausiai užbaigtu.

Pirmasis, minėtos CIA Triados, požymis yra elektroninių duomenų konfidencialumas, kuris bendriausia prasme reiškia viešai neskelbtinas, slaptas[13]. Pažymėtina, kad konfidencialumas yra neatsiejamas elementas nuo privatumo. Šios abi sąvokos yra siejamos su gebėjimu apsaugoti savo duomenis nuo kitų asmenų, kurie neturi teisės šiuos duomenis turėti, matyti, naudoti savo reikmėms ir pan.[14]. Apskritai duomenų konfidencialumas reiškia tai, kad tam tikri duomenys nėra prieinami kitiems asmenims kuriems tokia teisė nėra suteikta. Tokią konfidencialumo sampratą galima aptikti daugelio mokslininkų darbuose, kurie bendra prasme teigia, kad duomenų konfidencialumas pasireiškia tokių duomenų slaptumu ir prie tokių duomenų prieigą turi tik teisėtas vartotojas.

Elektroninių duomenų vientisumas yra antrasis elektroninių duomenų saugumo aspektas, kuris reiškia gebėjimą užkirsti kelią šių duomenų pakeitimui neteisėtu ar neleistinu būdu. Tai reiškia, kad elektroninius duomenis gali pakeisti tik tam turintis teise arba turintis prieiga asmuo. Elektroninių duomenų vientisumo savybė laikytina tokia, kad tokių duomenų apdorojimo metu jie buvo pakeisti tik tam įgaliotų asmenų[15]. Yra aptinkama mokslininkų, kurie išskiria vientisumą į dvi rūšis: duomenų vientisumą (*angl. information integrity*) ir autentiškumo vientisumą (*angl. origin integrity arba dar kitaip vadinama authentication integrity*)[16]. Duomenų vientisumas sietinas su tokių duomenų turiniu, kad elektroniniai duomenys išliko nepakeisti, nebuvo modifikuoti ar pažeisti. Duomenų autentiškumas siejamas su tokių duomenų kilme, t.y. duomenys perdavimo, siuntimo metu nebuvo modifikuoti ar pakeisti. Taigi neteisėtas duomenų pakeitimas ar sunaikinimas reiškia duomenų vientisumo praradimą, kurie yra pačioje informacinėje sistemoje, laikmenoje ir pan., arba kai tinklo technologijomis ir protokolais užtikrinama, kad ryšio kanalais perduota informacija negali būti pakeista[17]. Tokią elektroninių duomenų vientisumo savybę galima aptikti daugumos mokslininkų darbuose, kuriuose bendrai teigiama, kad elektroninių duomenų vientisumas yra siejamas su tokių duomenų originalumo išlaikymu ir, kad duomenys nebuvo pakeisti neteisėto vartotojo.

---

[13] Keinys, S. (vyr. red.). *Dabartinis lietuvių kalbos žodynas*. Septintas pataisytas ir papildytas leidimas. Vilnius: Lietuvių kalbos institutas, 2012, p. 324.
[14] Jason, A. *supra* note 11, p. 6.
[15] Marcinauskaitė, R., *supra* note 5, p. 44.
[16] Bishop, M. *Computer security: Art and Science*. Addison Wesley Professional, 2003, p. 5.; Hernandez, S. *Official (ISC)2 Guide to the HCISPP CKB*. Taylor & Francis Group. 2015, p. 143.
[17] Garla, E., Dubovskaja, V. *Kompiuterinių tinklų projektavimas*. Vilnius: UAB Ciklonas, 2008, p. 124.

Trečiasis elektroninių duomenų saugumo aspektas yra elektroninių duomenų prieinamumas, kuris reiškia gebėjimą naudotis duomenimis, bet kuriuo momentu kada mums to reikia[18]. Toks apibrėžimas apima skirtingus požiūrius, kas yra elektroninių duomenų prieinamumas. Daugumos mokslininkų darbuose elektroninių duomenų prieinamumas suprantamas kaip atitinkamus įgaliojimus turintiems asmenims elektroniniai duomenys yra prieinami be trukdžių ar kliūčių ir gaunami reikiamu formatu. „Elektroninių duomenų prieinamumas“ taip pat gali būti suprantama kaip priėjimas prie tokių duomenų bet kuriuo užklausos pateikimo momentu. Nors mokslininkų aiškinimas ir nėra vienodas, bet elektroninių duomenų priėjimas turi būti suprantamas taip, kad prie tokių duomenų priėjimą turi tik toks asmuo, kuris turi tam suteiktus ar paskirtus įgaliojimus ir prie tokių duomenų gali prieiti bet kuriuo metu kai jam to reikia.

Apibendrinant galima teigti, kad aiškinant elektroninių duomenų saugumo kaip vertybės turinį yra pasitelkiamas CIA Triados modelis, kuris leidžia suprasti elektroninių duomenų saugumą kaip baudžiamojo įstatymo saugomą vertybę. Taigi siekiant atskleisti elektroninių duomenų saugumą kaip vertybę, turi būti vadovaujamasi CIA Triada, vertinant elektroninių duomenų konfidencialumą, vientisumą ir prieinamumą. Pasitelkiant tokį elektroninių duomenų saugumo savybių išskyrimą, buvo suteikta galimybė išskirti, kaip minėta anksčiau, į savarankiškas rūšis BK XXX skyriuje kriminalizuotas nusikalstamas veikas. Pažymėtina ir tai, kad gali būti pažeidžiama ir fakultatyvinė baudžiamojo kodekso saugoma vertybė. Tokiomis vertybėmis gali būti nuosavybė, privataus gyvenimo neliečiamumas, literatūros, mokslo ar meno kūrinio autorinės teisės ir teisėti interesai, valstybės saugumas, ekonominiai, finansiniai interesai ir kt. Tai priklauso nuo to kokio pobūdžio informacija buvo neteisėtai sunaikinta, sugadinta, pašalinta, pakeista arba techninės, programinės įrangos ar kitais būdais buvo apribotas naudojimasis šiais duomenimis.

1.1.2 Elektroniniai duomenys kaip nusikalstamos veikos dalykas.

Neteisėto poveikio elektroniniams duomenims dalykas BK 196 str. 1 d. dispozicijoje įvardintas kaip elektroniniai duomenys.

Analizuojant sąvoką - elektroniniai duomenys - svarbu paminėti yra tai, kad kartu su elektroninių duomenų sąvoka yra vartojama kompiuterinių duomenų sąvoka. Kompiuterinių duomenų sąvoka yra apibrėžta Europos tarybos konvencijoje dėl elektroninių nusikaltimų. Šios konvencijos 1 str. b) punkte yra sakoma, kad „kompiuteriniai duomenys – tai bet kokia faktų, informacijos arba sąvokų pateiktis tokiu pavidalu, kad juos būtų galima apdoroti kompiuterine sistema, taip pat

[18] Jason, A., *supra* note 11, p. 5.

programa, pagal kurią kompiuterinė sistema gali vykdyti tam tikrą funkciją“[19]. Europos Parlamento ir Tarybos direktyvoje 2013/40/ES 2 straipsnio b) punkte kompiuteriniai duomenys yra apibrėžiami taip „<...> faktai, informacija ar sąvokos, pateiktos tokia forma, kuri tinkama tvarkyti informacinėje sistemoje, įskaitant programą, tinkamą tam, kad informacinė sistema atliktų funkciją“[20]. Šie apibrėžimai nėra vienodi, tačiau jų esmė išlieka ta pati. Apibrėžimai yra siejami su sistemingomis kompiuterinės sistemos arba programos operacijomis su duomenimis atlikimu ir apdorojimu. Nors šiuose apibrėžimuose ir nėra tiesiogiai minimi kokie būtent tai duomenys yra, tačiau iš šių suformuluotų apibrėžimų galima teigti, kad pagrindinis požymis apibūdinantis kompiuterinius duomenis yra šių duomenų sistemingas apdorojimas pasitelkiant kompiuterį. Tokių duomenų forma turėtų būti suprantama kaip skaitmenizuota ir išreikšta dvejetaine sistema (vienetais ir nuliais). Todėl tokie duomenys gali būti ne tik kompiuterinės programos pagalba sukurti duomenys pačioje sistemoje, bet ir fiziniai daiktai perkelti į tokią formą. Tokie fiziniai daiktai gali būti knyga, kuri paverčiama tokiais duomenimis pasitelkiant skaitytuvą. Taip pat, autoriaus nuomone, tokiais duomenimis gali būti 3D skaitytuvu nuskaityti fiziniai objektai, kurie yra paverčiami skaitmeniniais duomenimis ir vėliau gali būti dubliuojant pasitelkiant 3D spausdintuvą.

Įgyvendinus Konvenciją dėl elektroninių nusikaltimų ir Europos Parlamento ir Tarybos pagrindų sprendimą dėl atakų prieš informacines sistemas nuostatas buvo pasirinkta kiek kitokia terminologija ir pasirinkta sąvoka buvo ne kompiuteriniai duomenys, o elektroniniai duomenys. Baudžiamajame kodekse nėra tiesiogiai apibrėžta elektroninių duomenų samprata, todėl šios sąvokos apibrėžimo tenka ieškoti kituose teisės aktuose bei moksliniuose darbuose. Elektroninių duomenų sąvoka yra apibrėžta Lietuvos Respublikos elektroninio parašo įstatymo 2 str. 2 p. „Elektroniniai duomenys – visi duomenys, kurie tvarkomi informacinių technologijų priemonėmis“[21]. Taip pat panašus elektroninių duomenų apibūdinimas aptinkamas ir aiškinamajame telekomunikacijų terminų žodinę, kuriame sakoma, kad „elektroniniai duomenys – visi duomenys, kurie tvarkomi informacijos technologijų pagalba“[22]. Elektroninių duomenų ir kompiuterinių duomenų sąvokos yra bene panašios, tačiau elektroninių duomenų sąvoka yra kiek platesnė ir apimanti didesnį spektrą technologijų, kurių pagalba šie duomenys gali būti suvokiami. Taigi, kompiuterinių duomenų sąvoka, kuri naudojama Konvencijoje dėl elektroninių nusikaltimų, yra siejama su kompiuterine sistema, kurioje elektroniniai

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

[20] Europos Parlamento ir Tarybos direktyva 2013/40/ES 2013 m. rugpjūčio 12 d. dėl atakų prieš informacines sistemas, kuria pakeičiamas pamatinis sprendimas 2005/222/TVR.

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

[22] Valiukėnas, V., Sabaliauskaitė, R., Gabijūnienė, J. *Aiškinamasis telekomunikacijų terminų žodynas.* Vilnius: AB „Spauda“ 2004, p. 40.

duomenys yra apdorojami bei programa, pagal kurią kompiuterinė sistema gali vykdyti tam tikrą procesą. Taigi, šie duomenys yra neatskiriami nuo kompiuterio ir sietini su šių duomenų buvimu kompiuteryje. Kiek kitokia terminologija, apibrėžiant kompiuterinius duomenis, buvo pasirinkta Europos tarybos pamatiniame sprendime bei Europos Parlamento ir Tarybos direktyvoje, kurioje aiškinant kompiuterinių duomenų sąvoką yra minima informacinė sistema. Informacinė sistema, šiuose tarptautiniuose teisės aktuose, yra aiškinama kaip „prietaisas arba tarpusavyje sujungtų ar susijusių prietaisų grupė, iš kurių vienas arba daugiau pagal programą vykdo automatinį kompiuterinių duomenų tvarkymą, taip pat kompiuteriniai duomenys, saugomi, tvarkomi, išrenkami arba perduodami to prietaiso ar grupės prietaisų jo ar jų eksploatacijos, naudojimo, apsaugos ir priežiūros tikslais“[23]. Taigi, šiame aiškinime duomenys taipogi yra neatsiejami nuo kompiuterio, kuris yra sujungtas prietaisų (procesoriaus, kietojo disko, pagrindinės plokštės ir pan.) arba tai gali būti prietaisas, kurie leidžia kompiuteriui atlikti tam tikrus procesus, t.y. tokių duomenų apdorojimas informacinėje sistemoje (kompiuterinėje sistemoje). Taigi, apibrėžiant kompiuterinių duomenų sąvoką, Konvencijoje dėl elektroninių nusikaltimų, yra siejama su kompiuterine sistema, Direktyvoje 2013/40/ES bei Pamatiniame sprendime 2005/222/TVR yra siejama su informacine sistema, Lietuvos Respublikos teisėje elektroninių duomenų apibrėžimas siejamas su informacinėmis technologijomis, kurios iš esmės apima kompiuterinę bei informacinę sistemą, kadangi informacinės technologijos terminas yra aiškinamas bei suprantamas plačiai. Pavyzdžiui informacinės technologijos yra siejamos su kompiuterių bei kitų elektroninių prietaisų naudojimu[24] arba kaip informacijos apdorojimo būdų ir priemonių visuma, kuriai priklauso viskas, kas skirta įrašyti, perduoti ar išreikšti informaciją[25]. Darytina išvada, kad tarptautiniuose teisės aktuose minimas kompiuterinių duomenų apibrėžimas yra siejamas su duomenų sistemingu apdorojimu panaudojant kompiuterį. Kiek plačiau yra suvokiamas elektroninių duomenų apibrėžimas, kuriame duomenų apdorojimas siejamas su informacinėmis technologijomis. Taigi, elektroninių duomenų apibrėžimas numato kiek platesnį duomenų apdorojimo būdą. Tai tampa ne tik kompiuterinės sistemos arba programos, o absoliučiai visos technologijos, kurios geba apdoroti, išreikšti tokius duomenis asmeniui riekiama forma. Atkreiptinas dėmesys, kad nors ir skirtingai yra įvardijamos technologijos ir naudojama terminologija, tačiau visus šiuos apibrėžimus sieja vienas ir tas pats požymis, t.y. duomenų forma. Taigi pirmumas turėtų būti teikiamas

[23] Europos Parlamento ir Tarybos direktyva 2013/40/ES 2013 m. rugpjūčio 12 d. dėl atakų prieš informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR

[24] Woodfort, K. *Cambridge learner‘s dictionary*. Trečiasis leidimas. Cambridge University Press. 2007, p. 371.

[25] Skyrius, R., Mikalauskienė, A., Zaleckienė, L. *Informacijos ir komunikacijos technologijos*. Vilnius: Vilniaus Universitetas, 2008, p. 17.

duomenų formai, o ne konkrečiai įvardinant technologijas, kurios apdoroja tokius duomenis, kas leistu nepagrįstai susiaurinti nusikalstamos veikos dalyką arba jį išplėsti[26].

Analizuojant teismų praktiką, kuriose yra aiškinama elektroninių duomenų sąvoka yra matoma, kad dalyko aiškinimas yra beveik identiškas elektroninių duomenų sąvokai, pateiktai Elektroninio parašo įstatyme bei aiškinamajame telekomunikacijų terminų žodyne. Pavyzdžiui, „<...> *elektroniniai duomenys, kurie įvardijami, kaip duomenys, tvarkomi informacinių technologijų priemonėmis ir yra sukurti elektronine forma arba perkelti į tokią formą. Taip pat elektroniniai duomenys įvardijami ir, kaip ženklų seka, skirta perduoti informacijai, naudojant informacines technologijas*.<...>“[27], „*Elektroniniai duomenys – tai duomenys, kurie tvarkomi informacinių technologijų priemonėmis. Elektroniniai duomenys turi būti sukurti elektronine forma arba perkelti į tokią formą.*“[28]. Tačiau kitose bylose yra fragmentiškai minima elektroninių duomenų sąvoka, jos nedetalizuojant ir apsiribojant tik jos įvardijimu. Visgi esmė išlieka ta pati teismai elektroninių duomenų sąvoką interpretuoja kaip duomenis, kurie yra tvarkomi informacinių technologijų pagalba.

Analizuojant elektroninių duomenų sąvoką svarbu paminėti, kad elektroniniai duomenys turi tam tikras savybes. Pirmoji savybė yra tokia, kad elektroniniai duomenys nėra suvokiami tiesiogiai, o tam yra reikalingos specialios technologijos, kurių pagalbą šie duomenys yra perkelti į tokią formą, kuri atsispindi ekrane, popieriuje ar kitokioje formoje. Antroji savybė – elektroniniai duomenys gali būti lengvai perkeliami iš vienos formos į kitą formą, kopijuojami ar perkeliami į kitas laikmenas. Trečioji savybė – kopijuojami ar perkeliami duomenys išlieka pirminėje laikmenoje ar įrenginyje, prie tokių duomenų priėmimą gali turėti net keli asmenys vienu metu. Ketvirtoji savybė – elektroniniai duomenys gali patys keistis be tiesioginės žmogaus sąveikos[29].

Paminėta, kad elektroninius duomenis galima klasifikuoti pagal tam tikrus aspektus. Prie elektroninių duomenų priėjimo atžvilgiu, tokie duomenys gali būti laisvai prieinami ir ribotą prieigą turintys elektroniniai duomenys (nevieši), pastarųjų prieiga yra ribojama įstatymų ar kitų teisės aktų, įmonių, įstaigų vidaus tvarkos taisykles reglamentuojantys dokumentai. Vieši elektroniniai duomenys yra laisvai ir visuotinai prieinami duomenys visiems asmenims. Prie tokių duomenų priėjimas nėra ribojamas ir juos galima pasiekti netrukdomai. Nevieši elektroniniai duomenys nėra laisvai prieinami. Tokie duomenys yra skirti ne visiems ir kurių naudojimas yra ribojamas įstatymų, teisės aktų ir

[26] Marcinauskaitė, R., *supra* note 5, p. 112.
[27] Vilniaus apygardos teismo 2011 m. gruodžio 23 d. nuosprendis baudžiamojoje byloje (bylos Nr. 1A-977/2011)
[28] Vilniaus miesto 2 apylinkės teismo 2011 m. liepos 1 d. nuosprendis baudžiamojoje byloje (bylos Nr. 1-188-387/2011)
[29] Kuzminovas, M., *supra* note 2, p. 462.

įmonių, įstaigų organizacijų vidaus tvarkos reglamentuojančių dokumentų (plačiau žr. 2.1.2 Nevieši elektroniniai duomenys kaip nusikalstamos veikos dalykas).

Taigi, neteisėto poveikio elektroniniams duomenims dalykas yra elektroniniai duomenys. Pažymėtina, kad pirmumas turi būti teikiamas elektroninių duomenų formai, o ne apibūdinant technologijas, kurios geba tokius duomenis apdoroti. Taigi, tokie duomenys turi būti išreikšti skaitmenine forma (dvejetainė sistema). Tokiais duomenimis gali būti ne tik informacinėje sistemoje sukurti duomenys, bet ir tokie duomenys, kurie buvo perkelti į tokią formą, pavyzdžiui, skaitytuvo pagalba ir pan.

1.1.3 Neteisėtas elektroninių duomenų sunaikinimas, sugadinimas, pašalinimas, pakeitimas ar naudojimosi apribojimas kaip pavojingos veikos.

Nusikalstama neteisėto poveikio elektroniniams duomenims veika gali pasireikšti alternatyviomis veikomis – sunaikinimu, sugadinimu, pašalinimu, pakeitimu ar naudojimosi apribojimu - tai reiškia, kad asmenį patraukti baudžiamojon atsakomybėn užtenka, kad jis atliktų bent vieną iš minėtų veiksmų.

Pažymėtina, kad toks poveikis elektroniniams duomenims, visų pirmą, turi būti neteisėtas. Neteisėtumas reiškia, kad asmuo atlikdamas veiksmus su elektroniniais duomenimis nėra teisėtas elektroninių duomenų valdytojas arba neturi tam teisėto duomenų savininko ar valdytojo leidimo naudotis elektroniniais duomenimis arba naudoti, valdyti tokius elektroninius duomenis yra draudžiama pagal nacionalinius teisės aktus[30]. Konvencijos dėl elektroninių nusikaltimų aiškinamajame rašte (62 p.) yra paminėta, kad bendra veikla, kuri yra būdinga informacinių sistemų priežiūrai ar pakeitimams, negali būti laikoma neteisėtu poveikiu. Pavyzdžiui, yra vykdomi informacinės ar kompiuterinės sistemos tvarkymo arba priežiūros darbai, kurių metu yra sunaikinami elektroniniai duomenys. Tokiais atvejai asmuo veikia teisėtai ir negali būti traukiamas baudžiamojon atsakomybėn Pažymėtina, kad neteisėtas poveikis bus ir tokiu atveju, kai asmuo, nors ir turėdamas teisėtą prieigą prie elektroninių duomenų, tačiau viršydamas įgaliojimus šiuos duomenis pakeičia, sunaikina ir pan.

Nors ir negausioje teismų praktikoje yra matoma tai, kad BK 196 str. 1 d. esanti nusikalstama veika gali būti inkriminuojama ir tais atvejais kai kaltininkas turėdamas teisėtą prieigą prie informacinės sistemos savo aktyviais veiksmais pažeidžia nustatytas vidaus tvarkos taisykles arba nesilaiko teisės aktais nustatytų įpareigojimų. Pavyzdžiui, Panevėžio apygardos teismo 2014 m. kovo

[30] Kuzminovas, M. *supra* note 2, p. 463-464.

14 d. nuosprendyje baudžiamojoje byloje (bylos Nr. 1-35-366/2014) R. P. 182 straipsnio 2 dalį, 183 straipsnio 2 dalį, 196 straipsnio 1 dalį (elektroninių duomenų pakeitimas), 300 straipsnio 1 dalį. Šioje byloje teismas konstatavo, kad *R. P. nuo 1994-06-13 iki 2009-06-05, dirbdamas AB SEB banke <...> Anykščių skyriaus klientų aptarnavimo vadybininku <...> sukūrė ir neteisėtai panaudojo aštuonių realiai neegzistuojančių asmenų anketinius duomenis, sudarė šių asmenų vardu septynias einamųjų sąskaitų sutartis <...>, be to, R. P. laikotarpiu nuo 2010-02-05 iki 2012-05-17, dirbdamas AB Šiaulių banko Anykščių klientų aptarnavimo skyriuje, esančiame (duomenys neskelbtini), buhalterio pareigose, iš savanaudiškų paskatų, apgaule, klastodamas dokumentus ir duomenis neteisėtai pakeisdamas elektroninius duomenis bei neteisėtai atlikdamas finansines operacijas, savo naudai neteisėtai įgijo terminuotų indėlių sąskaitose laikomus indėlininkų pinigus, tokiu būdu pasisavino jam patikėtą ir jo žinioje buvusį didelės vertės svetimą AB Šiaulių banko turtą <...>* būtent šioje byloje buvo nustatyta, kad R. P. dirbdamas, AB SEB banko klientų aptarnavimo skyriuje bei AB Šiaulių banke buhalterio pareigose, turėjo teisėtą prieigą prie informacinės sistemos ir galėjo joje atlikti jam paskirtus įgaliojimus, tačiau pažeisdamas teisės aktus, vidaus tvarkos taisykles bei neturėdamas nukentėjusiųjų sutikimo ir žinios nutraukė terminuotų indėlių sutartis, t.y. neteisėtai pakeitė informacinėje sistemoje esančius elektroninius duomenis ir šiais neteisėtais veiksmais pasisavino indėlininkų turtą. Be to, neteisėtai sukūrė aštuonių realiai neegzistuojančių asmenų anketinius duomenis bei tokiais veiksmai pasisavino ne jam priklausantį turtą.

Analizuojant elektroninių duomenų sunaikinimą svarbu paminėti yra tai, kad elektroninių duomenų sunaikinimo veika yra prilyginama fizinio daikto sunaikinimui[31]. Toks elektroninių duomenų sunaikinimo palyginimas yra minimas ir Konvencijoje dėl elektroninių nusikaltimų aiškinamojoje ataskaitoje (61 punktas), kurioje taip pat nurodoma, kad sunaikinimas yra prilyginamas materialaus daikto sunaikinimui. Taigi, analizuojant elektroninių duomenų sunaikinimo sąvoką kaip pavojingą veiką, galima atsižvelgti į tai, kaip tokia veika yra suprantama kitų nusikalstamų veikų prasme, o būtent turto sunaikinimo ir sugadinimo baudžiamosiose bylose (BK 187 str.). Pavyzdžiui, nusikalstamų veikų turto sunaikinimo ar sugadinimo bylose sunaikinimas yra aiškinamas kaip „*Turtas laikomas sunaikintu, kai jis netenka savo ekonominės ir ūkinės vertės bei jo nebegalima naudoti pagal funkcinę paskirtį*[32]“, taigi sunaikinimas yra siejamas su materialaus daikto visišku sunaikinimu, visišku materialinės vertės praradimu arba, kad tokio materialaus turto nebegalima panaudoti pagal jo

[31] Civilka, M., *et al*., *supra* note 7, p. 517.
[32] Vilniaus apygardos teismo 2013 m. gegužės 22 d. nutartis baudžiamojoje byloje (bylos Nr. 1A-365-200/2013); Šiaulių apygardos teismo 2012 m. balandžio 26 d. nuosprendis baudžiamojoje byloje (bylos Nr. 1A-154-116/2012); Kauno apygardos teismo 2012 m. kovo 8 d. nutartis baudžiamojoje byloje (bylos Nr. 1A-224-557/2012) ir kt.

paskirtį. Taip pat materialaus turto sunaikinimas yra aiškinamas kaip tam tikras poveikis svetimam turtui, dėl kurio šis nustoja egzistuoti, visiškai praranda savo vertę ar tampa netinkamu naudoti ar vartoti pagal paskirtį[33]. Į tokį veikos interpretavimą turi būti orientuojamasi aiškinant elektroninių duomenų sunaikinimą, tačiau, šį apibrėžimą sieti su elektronine erdve. Taigi, tokie materialaus turto sunaikinimo aiškinimai negali būti tiesiogiai pritaikytini nusikalstamoms veikoms elektroninėje erdvėje, kadangi nusikalstamos veikos dalykas neleidžia kalbėti apie materialaus objekto sunaikinimą. Todėl pasitelkiant šį aiškinimą ir pritaikant elektroninės erdvės kontekste, galima kalbėti apie elektroninių duomenų sunaikinimą, kuris reikštų, kad elektroninių duomenų sunaikinimas – šių duomenų likvidavimas, ištrynimas, t.y. tokie veiksmai, kuriais elektroninių duomenų naudojimas padaromas negalimu. P. Grabosky duomenų sunaikinimą ir sugadinimą sieja su elektroninių duomenų ištrynimu. Taip pat atkreipia dėmesį į tai, kad duomenys gali būti užšifruoti/užkoduoti, tokių būdų padarant juos neprieinamais tiems asmenims, kurie neturi matematinių formulių, kuriomis galėtų duomenis atkoduoti. Be kita ko, teigia, kad duomenys gali prarasti savo vertę ar naudingumą[34]. Taigi, elektroninių duomenų sunaikinimas turėtų būti siejamas su elektroninių duomenų likvidavimu, kadangi, kaip realiai egzistuojančio daikto sunaikinimas praranda savo paskirtį ar tampa neatpažįstamu, be kita ko, ir sunaikinti elektroniniai duomenys praranda savo paskirtį, o tai reiškia, kad negalima su šiais duomenimis atlikti tam tikrų veiksmų ar prieiti prie elektroninių duomenų. Tokie duomenys tampa nenuskaitomais, taip pat prie sunaikintų elektroninių duomenų tam tikru laiku prieiga nėra galima, kadangi tokių duomenų nėra informacinėje sistemoje arba tam tikrose laikmenose. Pavyzdžiui Kauno apygardos teismo 2012 m. spalio 22 d. nutartis baudžiamojoje byloje (bylos Nr. 1A-94-175/2012) nustatyta, kad *A.A. padarė neteisėta poveikį elektroniniams duomenims, būtent, 2010 m. rugpjūčio 10 d. apie 19 val. 46 min. <...> neteisėtai sunaikino elektroninius duomenis, patalpintus internetinėje svetainėje www.syrokomla.lt, o 2010-08-11 apie 22 val. 16 min. pakeitė juos kitais, padarydamas vidurinei mokyklai didelę žalą.* <...>. Nuteistasis apeliaciniame skunde ginčijo elektroninių duomenų sunaikinimą, teigdamas, kad jis juos ištrynė, tačiau teismas konstatavo, kad elektroninių duomenų ištrynimas neturėjo įtakos jo veiksmų kvalifikavimui pagal BK 196 straipsnio 1 dalį, kadangi neteisėti veiksmai gali pasireikšti sugadinimu, sunaikinimu, pakeitimu. Būtent šioje byloje teismas pritarė pirmos instancijos teismo veikos kvalifikavimui ir pritarė, kad elektroniniai duomenys buvo sunaikinti. Elektroninių duomenų sunaikinimas pasireiškė duomenų ištrynimu, kurie buvo internetinėje svetainėje. Šioje byloje teismas nedetalizavo elektroninių duomenų sunaikinimo

[33] Fedosiukas, O. Nusikaltimai ir baudžiamieji nusižengimai nuosavybei, turtinėms teisėms ir turtiniams interesams. *Lietuvos baudžiamoji teisė. Specialioji dalis.* Pirmoji knyga: vadovėlis. Vilnius : Justitia, 2013, p 416.
[34] Grabosky, P. *Electronic crime*. New Jersey: Upper Saddle River, 2007, p. 25.

veikos, tačiau pasisakė, kad elektroninių duomenų ištrynimas iš esmės sutampa su elektroninių duomenų sunaikinimu tiek vienu tiek kitu atveju elektroniniai duomenys yra pašalinami iš informacinės sistemos, laikmenos ir pan.

Elektroninių duomenų sugadinimas yra siejamas su tokių duomenų poveikiu, kurio metu elektroninių duomenų dalis buvo pašalinta, pakeista. Būtent toks poveikis elektroniniams duomenims yra siejamas su elektroninių duomenų vientisumu, informacijos turiniu[35]. Sugadinant elektroninius duomenis yra pakeičiama tam tikra dalis informacijos, dėl ko elektroniniai duomenys tampa iškraipyti ir jų neįmanoma atpažinti arba suprasti pačio turinio. Konvencijos dėl elektroninių nusikaltimų aiškinamajame rašte (61 punktas) sugadinimas yra siejamas su neigiamu poveikiu duomenų ar programos vientisumui. Tai reiškia, kad elektroniniai duomenys praranda savo pirminę formą, t.y. pakeičiama duomenų dalis, kuri tampa nenuskaitoma, iškreipta ar nebesuprantama. Taigi, elektroninių duomenų sugadinimas pasireiškia tam tikros elektroninių duomenų dalies pašalinimu, pakeitimu ištrynimu, kurių pasekoje tokie duomenys tampa iškraipyti, nepilni, nenuskaitomi, iškreipti ir pan., t.y. tokie elektroniniai duomenys praranda vieną iš CIA Triados elementų, elektroninių duomenų vientisumą.

Elektroninių duomenų pakeitimas yra siejamas su tokių duomenų turinio pakeitimu arba turinio dalies pakeitimu kitokia informacija arba gali apimti ir kenksmingų programų, virusų įvedimą[36]. Taip pat duomenys gali būti pakeisti juos papildant naujais duomenimis arba pakeičiant jų formą ar turinį[37]. Pavyzdžiui, Vilniaus miesto apylinkės teismo 2013 m. balandžio 4 d. teismo baudžiamuoju įsakymu baudžiamojoje byloje (bylos Nr. 1-1471-716/2013) J. V., be kitų nusikalstamų veikų, nuteistas ir pagal BK 196 straipsnio 1 dalį, t.y. *jis prisijungdamas prie Vilniaus Universiteto informacinės sistemos ir panaudodamas SQL tipo injekcijos komandas ir programą „John the Ripper“ neteisėtai įgijo neviešus elektroninius duomenis <...> neteisėtai prisijungė prie VU informacinės sistemos administravimo dalies ir joje neteisėtai padarė poveikį elektroniniams duomenims <...>, būtent informacinėje sistemoje sau ir kitiems studentams keitė dėstomų dalykų pažymius* <...>. Taigi šiame teismo priimtame baudžiamajame įsakyme yra aiškiai matomas elektroninių duomenų pakeitimas, t.y. J. V. aktyviais veiksmais, neteisėtai prisijungdamas prie VU informacinės sistemos, neteisėtai pakeitė elektroninius duomenis, o būtent neteisėtai pakeitė studijų knygelėje savo bei kitų studentų esančius pažymius. Atkreiptinas dėmesys ir į tai, kad gali kilti problemų inkriminuojant šį požymį, kadangi elektroninių duomenų pakeitimas yra ganėtinai panaši

[35] Civilka, M., *et al*., *supra* note 7, p. 517.
[36] *Ibid*.
[37] Kuzminovas, M., *spra* note 2, p. 464-465.

veika į elektroninių duomenų sugadinimo bei sunaikinimo veikas. Pavyzdžiui, pakeičiant elektroninių duomenų dalį tokie duomenys gali būti ir sugadinti, t.y. pakeičiant elektroninius duomenis, tam tikrais, atvejais tokie duomenys tampa iškraipyti ar neatpažįstami informacinėje sistemoje, kas rodytų tokių duomenų sugadinimą. Taip pat pakeičiant elektroninius duomenis (pvz. visą jų turinį) tokie duomenys gali būti sunaikinti. Pavyzdžiui, asmuo, prisijungęs prie informacinės sistemos ir joje susiradęs jam reikiamą dokumentą, jame esančius visus duomenis ištrina bei pakeičia kitais duomenimis, taigi, tokiu atveju visi duomenys esantys elektroniniame dokumente yra ne tik pakeičiami *inter alia* yra ir sunaikinti, t.y. nelieka originalaus elektroninio duomens. Todėl, esant tokioms aplinkybėms turi būti nustatyta, būtent kaip asmuo norėjo paveikti elektroninius duomenis bei ko buvo siekiama tokiu tikslu, t.y. ar asmuo norėjo pakeisti, sugadinti ar sunaikinti elektroninius duomenis. Taip pat yra galimybė skirti ekspertizę nustatant koks poveikis buvo atliktas elektroniniams duomenims[38].

Elektroninių duomenų pašalinimas yra siejamas su tokių duomenų perkėlimu į kitą vietą, tai gali būti elektroninių duomenų perkėlimas iš kompiuterio standžiojo disko į kitą išorinę laikmeną arba perkeliant tokius duomenis į kitą aplankalą[39]. Autoriaus nuomone, toks šios veikos teisinis reglamentavimas yra netikslus bei netinkamas, kadangi elektroninių duomenų pašalinimas yra siejamas su tokių duomenų perkėlimu iš vienos vietos į kitą. Pašalinimas, autoriaus nuomone, turi būti suprantamas kaip sinonimas sunaikinimui, šiuo atveju siejant elektroninių duomenų pašalinimą su tokių duomenų likvidavimu (*pašalinimas – padaryti, kad nebebūtų*[40]). Įdomu yra tai, kodėl būtent tokią pavojingos veikos formuluotę pasirinko įstatymų leidėjas, kadangi tokia veika kaip elektroninių duomenų pašalinimas turėtų būti siejamas su elektroninių duomenų sunaikinimu, likvidavimu, o ne elektroninių duomenų perkėlimu. Analizuojant Konvenciją dėl elektroninių nusikaltimų bei Tarybos pagrindų sprendimą dėl atakų prieš informacines sistemas, šiuose tarptautiniuose teisės aktuose nėra numatyta tokia veika kaip elektroninių duomenų pašalinimas. Taip pat analizuojant Europos Parlamento ir Tarybos direktyvą 2013/40/ES[41] (*originalia anglų kalba*) ši pavojinga veika gali būti interpretuojama kaip tam tikrų apribojimų ar trikdžių sukūrimu asmenims, kurie turi teisėta prieigą prie elektroninių duomenų, o būtent blokavimu, apribojimu ar trikdžių sukėlimu naudotis elektroniniais duomenimis. Pavyzdžiui, perkeliant, paslepiant elektroninius duomenis arba slaptažodžio sukūrimas, taip sudarant kliūtis, prieigai prie elektroninių duomenų. Taigi, autoriaus

[38] Mockevičius, R., Valatkevičius, D. 196-198[2] straipsniai. *Lietuvos Respublikos baudžiamojo kodekso komentaras.* Specialioji dalis (99-212 straipsniai). Vilnius: Registrų centras, 2009, p. 421.
[39] Kuzminovas, M., *supra* note, p. 465.
[40] Keinys, S., *supra* note 14, p. 518.
[41] Europos Parlamento ir Tarybos direktyva 2013/40/ES 2013 m. rugpjūčio 12 d. dėl atakų prieš informacines sistemas, kurią pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR.

nuomone, toks veikos teisinis reglamentavimas, koks jis yra numatytas BK 196 straipsnio 1 dalies dispozicijoje, yra netinkamas ir tokios pavojingos veikos teisinio reglamentavimo derėtų atsisakyti. Pažymėtina, kad toks šios veikos aiškinimas turi būti siejamas su apribojimu naudotis tokiais elektroniniais duomenimis, kuri yra numatyta BK 196 straipsnio dispozicijoje.

Į neteisėto poveikio elektroniniams duomenims sudėtį kaip alternatyvą įtraukus kitokį elektroninių duomenų apribojimo požymį, šiai pavojingai veikai buvo suteikta plati apibrėžtis. Tokia pasirinkta formuluotė leidžia teigti, kad nustatant šį sudėties požymį nebuvo apsiribota esamomis technologijomis ir buvo atkreiptas dėmesys į tokių technologijų tobulėjimą bei galimybę kitokiais būdais apriboti naudojimąsi. Taip pat galim teigti, kad įstatymų leidėjas įtvirtino nebaigtinį pavojingų veikų sąrašą, kuriais gali būti daromas neteisėtas poveikis elektroniniams duomenims. Bendriausia prasme naudojimosi elektroniniais duomenimis apribojimas reiškia, kad teisėtą prieigą turintys asmenys negali naudotis jiems priklausančiais elektroniniais duomenimis[42]. Iš esmės, ši pavojinga veika gali apimti aukščiau išvardintas ir aptartas pavojingas veikas, tačiau svarbu paminėti yra tai, kad ši veika apima kitokius būdus, kurių neapima elektroninių duomenų sunaikinimas, sugadinimas, pakeitimas. Tokia veika gali pasireikšti ankščiau minėtu slaptažodžio nustatymu arba pasitelkiant kitas programines įrangas, kuriomis sutrikdoma prieiga prie elektroninių duomenų arba naudojama techninė įranga, kurios pagalba gali būti trikdomas telekomunikacijų, radijo bangų ryšys, keičiant maitinimo tinklo įtampą ir kitokiais būdais. Apriboti naudojimąsi elektroniniais duomenimis galima panaudojant tiek tam specialiai sukurtą kenkėjišką programinę įrangą bei teisėtiems tikslams sukurtą programinę įrangą[43]. Apribojimas elektroniniais duomenimis gali būti atliekamas panaudojant Denial of Service (DoS) arba Distributed Denial of Service (DDoS) atakas. Šio tipo atakos yra naudojamos apribojant naudojimąsi internetiniais puslapiais, tačiau šiomis atakomis gali būti apribojimas ir naudojimasis duomenimis. Taigi, šio tipo atakos veikia tokiu principu, kad yra siunčiamos prisijungimo užklausos arba duomenų srautai, kuriais yra užkemšama linija ir prieigą turintis asmuo nebegali naudotis internetiniame puslapyje esančiais duomenimis bei tokiu atveju gali būti sutrikdoma ir informacinės sistemos veikla, todėl veika gali būti kvalifikuojama iš sutapties pagal BK 197 straipsnį. Dar vienas tinkamas pavyzdys galėtų būti ne per seniausiai paplitęs virusas „*CTB-Locker*“, kuris patekęs į kompiuterį ar informacinę sistemą iškart užkoduoja tam tikrus arba visus duomenis esančius kompiuteryje (pvz. Word dokumentus, „folderius“ ir pan), taip apribojant prieigą prie jų[44].

[42] Kuzminovas, M., *spra* note 2, p. 465.
[43] *Ibid*.
[44] Norint, kad prieiga prie elektroninių duomenų būtų grąžinta yra reikalaujama, kad asmuo už tokių duomenų atkodavimą sumokėtų pinigus.

„Wiper“ virusas, kuris buvo išplitęs 2012 metais, patekdavęs į kompiuterį sunaikindavo visus duomenis esančius kompiuteryje. Taip pat gali būti naudojami virusai bendrai vadinami „Laiko bombomis“, kurios užkoduojamos taip, kad atlikus tam tikrą veiksmą kompiuteryje, esantys duomenys gali būti ištrinami, sunaikinami ar dar kitaip pakeičiami (*pvz. Groovemonitor, Maya ir pan*). Įvairiausio tipo „kirminai“ patekę į informacinę sistemą, kompiuterį juose esančius duomenis iškraipydavo ir tokiu būdu elektroniniai duomenys buvo iškraipomi, neatpažįstami. Autoriaus nuomone, kad pasirinkus tokią pavojingų veikų formuluotę, elektroninių duomenų sunaikinimas, sugadinimas, pakeitimas, pašalinimas neapima kai kurių virusų panaudojimo atvejų paveikiant šiuos elektroninius duomenis, todėl kitoks naudojimosi elektroniniais duomenimis apribojimas yra sietinas su kompiuterinių virusų panaudojimu paveikiant duomenis. Taigi panaudojant įvairiausių tipų virusus, kuriais elektroniniai duomenys yra ištrinami, pakeičiami ar sugadinami, gali būti inkriminuojama pavojinga veika kaip kitoks elektroninių duomenų naudojimosi apribojimas.

Pažymėtina, kad nors ir esant galimybei atkurti pašalintus, sunaikintus, sugadintus elektroninius duomenis arba yra tokių duomenų kopija, nepašalina baudžiamosios atsakomybės[45]. Teismų praktikoje yra pritariama tokiai pozicijai, konstatuojant „<...> *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 duomenimis nepašalina baudžiamosios atsakomybės. Jos nepašalina ir tas faktas, kad nukentėjusysis turi tokių duomenų kopiją*.“[46].Taigi, ir teismai laikosi tokios pozicijos, kad esant galimybei atkurti elektroninius duomenis nepašalina baudžiamosios atsakomybės. Tokiais atvejais, jei nėra sukelta didelė ar nedidelė žala, yra galimybė atleisti asmenį nuo baudžiamosios atsakomybės dėl mažareikšmiškumo[47].

Pagal komentuojamą straipsnį turi būti kvalifikuotos ir tokios veikos, kuriomis yra fiziškai kenkiama techninei įrangai, informacinei sistemai ar jos komponentams ir pan., kuria siekiama paveikti informacinėje sistemoje esančius elektroninius duomenis[48]. Pavyzdžiui, visiškas elektroninių duomenų sunaikinimas galimas tik sunaikinant kietąjį diską, pavyzdžiui, pasitelkiant plaktuką, kirvį ar kitokį naikinimui priskirtą fizinį objektą, bet kokiu kitu atveju bent iš dalies galima atkurti

[45] Mockevičius, R., Valatkevičius, D., *supra* note 38, p. 421.
[46] Kauno apygardos teismo 2012 m. spalio 22 d. nutartis baudžiamojoje byloje (bylos Nr. 1A-94-175/2012)
[47] Kuzminovas, M., *spra* note 2, p. 465.
[48] *Ibid.*

elektroninius duomenis, esančius kietajame diske. Pažymėtina, kad sunaikinant, sugadinant techninę įranga veika kvalifikuotina ir pagal turto sunaikinimo ar sugadinimo sudėtį.

Apibendrinant, neteisėtas poveikis elektroniniams duomenims galimas sunaikinant, sugadinant, pakeičiant ar kitais būdais apribojant naudojimąsi tokiais duomenimis, *inter alia* numato ir elektroninių duomenų pašalinimą, tačiau, autoriaus nuomone, tokia numatyta pavojinga veika BK 196 straipsnio 1 dalies dispozicijoje yra netiksli ir neatitinkanti tarptautinių teisės aktų, kurių pagrindu šį nusikalstama veika buvo kriminalizuota. Pažymėtina, kad tokiais aktyviais veiksmais atimama galimybė teisėtiems vartotojams naudoti, prieiti ar valdyti jiems priklausančius elektroninius duomenis pagal paskirtį, tikslą ir pan.. Neteisėtumas turi būti vertinamas ir tais atvejais, kai teisėtą prieigą turintis asmuo atlieka pakeitimus informacinėje sistemoje, tačiau peržengdamas jam suteiktus įgaliojimus ar pažeisdamas teisės aktus. Esanti galimybė atkurti elektroninius duomenis nereiškia, kad kaltininko veiksmuose nėra visų šios nusikalstamos veikos subjektyviųjų bei objektyviųjų požymių, tad, atitikus BK 37 straipsnyje numatytas sąlygas, asmuo gali būti atleistas nuo baudžiamosios atsakomybės dėl mažareikšmiškumo.

1.1.4 Neteisėto poveikio elektroniniams duomenims baigtumo momentas ir padariniai.

Komentuojamame BK 196 straipsnyje įtvirtintas būtinasis veikos požymis yra padariniai. Tokia kilusi žala turi būti didelė arba nedidelė. Nusikalstamos veikos baigtumo momentas yra nustatomas remiantis nusikalstamos veikos sudėties aprašymu baudžiamajame įstatyme ir priklauso nuo nusikalstamų ketinimų faktinio įgyvendinimo. Taigi BK 196 straipsnyje numatyto nusikaltimo sudėtis yra materialioji, todėl ši nusikalstama veika laikoma baigta, kai atsiranda įstatyme numatyti padariniai, šiuo atveju didelė arba nedidelė žala. Kiekvienu atveju inkriminuojant BK 196 straipsnyje numatytą veiką turi kilti žala, nesukėlus žalos patraukimas asmens baudžiamojon atsakomybėn nėra galimas. Taip pat atkreiptinas dėmesys į tai, kad jei asmuo siekia neteisėtai paveikti elektroninius duomenis bei siekia sukelti žalą, tačiau žala neatsiranda dėl nuo kaltininko valios nepriklausančių aplinkybių, veika kvalifikuojama kaip pasikėsinimas. Arba tokiais atvejais, kai asmuo siekė sukelti didelę žalą, tačiau padarė nedidelės žalos veika irgi kvalifikuotina kaip pasikėsinimas padaryti padaryti didelę žalą ir atvirkščiai. Tinkamiausias pavyzdys atspindintis pasikėsinimą galėtų būti toks, kai kaltininkas prie dokumento įvedą virusą (ar kitokią kenkėjišką programą, kuri paveikia elektroninius duomenis) ar tokį virusą įdiegia informacinėje sistemoje, tačiau informacinėje sistemoje esanti antivirusinė programa šį virusą aptinka jam dar nepradėjus veikti ir jį ištrina. Taigi tokiu atveju nusikalstama veika nėra baigta ir išvengta galimai kilsiančios žalos. Tokiais atvejais neišvengiamai

būtų susidurta su problema nustatinėjant kokia žala galėjo kilti, tačiau tokiais atvejais turi būti analizuojamas viruso tipas, veikimo principas, kokia apimtimi būtų paveikęs duomenis ir t.t.

Teisės moksliniuose darbuose yra aptinkama tokia nuomonė, kad padaroma žala gali būti įvairaus pobūdžio, o būtent tokia žala gali būti turtinė, socialinė, moralinė, kritęs prestižas, klientų nepasitenkinimas ir pan. Tokioms pozicijoms pritartina, kadangi, priklausomai nuo elektroninių duomenų pobūdžio, tokie duomenys gali turėti ne tik ekonominę, materialinę vertę, bet ir moralinę, socialinę ir kitokio pobūdžio vertę. Taigi, numatytą BK 196 straipsnyje įvardintą didelę žalą galima suskirstyti į turtinę ir neturtinę. Pažymėtina, kad žalos dydis yra vertinamasis požymis, kurį lemia baudžiamosios teisės principai bei konkrečios veikos aplinkybės[49]. Tokiomis aplinkybėmis gali būti elektroninių duomenų kiekis, jų pobūdis, kam tokie elektroniniai duomenys priklauso, ar tokių duomenų statusas ir pan.

Konvencijoje dėl elektroninių nusikaltimų valstybėms buvo palikta teisė pasirinkti, jog nustatant baudžiamosios atsakomybės pagrindus už BK 196 straipsnyje numatytą veiką gali būti reikalaujama didelės žalos. Konvencijoje taip pat numatyta, kad didelės žalos kriterijų nustatymas paliktas valstybės įstatymų leidėjo diskrecijai.

Nors yra matoma, kad įstatymų leidėjas, kriminalizuojant šią veiką, pasirinko didelės žalos kilimą kaip būtinąjį veikos požymį, tačiau nepateikė jokių kriterijų kokia kilusi žala turėtų būti laikoma didelę, dėl to teismams gali kilti sunkumų vertinant šį būtinąjį požymį. Pavyzdžiui, anksčiau minėtoje baudžiamojoje byloje[50], J. V. nuteistas pagal BK 196 straipsnio 1 dalį, už tai, kad neteisėtai, sau ir kitiems studentams, pakeitė elektroninius duomenis. Šioje byloje nebuvo pareikštas civilinis ieškinys, t.y. nebuvo reikalaujama atlyginti patirtos turtinės ir neturtinės žalos. Teismas šioje byloje vertino tik kilusią neturtinę žalą. Taigi, teismas ne turtinio pobūdžio žalą vertino atsižvelgdamas į VU vardo ir garbės sumenkinimą, žalos padarymu studijų kokybei, sąžiningai studijuojančių studentų konkurencijai ir šias aplinkybes bei kilusius padarinius pripažino kaip didelę žalą. Taip pat paminėtina ir Vilniaus miesto 2 apylinkės teismo 2009 m. gegužės 7 d. teismo baudžiamasis įsakymas baudžiamojoje byloje (bylos Nr. 1-515-478/2009) V. Č. be kitų nusikalstamų veikų nuteistas už BK 196 straipsnyje 3 dalyje numatytą nusikalstamą veiką, *t.y. jis neteisėtai perėmė, pasisavino ir laikė neviešus elektroninius duomenis <...> neteisėtai pakeitė elektroninius duomenis, padarydamas nedidelės žalos <...> neteisėtai prisijungė VšĮ (duomenys neskelbtini) kolegijos elektroninio dienyno adresu (duomenys neskelbtini) ir jame neteisėtai padarė poveikį elektroniniams duomenims, o būtent*

[49] Kuzminovas, M., *supra* note 2, p. 467.
[50] Vilniaus miesto apylinkės teismo 2013 m. balandžio 4 d. teismo baudžiamuoju įsakymu baudžiamojoje byloje (bylos Nr. 1-1471-716/2013)

elektroniniuose dienynuose pakeitė savo bei brolio pažymius <...>. Šioje byloje, antai prieš tai minėtoje, buvo pareikštas civilinis ieškinys 5000 Lt sumai, taip pat buvo vertinama ir kilusi neturtinė žala, o būtent 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. Tiek šioje byloje, tiek prieš tai minėtoje buvo vertinama kilusi neturtinė žala, tačiau žalos dydžio nustatymas buvo skirtingas. Įdomu yra tai, kodėl vis gi teismai skirtingai vertino kilusius padarinius, pirmuoju atveju padarinius pripažįstant kaip didelę žalą, o antruoju atveju kaip nedidelę. Abejose situacijose kilusi žala yra identiška, t.y. kritęs mokymosi įstaigos prestižas, vardas, buvo sukelta žala studijų kokybei bei sąžiningumui. Teismai vertindami padarinius tik įvardino, kokie padariniai kilo ir nepateikė, kokiais kriterijais vadovavosi vertinant žalą, tik pasisakant, kad nuteistųjų veiksmais buvo padaryta žala mokymosi įstaigų prestižui, vardui bei studijų kokybei, sąžiningumui. Analizuojant šias, panašias, bylas yra matoma, kad kilę padariniai yra beveik identiški, tačiau kilusios žalos dydis įvertintinas skirtingai, vienu atveju pripažinta kaip didelė žala - kitu nedidelė. Vertinant kilusios žalos dydį šių bylų kontekste, autoriaus nuomone, buvo atsižvelgta į poveikio elektroniniams duomenis kiekį, o būtent nustatant pakeistų duomenų kiekį bei žalos dydžio nustatymui galimai turėjo įtakos vertinant nusikalstamos veikos tęstinumą. Taigi pirmuoju atveju poveikis elektroniniams duomenims nebuvo vertinamas kaip viena tęstinė nusikalstama veika, t.y. nuteistojo atliktos nusikalstamos veikos nesiejo vieninga tyčia. Kiekvienu atveju, pakeisdamas elektroniniame dienyne esančius duomenis, kaltinamojo tyčia susiformuodavo iš naujo, t.y. kaltininko atliktos nusikalstamos veikos buvo vertinamos kaip atskiri epizodai. Teismas nustatė, kad nuteistasis elektroniniame dienyne esančius duomenis pakeitė 10 kartų. Antrojoje situacijoje buvo nustatyta, kad visus nuteistojo veiksmus siejo vieninga tyčia, t.y. neteisėtas poveikis elektroniniams duomenims pasireiškė vieninga tyčia bei nuteistojo atlikti neteisėti veiksmai buvo pripažinti kaip viena tęstinė nusikalstama veika. Antruoju atveju byloje teismas nustatė, kad neteisėtai elektroniniai duomenis buvo pakeisti 5 kartus. Taigi, analizuojant šias dvi panašias bylas darytina išvada, kad vertinant kilusios žalos mastą teismai atsižvelgė į elektroninių duomenų kiekį. Šis kriterijus gali būti taikomas ir vertinant žalos dydį kitais atvejais, tačiau kiekvienu konkrečiu atveju turi būti atsižvelgiama ir į kitas byloje esančias aplinkybes, kurios leistų lengviau įvertinti kilusios žalos mastą.

Paminėtina ir Kauno apygardos teismo 2012 m. spalio 22 d. nutartis baudžiamojoje byloje (bylos Nr. 1A-94-175/2012), kurioje nustatyta, kad *A. A. nuteistas pagal BK 196 straipsnio 1 dalį už tai, kad panaudodamas programinę įrangą, neteisėtai sunaikino elektroninius duomenis, paskelbtus*

interneto svetainėje (duomenys neskelbtini), o 2010 m. rugpjūčio 11 d., apie 22.16 val., pakeitė juos kitais, taip padarydamas Vilniaus Vladislavo Sirokolmės vidurinei mokyklai didelę žalą <...>. Taigi šioje byloje nuteistasis skundė nusikalstamos veikos kvalifikacija bei civilinį ieškinį. Teismas konstatavo, kad nusikalstama veika kvalifikuota teisingai. Priimtoje nutartyje pažymėjo, kad žala gali būti turtinė bei neturtinė, socialinė, moralinė ir pan., taip pat, kad sprendžiant žalos dydį, ne visais atvejais privaloma remtis tik padarytos žalos pinigine išraiška. Nors teismas sumažino priteistiną išmoką iki 3000 Lt, tačiau pažymėjo, kad civilinis ieškovas patyrė didelę žalą. Didelę žalą vertino atsižvelgdamas į tai, kad nusikalstama veika buvo padaryta prieš pat mokslo metų pradžią, kas sukėlė tam tikrų nepatogumų mokinių tėvams, darbuotojams, be to vertino ir tai, kad nukentėjusysis yra švietimo ir ugdymo įstaiga, t.y. jos statusą.

Taip pat paminėtina nutartis baudžiamojoje byloje, kurioje V. S. nuteistas pagal BK 196 straipsnio 3 dalį, šioje byloje nustatyta, kad *V. S. Sunaikino ir pakeitė elektroninius duomenis tuo padarydamas nedidelę žalą, o būtent prisijungęs prie internetinio puslapio (duomenys neskelbtini) administratoriaus teisėmis ir sunaikino ištrindamas iš šios sistemos standžiojo disko atminties įmonės klientų prisijungimo kodus, taip pat pakeitė informacinėje sistemoje buvusius duomenis apie siūlomas nuolaidas ir patalpino melagingą informaciją, tuo padarydamas UAB „O“ nedidelę 11808,92 Lt žalą. <...>*[51]. Taigi šioje byloje pirmos instancijos teismas vertino tik kilusią turtinę žalą, nustatant, kad buvo padaryta nedidelė žala. Tokiai, teismo pozicijai pritartina, žalos dydžio nustatymas atitinka baudžiamosios teisės principus, kuriais yra nustatinėjamas žalos dydis. Taip pat atkreiptinas dėmesys, kad teismas nevertino įmonės reputacijos sumenkinimo, kritusio klientų pasitikėjimo ir panašių aplinkybių. Įdomu ar tokiu atveju būtų pasikeitęs žalos įvertis ir ar kilę padariniai būtų pripažinti kaip didelė žala. Nors ir ši byla buvo nagrinėjama antrosios instancijos teisme, tačiau nebuvo keliamas klausimas dėl žalos dydžio, tik dėl veikos padarymo, ir paliko galioti pirmosios instancijos teismo nuosprendį.

Taigi, nusikalstama veika, šio komentuojamo straipsnio prasme, yra laikoma baigta kai kyla padariniai, šiuo atveju kai kyla didelė arba nedidelė žala. Tarp kilusių padarinių ir pavojingos veikos turi būti priežastinis ryšys. Žala turi kilti nusikalstamą veiką padariusio asmens, o ne kitų asmenų veiksmais ar informacinės sistemos techninės bei programinės įrangos trūkumai ir klaidos[52]. Autoriaus nuomone, turi būti nustatinėjama ar poveikį elektroniniams duomenims atlikęs asmuo tuo metu turėjo realią galimybę tokią veiką atlikti, kadangi prie asmeninio kompiuterio gali turėti prieigą

[51] Vilniaus apygardos teismo 2014 m. balandžio 16 d. nutartis baudžiamojoje byloje (bylos Nr. 1A-303-256/2014).
[52] Kuzminovas, M., *supra* note 2, p. 467.

ne vienas asmuo, dėl ko galimi atvejai, kad nekaltas asmuo bus pripažintas kaltu. Taip pat pažymėtina, kad veika gali būti kvalifikuota kaip pasikėsinimas, tokiu atveju kai asmuo siekia paveikti elektroninius duomenis ir žino, kad dėl to gali kilti žala, tačiau ne nuo jo priklausančių aplinkybių tokia žala nekyla.

Apibendrinant galima teigti, kad veikos baigtumo momentas siejamas su padarinių kilimu. Tokie padariniai priklausomai nuo aplinkybių gali būti vertinami kaip didelė ir nedidelė žala. Žalos dydis yra vertinamasis požymis, kiekvienu konkrečiu atveju, kokia žala padaryta - didelė ar nedidelė, sprendžia teismas. Aptinkami tam tikri teismų beformuojami žalos nustatymo kriterijai, atsižvelgiama į padarytos turtinė žalos dydį, elektroninių duomenų pobūdį, kiekį, jų statusą. Be šių jau teismų formuluojamų kriterijų galima išskirti ir kokia žala atsirado, kai nebuvo galimybės naudotis tokiais duomenimis, kiek kainavo tokių duomenų atkūrimas, kokios apsaugos priemonėmis buvo imtasi apsaugoti tokius duomenis, kokios Konstituciją, įstatymų ar kitų teisės aktų saugomos vertybės buvo pažeistos.

1.1.5 Elektroniniai duomenys, esantys strateginę reikšmę nacionaliniam saugumui ar didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinčiuose informacinėse sistemose kaip kvalifikuojantis sudėties požymis.

Komentuojamo BK 196 straipsnio 2 dalyje yra numatytas kvalifikuotas nusikalstamos veikos sudėties požymis – elektroniniai duomenys, esantys strateginę reikšmę nacionaliniam saugumui ar didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinčiuose informacinėse sistemose. Būtent ši kvalifikuota nusikalstama veika yra siejama su poveikiu elektroniniams duomenims, kurie yra strateginės reikšmės nacionaliniam saugumui ar didelės reikšmės valstybės valdymui, ūkiui ar finansų sistemoje.

Objektus, kurie priskiriami turintys strateginę reikšmę nacionaliniam saugumui, galima aptikti Lietuvos Respublikos strateginę reikšmę nacionaliniam saugumui turinčių įmonių ir įrenginių bei kitų nacionaliniam saugumui užtikrinti svarbių įmonių įstatyme[53]. Paminėtina, kad šis įstatymas yra nuolat keičiamas bei pildomas. Šiame įstatyme yra pateikta sąvokos „*Strateginę ar svarbią reikšmę nacionaliniam saugumui turinčios įmonės ir įrenginiai*“ išaiškinimas. Anot šio įstatymo tokiais objektais laikomi Lietuvos Respublikoje esančios ar įsteigtos įmonės, kurioms pagal jų paskirtį ir veiklos pobūdį, aukščiau minėtas įstatymas, priskiria strateginę arba svarbią reikšmę nacionaliniam

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

saugumui. Šiame įstatyme yra išvardintos įmonės, kurios priskiriamos tokiems objektams, pavyzdžiui, akcinė bendrovė Lietuvos paštas; valstybinė įmonė Ignalinos atominė elektrinė; Klaipėdos valstybinio jūrų uosto direkcija ir kt. Taigi, kokie objektai turi strateginę reikšmę nacionaliniam saugumui ar didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai, galima aptikti įstatymuose. Taip pat valstybinės reikšmės objektais gali būti pripažįstami ir kiti objektai, neatsižvelgiant į jo nuosavybės formą, kurios kontrolės ar funkcionavimo sutrikimas arba sutrikdymas keltų pavojų ar padarytų didelę žalą nacionaliniam saugumui[54]. Pavyzdžiui, sutrikdytų valstybės valdymą, ūkio sistemos, valstybei svarbios ūkio šakos ar infrastruktūros funkcionavimą. Tokiais objektais galėtų būti ir ne tik anksčiau minėtame įstatyme išvardintos įmonės. Tai gali būti ir Valstybinė mokesčių inspekcijos informacinėje sistemoje esantys duomenys, valstybės registrų centrų informacinėse sistemose esantys duomenys, bankų informacinėse sistemose esantys duomenys ir pan. Tokiu atveju turėtų būti atsižvelgiama į paveikta duomenų kiekį, jų turinį, padarytą žalą ir pan. Taip pat atkreiptinas dėmesys ir į ne per seniausiai priimtą Kibernetinio saugumo įstatymą[55]. Šio įstatymo 2 straipsnio 2 punkte yra pateiktas sąvokos ypatingos svarbos informacinės infrastruktūros apibrėžimas, kuris yra aiškinamas taip „*Ypatingos svarbos informacinė infrastruktūra – elektroninių ryšių tinklas ar jo dalis, informacinė sistema ar jos dalis, informacinių sistemų grupė ar pramoninių procesų valdymo sistema ar jos dalis, nepaisant to, ar jos valdytojas yra privatus ar viešojo administravimo subjektas, kuriuose įvykęs kibernetinis incidentas gali padaryti didelę žalą nacionaliniam saugumui, šalies ūkiui, valstybės ir visuomenės interesams*[56]“. Taigi ypatingą informacinę infrastruktūrą sudaro elektroninių ryšių tinklas, informacinė sistema, informacinių sistemų grupės ar pramoninių procesų valdymo sistemos bei šių tinklų ar sistemų dalys. Šių sistemų ypatingą reikšmę rodo galimus, didelės žalos nacionaliniam saugumui, šalies ūkiui, valstybinės ar visuomenės interesams, kriterijus. Tačiau atkreiptinas dėmesys į tai, kad šis įstatymas sieja ypatingos svarbos objektus su informacinėmis sistemomis, t.y. apibūdinamos ypatingos svarbos informacinės sistemos. Atkreiptinas dėmesys į tai, kad pripažįstant informacinę sistemą turinčią ypatingą svarbą, šiose sistemose tvarkomi elektroniniai duomenys ne visais atvejai gali būti pripažintais turinčiais ypatingą svarbą. Prezumpcija, kad tokiose informacinėse sistemose tvarkomi elektroniniai duomenys turi padidintą reikšmę negali būti taikytina[57], kadangi šiose informacinėse sistemose tvarkomi

[54] Lietuvos Respublikos vyriausybės 2010 m. birželio 7 d. Nr. 717 nutarimas „Dėl objektų pripažinimo valstybinės reikšmės objektais tvarkos aprašo patvirtinimas“. *Valstybės žinios*. 2010, Nr. 69-3442.
[55] Lietuvos Respublikos kibernetinio saugumo įstatymas. *TAR*. 2014, Nr. 2014-20553.
[56] *Ibid.*
[57] Marcinauskaitė, R., supra note 5, p. 151.

elektroniniai duomenys yra įvairiausio pobūdžio. Šiose informacinėse sistemose yra skirta organizacijos tikslams siekti, joms paskirtoms funkcijoms, užduotims atlikti. Taigi, sprendžiant ar elektroniniai duomenys, esantys ypatingos svarbos informacinėse sistemose, gali turėti padidintą reikšmę turi būti sprendžiama neatsižvelgiant į šių duomenų buvimą ypatingos svarbos informacinėse sistemose.

Taigi neužtenka vien tik poveikio elektroniniams duomenims esantiems anksčiau išvardintose informacinėse sistemose. Kiekvienu konkrečiu atveju turi būti sprendžiama ar informacinėje sistemoje esantys duomenys, kurie buvo sunaikinti, sugadinti, pakeisti ar apribotas naudojimasis, jais turi strateginę reikšmę nacionaliniam saugumui ar didelę reikšmę valstybės valdymui ūkiui ar finansų sistemai. Pavyzdžiui, sunaikinti ar pakeisti elektroniniai duomenys informacinėje sistemoje buvo asmeninio pobūdžio ar niekaip nesusiję su valstybės ūkio sistema ir pan., tokiais atvejais nusikalstama veika turi būti kvalifikuota pagal BK 196 straipsnio 1 dalį arba 3 dalį, jeigu kilo padariniai. Ar elektroniniai duomenys esantys informacinėje sistemoje turi strateginę reikšmę nacionaliniam saugumui ar didelę reikšmę valstybės, valdymui, ūkiui ar finansų sistemai kiekvienu konkrečiu atveju sprendžia prokuroras arba teismas, tačiau manytina, kad tokiais atvejai turi būti atsižvelgiama į tai, kokia grėsmė būtų sukelta paveikiant tokius duomenis, kaip būtų paveikta visuomenė, pačių duomenų turinį, kiekį, kokia grėsmė kilo ar galėjo kilti.

Kadangi nusikalstamos veikos BK 196 straipsnio 2 dalies sudėtyje yra nustatytas kvalifikuojantis požymis, kurį kaltininkas privalo suvokti, t.y. kaltininkas pagal visas aplinkybes turi suvokti, kad sunaikina, sugadina, pakeičia, pašalina ar kitais būdais apriboja naudojimąsi elektroniniais duomenimis, turinčiais strateginę reikšmę nacionaliniam saugumui ar didelę reiškę valstybės valdymui, ūkiui ar finansų sistemai. Taip pat kaltinamasis turi siekti sunaikinti, sugadinti, pakeisti arba apriboti naudojimąsi tokiais duomenimis. Gali kilti problemų nustatant kaltininko suvokimą, kad elektroniniai duomenys turi strateginę reikšmę nacionaliniam saugumui ar didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai, kadangi nėra nustatytų kriterijų kokiais turi būti vadovaujamasi ar elektroniniai duomenys esantys informacinėse sistemose turi strateginę reikšmę nacionaliniam saugumui ar didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai, kadangi yra palikta diskrecijos prokurorui arba teismui, laisvė tokiais duomenimis pripažinti ir, kurie nėra įtraukti į Lietuvos Respublikos strateginę reikšmę nacionaliniam saugumui turinčių įmonių ir įrenginių bei kitų nacionaliniam saugumui užtikrinti svarbių įmonių įstatymą. Taigi kiekvienu konkrečiu atveju turi būti sprendžiama ne tik ar tokie duomenys yra ypatingos reikšmės, bet ir ar kaltinamasis galėjo suvokti šių duomenų pobūdį bei atsižvelgti į tokių duomenų svarbą ir ko tokiu poveikiu kaltinamasis siekė.

Apibendrinant galima teigti, kad kaltininko veiksmus kvalifikuojant pagal BK 196 straipsnio 2 dalį turi būti atsižvelgiama į tokių elektroninių duomenų turinį, esančiose strateginę reikšmę nacionaliniam saugumui ar didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinčiose informacinėse sistemose. Pažymėtina, kad ne bet kokie duomenys gali būti pripažinti turintys strateginę ar didelę reikšmę, kiekvienu konkrečiu atveju turi būti sprendžiama ar tokie elektroniniai duomenys turi strateginę reikšmę nacionaliniam saugumui ar didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai. Toks vertinimas paliktas prokuroro bei teismo diskrecijai. Įstatymais yra nustatyta, kokie objektai gali būti priskiriami turintys ypatingos reikšmės, tačiau esant neužbaigtam sąrašui bei paliekant galimybę prie tokių objektų priskirti ir kitus objektus yra palikta laisvė šį sąrašą pildyti, tai gali sukelti šių duomenų suvokimo problemas kaltinamajam, todėl kiekvienu konkrečiu atveju turi būti sprendžiama ar kaltinamasis suvokė, kad tokie elektroniniai duomenys, esantys informacinėje sistemoje, turi strateginę reikšmę nacionaliniam saugumui ar didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai, t.y. tokių duomenų turinį, bei nustatyti ko siekė. Nustačius, kad asmuo nesuvokė tokių elektroninių duomenų reikšmės arba nekilus didelei žalai baudžiamoji atsakomybė pagal BK 196 straipsnio 2 dalį yra negalima.

1.2 Subjektyvieji neteisėto poveikio elektroniniams duomenims sudėties požymiai.

Šios nusikalstamos veikos subjektyviuosius požymius sudaro asmens pakaltinamumas ir tyčia. Taigi asmuo suvokia, kad neturėdamas teisėtos prieigos prie elektroninių duomenų tokius duomenis sunaikina, sugadina, pakeičia arba apriboja naudojimąsi jais bei tokiais veiksmais jis gali padaryti žalą arba nors ir padaryti tokios žalos nenori, tačiau sąmoningai leidžia jai atsirasti[58]. Taigi, ši veika gali būti padaryta tiek tiesiogine, tiek ir netiesiogine tyčia. Būtent tokios kaltės formos apribojimai numatyti Konvencijoje dėl elektroninių nusikaltimų bei Europos Tarybos pamatiniame sprendime dėl atakų prieš informacines sistemas, kuriose nurodoma, kad valstybės privalo kriminalizuoti sąmoningą, tyčinį neteisėtą poveikį elektroniniams duomenims. Tai išsprendė galimai kilsiančias problemas dėl plataus šio straipsnio taikymo, o būtent susiaurinus šios veikos kaltės formą iki tyčinės kaltės, tai padėjo išvengti nepagrįstos baudžiamosios atsakomybės taikymo dėl veiksmų, kuriais asmuo dėl neatsargumo, neatidumo ar išsiblaškymo sunaikino, sugadino, pašalino, pakeitė ar apribojo naudojimąsi elektroniniais duomenimis.

[58] Kuzminovas, M., *supra* note 2, p. 460.

2. NETEISĖTAS ELEKTRONINIŲ DUOMENŲ PERĖMIMAS IR PANAUDOJIMAS (BK 198 str.)

2.1 Objektyvieji neteisėto elektroninių duomenų perėmimo ir panaudojimo sudėties požymiai.

2.1.1 Elektroninių duomenų konfidencialumas kaip saugoma vertybė.

Elektroninių duomenų konfidencialumas yra vienas, iš anksčiau aptartos, CIA Triados elementas. Šis elementas bendriausia prasme yra siejamas su elektroninių duomenų slaptumu, tokių duomenų neatskleidimu kitiems asmenims ar sistemoms, kurie neturi įgaliojimų arba teisėtos prieigos su tokiais duomenimis susipažinti. Tokios pat pozicijos laikosi ir teismai, pavyzdžiui Vilniaus apygardos teismo nutartyje konstatuojama, kad „*Akcentuotina, kad šio nusikaltimo objektas – neviešų elektroninių duomenų saugumo turinio vienas aspektas – jų konfidencialumas. Duomenų konfidencialumas yra duomenų savybė, reiškianti tai, kad jie nebus prieinami ar pateikiami asmenims, kuriems nesuteikiama tokia teisė*“[59].

Kaip anksčiau minėta, elektroninių duomenų konfidencialumo sąvoka yra siejama su privatumo sąvoka, kadangi šios abi sąvokos yra siejamos su gebėjimu apsaugoti elektroninius duomenis nuo asmenų, kurie neturi teisės arba teisėtos prieigos prie tokių duomenų. Taigi, šioms abejoms sąvokoms esant labai glaudžiai susijusioms gali kilti neaiškumų dėl nusikalstamos veikos kvalifikavimo, kai yra neteisėtai stebimi, fiksuojami, perimami, įgyjami, laikomi, pasisavinami, paskleidžiami ar kitaip panaudojami elektroniniai duomenys, o būtent kvalifikuojant veiką pagal BK 198 straipsnį ar pagal atitinkamą BK 165-168 straipsnį. Tokią problemą pastebėjo ir kai kurie teisės mokslininkai. Pavyzdžiui, tokią teisės normų konkurenciją, R. Marcinauskaitė, siūlo spręsti taip, kad tam tikrais atvejais, kai elektroninėje erdvėje yra pažeidžiamas asmens privataus gyvenimo neliečiamumas nusikalstama veika turi būti kvalifikuojama atitinkamai pagal BK 165-168 straipsnius, o tais atvejais, kai yra nustatytas neviešų elektroninių duomenų disponavimas tada pagal BK 198 straipsnį[60]. Pavyzdžiui Vilniaus miesto apylinkės teismo 2013 m. lapkričio 20 d. nuosprendis baudžiamojoje byloje, kuria L. B. buvo nuteistas *pagal BK 198 straipsnio 1 dalį ir 198[1] straipsnio 1 dalį už tai, kad ikiteisminio tyrimo metu tiksliai nenustatytu laiku <...> pamatytais ir įsimintais prisijungimo prie D. J. naudojamos elektroninio pašto paskyros j@yahoo.de vardu ir slaptažodžiu,*

[59] Vilniaus apygardos teismo 2014 m. gegužės 15 d. nuosprendis baudžiamojoje byloje (bylos Nr. 1A-338/2014)
[60] Marcinauskaitė, R., *supra* note 5, p. 50.

neteisėtai, pažeisdamas informacinės sistemos yahoo.de apsaugos priemones, įvesdamas prisijungimo vardą ir slaptažodį, prisijungė prie elektroninio pašto paskyros, pažeisdamas asmenų susižinojimo neliečiamumą, neteisėtai perėmė bei nukopijavo į nešiojamo kompiuterio standųjį diską ir taip įgijo neviešus elektroninius duomenis. Be to L. B. nuteistas pagal 168 straipsni o1 dalį ir 198 straipsnio 1 dalį už tai, kad keršydamas D. J. Už tai, jog ši atsisako su juo artimai bendrauti <...> viešai paskleidė neviešus elektroninius – nusikalstamu būdu surinktą informaciją apie D. Č ir D. J. Privatų gyvenimą, jų susirašinėjimą elektroniniu paštu.<...>. Ši byla buvo nagrinėjama tiek apeliacinėje tiek kasacinėje instancijoje. Tiek pirmosios ir antrosios instancijos teismai, dėl pirmojo epizodo, kai elektroniniai duomenys esantys asmeniniame nukentėjusios elektroniniame pašte buvo neteisėtai perimti, L. B. pripažino kaltu pagal BK 198 straipsnio 1 dalį bei 198[1] straipsnio 1 dalį. Toks pasirinktas veikos kvalifikavimas kritikuotinas, kadangi teismai pripažino, kad buvo pažeistas asmens privataus gyvenimo neliečiamumas, perimant elektroniniame pašte esančius privačius asmens pokalbius, tačiau nustatė visus nusikalstamos veikos numatytos BK 198 straipsnyje 1 dalyje esančius subjektyviuosius ir objektyviuosius sudėties požymius. Įdomu yra tai, kodėl nustačius, kad buvo pažeistas asmens susižinojimo neliečiamumas, neteisėtai perimant ir įgyjant bei vėliau paskleidžiant privataus pobūdžio susirašinėjimą nebuvo pasirinkta kita nusikalstamos veikos kvalifikacija, o būtent pagal BK 168 straipsnio 1 dalį. Šiuo atveju baudžiamoji atsakomybė pagal BK 168 straipsnio 1 dalį kiltų, kai be asmens sutikimo viešai paskelbiama informacija apie kito žmogaus privatų gyvenimą, jeigu ji buvo surinkta darant BK 165-167 straipsniuose numatytą nusikalstamą veiką. Taigi šiuo atveju L. B. veiksmai neteisėtai gaunant privataus pobūdžio susirašinėjimą atitiktų BK 166 straipsnį ir vėlesnis tokių duomenų paskleidimas atitiktų visus nusikalstamos veikos numatytos BK 168 straipsnyje sudėties požymius. Tačiau šią klaidą ištaisė kasacinės instancijos teismas konstatuodamas, kad BK 168 straipsnyje esanti nusikalstama veika yra laikoma *lex specialis derogat legi generali* numatytai BK 198 straipsnyje nusikalstamai veikai bei toks šio straipsnio taikymas būtų perteklinis. Be to atkreipė dėmesį į tai, kad asmens susižinojimo neliečiamumo pažeidimus, padarytus neteisėtai gaunant ir laikant nebe siuntimo procese esančią informaciją, tinkamiau atspindi kitokio asmens susižinojimo neliečiamumo pažeidimo požymis[61].

Taigi, apibendrinant galima teigti, kad saugomos vertybės atskleidimui yra pasitelktas CIA Triados vienas iš elementų, o būtent elektroninių duomenų konfidencialumo požymis, kuris yra siejamas su tokių duomenų gebėjimu prieiti tik tiems asmenims, kurie turi teisėtą prieigą prie šių elektroninių duomenų. Galima įžvelgti problemų atribojant privatumą ir konfidencialumą, kas yra

[61] Lietuvos Aukščiausiojo Teismo 2015 m. sausio 6 d. nutartis baudžiamojoje byloje (bylos Nr. 2K-138/2015).

matoma ir teismų praktikoje. Atribojant elektroninių duomenų konfidencialumą ir asmens privataus gyvenimo neliečiamumą, turi būti vertinama kiekvienu konkrečiu atveju ar kaltininko veika pažeistas asmens privataus gyvenimo neliečiamumas ar ne. Nustačius, kad asmuo disponuoja neviešais elektroniniais duomenis, veika kvalifikuotina pagal BK 198 straipsnį.

2.1.2 Nevieši elektroniniai duomenys kaip nusikalstamos veikos dalykas.

Neteisėtas elektroninių duomenų perėmimo ir panaudojimo BK 198 straipsnio 1 dalies dispozicijoje dalykas - elektroniniai duomenys, tačiau, antai nei BK 196 straipsnio, tokie elektroniniai duomenys turi būti nevieši, t.y. nevieši elektroniniai duomenys.

Konvencijos dėl elektroninių nusikaltimų 3 straipsnyje yra nustatyta, kad turi būti priimtos teisės normos, nustatančios baudžiamosios atsakomybės pagrindus už tyčinį informacijos perėmimą, neturint tam teisės, kai tai padaroma pasinaudojant techninėmis priemonėmis bei informacija, perimama neviešai siunčiant kompiuterinę informaciją į kompiuterinę sistemą, iš jos arba jos viduje. Šia nuostata yra siekiama apsaugoti komunikacijos privatumą[62]. Būtent šia Konvencijos nuostata yra siekiama apsaugoti komunikavimo procesą, kad į jį nebūtų neteisėtai įsikišta, t.y. komunikavimo procesas būtų konfidencialus. Taip pat Konvencijos aiškinamajame rašte neviešumas (*angl. Non-public*) yra siejamas su komunikacijos procesu, bet ne su elektroninių duomenų turiniu. Pavyzdžiui, elektroniniai duomenys perduodami komunikacijos metu gali būti vieši, tačiau asmenys nori patį šį komunikavimo procesą išsaugoti kaip neviešą arba kitaip tariant asmenys nori, kad jų komunikavimas būtų konfidencialus, viešai neprieinamas. Europos Parlamento ir Tarybos direktyvos 6 straipsnyje yra nustatyta, kad valstybės narės imtųsi būtinų priemonių užtikrinti, kad už kompiuterinių duomenų, kurie yra ne viešai perduodami į informacinę sistemą, iš jos ar joje, įskaitant elektromagnetinę spinduliuotę, būtų baudžiama kaip už nusikalstamą veiką[63]. Taigi šioje direktyvoje kaip ir Konvencijoje dėl elektroninių nusikaltimų ne viešumas yra siejamas su komunikacijos procesu, o ne pačių elektroninių duomenų turiniu.

Akivaizdu yra tai, kad įstatymų leidėjas pasirinko kitokį teisinį reglamentavimą ir neviešumą susiejo su pačių elektroninių duomenų turiniu bei jų perdavimu, o ne tik su pačiu komunikacijos procesu, kuris tarptautinių teisės aktų reikalavimų turtų būti užtikrinamas. Taigi BK 198 straipsnyje numatytos nusikalstamos veikos dalykas yra nevieši elektroniniai duomenys, tokių duomenų neviešumas yra siejamas su pačiu elektroninių duomenų turiniu. Autoriaus nuomone, toks pasirinktos

[62] Štitilis, D., *supra* note 8, p. 35.
[63] Europos Parlamento ir Tarybos direktyva 2013/40/ES 2013 m. rugpjūčio 12 d. dėl atakų prieš informacines sistemas, kuria pakeičiamas pamatinis sprendimas 2005/222/TVR

veikos kriminalizavimas, ne viešumą siejant su elektroninių duomenų turiniu, gali lemti šios normos inkriminavimo problemas. Pavyzdžiui, ar tikrai bet kuriuo atveju turi būti taikoma griežčiausia atsakomybė, kai pats komunikavimo procesas yra neviešas, o perduodamų elektroninių duomenų turinys yra visuotinai prieinamas, taip pat yra galimi atvejai, kai veiką padaręs asmuo, prieš perimant ar panaudojant elektroninius duomenis, apie tokių elektroninių duomenų neviešumo pobūdi nežinojo, o sužinojo tik susipažinęs su tokių duomenų turiniu.

Analizuojant neviešų elektroninių duomenų sampratą aptinkamas gan pastovus ir vienodas aiškinimas, o būtent neviešus elektroninius duomenis siejant su konfidencialumu, kuris pasireiškia elektroninių duomenų slaptumu[64], viešam naudojimui neskirtais duomenimis[65], visuotinai nenaudojami[66], t.y. neviešumo pobūdis vertinamas taip pat tik taikant sinonimus. Elektroniniai duomenys gali būti nevieši dėl įvairių priežasčių, tai gali būti teisės aktuose nustatyti apribojimai prieigai prie elektroninių duomenų, įstaigų dokumentai, kuriais reguliuojama vidaus tvarka (*pvz. įstaigų dokumentai gali turėti ribotą prieigą dėl valstybinės, tarnybos ar kitokios paslapties*[67]) ir pan. Taip pat neviešais elektroniniais duomenimis bus laikytini ir asmenų tarpusavio susitarimai dėl tokių duomenų atskleidimo. Taigi galima išskirti du elektroninių duomenų neviešumo pagrindus: 1) subjektyvųjį; 2) objektyvųjį[68]. Pirmajam pagrindui būtų galima priskirti požymį, kai elektroninių duomenų viešumo apribojimus nustato teisės aktai. Antrajam – kai tokių duomenų konfidencialumas nustatomas tarpasmeniniu susitarimu, verslo partnerių[69] arba kitos aplinkybės, kuriomis buvo susitarta dėl tokių duomenų neatskleidimo ar konfidencialumo.

Konstatuojant elektroninių duomenų neviešumo pobūdį teismai dažniausiai nurodo kokiuose teisės aktuose ar vidaus tvarkos taisyklėse yra nustatyti elektroninių duomenų disponavimo apribojimai. Pavyzdžiui, Vilniaus apygardos teismo 2014 m. gegužės 15 d. nuosprendis baudžiamojoje byloje (bylos Nr. 1A-338/2014), nustatyta, kad <...> *V. Š. nurodė prekybos salono konsultantei R. G., neteisėtai iš UAB (duomenys neskelbtini) vidinės (duomenys neskelbtini) sistemos įgyti UAB (duomenys neskelbtini) klientų mobilaus telefono ryšio abonentinius numerius. bei detaliąsias sąskaitas nuo 2011 metų rugpjūčio mėnesio iki 2011 metų gruodžio mėnesio, duomenis apie UAB (duomenys neskelbtini) darbuotojos A. V. atostogas, šiuos visus išvardintus elektroninius*

[64] Kuzminovas, M., *supra* note 2, *p*. 471.
[65] Ghatan, A. M., Kratz, M. P.J., Mann, J. F., *Internet Law*. Canadian Ctalouging in Publishing Data, 1998, p. 151; Marcinauskaitė, R., *supra* note 5, p. 122.
[66] Mockevičius, R., Valatkevičius, D., *supra* note 38, p. 430.
[67] Kuzminovas, M., *op. cit.*
[68] Marcinauskaitė, R., *op. cit.*
[69] Walden, I., Angel, J., *Telecommunications Law and Regulation*. Antrasis leidimas. Oxford, 2005, p. 261.

duomenis atspausdinti popieriuje <...>. Šioje byloje teismas detaliai išvardino kokie duomenys yra laikomi neviešais pagal nustatytas UAB vidaus tvarkos taisykles, t.y. kokiems duomenims buvo taikomas konfidencialumo kriterijus, ir be kita ko nustatė, kad kaltinamasis pažeidė asmens duomenų teisinės apsaugos įstatymo 5 straipsnio 1 dalies 1 punktą, 6 straipsnio reikalavimus. Taip pat šioje byloje teismas pasisakė ir apie BK 198 straipsnyje nustatytą nusikalstamos veikos dalyką, o būtent, kad šios nusikalstamos veikos numatytos BK 198 straipsnyje dalykas yra nevieši elektroniniai duomenys, taip pat konstatavo, kad neviešų elektroninių duomenų įgijimas ir naudojimas siejamas su tam tikrais, apribojimais specialiais reikalavimais ar procedūromis, kurie gali būti nustatyti įstatymuose ar kituose teisės aktuose, įmonių, įstaigų organizacijų vidaus dokumentuose, taip ir tais atvejais, kai asmuo tikisi tokių duomenų privataus perdavimo.

Apibendrinant galima teigti, kad kiekvienu konkrečiu atveju turi būti atsižvelgiama į konkrečias bylos aplinkybes ir turi būti sprendžiama, kokie apribojimai buvo taikomi elektroninių duomenų turiniui ir ar tokie elektroniniai duomenys yra laikytini konfidencialiais, neviešais. Bendriausia prasme nevieši elektroniniai duomenys yra siejami su jiems taikomais apribojimais nustatytais tiek teisės aktais ir kitais dokumentais, tiek pačių asmenų susitarimu.

2.1.3 Neteisėtas stebėjimas, fiksavimas, perėmimas, įgijimas, laikymas, pasisavinimas, paskleidimas ar kitoks panaudojimas kaip pavojingos veikos

Nusikalstama, neteisėto poveikio elektroninių duomenų perėmimo ir panaudojimo, veikos gali pasireikšti alternatyviomis veikomis – stebėjimu, fiksavimu, perėmimu, įgijimu, laikymu, pasisavinimu, paskleidimu ar kitokiu panaudojimu - tai reiškia, kad asmenį patraukti baudžiamojon atsakomybėn užtenka, kad jis atliktų bent vieną iš minėtų veiksmų. Kaip ir BK 196 straipsnyje numatyta nusikalstama veika, veiksmai pasireiškiantys perėmimu ir panaudojimu elektroninius duomenis turi būti neteisėti (*apie neteisėtumą plačiau žr. 1.1.3 skyrelyje*). Konvencijoje dėl elektroninių nusikaltimų bei Europos Parlamento ir Tarybos direktyvoje 2013/40/ES yra tiesiogiai minimas neteisėtas elektroninių duomenų perėmimas, tačiau įstatymų leidėjas išplėtė elektroninių duomenų perėmimą kaip veiką, ne tik tiesiogiai įtvirtinus ją, bet ir tokios veikos pasireiškimo alternatyvas kaip neteisėtas elektroninių duomenų stebėjimas, fiksavimas, įgijimas, laikymas, pasisavinimas. Taip pat atkreiptinas dėmesys į tai, kad, ankščiau minėtų tarptautinių teisės aktų pagrindu, elektroninių duomenų panaudojimas nėra minimas. Įtvirtinus ne tik elektroninių duomenų perėmimą, bet ir šių duomenų panaudojimą, įstatymų leidėjas praplėtė šios nusikalstamos veikos

taikymo galimybes, siejant šią nusikalstamą veiką ne tik su elektroninių duomenų perėmimu, bet ir panaudojimu[70].

Nustačius tokias alternatyvias veikas, neviešus elektroninius duomenis tenka skirstyti į esamus informacinėje sistemoje arba elektroniniais ryšiais perduodamus[71] bei pastarąjį išskirti į turinio (*angl. Content data*) ir srauto (*angl. Traffic data*) duomenis. S. W. Brenner bei J. Clough turinio duomenis prilygino užklijuotam vokui, kurio laiške esanti informacija bus prilyginta elektroninių duomenų turiniui, o srauto duomenis siejant su informacija, kurios reikia laišką išsiųsti, kuris siejamas su laiško išorėje užrašytas vardas, pavardė, adresas[72]. Taigi, elektroninių duomenų turinys tinkamiausiai bus atspindėtas laiške esančiu pranešimu ir pan., o srauto duomenys kam šis laiškas yra siunčiamas, t.y. gavėjas. Taip pat srauto duomenys yra apibūdinti ir Konvencijoje dėl elektroninių nusikaltimų, kurioje srauto duomenys - kompiuteriniai duomenys, perduodami kompiuterine sistema, suformuoti kompiuterinės sistemos, kuri sudaro ryšio grandinės dalį, ir rodantys informacijos kilmę, paskirtį, perdavimo kelią, laiką, datą, dydį, trukmę arba pagrindinės paslaugos rūšį.

Elektroninių duomenų stebėjimas yra siejamas su galimybe nevešus elektroninius duomenis matyti, suvokti ir įvertinti. Taigi, elektroninių duomenų stebėjimas yra laikomas tokiais atvejais, kai asmuo tokius duomenis jau mato, suvokia ir gali vertinti jų turinį arba elektroninius duomenis užfiksuoja atmintyje[73]. Įdomu yra tai, kad nustačius elektroninių duomenų stebėjimą kaip alternatyvią nusikalstamą veiką, formaliai vertinant asmens atliktą nusikalstamą veiką, tokio stebėjimo užtenka patraukti asmenį baudžiamojon atsakomybėn. Diskutuotina ar tikrai vien tik neviešų elektroninių duomenų pamatymas ir šių duomenų turinio suvokimas iškart užtraukia baudžiamąją atsakomybę ar vien tik neviešų elektroninių duomenų stebėjimu yra padaroma žala ar pažeidžiama įstatymo saugomi interesai. Autoriaus nuomone, toks baudžiamojo įstatymo taikymas būtų per griežtas. Lietuvos Aukščiausiasis Teismas ne kartą yra konstatavęs, kad turi būti išvengta formalaus baudžiamojo įstatymo taikymo, pabrėždamas, kad *jei veika turi konkrečios nusikaltimo sudėties požymius, tačiau iš esmės nepadaro žalos baudžiamojo įstatymo saugomiems visuomeniniams santykiams arba kitiems teisiniams gėriams ar nesukelia realaus pavojaus tokiai žalai atsirasti, yra objektyvios prielaidos*

[70] Sauliūnas, D. Elektroninių nusikaltimų reglamentavimas Lietuvoje: reguliavimo tobulinimas ir teisinės spragos palygini su Konvencija dėl elektroninių nusikaltimų. *Jurisprudencija.* 2010, 4(122), p. 210.
[71] Marcinauskaitė, R., *supra* note 5, p. 123-125.
[72] Brenner, S. W., *Cybercrime: Criminal Threats from Cyberspace, California*. Santa Barbara: Praeger, 2010, p. 190.; Clough, J. *Principles of Cybercrime*. Cambridge: Cambridge University press, 2010, p. 152.
[73] Marcinauskaitė, R., *op. cit*, p. 122

išvadai, kad tokia veika vertintina kaip nereikšminga baudžiamojo įstatymo saugomoms vertybėms[74]. Taigi šiuo atveju, autoriaus nuomone, tam, kad inkriminuoti elektroninių duomenų stebėjimo veikai turi būti nustatinėjamos ir kitos reikšmingos aplinkybės, kurios pagrįstų baudžiamosios atsakomybės taikymą. Mokslinėje doktrinoje yra laikomasi tokios pozicijos, kad norint išvengti formalaus, BK 198 straipsnyje numatytos nusikalstamos veikos, taikymo turi būti nustatinėjamas ne tik stebėjimo faktas, bet turi būti nustatinėjamos ir kitos aplinkybės, kurios rodytų žalos baudžiamojo įstatymo saugomiems teisiniams gėriams kilimą arba akivaizdžią tokios žalos kilimo grėsmę[75]. Taigi elektroninių duomenų stebėjimo pavojingumą gali pagrįsti asmens ketinimai atlikti kitas nusikalstamas veikas, pažeidžiant prieigos prie duomenų apsaugos priemones, asmens neteisėti veiksmai prisijungiant prie informacinės sistemos ir tokiu būdu gaunant elektroninius duomenis arba neteisėtai įgyjant arba fiksuojant elektroninius duomenis, stebėtų elektroninių duomenų kiekis, tokių veiksmų atlikimo trukmė[76]. Taigi, kiekvienu konkrečiu atveju turi būti nustatinėjamas ne tik elektroninių duomenų stebėjimo faktas, bet ir kitos aplinkybės, kurios pagrįstų tokio stebėjimo pavojingumą.

Elektroninių duomenų fiksavimas yra siejamas su elektroninių duomenų paėmimu, kaip fizinį objektą, ir perkėlimu į savo asmeninį kompiuterį ar kitokią laikmeną[77]. Šį straipsnį komentavusių autorių fiksavimas yra siejamas su elektroninių duomenų perkėlimu iš informacinės sistemos į savo asmeninį kompiuterį arba išorinę laikmeną. Taigi, pateikiamas pavojingos veikos aiškinimas yra siejamas tik su tokių duomenų fiksavimu, kurie yra informacinėje sistemoje ir jų paėmimu savo dispozicijon. Autoriaus nuomone, elektroninių duomenų fiksavimas turi būti siejamas su perduodamų duomenų fiksavimu, o būtent siejant fiksavimą su srauto duomenimis. Taigi srauto duomenys, Konvencijoje dėl elektroninių nusikaltimų, yra aiškinami kaip kompiuteriniai duomenys, perduodami kompiuterine sistema, suformuoti kompiuterinės sistemos, kuri sudaro ryšio grandinės dalį, ir rodantys informacijos kilmę, paskirtį, perdavimo kelią, laiką, datą, dydį, trukmę arba pagrindinės paslaugos rūšį. Paprastai tokiam duomenų srauto fiksavimui yra reikalingos pagalbinės priemonės, kuriomis yra tokie duomenys „sugaunami“[78]. Taigi elektroninių duomenų fiksavimas bus siejamas ne su elektroninių duomenų turinio nuskaitymu, o su srauto duomenų nuskaitymu, kurie yra perduodami ryšio tinklais, kanalais. Pažymėtina, kad elektroninių duomenų fiksavimas nėra

[74] Lietuvos Aukščiausiojo teismo 2015 m. sausio 27 d. nutartis baudžiamojoje byloje (bylos Nr. 2K-180-693/2015); Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2010 m. gruodžio 21 d. nutartis baudžiamojoje byloje (bylos Nr. 2K-560/2010) ir kt.
[75] Marcinauskaitė, R., *ibid,* p. 133-134.
[76] Kuzminovas, M., *supra* note 2, p. 472; Mockevičius, R., Valatkevičius, D., *supra* note 38, p. 432.
[77] *Ibid*.
[78] Marcinauskaitė, R., *op. cit.*, p. 131.

įmanomas be elektroninių duomenų stebėjimo, tokios veikos išties yra gan glaudžiai susijusios. Įdomu yra tai, kodėl įstatymų leidėjas pasirinko tokią pavojingų veikų formuluotę atskirai išskiriant stebėjimą ir fiksavimą. Paprastai, siunčiamų elektroninių duomenų, stebėjimas yra įmanomas pasitelkiant įvairios techninės ar programinės įrangos pagalbą, tokios įrangos pagalba neišvengiamai yra fiksuojama siunčiama informacija, kurią asmuo gali matyti, suvokti. Tokiais atvejais, siunčiamų duomenų stebėjimui yra būtinas šių duomenų fiksavimas – programinė įranga, nuskaičius elektroninius duomenis, juos atvaizduoja tokia forma, kurią asmuo gali suprasti[79]. Taigi siunčiamų elektroninių duomenų stebėjimo metu neišvengiamai šie duomenys yra ir fiksuojami arba pasitelkus programinę įrangą šie duomenys yra fiksuojami ir vėliau šie užfiksuoti duomenys yra stebimi, t.y. šios pavojingos veikos lemia viena kitą. Paminėtina ir tai, kad srauto duomenų fiksavimas, autoriaus nuomone, gali būti ne tik išreikšti ar užfiksuoti skaitmenine formą, bet ir tokie duomenys, kurie vėliau atvaizduojami fizinėje erdvėje, atspausdinami, užrašomi ir pan. Teismų praktikoje aptinkama šių pavojingų veikų inkriminavimas, pavyzdžiui, Vilniaus miesto apylinkės teismo nutartis baudžiamojoje byloje, kurioje *Ž. S. buvo nuteistas už tai, kad neteisėtai perėmė ir pasinaudojo neviešais elektroniniais duomenimis, pasinaudojęs Vilniaus miesto apylinkės 7-ajam notaro biurui suteiktu prisijungimo vardu bei slaptažodžiu <...> 386 kartus neteisėtai prisijungė prie VI registrų centro duomenų bazės, stebėjo, fiksavo elektroninius duomenis apie privačių asmenų kilnojami, nekilnojamąjį turtą ir tokių būdu padarė Vilniaus miesto 7-ajam notarų biurui turtinę žalą*. Tiek pirmos instancijos teisme tiek ir nagrinėjant bylą antros instancijos teisme (Vilniaus apygardos teismo nutartis[80]) nebuvo motyvuojama kodėl buvo inkriminuotas elektroninių duomenų stebėjimas ir fiksavimas. Suteikiant neviešų elektroninių duomenų įgijimui platų turinį, manytina, kad šiuo atveju buvo galimybė ir inkriminuoti tokių duomenų įgijimą.

Elektroninių duomenų perėmimas yra tiesiogiai kildinamas iš Konvencijos dėl elektroninių nusikaltimų. Konvencijos aiškinamajame rašte perėmimas yra siejamas su techninių priemonių panaudojimu klausant, stebint arba fiksuojant komunikacijos turinį, taip gaunant duomenų turinį tiesiogiai, prisijungiant prie informacinės sistemos tiesiogiai ar netiesiogiai, arba naudojant pasiklausymo prietaisus. Taigi elektroninių duomenų perėmimas siejamas su tokių duomenų perėmimu, kurie yra siunčiami elektroninio ryšio tinklais, t.y. ši pavojinga veika yra siejama su elektroninių duomenų perėmimu, kai tokie duomenys yra siunčiami elektroninių ryšių kanalais, siuntimo metu. Tokios veikos siejimas su siunčiamų elektroninių duomenų perėmimu gali kelti

[79] Marcinauskaitė, R., *supra* note 5, p. 133.
[80] Vilniaus apygardos teismo 2009 m. lapkričio 24 d. nutartis baudžiamojoje byloje (bylos Nr. 1A-1052-312/2009).

neaiškumų nustatinėjant kada yra siunčiami elektroniniai duomenys, o kada toks procesas yra užbaigtas. Literatūroje aptinkamos kelios nuomonės kada elektroninių duomenų siuntimo procesas yra užbaigtas. Viena iš jų yra siejama su gautų duomenų perskaitymu, pamatymu, taigi tokių duomenų susipažinimo momentas kiekvienu konkrečiu atveju gali skirtis. Kita nuomonė yra tokia, kad elektroniniai duomenys laikomi gautais, kai jie yra pas gavėją ir gavėjas su šiais duomenimis gali susipažinti. Tokiu atveju, susipažinimas nėra kaip vienas iš privalomų veiksmų nustatant elektroninių duomenų perdavimo, gavimo baigtumo momentą, t.y. duomenų siuntimas būtų laikomas užbaigtu tada, kai duomenys yra gauti ir nebūtų atsižvelgiama į tai ar asmuo juos pamatė, perskaitė ar ne, bet turi galimybę su jais susipažinti. Pritartina antrajai nuomonei, kadangi tokiu atveju nereikės kiekvienu konkrečiu atveju spręsti ar gavėjas su duomenimis susipažino ar ne. Taigi elektroniniai duomenys bus laikomi siunčiamais tol, kol jie nepasiekė gavėjo. Taip pat pažymėtina, kad elektroninių duomenų perėmimas yra siejamas su elektroninių duomenų turinio perėmimu siuntimo metu, bet ne su srauto duomenų perėmimu. Pavyzdžiui, perėmimo veika inkriminuota Kaišiadorių rajono apylinkės teismo 2014 m. vasario 19 d. nuosprendyje baudžiamojoje byloje (bylos Nr. 1-20-359/2014) D. B, be kitų nusikalstamų veikų, buvo nuteistas ir už 198 straipsnyje 1 dalyje esančią nusikalstamą veiką ir inkriminuotas neviešų elektroninių duomenų perėmimo ir pasisavinimo požymis, t.y. *jis neteisėtai perėmė ir pasisavino 6 asmenų elektroninius duomenis, www.uzdarbis.lt prisijungimo vardus, slaptažodžius ir tinklalapyje pateiktą asmeninę informaciją ir juos panaudojo nusikalstamai veikai vykdyti*. Taigi teismas elektroninių duomenų įgijimą vertino kaip šių duomenų perėmimą, nors pagal visas bylos aplinkybes, darytina išvada, kad tokie nuteistojo veiksmai turėtų būti vertinami kaip neviešų elektroninių duomenų įgijimas, kadangi šie duomenys buvo perimti iš informacinės sistemos. Taip pat svarstytina, kad galėjo būti inkriminuojamas ir kitoks elektroninių duomenų panaudojimas, kadangi šiais perimtai duomenimis buvo atliekamos kitos nusikalstamos veikos.

Elektroninių duomenų įgijimas bendrai baudžiamojoje teisėje suprantamas kaip tam tikro dalyko gavimas neteisėtais būdais. Anot, M. Kuzminovo, elektroninių duomenų įgijimas suvokiamas kaip realus jų gavimas[81], toks elektroninių duomenų įgijimo aiškinimas suteikia ganėtinai plačia reikšmę, kadangi elektroninių duomenų įgijimas siejamas su bet kokiu neviešų elektroninių duomenų gavimu. Taip pat tokios pozicijos laikosi ir R. Mockevičius kartu su D. Valatkevičiumi teigdami, kad „elektroninių duomenų įgijimas yra vėliau po perėmimo vykstantis veiksmas, kurio metu asmuo realiai gauna šiuos duomenis[82]“, tačiau ne tik įgijimą siejant su bet kokiu, neviešų elektroninių

[81] Kuzminovas, M., *supra* note 2, p. 473.
[82] Mockevičius, R., Valatkevičius, D., *supra* note 38, p. 433.

duomenų, gavimu, šią veiką susiejo po perėmimo vykstančių procesu, t.y. įgijimas yra sekantis veiksmas po perėmimo. Toks aiškinimas aptinkamas ir teismų praktikoje, pavyzdžiui, Vilniaus apygardos teismo 2014 m. gegužės 15 d. nuosprendis baudžiamojoje byloje (bylos Nr. 1A-388/2014) „*elektroninių duomenų įgijimu laikomas po jų perėmimo ar pasisavinimo sekantis veiksmas, kurio metu asmuo realiai gauna šiuos duomenis*“. Manytina, kad toks veikos aiškinimas yra netinkamas, kadangi tokiu atveju įgijimas nebūtų įmanomas be perėmimo, t.y. įgijimas būtų sekantis veiksmas po perėmimo. Toks aiškinimas yra kritikuotinas, kadangi šios veikos būtų viena kita lemiančiomis. Tokios pat pozicijos laikosi ir R. Marcinauskaitė teikdama, kad perėmimas neturėtų būti laikomas pirminiu duomenų įgijimo etapu, o šioms nusikalstamoms veikoms suteikus savarankišką reikšmę, jos liudytų apie skirtingus ir dažnai nesusijusius neteisėto elektroninių duomenų gavimo variantus[83]“.

Taigi, neviešų elektroninių duomenų įgijimas baudžiamojoje teisėje yra aiškinamas plačiąją prasme ir apima įvairiausius veiksmus, kuriais neteisėtu būdu yra gaunamas nusikalstamos veikos dalykas. Toks platus aiškinimas bei įtvirtintos alternatyvios veikos kelia daug neaiškumų, kokiu atveju turi būti inkriminuojamas elektroninių duomenų fiksavimas, perėmimas ar bus inkriminuojamas įgijimo požymis, kadangi atlikus bet kurią iš prieš tai minėtų veikų, tokie duomenys bus įgyjami. Todėl, atkreipiant dėmesį į perėmimo ir įgijimo veikas yra siūloma atriboti pagal duomenų esamą vietą, t.y. ar duomenys buvo laikomi informacinėje sistemoje ar jie buvo perdavimo procese[84]. Tokiu atveju elektroninių duomenų įgijimas bus tiesiogiai siejamas su neviešų elektroninių duomenų pasisavinimu iš informacinės sistemos (pačiam tokius duomenis pasisavinant), juos perkant, mainant ar kitaip gaunant neviešus elektroninius duomenis, o elektroninių duomenų perėmimas bus siejamas su duomenų gavimu kai tokie duomenys yra siunčiami, perduodami elektroniniu ryšiu. Atribojant fiksavimą nuo įgijimo yra siūloma įgijimą susieti su galimybę disponuoti elektroniniais duomenimis[85], o elektroninių duomenų fiksavimo atveju tokia galimybė būtų nebūtina, t.y. sieti su veikos baigtumu. Taip pat yra manoma, kad vienas be kitų būdų atskirti fiksavimo ir įgijimo pavojingas veikas galėtų būti formos pakeitimas iš elektroninės į materialinę[86]. Pritartina tokiai nuomonei, kad be kitų būdų atskirti neviešų elektroninių duomenų įgijimą ir fiksavimą gali būti formos kitimas. Šiuo atveju, autoriaus nuomone, neviešų elektroninių duomenų fiksavimas bus laikomas baigtu ir tada, kai nevieši elektroniniai duomenys yra užrašomi, atspausdinami ir pan., o įgijimo veikos atveju toks formos kitimas nėra įmanomas, kadangi įgijimo veika laikoma baigta nuo neviešų elektroninių duomenų

[83] Marcinauskaitė, R., *supra* note 5, p. 131.
[84] *Ibid*., p. 137.
[85] Kuzminovas, M., *supra* note 2, p. 473.
[86] Marcinauskaitė, R., *op. cit.*, p. 135.

gavimo todėl jos formos kitimas neturi įtakos veikos inkriminavimui, antai fiksavimo veikai, kuriai formos kitimas, manytina, turėtų įtakos. Taigi elektroninių duomenų įgijimo apibrėžtis, atsižvelgiant į alternatyvias veikas, kurios numatytos BK 198 straipsnio 1 dalies dispozicijoje, yra susiaurinta ir apima tokius veiksmus, kuriais nevieši elektroniniai duomenys yra perkami, skolinamasi, mainomi ar „*paprašomi*[87]“ ir pan.

Laikymas kaip pavojinga veika baudžiamojoje teisėje yra siejama su atitinkamos nusikalstamos veikos dalyko turėjimu, valdymu ar buvimu kaltininko žinioje. BK 198 straipsnio prasme laikymas bus siejamas su šios nusikalstamos veikos dalyko buvimu kaltininko žinioje. Taigi neteisėto laikymo veiką susiejus su BK 198 straipsnyje numatytos nusikalstamos veikos dalyku – elektroniniais duomenimis –darytina išvada, kad laikymas siejamas su dalyko buvimo kaltininko žinioje ir su šių duomenų buvimo vieta (pvz. kietajame diske, USB atmintinėje, kompaktiniuose diskuose ir pan.). Svarbu, kad elektroniniai duomenys būtų kaltininko žinioje ir jis jais gali disponuoti, naudoti ar valdyti. Pavyzdžiui, kaltininkas laiko neviešus elektroninius duomenis asmeniniame kompiuteryje[88], savo kontroliuojamose informacinėse laikmenose, o būtent išoriniuose duomenų kaupikliuose, asmeniniame kompiuteryje[89]. Laikymo veika yra trunkamoji, todėl inkriminuojant šią veiką pradžios momentas bus laikomas, kai neteisėtais būdais gauti elektroniniai duomenys yra pas kaltininką, o baigtumas, kai jis tokią veiką nutraukia, t.y. kai tokių duomenų nebelieka pas kaltininką[90].

Elektroninių duomenų pasisavinimas yra siejamas su elektroninių duomenų „paėmimu iš konkrečios informacinės sistemos – kompiuterio, serverio arba iš išorinės laikmenos[91]“ arba „paėmimas sulyginamas su perėmimu, tačiau šiuo atveju duomenys nekeliauja ryšių tinklais, bet asmuo turi galimybę perimti duomenis esančius konkrečioje tinklo ar informacinėse sistemos vietoje ar laikmenoje[92]“. Tokie autorių aiškinimai yra siejami su elektroninių duomenų paėmimu iš informacinės sistemos, t.y. nejudami duomenys. Toks aiškinimas iš ties padeda atriboti elektroninių duomenų pasisavinimą ir elektroninių duomenų perėmimą, kadangi tokie aiškinimai siejami su elektroninių duomenų buvimo vieta. Tačiau neišvengiamai kyla kita problema kaip atriboti elektroninių duomenų pasisavinimo veiką nuo elektroninių duomenų įgijimo, kadangi minėti autoriai

[87] Vilniaus apygardos teismo 2014 m. gegužės 15 d. nuosprendis baudžiamojoje byloje (bylos Nr. 1A-338/2014).
[88] Vilniaus miesto 2 apylinkės teismo 2009 m. gegužės 27 d. teismo baudžiamasis įsakymas baudžiamojoje byloje (bylos Nr. 1-515-487/2009).
[89] Vilniaus miesto 1 apylinkės teismo 2011 gruodžio 6 d. nuosprendis baudžiamojoje byloje (bylos Nr. 1-1430-276/2011)
[90] Marcinauskaitė, R., *supra* note 5, p. 140.
[91] Kuzminovas, M., *supra* note 2, p. 473.
[92] Mockevičius, R., Valatkevičius, D., *supra* note 38, p. 433.

įgijimą aiškina plačiąją prasme siejant su bet kokiu įgijimu elektroninių duomenų. Manytina, kad inkriminuojant pasisavinimą turi būti atsižvelgiama į subjektą, kuris tokius duomenis pasisavino. Tokiu atveju, elektroninių duomenų pasisavinimą sieti su asmeniu, kuris turi teisėtą prieiga prie neviešų elektroninių duomenų, tačiau peržengdamas jam paskirtus įgaliojimus ar apribojimus, jis tokius duomenis pasiima savo valion. Tokiu atveju, elektroninių duomenų įgijimas būtų siejamas su asmenimis, kurie neturi teisėtos prieigos prie tokių duomenų ir juos paprasčiausiai pasiima sau iš informacinės sistemos. Apie tokią nusikalstamos veikos siejimo galimybes analizavo ir R. Marcinauskaitė bei pateikė kelis elektroninių duomenų pasisavinimo aiškinimo variantus. Pirmasis elektroninių duomenų pasisavinimo aiškinimo variantas būtų siejamas su veikos inkriminavimu tais atvejais, kai neteisėtai elektroninius duomenis gauna asmuo, kuriam yra suteikta prieigos teisė prie tokių duomenų. Kitu atveju, elektroninių duomenų pasisavinimas siejamas su turto pasisavinimo aiškinimu ir būtų inkriminuojamas tais atvejais, kai kaltininkas priklausė tai asmenų kategorijai, kurie yra tiesiogiai atsakingi už tokių elektroninių duomenų, kaip pirminio šaltinio, tvarkymą[93]. Pritartina, pirmajam aiškinimui, kadangi tokiu atveju siejant elektroninių duomenų pasisavinimą su specifiniu subjektu, asmeniu, kuris turi teisėtą prieigą, tokiu atveju nebūtų daromas poveikis elektroniniams duomenims (elektroniniams duomenims nėra daromas poveikis) bei nebūtų reikalaujama spręsti dėl BK 196 straipsnyje numatytos nusikalstamos veikos inkriminavimo.

Elektroninių duomenų paskleidimas bendriausia prasme yra siejamas su neviešų elektroninių duomenų atskleidimu. Tai gali būti paviešintos įstaigų ar įmonių vidaus dokumentai, kuriems yra nustatyti tam tikri apribojimai. Manytina, kad toks elektroninių duomenų paskleidimas turi būti siejamas ne tik su jų atskleidimu visuomenei, juos patalpinant tam tikruose tinklalapiuose ar paskleidžiant per televiziją, radijo stotis, bet ir suteikiant viešą prieigą prie tokių duomenų ar sudarant galimybes prie tokių duomenų prieiti palengvintu būdu. Tokios pat pozicijos laikosi ir R. Marcinauskaitė, M. Kuzminovas bei kiti autoriai. Anot jų elektroninių duomenų paskleidimas turi būti siejamas su tokių duomenų atskleidimui viešumai, toks atskleidimas gali pasireikšti raštu, žodžiu ar kitais būdais bei elektroninių duomenų patalpinimas į tokias vietas, kur šie duomenys tampa laisvai prieinami kitiems asmenims (pvz. nuorodų kūrimas, slaptažodžių ar kodų atskleidimas).

Kitoks elektroninių duomenų panaudojimas kaip alternatyvi veika buvo nustatyta dėl to, kad nebuvo užbaigtas pavojingų veikų sąrašas. Šiai veikai buvo suteikta gan plati reikšmė. Šios veikos inkriminavimas siejamas su neviešų elektroninių duomenų panaudojimu kitiems tikslams. Tokie tikslai gali būti įvairus, pavyzdžiui, kitų nusikalstamų veikų atlikimas, savanaudiškiems tikslams,

[93] Marcinauskaitė, R., *supra* note, p. 140.

parduodant neteisėtai gautus neviešus elektroninius duomenis ar interesų tenkinimui ir pan. Tokios pat pozicijos laikosi ir BK 198 straipsnį komentavę autoriai bendrai teikdami, kad kitoks elektroninių duomenų panaudojimas siejamas su elektroninių duomenų pritaikymu, pavartojimu kokiam nors tikslui, kitų nusikalstamų veikų atlikimui ir pan., be to, pamini ir neviešų elektroninių duomenų panaudojimą chuliganiškiems, savanaudiškiems ar kitokiems interesams tenkinti[94].

Apibendrinant galima teigti, kad toks alternatyvių veikų sąrašas nustatytas BK 198 straipsnio 1 dalies dispozicijoje gali kelti neaiškumų dėl požymių inkriminavimo. Tam tikros numatytos pavojingos veikos iš esmės yra panašios (pvz. įgijimas su fiksavimu arba perėmimu ir pan.) arba viena kita apima (pvz. stebėjimas su fiksavimu ir pan.) bei atsižvelgiant mokslinėje literatūroje apibūdinamus tam tikrų pavojingų veikų turinius nėra aišku kokia veika inkriminuojama. Teismų praktikoje matoma, kad teismai inkriminuodami sudėties požymius nemotyvuoja kodėl būtent stebėjimas ar fiksavimas, įgijimas ar perėmimas yra inkriminuojami. Numatytos pavojingos veikos BK 198 straipsnio 1 dalies dispozicijoje turi būti atskiriamos pagal tam tikrus suformuluotus kriterijus. Autoriaus nuomone, toks alternatyvių veikų sąrašas yra perteklinis, kadangi kaip minėta, šios veikos yra gan panašios ir gali apimti vieną kitą, todėl tikslinga būtų atsisakyti kai kurių pavojingų veikų ir paliktas tokias pavojingas veikas, kurios viena kitos nedubliuotų.

2.1.4 Neteisėtas perėmimas ir panaudojimas neviešų elektroninių duomenų, kurie turi strateginę reikšmę nacionaliniam saugumui ar didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai kaip kvalifikuojantis sudėties požymis.

Komentuojamo BK 198 straipsnio 2 dalyje yra numatytas kvalifikuotas nusikalstamos veikos sudėties požymis apibūdinantis elektroninius duomenys kaip šių duomenų strateginė reikšmė nacionaliniam saugumui ar didelė reikšmė valstybės valdymui, ūkiui ar finansų sistemai. Tokio sudėties požymio konstrukcija yra analogiška BK 196 straipsnio 2 dalies dispozicijoje numatytai nusikalstamai veikai, t.y. BK 198 straipsnio 2 dalyje bei 196 straipsnio 2 dalyje numatytas specifinis nusikalstamos veikos dalykas – strateginė reikšmė nacionaliniam saugumui ar didelė reikšmė valstybės valdymui, ūkiui ar finansų sistemai (*plačiau žr. 1.1.5 skyrelį*). Tačiau kokiais būdais pažeidžiami elektroninių duomenų saugumas yra skirtingas, bei saugoma specifinė vertybė elektroninių duomenų konfidencialumas.

Kadangi šios nusikalstamos veikos kvalifikuojantis požymis yra ganėtinai panašus į neteisėto poveikio elektroniniams duomenims kvalifikuojantį požymį, neišvengiamai tenka spręsti perimtų ir

[94] Marcinauskaitė, R., *supra* note 5, p. 145; Mockevičius, R., Valatkevičius, D., *supra* note 38, p. 433; Kuzminovas, M., *supra* note 2, p. 473.

panaudotų elektroninių duomenų pobūdį, t.y. ar perimti ir panaudoti nevieši elektroniniai duomenys turi strateginę reikšmę nacionaliniam saugumui arba didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai. Nenustačius tokio pobūdžio duomenims taikomų kriterijų, kiekvienu konkrečiu atveju yra sprendžiama ar tokie duomenys bus pripažinti strateginę reikšmę nacionaliniam saugumui arba didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai neviešais elektroniniais duomenimis. Taip yra atkreipiamas dėmesys, kad inkriminuojant šią kvalifikuotą sudėtį gali būti atsižvelgiama ir į tokių duomenų kiekį, pavyzdžiui, sukauptu dideliu kiekiu duomenų iš Sodros centrinės klientų duomenų bazės, Valstybinės mokesčių inspekcijos prie Lietuvos Respublikos finansų ministerijos duomenų bazės apie fizinius asmenis[95]. Taigi, tokia diskrecijos laisvė palikta, kiekvienu konkrečiu atveju spręsti, prokurorui arba teismui.

Nustačius tokį nusikalstamos veikos kvalifikuojantį požymį gali kilti sunkumų nustatinėjant ar asmuo galėjo suvokti tokių duomenų pobūdį. Kadangi perimant elektroninius duomenis kaltininkas gali nežinoti apie tokių duomenų turinį, kad jie yra nevieši ir priskiriami ypatingai rūšiai. Taigi kiekvienu konkrečiu atveju, turi būti atsižvelgiama ar asmuo perimdamas ar panaudodamas strateginę reikšmę nacionaliniam saugumui galėjo numatyti tokiems duomenims taikomus kriterijus. Būtent turi būti sprendžiama ar asmuo pagal savo galimybes ir patirtį galėjo suvokti, kad perima ar panaudoja tokius elektroninius duomenis.

Apibendrinant galima teigti, kad kaltininko veiksmus kvalifikuojant pagal BK 198 straipsnio 2 dalį turi būti atsižvelgiama į tokių elektroninių duomenų pobūdį bei turinį ar perimant ir panaudojant elektroninius duomenis kaltininkas galėjo suvokti jų pobūdį, t.y. kad perėmė ir panaudojo strateginę reikšmę nacionaliniam saugumui arba didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinčius neviešus elektroninius duomenis. Nustačius, kad asmuo nesuvokė tokių elektroninių duomenų reikšmės baudžiamoji atsakomybė pagal BK 198 straipsnio 2 dalį yra negalima.

2.2. Subjektyvieji neteisėto elektroninių duomenų perėmimo ir panaudojimo sudėties požymiai

Šios BK 198 straipsnyje numatytos nusikalstamos veikos subjektyviuosius požymius sudaro asmens pakaltinamumas ir tyčia. Toks veikos teisinis reglamentavimas pasirinktas dėl to, kad buvo nustatyti apribojimai Konvencijoje dėl elektroninių nusikaltimų bei Europos tarybos pamatiniame sprendime dėl atakų prieš informacines sistemas, kuriose yra nurodyta, kad valstybės privalo kriminalizuoti sąmoningą, tyčinį neteisėta neviešų elektroninių duomenų perėmimą ir panaudojimą.

[95] Marcinauskaitė, R., *supra* note 5, p. 140.

Nustačius tokią kaltės formą, buvo siekta nekriminalizuoti tokių atvejų, kai asmuo dėl neatsargumo, išsiblaškymo arba atlikdamas testavimo darbus ar netinkamo technologijų funkcionavimo sukeliami neigiami rezultatai[96]. Tai reiškia, kad nustatinėjant asmens tyčinę kaltę jis turi suvokti, kad stebi, fiksuoja, perima, įgyja, laiko, pasisavina, paskleidžia arba kitaip panaudoja neviešus elektroninius duomenis.

Tokia pasirinkta kaltės forma reiškia, kad asmuo turi suvokti, kad neteisėtais veiksmais perimą ir panaudoja neviešus elektroninius duomenis. Taip pat asmens tyčia turi apimti ir kvalifikuojantį požymį jei nustatoma, kad neteisėtai perimami ir panaudoji elektroniniai duomenys, kurie turi strateginę reikšmę nacionaliniam saugumui arba valstybės valdymui ūkiui ar finansų sistemai. Nustatinėjant ar asmuo suvokė šį kvalifikuojantį požymį gali kilti tam tikrų problemų, kadangi neteisėtai stebint, fiksuojant ar perimant elektroninius duomenis asmuo ne visais atvejais gali žinoti duomenų turinį ir jiems taikomus apribojimus, dėl to taip pat turi būti atsižvelgiama į asmens gebėjimą, patyrimą elektroninėje erdvėje, t.y. ar galėjo pagal visas aplinkybes numatyti elektroniniams duomenims taikomus apribojimus.

Apibendrinant galima teigti, kad nustačius tokią tyčinės kaltės formą, kiekvienu konkrečiu atveju turi būti sprendžiama ar asmuo pagal visas savo galimybes, patirtį elektroninėje erdvėje galėjo numatyti elektroniniams duomenims taikomus apribojimus, t.y. turi būti atsižvelgiama į tai ar asmuo suvokė, kad tokie elektroniniai duomenys yra nevieši arba pagal asmeninius bruožus ar veikos aplinkybes galėjo suprasti šių elektroninių duomenų pobūdį. Taip pat, veiką kvalifikuojant pagal BK 198 straipsnio 2 dalį, asmens suvokimas turi apimti ir kvalifikuojantį požymį.

[96] Marcinauskaitė, R., *supra* note 5, p. 153.

3. NUSIKALSTAMŲ VEIKŲ ELEKTRONINIŲ DUOMENŲ SAUGUMUI ATRIBOJIMAS NUO PANAŠIŲ VEIKŲ.

Lietuvos Respublikos Konstitucinis Teismas ne kartą yra pasisakęs dėl konstitucinės valstybės principo, kuris - universalus principas, kuriuo grindžiama visa Lietuvos teisės sistema ir pati Konstitucija. Taip pat, kad Konstitucinės valstybės principas suponuoja įvairius reikalavimus įstatymų leidėjui vienas iš jų būtų, kad įstatymuose ir kituose teisės aktuose teisinis reguliavimas turi būti aiškūs, suprantamas, nepriešTaringas, teisės aktų formuluotės turi būti tikslios, turi būti užtikrinami teisės sistemos nuoseklumas ir vidinė darna, teisės aktuose neturi būti nuostatų, vienu metu skirtingai reguliuojančių tuos pačius visuomeninius santykius[97].

Taigi nustačius baudžiamąją atsakomybę už nusikalstamas veikas elektroninių duomenų saugumui neišvengiamai buvo sukurta situacija, kai esančios tradicinės nusikalstamos veikos ėmė konkuruoti tarpusavyje. Tokia normų konkurencija buvo sprendžiama praplečiant normų turinį arba siaurinant nusikalstamos veikos sudėties požymių apibrėžimus. Tačiau toks baudžiamojo įstatymo bei požymių aiškinimas nepadėjo išspręsti kylančių problemų kvalifikuojant nusikalstamas veikas bei nustatant kylančios atsakomybės rūšį. Taigi atkreiptinas dėmesys į tai, kad nors ir nustačius baudžiamąją bei administracinę atsakomybę už veiksmus, kuriais yra neteisėtai renkama ar pakeičiama informacija valstybės įstaigose esančius elektroninius duomenis, informacinėse sistemose.

Įstatymų leidėjui pasirinkus tokį veikų reglamentavimą, akivaizdžiai buvo neatsižvelgta į galimus skirtumus tarp nusikalstamų veikų elektroninių duomenų saugumui ir administracinės atsakomybės. Toks teisinis reglamentavimas kelia neaiškumų, kokiu atveju, kuri atsakomybė turi būti taikoma.

3.1 Nusikalstamos veikos elektroninių duomenų saugumui (BK 196 straipsnis) bei nusikalstamų veikų intelektinei ir pramoninei nuosavybei (BK 193 straipsnis) santykis.

Technologijų vystymasis bei šių technologijų panaudojimas, inkorporavimas į kasdieninį gyvenimą palengvino kūrinių platinimą panaudojant tokias priemones kaip internetą. Autoriams buvo

[97] Lietuvos Respublikos Konstitucinio teismo 2006 m. sausio 16 d. nutarimas „Dėl Lietuvos Respublikos baudžiamojo proceso kodekso 131 straipsnio 4 dalies (2001 m. rugsėjo 11 d. redakcija) atitikties Lietuvos Respublikos Konstitucijai, Dėl Lietuvos Respublikos baudžiamojo proceso kodekso 234 straipsnio 5 dalies (2003 m. balandžio 10 d., 2003 m. rugsėjo 16 d. redakcijos), 244 straipsnio 2 dalies (2003 m. balandžio 10 d., 2003 m. rugsėjo 16 d. redakcijos), 407 straipsnio (2003 m. birželio 19 d. redakcija), 408 straipsnio 1 dalies (2002 m. kovo 14 d. redakcija), 412 straipsnio 2 ir 3 dalių (2002 m. kovo 14 d. redakcija), 413 straipsnio 5 dalies (2002 m. kovo 14 d. redakcija), 414 straipsnio 2 dalies (2002 m. kovo 14 d. redakcija) atitikties Lietuvos Respublikos Konstitucijai ir dėl pareiškėjo – Šiaulių rajono apylinkės teismo prašymų ištirti, ar Lietuvos Respublikos baudžiamojo proceso kodekso 410 straipsnio (2002 m. kovo 14 d. redakcija) neprieštarauja Lietuvos Respublikos Konstitucijai.“ *Valstybės žinios*. 2006, Nr. 7-254.; ir kt.

suteikta galimybė savo kūriniais dalintis ne tik fizinėje erdvėje bet ir elektroninėje erdvėje. Taigi, buvo suteikta platesnė galimybė skleisti autoriams savo kūrinius pasitelkiant elektroninę erdvę ir neišvengiamai atsirado būtinybė teisių turėtojams pasitelkti priemones, kuriomis būtų apsaugotos autorių teisės bei suteikti informacija apie kūrinio naudojimo sąlygas.

Konvencijoje dėl elektroninių nusikaltimų 10 straipsnyje, kuriame yra reikalaujama, kad būtų priimti tokie teisės aktai, kuriais būtų nustatančios baudžiamosios atsakomybės pagrindus už autorių teisių ir gretutinių teisių pažeidimą (taip kaip apibrėžta vidaus teisėje laikantis įsipareigojimų, kuriuos prisiėmė pagal Berno konvencija, Paryžiaus aktą, ir t.t.), padarytą naudojant kompiuterinę sistemą, esant komerciškam tikslui.

Atsakomybė dėl nusikalstamų veikų intelektinei ir pramoninei nuosavybei yra numatyta BK XXIX skyriuje. Šiame skyriuje nusiklastomomis veikomis įvardintas autorystės pasisavinimas (191 str.), literatūros, mokslo, meno kūrinio ar gretutinių teisių objekto neteisėtas atgaminimas, neteisėtų kopijų platinimas, gabenimas ar laikymas (192 str.), informacijos apie autorių teisių ar gretutinių teisių valdymą sunaikinimas arba pakeitimas (193 str.), neteisėtas autorių teisių ar gretutinių teisių techninių apsaugos priemonių pašalinimas (194 str.), pramoninės nuosavybės teisių pažeidimas (195 str.).

Intelektualinės nuosavybės teisių pažeidimai yra viena iš labiausiai elektroninėje erdvėje paplitusių pavojingų veikų, kuriomis yra daroma didelė žala autorių teisių turėtojams. Apsaugotų darbų dauginimas ir platinimas internete be autorių teisių savininko leidimo yra dažnas. Atkreiptinas dėmesys, kad autorių teisės gali būti pažeidžiamos labai įvairiai, tai gali būtų autorystės pasisavinimas, autorių kūrinių atgaminimas ir kt. bei informacijos apie autorių teisių valdymą sunaikinimas ar pakeitimas, autorių teisių techninių apsaugos priemonių pašalinimas ir pan[98]. Taigi, elektroninėje erdvėje talpinami autorių kūriniai yra apsaugoti techninėmis priemonėmis, kuriomis siekiama apriboti veiksmus, kuriais būtų pažeistos jų teisės. Taip pat yra pateikiama informacija apie autorių ir gretutinių teisių valdymą.

Pasirinktas BK 196 straipsnio teisinis reglamentavimas, numatantis atsakomybę už neteisėtą poveikį elektroniniams duomenims, neišvengiamai susietinas su autorių teisių bei gretutinių teisių pažeidimais elektroninėje erdvėje. Numatytos BK 196 straipsnio dispozicijoje pavojingos veikos sunaikinimas, pakeitimas yra identiškas numatytai BK 193 straipsnio dispozicijoje. Taigi, vertinant šias veikas yra matoma, kad tiek neteisėtas poveikis elektroniniams duomenims ir informacijos apie autorių teisių ir gretutinių teisių sunaikinimas arba pakeitimas elektroninėje erdvėje iš esmės sutampa, kadangi abiem atvejais nusikalstamos veikos yra atliekamos neteisėtais veiksmais, t.y. pažeidžiamas

[98] Štitilis, D., supra note 8, p. 18.

elektroninių duomenų vientisumas bei autorinės ir gretutinės teisės. Toks pasirinktas teisinis reglamentavimas sukelia baudžiamojo įstatymo normų konkurencijos problemą, kai keli straipsniai gali būti pritaikyti tai pačiai nusikalstamai veikai.

BK 196 ir 193 straipsnių kvalifikavimo problema kyla sprendžiant pagal kurį straipsnį bus kvalifikuotina veika, kai skaitmeninės formos pateiktų kūrinių duomenys, apie autorines teises, yra pakeičiami ar sunaikinami. Iš esmės, kiekvienu atveju, kai yra pakeičiami ar sunaikinami duomenys apie autorinių teisių ir gretutinių teisių valdymą elektroninėje erdvėje pritaikytina BK 193 straipsnio norma turi ir visus BK 196 straipsnio normos požymius. Poveikio elektroniniams duomenims atveju, sunaikinant ar pakeičiant elektroninius duomenis, apima ir informacijos apie autorių teisių ir gretutinių teisių valdymą sunaikinimą ir pakeitimą. Pavojingos veikos iš esmės sutampa tiek vienu, tiek kitu atveju elektroniniai duomenys yra pakeičiami ar sunaikinami. Taip pat analizuojant BK 196 straipsnyje numatytus nusikalstamos veikos požymius matyti, kad šie požymiai yra bendresnio pobūdžio, t.y. nėra detalizuojama kokių duomenų vientisumas yra pažeidžiamas.

Visu pirma atkreiptinas dėmesys į tai, kad neteisėto poveikio elektroniniams duomenims atveju sunaikinimas pasireiškia viso elektroninės formos duomens sunaikinimu, t.y. nėra paliekama jokia dokumento dalis, kuri būtų tiesiogiai prieinama neatkuriant ar neatstatant tokio dokumento ar šiuo atveju kūrinio. Taigi tiek vienu tiek kitu atveju yra sunaikinami duomenys, tačiau BK 196 straipsnio prasme toks sunaikinimas apima viso dokumento ar kūrinio sunaikinimą, o BK 193 straipsnio prasme sunaikinimas yra siejamas su tam tikra duomenų dalimi, t.y. informacijos apie autorių teisių ar gretutinių teisių valdymą. Informacijos pakeitimas tiek BK 196 straipsnio tiek ir 193 straipsnio iš esmės sutampa. Pakeitimas yra siejamas tik su tam tikros informacijos dalies pakeitimu, taigi pakeičiant elektroninius duomenis gali būti pakeičiama ir tik tam tikra dalis, o būtent informacija apie autorių teisių ar gretutinių teisių valdymą. Tačiau atsižvelgiant į šias normas yra matoma, kad BK 193 straipsnyje, lyginant su BK 196 straipsniu, išskirtos specifinės aplinkybės, kurios taikytinos pažeidžiant intelektualinės nuosavybes teises. Galima būtų teigti, kad kai yra pakeičiama būtent specifinė informacija apie autorių teisių ir gretutinių teisių valdymą tokia veika bus kvalifikuojama pagal BK 193 straipsnyje numatyta nusikalstamą veiką, kuria yra saugomas specifinis objektas - intelektualinės nuosavybės teisiniai santykiai dėl autorių teisių ar gretutinių teisių valdymo.

Atkreiptinas dėmesys į tai, Autorinių teisių ir gretutinių teisių įstatymo (Toliau – ATGTĮ) 2 straipsnio 13 punkte yra nurodyta, kad „*informacija apie teisių valdymą – bet kokia autorių, gretutinių teisių ir sui generis teisių subjektų teikiama informacija, pagal kurią identifikuojamas kūrinys, gretutinių teisių ar sui generis teisių objektas, šių teisių subjektai, arba informacija apie kūrinio,*

gretutinių ar sui generis teisių objekto naudojimo nuostatas ir sąlygas, taip pat bet kokius numerius, grafinius žymenis ar kodus, žyminčius tokią informaciją[99]“. Taigi šio įstatymo nuostatos tiesiogiai sieja informaciją apie teisių valdymą su autorių teisių, gretutinių teisių bei *sui generis* teisių subjektais[100]. BK 193 straipsnio 1 dalyje yra konkrečiai įvardijama kokia laikoma informacija apie autorių teisių ir gretutinių teisių valdymą, t.y. nurodomi autorių teisių ir gretutinių teisių subjektai. Matyti, kad BK 193 straipsnio dispozicijoje nėra minimi *sui generis* teisių subjektai, t.y. pakeičiant informaciją apie *sui generis* teisių valdymą pagal šį straipsnį, atlikta nusikalstama veika, negali būti kvalifikuojama. Taigi kai yra pakeičiama, sunaikinama informacija apie *sui generis* teisių valdymą veika kvalifikuotina tik pagal BK 196 straipsnį, žinoma, kai atlikta nusikalstama veika atitinka visus šios nusikalstamos veikos sudėties požymius.

Informacija apie *sui generis* teisių valdymą yra saugoma identiškai kaip ir informacija apie autorių teisių ir gretutinių teisių valdymą. ATGTĮ 76 straipsnyje yra minima, kad informacija apie teisių valdymą pažeidimu laikoma bet kokios informacijos apie teisių valdymą panaikinimas ar pakeitimas be teisių subjektų leidimo, taip pat autorių teisių, gretutinių teisių ir *sui generis* teisių objektų, kuriose be leidimo panaikinta ar pakeista informacija apie teisių valdymą. Taip pat šio įstatymo 87 straipsnyje yra pasakyta, kad už autorių teisių, gretutinių teisių ir *sui generis* teisių pažeidimus nustato atitinkamai ir baudžiamasis kodeksas. Tačiau 193 straipsnio reglamentavimas išskiria tik informacijos apie autorių teisių ir gretutinių teisių valdymą panaikinimą ar sunaikinimą, tačiau nėra numatytas informacijos apie *sui generis* teisių valdymą sunaikinimą ar panaikinimą. Taigi neišvengiamai už informacijos apie *sui generis* teisių valdymą panaikinimą ar pakeitimą veika kvalifikuotina pagal BK 196 straipsnį. Iš esmės informacijos apie *sui generis* teisių valdymą pakeitimas yra lygiavertis informacijai apie autorių teisių ir gretutinių teisių valdymo pakeitimui. Taigi pakeičiant informacija apie *sui generis* teisių valdymą yra kėsinamasi į intelektinės nuosavybės teisinius santykius. Tačiau atsižvelgiant į šių BK 196 ir 193 straipsnių sankcijas matyti, kad informacijos apie *sui generis* teisių valdymą pakeitimas yra nepagrįstai griežčiau vertinama nei informacijos apie autorių teisių ar gretutinių teisių valdymą pakeitimas. Už tokius veiksmus turi būti numatytos vienodos bausmės, tokiais atvejais yra nepagrįstai griežtinama asmens atsakomybė. Įstatymų leidėjui neatsižvelgus į BK 193 straipsnio reglamentavimą bei galimas situacijas kai yra pakeičiama informacija apie *sui generis* teisių valdymą yra baudžiama kelis kartus griežčiau nei

[99] Lietuvos Respublikos Autorinių teisių ir gretutinių teisių įstatymas. *Valstybės žinios.* 1999, Nr. 50-1598.

[100] ATGTĮ 2 straipsnio 26 punktas: „*Sui generis teisių subjektas – duomenų bazės gamintojas, kuris parinkdamas, sudarydamas, tikrindamas bei pateikdamas duomenų bazės turinį padarė esminių kokybinių ir (ar) kiekybinių (intelektinių, finansinių, organizacinių) investicijų, taip pat fizinis arba juridinis asmuo, kuriam perėjo duomenų bazių gamintojo sui generis teisės*“

informacijos apie autorių teisių ir gretutinių teisių valdymą pakeitimas – BK 196 straipsnio 1 dalyje numatyta nusikalstama veika yra – apysunkis nusikaltimas, o BK 193 straipsnio 2 dalyje numatyta nusikalstama veika yra – nesunkus nusikaltimas.

3.2 Baudžiamosios ir administracinės atsakomybės už neteisėtą informacinių sistemų duomenų rinkimą, kaupimą, saugojimą, sunaikinimą ir asmens duomenų tvarkymo ir privatumo taisyklių pažeidimą atribojimas (ATPK 214^{15}).

Administracinės teisės pažeidimas ir nusikaltimas dažnai turi panašių požymių ir kvalifikuojant veiką, daugiausiai kyla klausimų dėl to, kuris kodeksas – Administracinių teisės pažeidimų ar Baudžiamasis – nustato atsakomybę už ją priemones.

Lietuvos Respublikos Konstitucinis Teismas yra pasisakęs, kad įstatymų leidėjas, paisydamas Konstitucijos, *inter alia* iš jos kylančio teisės sistemos nuoseklumo, vidinio neprieštaravimo imperatyvų, gali pasirinkti, kurios teisės šakos normomis apibrėžti tam tikrus teisės pažeidimus ir kokias sankcijas už juos nustatyti. Taigi, įstatymų leidėjas gali pasirinkti įvairias priemones, ar baudžiamosios ar administracinės ir kt., kuriomis būtų nustatyti tam tikri teisės pažeidimai. Taip pat vertinant, ar teisinė atsakomybė priskirtina administracinei, ar baudžiamajai teisei, pabrėžtina, kad tarp administracinės ir baudžiamosios teisinės atsakomybės esama nemaža panašumų, bet yra ir esminių skirtumų. Administracinių teisės pažeidimų ir nusikalstamų veikų pavojingumas yra ne vienodas, skiriasi ir patraukimo administracinėn ar arba baudžiamojon atsakomybėn padariniai. Teismas yra pabrėžęs, kad įstatymų leidėjas turi siekti tarpšakinio administracinių ir baudžiamųjų sankcijų suderinamumo.[101]

Taigi BK 196 ir 198 straipsniuose numatytas kvalifikuojantis požymis jei veika padaroma elektroninių duomenų, turinčių strateginę reikšmę nacionaliniam saugumui ar didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai, atžvilgiu, t.y. tokios informacinės sistemos, kurios yra ypatingos svarbos. ATPK 214^{15} straipsnyje yra nustatyta, kad „*Valstybės informacinių sistemų duomenų (išskyrus asmens duomenis) rinkimas, kaupimas, saugojimas, papildymas, keitimas, taisymas, klasifikavimas, sunaikinimas, teikimas arba atsisakymas juos teikti pažeidžiant informacinių sistemų tvarkymą reglamentuojančius teisės aktus* <...>“, taigi šiame straipsnyje yra numatyta administracinė atsakomybė už neteisėtą valstybės informacinių sistemų duomenų tvarkymą.

[101] Lietuvos Respublikos Konstitucinio Teismo 2005 m. lapkričio 10 d. nutarimas „Dėl Lietuvos Respublikos administracinių teisės pažeidimų kodekso 163^{2} straipsnio (2002 m. liepos 5 d. redakcija) 5 dalies ir šio straipsnio (2003 m. liepos 4 d. redakcija) 6 dalies atitikties Lietuvos Respublikos Konstitucijai.“ *Valstybės žinios*. 2005, Nr. 134-4819.

Šių sistemų tvarkymą reglamentuoja keturi[102] teisės aktai, tačiau svarbiausias šiuo atveju yra vienas Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas[103]. Šiame įstatyme yra pateikta valstybės informacinės sistemos sąvoka (2 str. 13 p.), kuri yra aiškinama taip „*Valstybinės informacinės sistema - valstybės institucijai (institucijoms) ar valstybės įstaigai (įstaigoms) teisės aktų nustatytoms funkcijoms išskyrus vidaus administravimą, atlikti reikalingą informaciją apdorojant teisinių, organizacijų, techninių ir programinių priemonių visumą.*“[104]. Taip pat atkreiptinas dėmesys, kad Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 3 straipsnyje yra nurodytos valstybės informacinių išteklių rūšys, kurios yra skirstomos į: 1) ypatingos svarbos valstybės informaciniai ištekliai, kuriuos sudaro valstybei svarbi informacija, apdorojama valstybės informacinėse sistemose ir pagrindiniuose valstybės registruos, ir ją apdorojančios valstybės informacinės sistemos ir pagrindiniai valstybės registrai; 2) svarbūs valstybės informaciniai ištekliai, kuriuos sudaro kelioms institucijoms svarbi informacija, apdorojama valstybės informacinėse sistemose ir valstybės registruose, ir ją apdorojančios valstybės informacinės sistemos ir žinybiniai registrai; 3) žinybinės svarbos valstybės instituciniai ištekliai, kuriuos sudaro vienai institucijai svarbi informacija, apdorojama valstybės informacinėse sistemose ir žinybiniuose registruose, ir ją apdorojančios valstybės informacinės sistemos ir žinybiniai registrai. 4) kiti valstybės informaciniai ištekliai, kurią valdo institucija, atlikdama vidaus administravimo funkcijas, apdorojama kitomis informacinėmis sistemose ir šią informaciją apdorojančios informacinės sistemos. Taigi, šis įstatymas taip pat išskiria informacinių sistemų išteklių svarbumą.

Atsižvelgiant į šio straipsnio formuluotę darytina išvada, kad šiuo metu galiojančiame baudžiamajame kodekse ir administracinių teisių pažeidimų kodekse yra numatytos tokios veikos, kuriomis yra kėsinamasi į tapatų objektą. BK 196 ir 198 straipsnio kvalifikuojantys požymiai neišvengiamai susietini su numatytu Administracinių teisės pažeidimų kodekso 214[15] straipsnyje numatytu požymiu – valstybės informacinių sistemai, kurios viena iš rūšių yra ypatingos svarbos valstybės informaciniai ištekliai. Taip pat atkreiptinas dėmesys, kad tiek administracinių teisės pažeidimų kodekse tiek baudžiamajame kodekse iš esmės yra panašios, kai kurios net tapačios veikos

[102] Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas. *Valstybės žinios*. 2011, Nr. 163-7739; Lietuvos Respublikos Vyriausybės 2013 m. vasario 27 d. nutarimas Nr. 180 „Dėl valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašo patvirtinimo“. *Valstybės žinios*. 2013, Nr. 23-1122.; Lietuvos Respublikos vyriausybės 2012 m. spalio 16 d. nutarimas Nr. 1263 „Dėl registrų sąrašo reorganizavimo į registrų ir valstybės informacinių sistemų registrą ir registrų ir valstybės informacinių sistemų registro nuostatų patvirtinimo“. *Valstybės žinios*. 2012, Nr. 122-6146.; Informacinės visuomenės plėtros komiteto prie susisiekimo ministerijos direktoriaus 2014 m. vasario 25 d. Nr. T-29 „Dėl valstybės informacinių sistemų gyvavimo ciklo valdymo metodikos patvirtinimo“. *TAR*. Nr. 2014-02033;

[103] *Ibid.*

[104] *Ibid.*

kuriomis yra atliekama tokia veika (*pvz. sunaikinimas; taisymas, papildymas prilygintinas elektroninių duomenų pakeitimui; kaupimas, rinkimas prilygintinas įgijimui ir pan*.). ATPK 214[15] straipsnyje yra minimas rinkimas, kaupimas, saugojimas papildymas, keitimas, ištrynimas taisymas, klasifikavimas, sunaikinimas yra siejamas su informacinėse sistemoje esančiais duomenimis, taigi, duomenų forma, kokia jie yra išreikšti, nėra minima tačiau atsižvelgiant į pačią straipsnio formuluotę darytina išvada, kad šie duomenys gali būti ne tik skaitmeninės formos duomenys, bet ir materialūs duomenys. Taip pat teisės aktų tvarkos nesilaikymas sietinas su neteisėtumo požymiu t.y. neteisėtumas siejamas su teisės aktų, reglamentuojančių informacinėse sistemose esančių elektroninių duomenų tvarkymą, pažeidimu, minėtų teisės aktų nesilaikymu ir pan.

ATPK 9 straipsnyje yra numatyta, kad administraciniu teisės pažeidimu (nusižengimu) laikomas priešingas teisei, kaltas (tyčinis arba neatsargus) veikimas arba neveikimas, kuriuo kėsinamasi į valstybinę arba viešąją tvarką, nuosavybę, piliečių teises ir laisves, į nustatytą valdymo tvarką, už kurį įstatymai nustato administracinę atsakomybę. Administracinė atsakomybė už Lietuvos Respublikos administracinių teisės pažeidimų kodekse nurodytus pažeidimus atsiranda, jeigu savo pobūdžiu šie pažeidimai pagal galiojančius įstatymus neužtraukia baudžiamosios atsakomybės. Vienas pagrindinių požymių, leidžiančių atskirti administracinio teisės pažeidimo atribojimo nuo nusikaltimo kriterijus yra skirtingas jų pavojingumo visuomenei laipsnis[105]. Taigi administracinis teisės pažeidimas yra mažiau pavojingas visuomenei nei nusikalstama veika.

Taip pat administraciniai nusižengimai skiriasi nuo nusikalstamų veikų tuo, kad jie numatyti administracinę atsakomybę nustatančiuose įstatymuose ar kituose teisės aktuose, o nusikalstamos veikos numatytos tiktai baudžiamajame kodekse[106]. Taigi, administracinės atsakomybės skirtumas nuo baudžiamosios atsakomybės pasireiškia, pirmiausia, jos taikymo pagrindu. Administracinės atsakomybės pagrindas – administracinės teisės pažeidimas, nustatytas Lietuvos Respublikos įstatymų. Baudžiamosios atsakomybės pagrindas – nusikaltimas, kurio požymiai nustatyti Lietuvos Respublikos įstatymu. Vienas iš pagrindinių požymių leidžiantis atskirti šias teisės pažeidimų rūšis, yra skirtingas jų pavojingumo visuomenei laipsnis.

BK 196 straipsnio 2 dalyje numatyta kvalifikuota nusikalstamos veikos sudėtis, kurios pavojingumą didina specialus nusikalstamos veikos dalykas, t.y. elektroniniai duomenys, esantys strateginę reikšmę nacionaliniam saugumui ar didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinčiose informacinėse sistemose. Taigi, kai yra pakeičiami, sugadinami ar pašalinami

[105] Šedberas S., Administracinė atsakomybė. Vadovėlis. Vilnius: Justitia, 2005, p. 176.
[106] I*bid*, p. 178.

elektroniniai duomenys arba kitais būdais apribojamas naudojimasis tokiais duomenimis bei kilus padariniams veika kvalifikuotina pagal BK 196 straipsnio 2 dalį. Taigi kaip minėta anksčiau toks nusikalstamos veikos kvalifikuotas požymis iš esmės yra panašus į ATPK 214[15] straipsnyje įtvirtintai pavojingai veikai, tačiau atsižvelgiant į BK 196 straipsnyje numatytos nusikalstamos veikos sudėtį, yra matoma, kad ši nusikalstama veika yra materialios sudėties, taigi, yra reikalaujamas padarinių kilimas kaip būtinasis požymis. Neteisėto poveikio elektroniniams duomenims padariniai, nors ir yra pagrindinis požymis skiriantis šią nusikalstamą veiką nuo administracinio teisės pažeidimo, tačiau šis požymis yra suformuluotas abstrakčiai, kaip didelė žala. Taigi, šis požymis ir skiria neteisėto poveikio elektroniniams duomenims nuo ATPK 214[15] straipsnio.

Kiek kitokia situacija yra matoma BK 198 straipsnio 2 dalies ir ATPK 214[15] straipsnio atribojimo atveju. BK 198 straipsnio sudėtis yra formalioji, tai reiškia, kad nėra reikalaujamas padarinių kilimas. BK 198 straipsnio 2 dalyje bei ATPK 214[15] straipsnio 1 dalyje numatytos pavojingos veikos iš esmės yra panašios ir prilygintinos viena kitai. Pavojingos veikos numatytos neteisėto elektroninių duomenų perėmimo ir panaudojimo atveju iš esmės apima ir tokias veikas, kurios yra numatytos ATPK 214[15] straipsnyje, kadangi pavojingoms veikoms yra suteiktas ganėtinai platus aiškinimas. Atkreiptinas dėmesys, kad norint išvengti pernelyg dažno šios baudžiamosios atsakomybės taikymo turi būti atsižvelgiama į šios atliktos nusikalstamos veikos aplinkybes. Pavyzdžiui, tokiais atvejais grindžiant nusikalstamos veikos pavojingumą, autoriaus nuomone, turėtų būti atsižvelgiama į patį atliktos nusikalstamos veikos pobūdį, ar tokiu atveju yra itin šiurkščiai pažeidžiamos žmogaus teisės ar laisvės, kitos Konstitucijos saugomos bei ginamos vertybės, ar daromas neigiamas poveikis visuomenei, ar kėsinamasi į valstybės ir visuomenės gyvenimo pagrindus. Visų pirma, turi būti atsižvelgiama į tokių elektroninių duomenų pobūdį, jų turinį, kiekį[107] ir pan. Taip pat turi būti atsižvelgiama į asmens, gavusio tokius duomenis, tolimesnius veiksmus, t.y. nustatyti tikslą kokio siekė perimant tokius elektroninius duomenis esančius valstybės informacinėse sistemose. Tokio tikslo nustatymas taip pat rodytų veikos pavojingumą, kurio pagrindu baudžiamosios atsakomybės taikymas būtų pagrįstas. Tokios nusikalstamos veikos inkriminavimo galimybes pagrįstu ir tokie atvejai, kai tokie duomenys yra gaunami atliekant kitas nusikalstamas veikas, arba pačios veikos pavojingumą rodytų pats elektroninių duomenų perėmimas ir vėlesnis jų panaudojimas. Be abejo taikant baudžiamąją atsakomybę turėtų būti atsižvelgiamą į tokių duomenų kiekį, jų turinį,

[107] Autoriaus nuomone, elektroninių duomenų esančių valstybinės informacijos sistemose ne visada gali pagrįsti veikos pavojingumą. Turi būti atsižvelgiama ir į šių duomenų turinį. Kadangi galimi atvejai kada yra perėmimas didelis šių duomenų kiekį, kurie nesudaro visumos ir tokie pavieniai dokumentai neturi jokios reikšmės arba yra niekiniai. Taigi atsižvelgiant į duomenų kiekį turi būti vertinamas ir jų turinys kaip pavienių duomenų ir kaip visumos.

kas irgi rodytų veikos pavojingumą. Taip pat, atkreiptinas dėmesys, ir į subjektą, kuriam yra suteikti įgaliojimai tvarkyti elektroninius duomenis, esančius valstybės informacinėse sistemose. ATPK 214^{15} straipsnyje numatytas administracinės teisės pažeidimas, sietinas su subjektu, kuriam tvarkyti šiuos elektroninius duomenis yra suteikta prieigos ir valdymo teisė teisės aktų nustatyta tvarka. Atkreiptinas dėmesys į tai, kad neteisėtumui nusikalstamos veikos BK 198 straipsnio kontekste yra suteiktas gan platus aiškinimas, tačiau jam yra būdinga tai, kad asmuo apskritai neturi teisėtos prieigos prie elektroninių duomenų. Taigi, tokiais atvejais turėtų būti atsižvelgiama į subjektą, kuris šiose informacinėse sistemose tvarko elektroninius duomenis. Nustačius, kad asmuo yra atsakingas už elektroninių duomenų tvarkymą, esančius valstybės informacinėse sistemose, ir pažeisdamas teisės aktų reikalavimus šiuos duomenis perima, tokie veiksmai turi būti vertinami kaip administracinis teisės pažeidimas pagal ATPK 214^{15} straipsnį, o tokiais atvejais, kai asmuo neturėdamas prieigos teisės ne tik prie elektroninių duomenų, bet ir prie valstybės informacinės sistemos, perima joje esančius elektroninius duomenis, tokie jo veiksmai kvalifikuotini pagal BK 198 straipsnį, t.y. kai asmuo neturi teisėtos prieigos prie valstybės informacinės sistemos ir perima joje esančius elektroninius duomenis, tokie veiksmai kvalifikuotini pagal BK 198 straipsnį. Taigi, atsižvelgiant į šiuos kriterijus pirmenybė būtų teikiama administracinės atsakomybės nustatymo pagrindui, o ne baudžiamajai atsakomybei.

Taigi, apibendrinant galima teigti, kad atribojant baudžiamąją ir administracinę atsakomybę turi būti atsižvelgiama į atliktos veikos aplinkybes. BK 196 straipsnio 2 dalyje nustatyta būtina padarinių kylimo sąlyga yra vienas iš kriterijų rodantis šios veikos pavojingumą lyginant su ATPK 214^{15} straipsnyje nustatytam pažeidimui. Atskiriant BK 198 straipsnio 2 dalyje numatytą nusikalstamą veiką ir ATPK 214^{15} straipsnyje 1 dalyje numatytą administracinį teisės pažeidimą, būtina įvertinti atliktos veikos aplinkybes, kurios rodytų padarytos nusikalstamos veikos pavojingumą. Tokie kriterijai gali būti: perimtų duomenų panaudojimo tikslas, kokiu būdu šie duomenys buvo gauti, perimtų duomenų kiekis, turinys, pobūdis, motyvai, atliktos nusikalstamos veikos aplinkybės ar buvo itin šiurkščiai pažeistos žmogaus teisės ar laisvės, kitos saugomos Konstitucijos vertybės bei gėriai, sukeltas neigiamas poveikis ir kitas aplinkybes.

Išvados

1. Elektroninio duomenų saugumo turinio atskleidimui yra taikytinas klasikinis CIA Triados modelis, kuris nustato tris kriterijus apibūdinančius elektroninių duomenų saugumą: konfidencialumas, vientisumas, prieinamumas. Elektroninių duomenų konfidencialumas rodo elektroninių duomenų slaptumą, prieigos teisių apribojimą, t.y. prieiga prie tokių duomenų turi tik tie asmenys, kuriems yra suteiktas atitinkamas leidimas. Vientisumas rodo elektroninių duomenų originalumą, integralumą, tokių duomenų nepakeičiamumą, t.y. kad duomenys buvo pakeisti tik teisėtus įgaliojimus turinčių asmenų.

2. Nusikalstamų veikų elektroninių duomenų saugumui dalykas – elektroniniai duomenys. Elektroniniai duomenys turi būti suvokiami kaip skaitmenine (dvejetaine) forma išreikšti duomenys, kurie yra apdorojami informacinėmis technologijomis, tačiau pirmenybė turi būti teikiama jų formai, o ne technologijoms apdorojančioms šiuos duomenis. Nusikalstamos veikos numatytos BK 196 straipsnyje dalykas nėra konkretizuojamas, t.y. į elektroninių duomenų sąvoka patenka visi duomenys, priešingu atveju BK 198 straipsnyje nusikalstamos veikos dalykas yra siejamas su rūšiniu požymiu – neviešais elektroniniais duomenimis. Šių duomenų neviešumą rodo jų konfidencialumas, prieigos teisių apribojimas. Neviešais elektroniniais duomenimis gali būti ne tik įstatymų ir kitų teisės aktų nustatyti apribojimai, bet ir asmenų susitarimu, siekiant šiuos duomenis išlaikyti konfidencialiais.

3. Nusikalstamų veikų elektroninių duomenų saugumui kvalifikuojantis požymis – strateginę reikšmę nacionaliniam saugumui arba didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turintys elektroniniai duomenys – rodo padidintą veikos pavojingumą. Šiose padidintos svarbos informacinėse sistemose esantys duomenys ne visais atvejais gali būti pripažinti turintys padidintą reikšmę. Kiekvienu konkrečiu atveju turi būti sprendžiama ar tokie duomenys gali būti pripažinti ypatingos svarbos ar ne. Šių duomenų svarbą, padidintą reikšmę rodytų kilusios ar galimai kilsiančios grėsmės pavojus, poveikis visuomenei, duomenų turinys bei, tam tikromis aplinkybėmis, tokių duomenų padidintą svarbą gali rodyti ir duomenų kiekis.

4. Išanalizavus pavojingas veikas numatytas BK 196 straipsnio dispozicijoje yra matoma, kad pašalinimas, kaip pavojinga veika, neatitinka tarptautinių teisės aktų, kurių pagrindu ši pavojinga veika buvo įtvirtinta BK 196 straipsnyje. Elektroninių duomenų sugadinimas sietinas su tradicinės pavojingos veikos aiškinimu, kurį pasitelkus ir integravus į elektroninės erdvės kontekstą, reikštų tokių duomenų likvidavimą, visišką šių duomenų prasmės praradimą. Sugadinimas sietinas su tokiu poveikiu, kai duomenų dalis tampa nenuskaitoma, iškraipyta ar neatpažįstama. Pakeitimas sietinas su tokiu poveikiu, kai pirminiai duomenys ar jų dalys yra pakeičiami kita informacija. Kitoks

naudojimosi elektroniniais duomenimis apribojimas rodo nebaigti pavojingų veikų sąrašą, ši veika sietina su prieigos apribojimu asmeniui, kuris turi teisėtą prieigą.

5. BK 196 straipsnyje numatyta būtina padarinių kilimo sąlyga, didelė ar nedidelė žala, kuri yra vertinamasis kriterijus. Išanalizavus teismų praktiką yra matomi formuluojami kriterijai, kuriais teismai vadovaujasi nustatant žalą, tačiau pats žalos dydis vertinamas skirtingai. Teismų praktikoje yra vertinamos šios aplinkybės: nustatinėjamas padarytos turtinės žalos dydis, paveiktas elektroninių duomenų kiekis, jų statusas, pobūdis. Be šių teismų formuluojamų kriterijų teismai nagrinėdami baudžiamąsias bylas, gali atsižvelgti ir į tai, kokios saugomos vertybės buvo pažeistos ar buvo kėsinamasi į šias vertybes, nukentėjusiojo asmens patirta neturtinė žala, nukentėjusiųjų skaičius bei kiti požymiai, kurie pagrįstai būtų laikomi svarbiais nustatant žalos dydį, nagrinėjat baudžiamąją bylą.

6. BK 198 straipsnyje pavojingų veikų analizė parodė, kad numatytos pavojingos veikos stebėjimas, fiksavimas, perėmimas, įgijimas yra glaudžiai susijusios bei dispozicijoje įtvirtintas dalyko apibrėžimas nekonkretizuojamas, todėl nėra galimybių išimtinai susieti pavojingas veikas su esančiais informacinėse sistemose ar perduodamais ryšių tinklais. Atkreiptinas dėmesys, kad nustačius elektroninių duomenų stebėjimą kaip alternatyvią veiką, turi būti atsižvelgiama ir į kitas aplinkybes rodančias šios veikos pavojingumą, t.y. kėsinimąsi į kitas saugomas vertybes. Fiksavimas sietinas su srauto duomenų perėmimu. Perėmimas sietinas su perduodamų turinio duomenų gavimu. Įgijimas sietinas su šių duomenų, esančių informacinėje sistemoje, gavimu. Laikymas – duomenų buvimu kaltininko žinioje. Pasisavinimas – jam suteiktų teisėtų įgaliojimų peržengimu. Paskleidimas – tokių duomenų paviešinimas ar prieigos palengvinimas. Kitoks panaudojimas rodo nebaigtą pavojingų veikų sąrašą ir sietinas su kitų nusikalstamų veikų atlikimu.

7. Baudžiamoji atsakomybė už neteisėtą poveikį elektroniniams duomenims veiksmus numatyta ne tik BK 196 straipsnyje, bet BK 193 straipsnyje. Nustačius autorinių ar gretutinių teisių valdytojų teisių pažeidimą, veika kvalifikuotina pagal BK 193 straipsnį. Atkreiptinas dėmesys, kad šiame straipsnyje nėra apsaugotos *sui generis* subjektų teisės, todėl tokiais atvejais veika kvalifikuotina pagal BK 196 straipsnį. Toks pasirinktas teisinis reglamentavimas sukuria situaciją kai už tapačią veiką yra baudžiama griežčiau nei tiesiogiai numatantį intelektinės nuosavybės teisių pažeidimą.

8. Taip pat atkreiptinas dėmesys ir į baudžiamosios (BK 198 str. 2 d.) ir administracinės (ATPK 214^{15} str.) atsakomybės kylančias problemas taikant vieną iš šių atsakomybės rūšių. Siūlytina atsižvelgti į: subjektą, asmens veiksmus, kuriais galimai buvo pažeistos Konstitucijos saugomos teisės bei gėriai arba kitų teisės aktų saugomos vertybės, ketinimus atlikti kitas nusikalstamas veikas, perimtų duomenų kiekį, turinį, pobūdį ir pan.

Pasiūlymai

Atsižvelgiant į magistro baigiamajame darbe atrastas problemas bei neatitikimus pagal priimtus tarptautinės teisės aktus siūlytini tokie BK 196 ir 198 straipsnių pakeitimai:

„196 straipsnis. Neteisėtas poveikis elektroniniams duomenims

1. Tas, kas neteisėtai sunaikino, sugadino, ~~pašalino~~ ar pakeitė elektroninius duomenis arba technine įranga, programine įranga ar kitais būdais apribojo naudojimąsi tokiais duomenimis padarydamas didelės žalos,

baudžiamas viešaisiais darbais arba bauda, arba laisvės atėmimu iki **trejų** metų.

2. Tas, kas šio straipsnio 1 dalyje numatytą veiką padarė strateginę reikšmę nacionaliniam saugumui ar didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinčios informacinės sistemos elektroniniams duomenims,

baudžiamas bauda arba areštu, arba laisvės atėmimu iki **penkerių** metų.“

„198 straipsnis. Neteisėtas <u>neviešų</u> elektroninių duomenų perėmimas ir panaudojimas

1. Tas, kas neteisėtai stebėjo, fiksavo, perėmė **elektroninių ryšių tinklais perduodamus neviešus elektroninius duomenis arba neteisėtai** įgijo, laikė, pasisavino, paskleidė ar kitaip panaudojo neviešus elektroninius duomenis,

baudžiamas bauda arba laisvės atėmimu iki ketverių metų.

2. Tas, kas neteisėtai stebėjo, fiksavo, perėmė **elektroninių ryšių tinklais perduodamus neviešus elektroninius duomenis arba neteisėtai** įgijo, laikė, pasisavino, paskleidė ar kitaip panaudojo strateginę reikšmę nacionaliniam saugumui arba didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinčius neviešus elektroninius duomenis,

baudžiamas laisvės atėmimu iki šešerių metų."

LITERATŪROS SĄRAŠAS

Lietuvos Respublikos įstatymai ir kiti norminiai teisės aktai:

1. Lietuvos Respublikos Konstitucija. *Valstybės žinios.* 1992, Nr. 33-1014.
2. Lietuvos Respublikos Baudžiamasis kodeksas. *Valstybės žinios.* 2000, Nr. 89-2741.
3. Lietuvos Respublikos baudžiamojo proceso kodeksas. *Valstybės žinios.* 2002, Nr. 37-1341.
4. Lietuvos Respublikos administracinių teisės pažeidimų kodeksas. *Valstybės žinios*. 1985, Nr.1-1.
5. Lietuvos Respublikos Autorinių teisių ir gretutinių teisių įstatymas. *Valstybės žinios.* 1999, Nr. 50-1598
6. Lietuvos Respublikos elektroninių ryšių įstatymas. *Valstybės žinios*. 2004, Nr. 69-2382.
7. Lietuvos Respublikos elektroninio parašo įstatymas. *Valstybės žinios*. 2000, Nr. 61-1827.
8. Lietuvos Respublikos kibernetinio saugumo įstatymas. *TAR*. 2014, Nr. 2014-20553.
9. Lietuvos Respublikos strateginę reikšmę nacionaliniam saugumui turinčių įmonių ir įrenginių bei kitų nacionaliniams saugumui užtikrinti svarbių įmonių įstatymas. Valstybės žinios. 2002, Nr. 103-4604.
10. Lietuvos Respublikos Vyriausybės 2010 m. birželio 7 d. nutarimas Nr. 717 Dėl objektų pripažinimo valstybinės reikšmės objektais tvarkos aprašo patvirtinimas. *Valstybės žinios*. 2010, Nr. 69-3442.
11. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas. *Valstybės žinios*. 2011, Nr. 163-7739;
12. Lietuvos Respublikos Vyriausybės 2013 m. vasario 27 d. nutarimas Nr. 180 „Dėl valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašo patvirtinimo“. *Valstybės žinios*. 2013, Nr. 23-1122.;
13. Lietuvos Respublikos Vyriausybės 2012 m. spalio 16 d. nutarimas Nr. 1263 „Dėl registrų sąrašo reorganizavimo į registrų ir valstybės informacinių sistemų registrą ir registrų ir valstybės informacinių sistemų registro nuostatų patvirtinimo“. *Valstybės žinios*. 2012, Nr. 122-6146.;

14. Informacinės visuomenės plėtros komiteto prie susisiekimo ministerijos direktoriaus 2014 m. vasario 25 d. Nr. T-29 „Dėl valstybės informacinių sistemų gyvavimo ciklo valdymo metodikos patvirtinimo“. *TAR.* Nr. 2014-02033

Tarptautiniai ir Europos Sąjungos teisės aktai:

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

16. EUROPOS PARLAMENTO IR TARYBOS DIREKTYVA 2013/40/ES 2013 m. rugpjūčio 12 d. dėl atakų prieš informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR.

Lietuvos Respublikos Konstitucinio Teismo praktika:

17. Lietuvos Respublikos Konstitucinio teismo 2006 m. sausio 16 d. nutarimas „Dėl Lietuvos Respublikos baudžiamojo proceso kodekso 131 straipsnio 4 dalies (2001 m. rugsėjo 11 d. redakcija) atitikties Lietuvos Respublikos Konstitucijai, Dėl Lietuvos Respublikos baudžiamojo proceso kodekso 234 straipsnio 5 dalies (2003 m. balandžio 10 d., 2003 m. rugsėjo 16 d. redakcijos), 244 straipsnio 2 dalies (2003 m. balandžio 10 d., 2003 m. rugsėjo 16 d. redakcijos), 407 straipsnio (2003 m. birželio 19 d. redakcija), 408 straipsnio 1 dalies (2002 m. kovo 14 d. redakcija), 412 straipsnio 2 ir 3 dalių (2002 m. kovo 14 d. redakcija), 413 straipsnio 5 dalies (2002 m. kovo 14 d. redakcija), 414 straipsnio 2 dalies (2002 m. kovo 14 d. redakcija) atitikties Lietuvos Respublikos Konstitucijai ir dėl pareiškėjo – Šiaulių rajono apylinkės teismo prašymų ištirti, ar Lietuvos Respublikos baudžiamojo proceso kodekso 410 straipsnio (2002 m. kovo 14 d. redakcija) neprieštarauja Lietuvos Respublikos Konstitucijai.“ *Valstybės žinios*. 2006, Nr. 7-254.

18. Lietuvos Respublikos Konstitucinio Teismo 2005 m. lapkričio 10 d. nutarimas „Dėl Lietuvos Respublikos administracinių teisės pažeidimų kodekso 163^2 straipsnio (2002 m. liepos 5 d. redakcija) 5 dalies ir šio straipsnio (2003 m. liepos 4 d. redakcija) 6 dalies atitikties Lietuvos Respublikos Konstitucijai.“ *Valstybės žinios*. 2005, Nr. 134-4819.

Lietuvos Tesimų praktika:

19. Lietuvos Aukščiausiojo teismo 2015 m. sausio 27 d. nutartis baudžiamojoje byloje (bylos Nr. 2K-180-693/2015)

20. Lietuvos Aukščiausiojo Teismo baudžiamųjų bylų skyriaus 2015 m. sausio 20 d. nutartis baudžiamojoje byloje (bylos Nr. 2K-93-489/2015).

21. Lietuvos Aukščiausiojo Teismo baudžiamųjų bylų skyriaus 2015 m. sausio 6 d. nutartis baudžiamojoje byloje (bylos Nr. 2K-138/2015).

22. Lietuvos Aukščiausiojo Teismo baudžiamųjų bylų skyriaus 2012 m. birželio 26 d. nutartis baudžiamojoje byloje (bylos Nr. 2K–375/2012).

23. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2010 m. gruodžio 21 d. nutartis baudžiamojoje byloje (bylos Nr. 2K-560/2010).

24. Kauno apygardos teismo 2014 m. balandžio 5 d. nutartis baudžiamojoje byloje (bylos Nr. 1A-36-485-2014).

25. Kauno apygardos teismo 2012 m. spalio 22 d. nutartis baudžiamojoje byloje (bylos Nr. 1A-94-175/2012).

26. Kauno apygardos teismo 2012 m. kovo 8 d. nutartis baudžiamojoje byloje (bylos Nr. 1A-224-557/2012)

27. Kauno apygardos teismo 2010 m. spalio 14 d. nuosprendis baudžiamojoje byloje (bylos Nr. 1-201-579/2010).

28. Panevėžio apygardos teismo 2014 m. kovo 14 d. nuosprendis baudžiamojoje byloje (bylos Nr. 1-35-366/2014).

29. Panevėžio apygardos teismo 2013 m. spalio 22 d. nutartis baudžiamojoje byloje (bylos Nr. 1A-551-337/2013).

30. Panevėžio apygardos teismo 2008 m. gegužės 14 d. nutartis baudžiamojoje byloje (bylos Nr. 1S-328-350/2008).

31. Šiaulių apygardos teismo 2012 m. balandžio 26 d. nuosprendis baudžiamojoje byloje (bylos Nr. 1A-154-116/2012).

32. Vilniaus apygardos teismo 2014 m. gegužės 15 d. nuosprendis baudžiamojoje byloje (bylos Nr. 1A-338/2014)

33. Vilniaus apygardos teismo 2013 m. gegužės 22 d. nutartis baudžiamojoje byloje (bylos Nr. 1A-365-200/2013).

34. Vilniaus apygardos teismo 2011 m. gruodžio 23 d. nuosprendis baudžiamojoje byloje (bylos Nr. 1A-977/2011).

35. Vilniaus apygardos teismo 2010 m. balandžio 12 d. nutartis baudžiamojoje byloje (bylos Nr. 1A-45/2010).

36. Vilniaus apygardos teismo 2009 m. lapkričio 24 d. nutartis baudžiamojoje byloje (bylos Nr. 1A-1052-312/2009).

37. Vilniaus apygardos teismo 2009 m. sausio 28 d. nutartis baudžiamojoje byloje (bylos Nr. 1A-23/2009).

38. Kaišiadorių rajono apylinkės teismo 2014 m. vasario 19 d. nuosprendis baudžiamojoje byloje (bylos Nr. 1-20 -359/2014).

39. Šilalės rajono apylinkės teismo 2011 m. balandžio 7 d. nuosprendis baudžiamojoje byloje (bylos Nr. 1-45-799/2011).

40. Trakų rajono apylinkės teismo 2013 m. sausio 7 d. nutartis baudžiamojoje byloje (bylos Nr. 1-80-272/2013).

41. Kėdainių rajono apylinkės teismo 2014 m. birželio 27 d. nuosprendis baudžiamojoje byloje (bylos Nr. 1-95-836/2014).

42. Vilniaus miesto apylinkės teismo 2013 m. balandžio 4 d. teismo baudžiamasis įsakymas baudžiamojoje byloje (bylos Nr. 1-1471-716/2013).

43. Vilniaus miesto 1 apylinkės teismo 2011 gruodžio 6 d. nuosprendis baudžiamojoje byloje (bylos Nr. 1-1430-276/2011).

44. Vilniaus miesto 2 apylinkės teismo 2011 m. liepos 1 d. nuosprendis baudžiamojoje byloje (bylos Nr. 1-188-387/2011).

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

Mokslinė ir kita specialioji literatūra:

46. Brenner, S. W. *Cybercrime: Criminal Threats from Cyberspace*. California, Santa Barbara: Praeger, 2010.

47. Brenner, S. W., et al. *Cybercrime and Jurisdiction: A Global Survey*. The Hague: T.M.C Asser Press, 2006.

48. Britz, M. T. *Computer Foresenics and Cyber Crime: an introduction*. Antrasis leidimas. New Jersey: Upper Saddle River, 2009.

49. Bishop, M. *Computer security: Art and Science*. Addison Wesley Professional, 2003.

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

51. Clough, J. *Principles of Cybercrime*. Cambridge: Cambridge University press, 2010.

52. Fedosiukas, O. Nusikaltimai ir baudžiamieji nusižengimai nuosavybei, turtinėms teisėms ir turtiniams interesams. *Lietuvos baudžiamoji teisė. Specialioji dalis.* Pirmoji knyga: vadovėlis. Vilnius : Justitia, 2013.

53. Garla, E., Dubovskaja, V. *Kompiuetrinių tinklų projektavimas*. Vilnius: UAB Ciklonas, 2008.

54. Ghatan, A. M., Kratz, M. P.J., Mann, J. F., *Internet Law*. Canadian Ctalouging in Publishing Data, 1998.

55. Goel, S. Digital Foresenics and Cyber Crime: First International ICST Conference. New York: University if Albany, 2009.

56. Grabosky, P. *Electronic crime*. New Jersey: Upper Saddle River, 2007.

57. Hernandez, S. *Official (ISC)2 Guide to the HCISPP CKB*. Taylor & Francis Group. 2015.

58. Higgins, G. E. *Cybercrime: An Introduction to an Emerging Phenomenon*. New York: McGraw-Hill, 2010.

59. Jason, A. *The basics of information security: understanding the fundamentals of InfoSec in theory and practice*. Antrasis leidimas. Waltham, MA: Syngress, 2014.

60. Kalinauskaitė, A. Elektroninė forma ir elektroninis parašas: Lietuvos teisinė bazė globaliniame kontekste. *Teisės problemos.* 2012, 1(75): P. 66-98.

61. Kalpokas, V. Skaitmeninės reguliavimas ir kontrolė: saugumo aspektai. *Teisės problemos.* 2010, 4 (70): P. 133-158.

62. Kalpokas, V. Nusikaltimai elektroninėje erdvėje: kriminologinės sampratos dilemos. *Teisės problemos.* 2009, 1 (63): P. 75-88.

63. Kanellis, P., *et al. Digital Crime and Foresenic Science in Cyberspace*. London: Idea Group Publishing, 2006.

64. Keinys, S. (vyr. red.). *Dabartinis lietuvių kalbos žodynas*. Septintas pataisytas ir papildytas leidimas. Vilnius: Lietuvių kalbos institutas, 2012.

65. Kiškis, M., *et al*., *Teisės informatika ir informatikos teisė*. Vadovėlis. Vilnius: Mykolo Romerio universitetas, 2006.

66. Kovacich, G. L., Boni W. C. *High-Technology-Crime Investigator's Handbook:Working in the Global Information Enviroment*. Butterworth-Heinemann, 2000.

67. Kuzminovas, M., Nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui. *Lietuvos baudžiamoji teisė. Specialioji dalis.* Pirmoji knyga: vadovėlis. Vilnius: Justitia, 2013.

68. Marcinauskaitė, R. *Nusikalstamos veikos elektroninių duomenų ir informacinių sistemų konfidencialumui (Lietuvos Respublikos baudžiamojo kodekso 198 ir 198[1] straipsniai).* Daktaro disertacija. Socialiniai mokslai, teisė (01 S). Vilnius: Mykolo Romerio universitetas, 2013.

69. Marcinauskaitė, R. Nusikalstamomis veikomis elektroninėje erdvėje pažeidžiamos pagrindinės baudžiamojo įstatymo saugomos vertybės nustatymo problema. *Socialinių mokslų studijos.* Mokslo darbai. 2011, 3 (3).

70. Mockevičius, R., Valatkevičius, D. 196-198[2] straipsniai. *Lietuvos Respublikos baudžiamojo kodekso komentaras.* Specialioji dalis (99-212 straipsniai). Vilnius: Registrų centras, 2009.

71. Morkytė, E. Saitai intelektinės nuosavybės teisės požiūriu (autorių teisių aspektai). *Teisė: mokslo darbai.* 2007, 64: P. 76-92.

72. Sauliūnas, D. Elektroninių nusikaltimų reglamentavimas Lietuvoje: reguliavimo tobulinimas ir teisinės spragos palygini su Konvencija dėl elektroninių nusikaltimų. *Jurisprudencija.* 2010, 4(122): P. 203-221.

73. Skyrius, R., Mikalauskienė, A., Zaleckienė, L. *Informacijos ir komunikacijos technologijos*. Vilnius: Vilniaus Universitetas, 2008.

74. Šedberas S., Administracinė atsakomybė. Vadovėlis. Vilnius: Justitia, 2005.

75. Štitilis, D. *Elektroniniai nusikaltimai*. Metodinė priemonė. Vilnius: Mykolo Romerio universitetas, 2011.

76. Štitilis, D. *Teisinės atsakomybės pagrindų nustatymo už neteisėtas veikas elektroninėje erdvėje problemos*. Daktaro disertacija. Socialiniai mokslai, teisė (01 S). Vilnius: Lietuvos teisės universitetas, 2002.

77. Valiukėnas, V., Sabaliauskaitė, R., Gabijūnienė, J. *Aiškinamasis telekomunikacijų terminų žodynas.* Vilnius: AB „Spauda“ 2004.

78. Walden, I., Angel, J., *Telecommunications Law and Regulation*. Antrasis leidimas. Oxford, 2005.

79. Williams, M. *Virtually Criminal:Crime, deviance and regulation online*. London and New York: Routledge Tailor & Francis Group, 2006.

80. Woodfort, K. *Cambridge learner‘s dictionary*. Trečiasis leidimas. Cambridge University Press. 2007.

Internetinės svetainės:

81. Lietuvos Respublikos Prokuratūros veiklos 2013 metais ataskaita. [interaktyvus], [žiūrėta 2015-02-13], <http://www.prokuraturos.lt/LinkClick.aspx?fileticket=3I95v%2Bn6dGs%3D&tabid=515>.

ANOTACIJA LIETUVIŲ IR ANGLŲ KALBOMIS

Šio magistro baigiamajame darbe nagrinėta viena iš nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui rūšių, išskiriant šias veikas pagal kėsinimosi objektą – elektroninių duomenų saugumui, kurios numatytos Lietuvos Respublikos baudžiamojo kodekso 196 ir 198 straipsniuose bei vertinamas jų teisinis reglamentavimas. Analizuoti teisės aktai, kurių pagrindu šios veikos buvo kriminalizuotos *per se*, taip pat atkreipiamas dėmesys į teismų praktiką taikant šias normas. Analizuojami neteisėto poveikio elektroniniams duomenims ir neteisėto elektroninių duomenų perėmimo ir panaudojimo nusikalstamų veikų sudėties požymiai bei pateiktos teisinio reguliavimo tobulinimo galimybės. Taip pat atkreiptas dėmesys į nusikalstamų veikų elektroninių duomenų saugumo santykio su nusikalstamomis veikomis intelektinei ir pramoninei nuosavybei nustatymą bei pateikiami baudžiamosios ir administracinės atsakomybės pagrindų taikymo kriterijai.

Reikšminiai žodžiai: elektroninių duomenų saugumas, neteisėtas poveikis, neteisėtas perėmimas ir panaudojimas.

ANNOTATION

In this Master‘s thesis are analyzed one type of criminal offences against the security of electronic data and information system security, distinguishing these offenses by encroachment object – electronic data security, provided in Articles 196 and 198 of the Criminal code of the Republic of Lithuanian and evaluation of its legal regulation. Legislation is analyzed on the basis acts which this offenses were criminalized per se, also attention was drawn to the case-law, which used the following offenses attributes. Analysis of unlawful modification of electronic data (CC Article 196) and unlawful interception and use of electronic data (CC Article 198) constituent elements are presented in this Master’s thesis and also legal regulation opportunities for improvement. Author also discussed the correlations between criminal offenses of electronic data security and similar offences of intellectual and industrial property and also discussed criminal and administrative liability framework application criteria

Key words: electronic data security, unlawful modification, unlawful interception and use.

SANTRAUKA LIETUVIŲ KALBA

Nusikalstamos veikos elektroninių duomenų ir informacinių sistemų saugumui.

Magistro baigiamajame darbe nagrinėjama viena iš BK XXX skyriuje numatytų nusikalstamų veikų rūšių, kurias struktūrizavus pagal nusikalstamos veikos dalyką, kuri sietina su elektroniniais duomenimis. Pasirinkus šią nusikalstamų veikų rūšį, buvo nagrinėjamos nusikalstamos veikos elektroninių duomenų saugumui (BK 196 ir 198 straipsnių) teoriniai ir praktiniai aspektai. Šio baigiamojo darbo tikslas atskleisti nusikalstamų veikų elektroninių duomenų saugumui (BK 196 ir 198 straipsnių) objektyviuosius ir subjektyviuosius požymius. Nagrinėjant šių nusikalstamų veikų sudėties požymius teoriniu aspektu, be kita ko, analizuojami tarptautiniai teisės aktai, kurių pagrindu šios veikos buvo kriminalizuotos *per se* ir teismų praktiką, siekiant atskleisti sudėties požymių taikymo kriterijus ir aiškinimą, nagrinėjant nusikalstamų veikų elektroninių duomenų saugumui baudžiamąsias bylas.

Tyrimo metu nustatyta, kad nusikalstamų veikų elektroninių duomenų saugumui teisinis reglamentavimas dalinai atitinka tarptautinius teisės aktus, kurių pagrindu šios veikos buvo kriminalizuotos *per se*. Aptinkami BK 196 ir 198 straipsniuose reglamentuotų veikų neatitikimai tarptautinės teisės aktams, kurios reglamentuoja baudžiamosios atsakomybės nustatymą už šias nusikalstamas veikas. Pašalinimo pavojinga veika nėra kildinama iš tarptautinių teisės aktų, kurių pagrindu ši nusikalstama veika buvo kriminalizuota. Taip pat nusikalstamos veikos numatytos BK 198 straipsnyje dalykas yra išplėstas ir siejamas ne tik su elektroninių duomenų perdavimo procesu, bet ir su esančiais informacinėse sistemoje. Analizuojant teismų praktiką dėl žalos dydžio nustatymo baudžiamosiose bylose neteisėto poveikio elektroniniams duomenims kontekste yra matomi beformuluojami kriterijai, kuriais teismai vadovaujasi nustatant žalą, tačiau pats žalos dydis vertinamas skirtingai kiekvienu konkrečiu atveju.

Taip pat nagrinėjamas neteisėto poveikio elektroniniams duomenims santykis su nusikalstamomis veikomis intelektinės nuosavybės teisėms. Analizė parodė trūkumus nustatant baudžiamosios atsakomybės pagrindus už informacijos apie autorių ir gretutinių teisių valdymą sunaikinimą ar pakeitimą, nenumatant ir *sui generis* teisių subjektų. Taigi, neišvengiamai sukurta situacija, kai pakeičiama ar sunaikinama intelektinės nuosavybės informacija apie *sui generis* teisių valdymą baudžiama griežčiau nei informacijos apie autorių ar gretutinių teisių valdytojo informacijos pakeitimas ar sunaikinimas. Taip pat analizuojami ir pateikiami baudžiamosios su administracinės atsakomybės atskyrimo kriterijai, siekiant nustatyti veikos pavojingumą, siūlytina atsižvelgti ir

nustatyti: kokios saugomos Konstitucijos vertybės buvo pažeistos ar į jas buvo kėsintasi, taip pat į elektroninių duomenų kiekį, turinį, pobūdį, tolimesnius kaltininko ketinimus, gavus šiuos duomenis, ir pan.

SANTRAUKA ANGLŲ KALBA

Criminal offences against electronic data and information security.

Master's thesis analysis one of CC XXX chapter offences which can be structured according to object which is linked to electronic data. Selecting this type of offences Master's thesis analysis theoretical and practical aspects related to criminal offences against electronic data security (Articles 196 and 198 of the Criminal Code of the Republic of Lithuanian). The main aim of this theses was to analyze criminal offences against electronic data security constituent elements. Examination of this constituent elements included not only theoretical but also international law on the basis of these offences were criminalized *per se*, and the case-law in order to reveal constituent elements, interpretations of such elements and criteria of which are headed by the courts, examining offences of electronic data security criminal cases.

After analyzing that the offences related to electronic data security legal regulation has some flaws and partially complies with international acts which these offences were criminalized. Discrepancies are found in the capability relation between current legal regulation of the Criminal Code of the Republic of Lithuania and international laws which regulate governing the determination of criminal liability for these offences. Removal of electronic data does not comply with the way it is explained in legal system of Republic of Lithuania also this unlawful act is not derived from international law, the basis of which the offense was criminalized. Criminal offense provided in Article 198 of the Criminal Code electronic data concept is expanded and associated not only with communication process but also with data that is stored in information systems. Case-law analysis shows that determining the amount of damages, in criminal cases unlawfully modifying electronic data, are formulated but it differs in each case.

Also in this Master's thesis are examined correlation between unlawful modification of electronic data and intellectual property rights. Analysis has shown cons in the determination of criminal responsibility for the information of authors and related rights of the management destruction or modification, which doesn't include *sui generis* subject rights. So inevitably created a situations where the alteration or destruction of intellectual property information of sui generis rights management is punished more severely than information of authors and related tights of the information's management destruction or modification. Thereby establishing criminal and

administrative responsibility separation criteria to determine peril of the activity is proposed to take into account which values protected by the Constitution have been violated or would be, as well as to take account the amount of electronic data, content, nature and the future intentions of the perpetrator after acquiring such data and so on.

Forma patvirtinta Mykolo Romerio universiteto
Senato 2012 m. lapkričio 20 d. nutarimu Nr.1SN-10

PATVIRTINIMAS APIE ATLIKTO DARBO SAVARANKIŠKUMĄ

2015 -05-01
Vilnius

Aš, Mykolo Romerio universiteto (toliau – Universitetas),
Teisės fakulteto, baudžiamosios teisės ir kriminologijos studijų programos
(fakulteto / instituto, programos pavadinimas)

Studentas (-ė) Mantas Mickevičius ,
(vardas, pavardė)

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

„Nusikalstamos veikos elektroninių duomenų ir informacinių sistemų saugumui.“:

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.

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