Vilniaus universiteto Teisės fakulteto

Baudžiamosios justicijos katedra

Tomo Versekėno,

V kurso, baudžiamosios justicijos

studijų šakos studento

Magistro darbas

Kibernetinių nusikaltimų sąvoka ir sistema

Vadovas: Lekt. Dr. Justas Namavičius

Recenzentas: Lekt. Dr. Audrius Juozapavičius

Vilnius

2017

Turinys

Įvadas 2
1. Kibernetinių nusikaltimų samprata, sąvoka ir pagrindiniai požymiai 5
1.1. Kibernetinių nusikaltimų istorinė raida 5
1.1.1. Technologijų ir kibernetinio saugumo raida 5
1.1.2. Priemonių prieš kibernetinius nusikaltimus paieškos pradžia 7
1.2. Kibernetinių nusikaltimų samprata ir rūšys 10
1.2.1. Kibernetinių nusikaltimų fenomenas bei problematika 10
1.2.2. Kibernetinių nusikaltimų sampratos bei klasifikacijų analizė 13
1.2.3. Kibernetinių nusikaltimų požymiai 20
1.2.4. Terminai ir sąvoka 24
2. Nusikaltimų elektroninių duomenų ir informacinių sistemų saugumui sistema, probleminiai inkriminavimo aspektai 26
2.1. Lietuvos Respublikos baudžiamojo kodekso XXX skyriaus sistema 26
2.1.1. Nusikaltimų elektroninių duomenų ir informacinių sistemų saugumui objektas 26
2.1.2. Nusikaltimų elektroninių duomenų ir informacinių sistemų saugumui sistema 30
2.2. Nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui teismų praktikoje 35
2.2.1. Atribojimas nuo kitų nusikalstamų veikų 35
2.2.2. Sudėties požymių aiškinimo problemos 40
3. Kibernetiniai nusikaltimai užsienio šalyse, tendencijos tarptautiniu mastu 45
3.1. Užsienio šalių teisinis reglamentavimas 45
3.2. Kibernetiniai nusikaltimai ir Tarptautinis baudžiamasis teismas 50
3.2.1. Tarptautinio baudžiamojo persekiojimo idėja 50
3.2.2. Romos Statuto pataisos 51
3.2.3. Kibernetiniai nusikaltimai – agresijos nusikaltimai? 53
Išvados 58
Šaltinių sąrašas 60
Santrauka 71
Summary 72
Priedai 73

Įvadas

Temos aktualumas – turbūt nėra geresnės iliustracijos teiginiui „nusikaltimai seka galimybes“ nei kompiuterių ir jų tinklų panaudojimas nusikalstamoms veikoms daryti. Skaitmeninių technologijų paplitimas bei kompiuterinių ir komunikacinių įtaisų susiliejimas pakeitė būdus, kuriais mes bendraujame, atliekame kitus svarbius darbus ir kt. Šios technologijos taip pat atvėrė platų diapazoną išnaudoti jas nusikalstamiems tikslams. Internetas suteikia prieigą prie neaprėpiamo skaičiaus potencialių aukų interaktyvioms apgaulėms įvykdyti. Skaitmeninės nuotraukos leidžia globaliai, milžiniškais dydžiais paskirstyti vaikų seksualinio išnaudojimo medžiagą. Skaitmeninė informacija gali būti kopijuojama ir ja dalijamasi, sudarant galimybę pažeisti autorines ir gretutines teises. Socialiniai tinklai gali būti naudojami grasinimo tikslais bei patyčioms. Didėjanti žmonijos priklausomybė nuo kompiuterių bei skaitmeninių tinklų, pačias technologijas paverčia nusikalstamų veikų taikiniu[1]. Visos šios ir kitos su informacinėmis technologijomis susijusios veikos dažnu atveju yra vadinamos kibernetiniais nusikaltimais. Tačiau teisės moksle vis dar nėra visuotinai bendrai priimtos kibernetinių nusikaltimų sąvokos[2].

Tai, kad šių nusikalstamų veikų rūšies analizė reikšminga ne tik teorijai, bet ir praktikai, parodo ir augantis šių nusikalstamų veikų skaičius[3]. Lietuvos Respublikos baudžiamojo kodekso XXX skyriuje įtvirtintos nusikalstamos veikos yra taikomos vis dažniau – per dešimtį metų Lietuvoje užregistruotų minėto skyriaus nusikalstamų veikų skaičius išsaugo daugiau nei septyniasdešimčia kartų[4]. Padidėjusi, iki 2010 m. mažai taikyta Lietuvos Respublikos baudžiamojo kodekso 196–198[2] straipsnių „apyvarta“ neišvengiamai iškėlė poreikį spręsti baudžiamojo įstatymo konkurencijos problemas, išryškino nesuderintos teismų praktikos atvejus, skirtingą veikų kvalifikavimą, nevienodą šių nusikalstamų veikų sudėčių požymių taikymą ir aiškinimą. Tiesa, tikslaus paaiškinimo, kodėl krito 2016 m. statistiniai rodikliai, nėra. Galima tik prielaida, kad šie pokyčiai kito dėl naujos Nusikalstamų veikų žinybinio registro duomenų pagrindu rengiamų nusikalstamumo pagrindinių statistinių rodiklių apskaičiavimo tvarkos, kadangi užregistruotų nusikalstamų veikų skaičiaus, pagal skirtingus baudžiamojo įstatymo straipsnius, proporcija išliko tokia pati.

---

[1] CLOUGH, J. Cybercrime. *Commonwealth law bulletin*, 2011, Vol., 37, Issue 4, p. 671–680.
[2] ŠTITILIS, D., *et al. Interneto ir technologijų teisė*. Vilnius: Mykolo Romerio universitetas, 2016.
[3] BILEVIČIENĖ, T. Dynamics of crimes against the security of electronic data and information systems, and its influence on the development of electronic business in Lithuania. *Jurisprudencija*, 2011, Nr. 18(2), p. 689–702.
[4] Priedas Nr.1 – Grafikas ir lentelė „Duomenys apie Lietuvos Respublikos baudžiamojo kodekso XXX skyriaus uždraustas veikas, padarytas Lietuvos Respublikoje 2004 m. – 2016 m. laikotarpiu“.

Žinoma nedera pamiršti, kad kibernetiniai nusikaltimai neapsiriboja ties viena valstybe – netyla ir užsienio žiniasklaida apie pasaulinio masto atakas prieš didžiausius internetinius tinklalapius[5], netgi valstybes[6,7].

Tyrimo tikslas – išanalizuoti kibernetinių nusikaltimų fenomeną, jo sampratą, taip pat atskleisti Lietuvos teisinėje sistemoje kibernetinių nusikaltimų sistemos probleminius aspektus.

Tyrimo uždaviniai:

1. Išanalizuoti kibernetinių nusikaltimų sampratą, būdingus šiai nusikaltimų grupei esminius požymius bei pateikti kibernetinių nusikaltimų apibrėžimą;
2. Išryškinti Lietuvos Respublikos baudžiamojo kodekso XXX skyriaus normų problematiką, išanalizuoti harmonizavimą su tarptautiniais teisės aktais, Lietuvos teismų praktiką;
3. Atskleisti kibernetinių nusikaltimų vietą užsienio šalių baudžiamuosiuose įstatymuose, išskirti esminius Lietuvos baudžiamojo įstatymo skirtumus, perspektyvas priskirti kibernetinius nusikaltimus Tarptautinio baudžiamojo teismo jurisdikcijai.

Tyrimo objektas – kibernetinių nusikaltimų sąvoka, sistema Lietuvos baudžiamajame įstatyme.

Pasitelkti šie tyrimo metodai: istorinis (kibernetinio saugumo ir kibernetinių nusikaltimų vystymosi raidai apibūdinti), mokslinės teorijos analizės (gilinantis į kibernetinių nusikaltimų sampratą bei apibrėžimus), lyginamasis (lyginant užsienio šalių baudžiamuosius įstatymus), lingvistinis ir analizės (naudojama aiškinant teisės aktų normas), sisteminis ir teleologinis (atskleidžiant Lietuvos Respublikos baudžiamojo kodekso XXX skyriaus normų ryšius, sąveiką su teisės principais ir kitomis baudžiamosios teisės normomis) bei loginis metodai.

Originalumas – šiame darbe nemažas dėmesys yra skiriamas kibernetinių nusikaltimų sampratos bei sąvokos analizei. Skirtingai nei Lietuvos mokslinėje literatūroje, šiame darbe remiantis užsienio autorių darbais išskiriami kibernetiniams nusikaltimams būdingi požymiai, pateikiama šio darbo autoriaus kibernetinių nusikaltimų sąvoka. Lietuvos moksliniuose darbuose galima rasti teismų praktikoje pasitaikančių Lietuvos baudžiamojo kodekso XXX skyriaus probleminių inkriminavimo aspektų

[5] O'Brien, S. A. Widespread cyber attack takes down sites worldwide [interaktyvus; žiūrėta 2017 m. vasario 27 d.]. Prieiga per internetą: <http://money.cnn.com/2016/10/21/technology/ddos-attack-popular-sites/>.
[6] NATO Review. The history of cyber attacks – a timeline [interaktyvus; žiūrėta 2017 m. vasario 27 d.]. Prieiga per internetą: <http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm>.
[7] BNS. Atakos prie Lietuvą dažnėja [interaktyvus; žiūrėta 2017 m. vasario 27 d.]. Prieiga per internetą: <http://www.delfi.lt/news/daily/lithuania/vsd-vadovas-atakos-pries-lietuva-dazneja.d?id=73396080>.

tyrimą, darbų, kuriuose koncentruojamasi ties baudžiamojo įstatymo terminologijos bei reguliavimo modelio dilemomis, harmonizavimo Europos Sąjungos teisės aktų klausimais. Atitinkamai šiame darbe nagrinėjami nauji 2015, 2016 m. baudžiamojo įstatymo pakeitimai, atskirų nusikalstamų sudėčių požymiai, peržvelgiama 2015, 2016 m. teismų praktika bei problematika. Be to, darbe gilinamasi į kibernetinių nusikaltimų priskyrimo Tarptautinio baudžiamojo teismo jurisdikcijai perspektyvas.

Svarbiausi šaltiniai: magistriniame darbe yra remiamasi įvairiais literatūros šaltiniais: tarptautiniais, užsienio šalių, nacionaliniais teisės aktais, teisės aktų projektais, statistine medžiaga, teismų formuojama praktika, užsienio bei Lietuvos autorių moksliniais darbais. Pirmoje darbo dalyje išskirtini S. Schjolberg[8], D. Wall[9], I. Walden[10] darbai, 2001 m. lapkričio 23 d. Konvencija dėl elektroninių nusikaltimų. Antrojoje darbo dalyje pagrindinius šaltinius sudarė Lietuvos teismų praktika, Europos Parlamento ir Tarybos 2013 m. rugpjūčio 12 d. direktyva[11]. Trečiojoje dalyje svarbus O. Triffterer ir K. Ambos 2016 m. parengtas Tarptautinio baudžiamojo teismo Romos Statuto komentaras[12].

[8] SCHJOLBERG, S. *The history of cybercrime – 1976-2014*. Norderstedt: Books on demand, 2014.
[9] WALL, D. What are cybercrimes? *Criminal Justice Matters*, 2008, Vol. 58:1, p. 20–21.
[10] WALDEN, I. *Computer Crimes and Digital Investigation*. Oxford: Oxford university press, 2007.
[11] 2013 m. rugpjūčio 12 d. Europos Parlamento ir Tarybos direktyva 2013/40/ES dėl atakų prieš informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR (OL 2013 L 218, p. 8).
[12] TRIFFTERER, O.; AMBOS, K. *The Rome Statute of the International Criminal Court. A Commentary Third Edition.* Oxford: Hart, 2016.

1. Kibernetinių nusikaltimų samprata, sąvoka ir pagrindiniai požymiai

1.1. Kibernetinių nusikaltimų istorinė raida

1.1.1. Technologijų ir kibernetinio saugumo raida

Kibernetinių nusikaltimų istorija bei raida neabejotinai yra siejama su kompiuterio bei technologijų atsiradimo epocha. Žinoma, kibernetiniai nusikaltimai netapo visuotinai žinomu reiškiniu vos tik atsiradus pirmiesiems kompiuteriams. Anuomet kompiuteris buvo milijonus kainuojanti mašina, kuri neturėjo aiškios instrukcijos kaip ja naudotis. Kibernetinio nusikalstamumo problema išaugo kartu vystantis kompiuterijai – jai pingant ir taip tampant labiau pasiekiamai didesnei visuomenės daliai, paprastėjant naudojimuisi[13]. Atsirandant naujoms technologijoms didėjo informacijos sklaida, augo galimybės, bet kartu ir grėsmės. Verta paminėti, kad naujos technologijos turėjo įsitvirtinti kasdieniniame gyvenime. Štai D. Gollmann skiria keturis laikotarpius, kurių metu augo ir kito, kompiuterių saugumas, o kartu ir kibernetiniai nusikaltimai: 1970 m. (pagrindinė įranga), 1980 m. (asmeninis kompiuteris), 1990 m. (internetas), 2000 m. (tinklas) [14].

1970 m. pradėta naudotis atminties įtaisais, kurie gelbėjo daugiausiai valstybės institucijoms ar didelėms komercinėms organizacijoms disponuoti, valdyti didesnius kiekius informacijos. Valstybinės institucijos kaupusios neužslaptintą, bet privačią informaciją apie piliečius, nuo šio laikmečio, galėjo tai daryti didesniu mastu. Imta ieškoti būdų, kaip būtų galima apsaugoti duombazėse esančius duomenis nuo pašalinių asmenų. Pradėta plačiai naudoti bei studijuoti kriptografiją, buvo kuriami specialūs saugos algoritmai[15].

1980 m. kompiuterio komponentų mažinimas lėmė tai, kad kompiuteriams nebereikėjo didelių atskirų patalpų, kompiuteris tapo vieno žmogaus valdoma mašina telpanti ant namuose esančio darbastalio. Asmeninio kompiuterio pagrindinė funkcija skirianti jį nuo savo pirmtakų buvo tekstinių dokumentų apdorojimas. Kompiuteriuose pradėti kaupti asmeniniai dokumentai ir juose esanti informacija. Teko sukurti sistemą, kuri saugotų nuo asmenų besinaudojančių tuo pačiu kompiuteriu, tačiau neturinčio prieigos prie asmeninės, konfidencialios informacijos, todėl pradėta vystyti daugiasluoksnė saugumo sistema, kuri leido naršyti neslaptą informaciją, tačiau nesuteikė prieigos prie slaptos. Atsirado pirmieji kompiuterių virusai. Kibernetinių nusikaltimų

[13] SHINDER, D. L. *Scene of the cybercrime. Computer forensics handbook*. Rockland: Syngress Publishing Inc., 2002, p. 2.
[14] GOLLMANN, D. *Computer security*. West Sussex: John Wiley & Sons, Ltd, 2011, p. 3–8.
[15] *Ibid.*

daroma žala tapo matoma didesnei visuomenės daliai. Štai pirmasis įsilaužėlis arba „hakeris“ Jungtinėje Karalystėje už tai, kad neteisėtai prisijungė prie universiteto kompiuterio tinklo, modifikavo ir trynė sistemos vartotojų failus, 1991 m. apeliacinio teismo nuteistas laisvės atėmimo bausme pagal 1971 m. Nusikalstamos žalos aktą (angl. *UK Criminal Damage Act of 1971*)[16].

1990 m. galutinai buvo išspręstas duomenų perdavimo metodas – fakso paslaugas, kurias teikė tradiciniai telefoninių tinklų operatoriai, nukonkuravo elektroninis paštas ir interneto paslaugos. Pažymėtina, kad internetas buvo sukurtas gerokai anksčiau, tačiau tik 1992 m. buvo atvertas komerciniam naudojimui, taip pat tapo labiau prieinamas. Asmeninio kompiuterio prijungimas prie pasaulinio tinklo kėlė naujus saugumo iššūkius, kadangi privatus vartotojas jau nebegalėjo kontroliuoti, kas ir kokio pobūdžio impulsus, signalus siunčia į jo asmenę mašiną. Grafinio dizaino sukūrimas leido dalintis ne tik duomenimis, bet ir tapo nauja pramogų platforma. Neabejotinai aktuali tapo ir autorinių teisių problema[17].

2000 m. nors technologija gerokai patobulėjo, iš esmės liko tokia pati. Esminis šio laikotarpio bruožas yra tai, kad tinklo naudojimas masiškai išplito visame pasaulyje. Stambiais mastais išaugo interneto tinklo naudojimas komerciniais tikslais, privačių asmenų finansinių operacijų, atliekamų interneto pagalba, skaičius. Šiuo laikotarpiu išaugo ir įvairių saugumo sistemų rūšių, specializuotų tam tikrai sistemų apsaugos sričiai, pavyzdžiui, antivirusinės programos, programos saugančios nuo išorės kenkėjiškų duomenų patekimo į kompiuterį, apsaugančių informaciją siuntimo, perdavimo, gavimo metu ir pan. Įsilaužėliai ėmė naudotis labiau išmanesne programine įranga, taip įsilaužiant į kompiuterius nepaliekant akivaizdžių įsibrovimo pėdsakų, paslapčia sekant ir ieškant banko prisijungimo kodų ir kitų duomenų[18].

Žinoma, technologijos nuolatos vystosi ir tobulėja, todėl kai kurie mokslininkai teigia, kad jau galima kalbėti apie naują kompiuterio saugumo bei kibernetinių nusikaltimų kartą, atsiradus bevieliui interneto ryšiui[19].

Ši paminėta informacinių technologijų evoliucija padeda paaiškinti, suvokti kibernetinius nusikaltimus. Štai 1980 m. baudžiamasis persekiojimas nebuvo dažnas reiškinys, nes veikos, susijusios su kompiuteriais, nebuvo aiškiai identifikuojamos kaip grėsmingos[20]. Antai jau 1990 m. vadovėliuose neteisėtas veikimas internetinėje erdvėje išskiriamas kaip nusikalstamas elgesys, tačiau pažymima, kad nors ir gaunama nemažai

[16] GOLLMANN, D. *Computer security*. West Sussex: John Wiley & Sons, Ltd, 2011, p. 3–8.
[17] *Ibid.*
[18] *Ibid.*
[19] JEWKES, Y.; YAR, M., *et al. Handbook of internet crime*. New York: Routledge, 2011, p. 13.
[20] PFLEEGER, C., *et al. Security in computing*. New Jersey: Prentice hall, 2002, p. 587.

pranešimų apie nusikalstamą elgesį, patraukimo baudžiamojon atsakomybėn atvejų nėra itin daug[21]. Atitinkamai, vadovaujantis Jungtinių Amerikos Valstijų (toliau – JAV) finansų ministerijos duomenimis, 2005 m. kibernetinių nusikaltimų atžvilgiu buvo iškelta daugiau bylų nei prekybos narkotikais atvejų; Vokietijoje 2004 m. kibernetiniai nusikaltimai sudarė vos 3 procentus visų registruotų nusikalstamų veikų, tačiau apskaičiuota jais padaroma materialinė žala siekė net 57 procentus visų nusikalstamų veikų kontekste; 2009 m. JAV Federalinis tyrimų biuras gavo 336 655 nusiskundimus dėl internetinių nusikaltimų, kartu susiejant su jais padarytus 559,7 milijono JAV dolerių nuostolius[22]. Iš pateiktų rodiklių matoma, kad kibernetinis nusikalstamumas ne auganti, o jau visiškai susiformavusi, vyraujanti problema. Savaime suprantama, didėjant šiai naujai grėsmei turėjo formuotis atitinkamas valstybės institucijų atsakas.

1.1.2. Priemonių prieš kibernetinius nusikaltimus paieškos pradžia

Dėmesį į kibernetinius nusikaltimus bene pirmasis atkreipė D. B. Parker, kuris laikomas vienas iš pirmųjų apibrėžusių kompiuterinius nusikaltimus. D. B. Parker jau nuo 1970 m. tyrinėjo kompiuterių nusikaltimus bei saugumo problemas. Jis tarnavo kaip vyresnysis kompiuterių saugumo konsultantas Stanfordo tyrimo institute ir buvo pagrindinis, JAV teisėsaugos institucijoms 1979 m. parengto vadovo – „Kompiuteriniai nusikaltimai – baudžiamosios justicijos mokymosi vadovas“ (angl. *Computer crime – criminal justice recourse manual*) autorius. Savo ruožtu, pirmasis akademinis kompiuterinių nusikaltimų tyrinėjimas pradėtas 1977 m. Vokietijoje, kurį atliko U. Sieber[23].

Pirmoji tarptautinė iniciatyva prieš kompiuterinius nusikaltimus vyko Starbūre 1976 m. kai Europos Taryba surengė konferenciją apie ekonominių nusikaltimų kriminologinius aspektus[24]. Jos metu buvo pristatytos kelios kompiuterinių nusikaltimų kategorijos. Europos Taryba 1989 m. priėmė rekomendacijas[25], kuriose pažymima, kad reikalingas įstatymų bei praktikos harmonizavimas, tarptautinė teisinė pagalba. Jose skatinama valstybes, kuriant įstatymus ar priimant jų pataisas, atsižvelgti į Europos nusikalstamumo problemų komiteto (angl. *European Committee on Crime Problems*)

[21] STREET, F. L. *Law of the Internet*. Charlottesville: Lexis law publishing, 1998, p. 561.
[22] BOYLE, R., *et al. Corporate computer security*. Essex: Person, 2014, p. 58.
[23] SCHJOLBERG, S. The history of global harmonization on cybercrime legislation – the road to Geneva [interaktyvus; žiūrėta 2017 m. sausio 1 d.]. Prieiga per internetą: <http://www.cybercrimelaw.net/documents/cybercrime_history.pdf>.
[24] *Ibid.*
[25] 1989 m. rugsėjo 13 d. Europos Tarybos Ministrų komiteto rekomendacija valstybėms narėms Nr. R(89) 9 dėl su kompiuteriais susijusių nusikaltimų [interaktyvus; žiūrėta 2017 m. sausio 3 d.]. Prieiga per internetą: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804f1094>.

ataskaitą, kurioje aptarti su kompiuteriais susiję nusikaltimai, bei nurodoma iki 1993 m. Europos Tarybos generaliniam sekretoriui pateikti apžvalgą apie įgyvendintą progresą šioje srityje. Šioje ataskaitoje su kompiuteriais susiję nusikaltimai gana kruopščiai ištyrinėti, pateikiant naujo fenomeno apibūdinimą, siūlant nusikalstamų veikų sąrašą, kurį rekomenduojama perkelti į baudžiamuosius kodeksus taip formuojant baudžiamąją politiką, aptariant tiek baudžiamojo proceso problemas, tiek tarptautinius šių nusikaltimų teisinius aspektus[26]. Kita svarbi Europos Tarybos rekomendacija buvo priimta 1995 m. Joje pažymima, kad didėja rizika, jog elektroninės sistemos ir elektroninė informacija gali būti naudojama nusikalstamoje veikloje, kad valstybių narių baudžiamojo proceso teisė nesuteikia reikiamų galių ieškoti bei rinkti įrodymų elektroninėse sistemose. Atkreipiamas dėmesys, kad potencialiai egzistuoja rizika, jog valstybės nesugebės tinkamai ir efektyviai teikti teisinę pagalbą, kai bus prašoma bendradarbiavimo renkant įrodymus elektroninėse informacinėse sistemose (toliau – IS). Dėl šių priežasčių, rekomendacijos buvo skirtos baudžiamojo proceso problemoms, teikiamos gairės procesinių prievartos priemonių atžvilgiu (krata ir areštas, techninis sekimas), taip pat akcentuojant darnaus tarptautinio bendradarbiavimo svarbą renkant duomenis, nurodant, jog pravartu ir reikalinga įsteigti specialius padalinius, kurie būtų paruošti atitinkamai dirbti su informacinėmis technologijomis atliekant ikiteisminius tyrimus[27]. Tai buvo vieni iš pirmųjų žingsnių tarptautiniu mastu siekiant koordinuoti įstatymų leidybą bei teisėsaugos institucijų darbą kompiuterinių nusikaltimų srityje. Tačiau bene didžiausiu Europos Tarybos pasiekimu šioje srityje yra laikoma Europos Tarybos Konvencija dėl elektroninių nusikaltimų[28] (toliau – Budapešto konvencija). Ją ratifikavo 51 valstybė, tarp kurių 10 valstybių nėra Europos Tarybos narės (pavyzdžiui, Australija, Kanada, Dominykos Respublika, Izraelis, Japonija, Mauritanija, Panama, Senegalas, Šri Lanka bei JAV)[29].

Savo ruožtu pirmoji tarptautinė organizacija, atkreipusi dėmesį į kompiuterinius nusikaltimus, buvo Interpolas, kai 1979 m. Paryžiuje vykusioje konferencijoje, pristatymo

[26] 1989 m. rugsėjo 13 d. Europos Tarybos Ministrų komiteto rekomendacija valstybėms narėms Nr. R(89) 9 dėl su kompiuteriais susijusių nusikaltimų ir Europos Tarybos Europos nusikalstamumo problemų komiteto galutinė atskaita. (Recommendation No. R (89) 9 on computer-related crime and final report of the European Committee on Crime Problems). Strasbūras: Publishing and Documentation Service, 1990 [interaktyvus; 2017 m. sausio 3 d.]. Prieiga per internetą: <http://www.oas.org/juridico/english/89-9&final%20report.pdf>.

[27] 1995 m. rugsėjo 11 d. Europos Tarybos Ministrų komiteto rekomendacija valstybėms narėms Nr. R(95) 13 dėl baudžiamojo proceso teisės problemų, susijusių su informacinėmis technologijomis [interaktyvus; žiūrėta 2017 m. sausio 3 d.]. Prieiga per internetą: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804f6e76>.

[28] 2001 m. lapkričio 23 d. Konvencija dėl elektroninių nusikaltimų. *Valstybės žinios*, 2004, Nr. 36-1188.

[29] 2001 m. lapkričio 23 d. Konvencijos dėl elektroninių nusikaltimų pasirašymo ir ratifikavimo lentelė [interaktyvus; žiūrėta 2017 m. sausio 3 d.]. Prieiga per internetą: <http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures>.

metu pabrėžė: „Kompiuterinių nusikaltimų prigimtis yra tarptautinė dėl stabilaus telefonų, satelitų ir kt. priemonių komunikacijų tarp skirtingų šalių augimo. Tarptautinės organizacijos, tokios kaip Interpolas, turėtų šiam aspektui skirti daugiau dėmesio“[30]. Interpolas nagrinėdamas šiuos nusikaltimus rinko apie juos informaciją, atlikinėjo apklausas. Jau 1981 m. gruodžio 7–11 d., Paryžiuje, buvo surengtas pirmasis Interpolo kompiuterinių nusikaltimų pratybų seminaras tyrėjams, kuriame dalyvavo 66 delegatai iš 26 valstybių[31]. 1998 m. taip pat vadinamųjų „G-8“ valstybių[32] grupės transnacionalinio organizuoto nusikalstamumo vyriausiųjų ekspertų aukštųjų technologijų pogrupis įkūrė specialistų tinklą, padedantį tirti aukštųjų technologijų nusikaltimus. „G-8“ grupė taip pat išryškino principus, kuriais turėtų vadovautis skirtingų valstybių teisėsaugos institucijos tarpusavyje bendradarbiaujant. Šie principai numatė galimybę vienai valstybei reikalauti, jog tam tikra kompiuterių sistemos informacija, esanti kitoje valstybėje, būtų išsaugota, pasisakyta, dėl to, jog valstybės turėtų suteikti prieigą prie tam tikros tyrimui svarbios informacijos, kaip galima greičiau nagrinėti teisinės pagalbos prašymus[33].

Apibendrinant aptartus kibernetinių nusikaltimų raidos aspektus, matoma, kad šie nusikaltimai nėra senas reiškinys. Tačiau kintant gyvenimo būdui, sparčiai vystantis informacinėms technologijoms ir jų panaudojimui kasdieniame gyvenime įgaunant vis didesniam pagreičiui, įtaka ir jais padaroma žala nuolat augo. Nepaisant to, matoma, jog teisinis atsakas šiai nusikaltimų rūšiai atsirado pakankamai anksti. Pažymėtina, kad ganėtinai anksti įžvelgta ir bendradarbiavimo nauda, pradėti koordinuoti valstybių teisėsaugos tarpusavio veiksmai. Tačiau vertinant D. Wall teiginius, jog nauja technologijų karta naudojant bevielį ryšį, atsirandant vis daugiau išmaniųjų technologijų, vėl sudarys sąlygas naujoms kibernetinių nusikaltimų galimybėms, galima daryti prielaidas, jog teisinis reglamentavimas turės nuolatos adaptuotis ir kaip galima sparčiau keistis siekiant efektyviai veikti prieš kibernetinių nusikaltimų reiškinį.

[30] SCHJOLBERG, S. *The history of cybercrime – 1976-2014*. Norderstedt: Books on demand, 2014, p. 33–34.
[31] *Ibid.*
[32] Jas sudaro Prancūzija, JAV, Jungtinė Karalystė, Rusija, Vokietija, Japonija, Italija, Vokietija. Žiūrėti: <http://www.g8.utoronto.ca/g.html>.
[33] SCHJOLBERG, S. The history of global harmonization on cybercrime legislation – the road to Geneva [interaktyvus; žiūrėta 2017 m. sausio 1 d.]. Prieiga per internetą: <http://www.cybercrimelaw.net/documents/cybercrime_history.pdf>.

1.2. Kibernetinių nusikaltimų samprata ir rūšys

1.2.1. Kibernetinių nusikaltimų fenomenas bei problematika

Informacinių technologijų naudojimas nusikaltimams daryti yra tikras iššūkis valstybei bei teisėsaugos institucijoms. Šį iššūkį sudaro keletas priežasčių. Pirmoji – sunkumai tiriant šias nusikalstamas veikas. Tyrėjai pradėjo susidurti su įtaisais, nežinodami, kokie jų veikimo principai, kaip derėtų išsaugoti tyrimui svarbią informaciją. Be to, tiriant duomenų sistemas ar kompiuterius, egzistuoja galimybė gauti duomenis, kurie nepatenka į tyrimo ribas[34]. F. L. Street taip pat pažymi, kad dauguma nusikaltėlių niekada fiziškai nėra atsidūrę nusikaltimo vietoje, technologijos leidžia komunikuoti, išlikti anonimiškam, kompiuteriniai įrašai gali būti sunaikinti, nepaliekant jokių nusikaltimų pėdsakų, dažnu atveju nėra jokio ryšio tarp kaltininko ir aukos[35]. Antroji t. y. šių nusikaltimų banga sukėlė suvokimą, jog egzistuojantis teisinis reguliavimas nesugebės būti pritaikytas kompiuterizuotoms sistemoms. Pavyzdžiui, *„I love you“* viruso, kuris 2000 m. sukėlė didelę žalą pasauliniu mastu, kūrėjas negalėjo būti patrauktas baudžiamojon atsakomybėn, kadangi Filipinuose, šalyje, iš kur kaltininkas buvo kilęs, tokia veika nebuvo pripažinta nusikalstama. Todėl kaltinimai tebuvo galimo pažeidimo interpretacija, kurių, žinoma, nepakako nuteisti viruso kūrėjams. Įdomu tai, kad po šio incidento Filipinuose, įstatymų leidėjas pakoregavo galiojusius teisės aktus[36]. Galiausiai trečioji P. Kleve, R. D. Mulder, K. van Noortwijk įvardijama problema – interneto suteikiamos galimybės, kurios lemia kibernetinių nusikaltimų beribiškumą ir globalizacija. Internetas yra tapęs informacinės visuomenės ekvivalentu, prisijungimas prie interneto tolygu prisijungimui prie šios visuomenės. Tai visuomenė, kuri nėra apribota valstybių sienomis ar kitokiais barjerais. Informacinės technologijos galimybę, dalyvauti įvykiuose be būtinybės keliauti fiziškai, paverčia realybe. Atitinkami veiksmai momentaliai sukelia pasekmes bet kuriame pasaulio krašte. Taigi, tai baudžiamosios teisės atžvilgiu kelia ir jurisdikcijos problemą[37]. Šią problemą gerai iliustruoja R. C. Griffin straipsnyje pateikiama JAV byla, kurioje 2000 m. rusų įsilaužėliai įsibrovė ir pagrobė iš vienos JAV kompanijos duomenis, kurie nusakė mainų sandorio slaptas detales, ir grasino juos paviešinti. Tarp Rusijos ir JAV nebuvo sudaryta jokia kibernetinių nusikaltimų atžvilgiu galiojanti ekstradicijos sutartis. Vyraujant tokiai nebaudžiamumo galimybei, įsilaužėliai

[34] KLEVE, P., *et al*. The definition of ICT crime. *Computer law & security review*, 2011, Vol. 27, p. 162–167.
[35] STREET, F. L. Law of the Internet. Charlottesville: Lexis law publishing, 1998, p. 561.
[36] KLEVE, P., *et al*. The definition of ICT crime. *Computer law & security review*, 2011, Vol. 27, p. 162–167.
[37] *Ibid.*

net nesistengė nuslėpti savo tapatybių[38]. Tačiau jurisdikcija nėra vienintelė problema susijusi su interneto beribiškumo galimybėmis. P. Kleve taip pat išskiria ir globalizaciją, kuri kaip terminas šiame kontekste vartojama platesne prasme, apibrėžiant laisvą pinigų, prekių, paslaugų, asmenų ar informacijos judėjimą, šiuo atveju išryškinanti skirtumus tarp teisinių sistemų, tautų kultūrų, bei skirtingų valstybių interesų. Be abejo, į tautų kultūros bei tradicijų skirtumus verta atsižvelgti ir kibernetinių nusikaltimų kontekste[39].

Visi šie paminėti iššūkiai, lėmė tai, jog atsirado poreikis išskirti kibernetinius nusikaltimus į atskirą grupę, kadangi šioms nusikalstamoms veikoms tirti būtinas specialių žinių bagažas. Siekiant atlikti tyrimą automatizuotoje aplinkoje, būtina suprasti, kaip ji veikia[40]. Informacijos sklaidos mastas bei greitis lemia tai, kad ankstesniuose tyrimuose naudoti būdai bei metodai neleis operatyviai bei tiksliai nustatyti duomenų, svarbių tyrimui, buvimo vietų, jų išgauti. Skirtingi ir pėdsakų susidarymo, jų slėpimo mechanizmai, pačios nusikalstamos veikos padarymo būdai. Todėl kibernetinių nusikaltimų išskyrimas į atskirą grupę turi ne tik mokslinę, bet ir praktinę reikšmę. Išskiriant nusikalstamas veikas į tam tikras grupes galima tikslingai rinkti apie jas statistiką. Teisėsaugos institucijos gali formuoti specialius skyrius ar padalinius, kurie specializuotųsi konkrečioje srityje, taptų ekspertais[41]. Ir šiuo metu tai jau yra daroma. Kibernetiniai nusikaltimai dėl savo specifiškų padarymo, atskleidimo, tyrimo ir prevencijos dėsningumų jau yra tapę nusikalstamų veikų tyrimo metodikos, kaip savarankiškos kriminalistikos mokslo dalies, tyrimo objektu[42]. Jau dabar yra keliami tikslai supaprastinti kompleksišką kibernetinių nusikaltimų tyrimą, įveikiant minėtus iššūkius, pateikiant tyrėjams tyrimo planavimo gaires[43].

Mokslinėse diskusijose netgi keliami klausimai, ar kibernetinius nusikaltimus būtų galima priskirti atskirai teisės disciplinai arba baudžiamosios teisės pošakiui? Tačiau nepaisant to, jog kai kurie šios srities tyrimo objektai turėjo reikšmės plėtojant teisinę doktriną, terminologiją ir sąvokas, pažymima, kad kibernetiniai nusikaltimai nėra charakterizuojami naujų išplėtotų teorijų, kurios būtų kuo nors skirtingos nuo tradicinių baudžiamosios teisės teorijų ar pagrindų. Juolab, kad specialūs terminai, naudojami

[38] GRIFFIN, R. C. Cybercrime. *Journal of International Commercial Law and Technology*, 2012, Vol. 7 (2), p. 136–153.
[39] KLEVE, P., *et al*. The definition of ICT crime. *Computer law & security review*, 2011, Vol. 27, p. 162–167.
[40] *Ibid*.
[41] SHINDER, D. L. *Scene of the Cybercrime. Computer forensics handbook.* Rockland: Syngress Publishing, Inc., 2002, p. 15.
[42] BILEVIČIŪTĖ, E., *et al. Kriminalistika. Taktika ir metodika*: Vadovėlis. Vilnius: Mykolo Romerio universitetas, 2013, p. 629–676.
[43] HUNTON, P. The growing phenomenon of crime and the internet: A cybercrime execution and analysis model. *Computer law & security review*, 2009, Vol. 25, p. 528–535.

kibernetiniuose nusikaltimuose, neįgyja skirtingos reikšmės nei baudžiamosios teisės kontekste, nei juos naudojant civilinės teisės ar kitos teisės srities kontekste[44]. Autoriai taip pat pažymi, kad kibernetinių nusikaltimų nebūtų galima išskirti į atskirą baudžiamosios teisės pošakį, kadangi sritys, kurias apima šie nusikaltimai, yra pernelyg įvairios. Jie teigia, kad galima tik viena išvada, jog tai nusikalstamos veikos, kaip priešingas baudžiamajam įstatymui reiškinys, susijusios su kompiuteriais ir nieko daugiau[45].

Tačiau čia ir kyla esminis klausimas – kas yra laikoma kibernetiniais nusikaltimais? Kokias nusikalstamas veikas šie kibernetiniai nusikaltimai apima?

Žinoma, dauguma numano, kad kibernetiniai nusikaltimai egzistuoja, nujaučia, ką būtų galima laikyti kibernetiniu nusikaltimu, ko – ne, tačiau nėra visuotinai apibendrinančios sąvokos ir sampratos, kas iš tikrųjų tai yra. Tam, kad būtų galima toliau nagrinėti šią nusikalstamų veikų sritį, yra būtinas supratimas, kas yra kibernetiniai nusikaltimai. Tam tikrais atvejais, konsensuso paieškos dėl vieningo apibrėžimo stringa, net nesutariant dėl kompiuterinių nusikaltimų prigimties[46].

Antai P. Grabosky tvirtina, kad kibernetiniai nusikaltimai tėra tiesiog seni nusikaltimai padaryti naujais būdais: „virtualus nusikalstamumas tai tik senas vynas naujuose buteliuose“[47]. Autorius pažymi, jog motyvai, kuriais veikiama, nėra nauji – technologijos gali kisti greitai, tačiau žmogaus prigimtis nekinta[48]. Šią idėją palaiko ir S. W. Brenner, teigdama, kad kibernetinius nusikaltimus nuo „tradicinių“ nusikaltimų skiria tik įrankis t. y. vietoj ginklo – naudojamas kompiuteris. Autorė, nurodo, kad net grynoje kompiuterinėje atakoje, tokioje kaip DoS (angl. *Denial of System*) galima įžvelgti „tradicinį“ nusikaltimą, kadangi DoS atakos dažnai yra naudojamos siekiant išgauti pinigų – kaltininkai atakuoja tinklalapį ar duomenų sistemą, taip sustabdo šių veiklą ir siūlydami apsaugą nuo tokių atakų, reikalauja pinigų. O tai jau atitinka turto prievartavimą, kaip seniai žinomą nusikaltimą. Žinoma, yra ir priešingų nuomonių, kaip pavyzdžiui, M. Yar, kuris kompiuterinius nusikaltimus laiko visiškai nauju reiškiniu, kadangi kibernetinė erdvė sudaro galimybę beveik akimirksniu tarp dviejų dalyvių sukurti sąveiką. Kibernetinė erdvė sugriauna atstumo ir laiko barjerus, sukuria galimybę kontaktuoti su neribotu kiekiu žmonių, sudaro prielaidas anonimiškumui bei tapatybės

[44] KLEVE, P., *et al*. The definition of ICT crime. *Computer law & security review*, 2011, Vol. 27, p. 162–167.
[45] *Ibid.*
[46] SIMION, R. Cybercrime and its challenges between reality and fiction. Where do we actually stand? *The Criminology, Victimology and Security Review*, 2010, Vol. 4, Issue 1, p. 296–312.
[47] GRABOSKY, P. N. Virtual Criminality: old wine in new bottles? *Social & legal studies*, 2001, Vol. 10(2), p. 243–249.
[48] *Ibid.*

keičiamumui. Tai sukuria pagrindą naujoms nusikalstamoms veikos formoms bei modeliams[49].

Ypatingai paini tendencija yra ta, kad kompiuteriniais nusikaltimais yra vadinamos, bet kokios nusikalstamos veikos, kurios turi nors menkiausią ryšį su kompiuteriais ar informacinėmis technologijomis[50]. Todėl globaliai įsigalėjęs įstatymų leidėjų, teisėsaugos institucijų tikėjimas ir įsivaizdavimo „žinau, kai tai pamatau“[51] naudojimas, kalbant apie kibernetinius nusikaltimus, yra daugiau aklas vadovavimasis nuojauta, geriausiu atveju, vidiniu supratimu, kas tai per reiškinys, tačiau taip ir neišgryninat specifinių šios nusikaltimų rūšies požymių, leidžiančių nusakyti kibernetinių nusikaltimų sąvoką. Literatūroje vis dar pabrėžiama, kad elektroninio nusikaltimo samprata nėra išsamiai analizuota[52]. Stinga aiškiai apibrėžtų atskaitos taškų, kuriais remiantis būtų galima sudaryti konkrečią kibernetinių nusikaltimų sąvoką.

Siekiant atskleisti bei suformuoti konkrečią sąvoką, toliau bus nagrinėjami autorių pateikiami apibrėžimai, kai kurios kibernetinių nusikaltimų klasifikacijos bei šių nusikaltimų rūšys, kurios priskirtos prie minėtų nusikalstamų veikų kategorijos.

1.2.2. Kibernetinių nusikaltimų sampratos bei klasifikacijų analizė

Kaip jau buvo minėta, D. Parker, vienas pirmųjų, tyrinėjęs kompiuterinius nusikaltimus, pažymėjo, kad kompiuteriniai nusikaltimai gali būti suprantami keliomis prasmėmis. Pirmoji autoriaus išskirta prasmė – supratimas, jog kompiuteriniai nusikaltimai yra ekonominio pobūdžio nusikaltimų (angl. *white-collar crime*) porūšis, kadangi dažnu atveju būtent kompiuteris yra naudojamas atliekant finansinio pobūdžio veiksmus. Antroji prasmė, kuri žymiai platesnė už pirmąją – kompiuteriniu nusikaltimu laikytinos tos veikos, kurios turi sąryšį su kompiuteriu. D. Parker teigia, kad bet kokia neteisėta veika, grįsta supratimu apie kompiuterines technologijas, gali būti priskirta su kompiuteriu susijusių nusikaltimų kategorijai, pavyzdžiui, nusikaltimai, kuriais naikinami kompiuteriai ar jų turinys, kartu kelia riziką žmogaus gyvybei (autorius nurodo pavyzdį, kai žmogaus sveikata ar gerovė priklauso nuo tinkamo kompiuterių funkcionavimo). Trečioji – piktnaudžiavimas kompiuteriu, autoriaus apibrėžiamas, kaip tyčinis veiksmas, apimantis naudojimąsi kompiuteriu, kai kaltininkas gauna kažkokios naudos, o auka patiria nuostolius. D. Parker nurodo, kad tokios veikos nebūtinai gali būti uždraustos

[49] YAR, M. *Cybercrime and Society*. London: SAGE Publications Inc., 2013, p. 10–12.
[50] WALL, D. What are cybercrimes? *Criminal Justice Matters*, 2008, Vol. 58:1, p. 20–21.
[51] SHINDER, D. L. *Scene of the Cybercrime. Computer forensics handbook.* Rockland: Syngress Publishing, Inc., 2002, p. 4.
[52] ŠTITILIS, D., *et al. Interneto ir technologijų teisė*. Vilnius: Mykolo Romerio universitetas, 2016, p. 402–403.

baudžiamuoju įstatymu. Deja, autorius nepateikia šios kategorijos pavyzdžių, dėl to nėra aišku, kuo pastaroji skiriasi nuo minėtosios antrosios prasmės, kuri apima apskritai veikas susijusias su kompiuteriu. Galiausiai D. Parker pateikė apibendrintą kompiuterinių nusikaltimų apibrėžimą: „tai visos tyčinės veikos, vienaip ar kitaip susijusios su kompiuteriais, dėl kurių nukentėjusysis patyrė ar galėjo patirti žalą, o nusikaltimo subjektas turėjo ar galėjo gauti iš to naudos[53]“.

Pateikiamas apibrėžimas akivaizdžiai yra pernelyg platus, kadangi jame egzistuoja nemažai vertinamųjų kriterijų, kurių turinys yra nuolatos kintantis ir labai įvairus. Tarkime, dalis apibrėžime, kurioje teigiama, kad tai „visos veikos <...> vienaip ar kitaip susijusios“ suponuoja absoliučiai bet kokių nusikalstamų veikų, bet kokį sąryšį su kompiuteriais ir tokią dviejų komponentų išdavą galėsime vadinti kompiuteriniu nusikaltimu. Galima tai iliustruoti šiuo pavyzdžiu – neapykantos kurstymas tautybės, rasės, lyties ar kitais pagrindais pasitelkiant kompiuterį. Diskriminacijos kurstymas netaps kompiuteriniu nusikaltimu tik dėl to, kad šio nusikaltimo objektyviąją pusę galima realizuoti pasinaudojant kompiuteriu. Taigi tokia plati apibrėžimo traktuotė palieka daug erdvės įvairioms interpretacijoms, todėl iš esmės neatlieka detalizuojančios savo funkcijos. Taip pat neapibrėžtos žalos bei gaunamos naudos sąvokos. Daroma išvada, jog tokia sąvoka ydinga dėl pernelyg plačios traktuotės, kuri vietoje specifinės nusikaltimų rūšies (kompiuterinių nusikaltimų) apima bene visą priešingą teisei elgesį. Šiame apibrėžime vis dėlto galima įžvelgti tai, jog esminis šios formuluotės akcentas yra kompiuteris, kompiuterinės technologijos – tie nusikalstami veiksmai, kurie turi sąryšį su kompiuterinėmis technologijomis ar reikalauja žinių iš šios srities, gali būti priskirti kompiuteriniams nusikaltimams. Kadangi pats kompiuteris šiuo atveju, D. Parkerio teigimu, yra centrinė ašis aplink, kurią sukasi kompiuterinių nusikaltimų fenomenas, jis pateikė tokią klasifikaciją, kuri nurodo, jog visuose žinomuose kompiuteriniuose nusikaltimuose kompiuteris atlieka vieną iš keturių vaidmenų:

1) Objektas – naikinami kompiuteriai, duomenys ar programos, taip pat pagalbiniai kompiuterių įrenginiai (tokie kaip oro aušinimo sistema, elektros tiekimas t. y. tokie įrenginiai, kurie leidžia kompiuteriams funkcionuoti).
2) Kategorija – kompiuteris gali būti nusikaltimo vieta ar aplinka, kaip nusikalstamos veikos priežastis, unikalios formos žalai kilti. Atliktas sukčiavimas pakeitus banko paskyroje esantį balansą kaip finansinius duomenis laikomus kompiuteryje, leidžia tokį nusikaltimą priskirti kompiuterių kategorijai.

[53] PARKER D. B. Computer Crime. Criminal Justice Resource Manual [interaktyvus; žiūrėta 2017 m. sausio 25 d.]. Prieiga per internetą: <https://www.ncjrs.gov/pdffiles1/Digitization/118214NCJRS.pdf>.

3) Įrankis (instrumentas) – kai kurie metodai tiek sudėtingi, jog jiems atlikti būtinas kompiuteris kaip įrankis, pavyzdžiui, kompiuteris gali būti naudojamas automatiškai skanuoti telefoninius kodus, tam, kad vėliau būtų sudaryta prielaida neautorizuotai prisijungti prie telefonų sistemos.
4) Simbolis – kompiuteris gali būti naudojamas kaip simbolis gąsdinimui arba apgaulei. Kaip pavyzdį D. Parkeris nurodo, kad tai galėtų įtraukti tuos atvejus, kai organizacija melagingai teigia naudojanti neegzistuojančius kompiuterius.

Ši pateikta D. Parkerio klasifikacija turi trūkumų ir gali būti kritikuojama. Štai ketvirtosios grupės išskyrimas labai abejotinas. Ar tikrai pakanka to, kad kompiuteris būtų tik kaip nusikalstamos veikos simbolis, trumpai tariant, smulkus fragmentas panaudotas neteisėtoje veikoje? Tokio smulkaus fragmento sureikšminimas iš esmės nulemia tai, jog absoliučiai bet kokia neteisėta veika, galėtų būti priskirta kompiuterinių nusikaltimų kategorijai. Tokiu atveju galima ir kritikuoti paties kompiuterio sąryšį su nusikalstama veika – jei jis nebuvo naudotas kaip įrankis, ar jis nebuvo nusikalstamos veikos dalyku – tai kokią reikšmę jis turės baudžiamojoje byloje, baudžiamojo proceso metu? Panašiai ne itin suprantama yra antroji grupė – kompiuteris, kaip nusikalstamos veikos kategorija. Pagal pateiktą autoriaus paaiškinimą, galima suprasti, kad kompiuteris kaip kategorija, atlieka nusikalstamų veikų skirstymo pagal rūšis vaidmenį. Tačiau, kokia tokios grupės išskyrimo nauda ar reikšmė, lieka visiškai neaišku. Šią grupę kritikuoja ir kiti autoriai[54].

Tokia kompiuterinių nusikaltimų samprata remiasi ir kiti autoriai. Tiesa, kompiuterio rolė yra šiek tiek pakoreguota. Štai G. E. Higgins siūlo kompiuterinius nusikaltimus išskirti į tris kategorijas. Pirmoji – kuriuose kompiuteriai naudojami kaip įrankiai, instrumentai. Pavyzdžiui, kompiuteris kaip įrankis naudojamas nelegaliai atsisiųsti muziką, filmus ar tam tikrą programinę įrangą. Antroji – kuriuose kompiuteris yra nusikalstamos veikos objektas t. y. įsilaužėliai naudoja tam tikrus būdus, kuriais patenka į konkretų individualų kompiuterį, jo sistemą. Trečioji – nusikaltimai, kuriuose kompiuteris naudojamas kaip talpykla, saugykla. Kaip pavyzdys yra pateikiamas nelegalių pornografinio turinio duomenų arba nelegaliai gautų programų laikymas[55]. Tiesa, nors G. Higgins atsiribojo nuo kompiuterių kaip subjekto ir simbolio, trečioji pateikiama grupė taip pat neišskiria skirtingo kompiuterio vaidmens. Kompiuterio kaip talpyklos naudojimas iš esmės gali būti priskirtas kompiuterio kaip įrankio ar priemonės

[54] KLEVE, P., *et al*. The definition of ICT crime. *Computer law & security review*, 2011, Vol. 27, p. 162–167.
[55] HIGGINS, G. E. *Cybercrime. An introduction to an Emerging Phenomenon.* New York: McGraw-Hill, 2010, p. 1–3.

vaidmeniui t. y. pirmajam G. Higgins pogrupiui. Kai kur kibernetinių nusikaltimų apibrėžimas yra dar labiau siaurinamas paliekant iš esmės tik du vaidmenis: „kibernetinis nusikaltimas, tai nusikaltimas, kuris yra įgalintas kompiuterių arba nutaikytas į kompiuterius“[56].

Minėtų autorių pateiktos sąvokos bei sampratos vienareikšmiškai sieja kompiuterinius nusikaltimus su kompiuteriais. Belieka tik pakartoti, kad pasauliui įžengus į dvidešimt pirmąjį amžių, itin išplito interneto naudojimas. Atsižvelgiant į tai, kito ir mokslininkų pateikiamas kibernetinių nusikaltimų apibrėžimas, šiuos nusikaltimus susiejant ne tik su kompiuteriu, bet ir tinklo naudojimu. Antai N. Kshetri nurodo tokią sąvoką: „kibernetiniai nusikaltimai – tai nusikalstama veika, kurioje kompiuteriai ar kompiuterių tinklai yra pagrindinė, principinė priemonė padarant pažeidimą, priešingą įstatymams, taisyklėms ar nurodymams“[57]. Kai kurie autoriai kibernetinius nusikaltimus susieja vien tik su kibernetine erdve, paliekant kompiuterius nuošalyje, pavyzdžiui J. J. Rho nurodo, kad: „kibernetinis nusikaltimas – tai visa neteisėta veika padaryta privataus individo kibernetinėje erdvėje“[58].

Tačiau pastebėtina kad, visi šie pateikti apibrėžimai susiejant kompiuterinius nusikaltimus su kompiuteriais bei jų tinklais išlieka tokie pat platūs ir nekonkretūs kaip D. Parker pateiktas apibrėžimas. Tiesą pasakius, nemažai autorių netgi priešingai – tvirtina, kad neverta apsiriboti bandymais apčiuopti kibernetinius nusikaltimus kaip išskirtą fenomeną, bet dera šiam apibrėžimui priskirti platų spektrą neteisėtų veikų, kurių bendras vardiklis būtų kompiuterių tinklai, informacinės bei komunikacijų technologijos[59].

Štai G. Urbas tvirtina, kad elektroniniai nusikaltimai turi apimti neteisėtus veiksmus naudojant kompiuterį, kaip neteisėtą prieigą prie kompiuterinės sistemos, neteisėtą kompiuterinės informacijos perėmimą, neteisėto turinio medžiagos siuntimą, atliekant sukčiavimą ir kitas nusikalstamas veikas[60]. N. Kshetri teigia, kad prie kibernetinių nusikaltimų priskirtinos ir tokios veikos kaip kibernetinė vagystė, kibernetinis turto

[56] WILSON, C. Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. CRS report for congress [interaktyvus; žiūrėta 2017 m. vasario 1 d.]. Prieiga per internetą: <https://fas.org/sgp/crs/terror/RL32114.pdf>.
[57] KSHETRI, N. Positive externality, increasing returns, and the rise in cybercrimes. *Communications of the ACM*, 2009, Vol. 52, Issue 12, p. 141–144.
[58] RHO, J. J. Blackbeards of the Twenty-First Century: Holding Cybercriminals Liable under the Alien Tort Statute. *Chicago Journal of International Law*, 2007, Vol. 7, Issue 2, p. 695–718.
[59] YAR, M. *Cybercrime and society*. London: SAGE Publications Inc., 2013, p. 9.
[60] URBAS G., Cybercrime Legislation in the Asia-Pacific Region [interaktyvus; žiūrėta 2017 m. vasario 1 d.]. Prieiga per internetą: <https://www.google.lt/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwjEzMTJ5e7RAhXqHpoKHZ_iDgEQFggcMAE&url=http%3A%2F%2Fwww.ibrarian.net%2Fnavon%2Fpaper%2FCybercrime_Legislation_in_the_Asia_Pacific_Region.pdf%3Fpaperid%3D3127647&usg=AFQjCNGqkQ9XZ09aHw7bl9EGAvdx7Z7m4Q>.

prievartavimas[61]. J. Clough tvirtina, kad tai ne vieno tipo pažeidimai, bet jų įvairovė, susijusi su technologijos naudojimu[62]. Kai kurie autoriai priskiria kompiuterinius nusikaltimus šioms kategorijoms: paslaugų vagystė, kuriose autorizuotas asmuo naudoja kompiuterį tikslams, kuriems jis neturi leidimo, arba neturintis leidimo asmuo įsiskverbia į sistemą; informacijos, laikomos kompiuteryje, panaudojimas asmeniniam pelnui išgauti; kompiuterių, kurie atlieka įvairias finansines operacijas, naudojimas siekiant išgauti turtą; ir turto vagystė per kompiuterį asmeniniams tikslams ar pelno gavimas[63].

D. L. Shinder išskaido kibernetinius nusikaltimus į dvi plačias kategorijas – į smurtinius ar potencialiai smurtinius nusikaltimus bei į nesmurtinius nusikaltimus[64]. Smurtinių arba potencialiai smurtinių kibernetinių nusikaltimų, kuriais aukoms keliama fizinė grėsmė, kategoriją D. L. Shinder suskaido į keturis pogrupius. Pirmasis, kibernetinis terorizmas – teroro aktas atliktas, planuotas ar koordinuotas kibernetinėje erdvėje t. y. per kompiuterių tinklus. Į šį pogrupį patenka ir el. laiškų naudojimas komunikacijai, taip pat naujų narių verbavimas. Autorės nuomone, tai galėtų pasireikšti ir elektroninių duomenų srauto sutrikdymu, pavyzdžiui, sutrikdžius oro uosto kompiuterių sistemą ir taip sukeliant lėktuvų aviakatastrofą. Antroji, grasinimas – tarkim atliekant el. paštu, grasinama sutrikdyti sveikatą, atimti gyvybę ir pan. Trečioji, kibernetinis persekiojimas – kaip elektroninio priekabiavimo, įžeidinėjimo forma, naudojama įbauginti auką, leidžiant suprasti, kad visa gali peraugti į žiaurų elgesį realiame gyvenime. Ketvirtoji, vaikų pornografija – D. L. Shinder nuomone, apima daug aspektų t. y. žmones, kurie kuria pornografinio turinio medžiagą išnaudojant vaikus, asmenis, kurie platina tokią medžiagą ir tuos, kuriuos ta medžiaga pasiekia. Tuo atveju, kai naudojamas internetas ar kitoks tinklas – tai tampa kibernetiniu nusikaltimu. Pabrėžiama, jog vaikų pornografija priskiriama prie smurtinių kibernetinių nusikaltimų, nors tiesioginio kontakto, pvz., su asmeniu platinančiu tokią medžiagą, gali ir nebūti, kadangi tokiai medžiagai išgauti bet kokiu atveju reikalingas seksualinis išnaudojimas[65]. Prie nesmurtinių kibernetinių nusikaltimų, kuriais auka nėra paveikiama jokiu tiesioginiu ar netiesioginiu fiziniu kontaktu, kategorijos priskiriami penki pogrupiai[66]. Pirmasis, kibernetinis ribų pažeidimas – neteisėtai prisijungiant prie kompiuterio ar tinklų,

[61] KSHETRI, N. Positive externality, increasing returns, and the rise in cybercrimes. *Communications of the ACM*, 2009, Vol. 52, Issue 12, p. 141–144.
[62] CLOUGH, J. Cybercrime. *Commonwealth law bulletin*, 2011, Vol. 37, Issue 4, p. 671–680.
[63] White-Collar crime: Second Annual Survey of Law: Substantive Crimes. The American criminal law review. *American Bar Association, section of criminal just*, 1981, Vol. 2, p. 499–509.
[64] SHINDER, D. L. *Scene of the Cybercrime. Computer forensics handbook.* Rockland: Syngress Publishing, Inc., 2002, p. 18–33.
[65] *Ibid.*
[66] *Ibid.*

nenaudojant ar pažeidžiant juose esančių duomenų vientisumą. Antrasis, kibernetinė vagystė – naudojamas kompiuteris ar internetas pagrobti informaciją, pinigus ir kitas vertybes. Į šį pogrupį patenka tokios veikos kaip lėšų pasisavinimas, kai turima teisėta prieiga prie kompiuterinės sistemos, kuria atliekamos finansinės operacijos, komercinis šnipinėjimas, plagiavimas, piratavimas, tapatybės vagystė, domenų vardų sistemos pamėgdžiojimas ir pan. D. L. Shinder pažymi, kad šis pogrupis labai panašus į kibernetinę apgaulę, kuri apima neteisėtą pinigų pasisavinimą ir kt. Trečiasis – kibernetinis sukčiavimas. Įdomu ir tai, kad pati autorė pažymi, jog kibernetinė apgaulė apima tokius metodus ir schemas, kurie buvo naudoti gerokai prieš atsirandant kompiuteriams bei tinklams. Kaip pavyzdys pateikiamas atvejis, kai kaltininkas el. paštu nusiunčia prašymą „aukoti“ pinigų našlaičiams ir pan. Ketvirtasis – naikinantys kibernetiniai nusikaltimai. Šie, autorės skirstymu, nusikaltimai sutrikdo tinklų sistemų darbą, pažeidžia ar sunaikina duomenis, vietoje jų pasisavinimo. Tai nusikalstamos veikos, kai įsilaužiama į tinklą, internetinį puslapį, platinant virusus, kirminus, atliekant sistemos sutrikdymo (DoS) ataką. Penktoji – kiti nesmurtiniai kibernetiniai nusikaltimai. Šie apima prostitucijos reklamavimą, azartinių žaidimų lošimą internete, narkotinių medžiagų pardavimą internete, kibernetinį neteisėtai įgytų pinigų legalizavimą (arba „pinigų plovimas“), kibernetinę kontrabandą.

Kai kurie autoriai apskritai tokias veikas kaip įsilaužimas į informacines sistemas, virusų ar kitos kenkėjiškos programinės įrangos naudojimą priskiria prie internetinio sukčiavimo, kuris taip pat apima ir tapatybės vagystę, interaktyvų su mokėjimais susijusį sukčiavimą, vartotojų apgaulę pasitelkiant į internetą ir kt[67].

Galiausiai Budapešto konvencija dėl elektroninių nusikaltimų pateikia šias keturias kategorijas:

1. nusikaltimus kompiuterinių duomenų ir sistemų konfidencialumui, vientisumui ir prieinamumui:
    a. neteisėta prieiga – neteisėta prieiga prie visos kompiuterinės sistemos arba jos dalies;
    b. neteisėta perimtis – neteisėtas neviešo kompiuterinių duomenų perdavimas į kompiuterinę sistemą, iš jos ir jos viduje perimtis techninėmis priemonėmis, taip pat emisijos iš kompiuterinės sistemos, perduodančios tokius kompiuterinius duomenis, perimtis;

[67] WELLS, T. J. *et al. Internet fraud casebook. The world wide web of deceit*. Hoboken, New Jersey: John Wiley & Sons, Inc., 2010, p. 5.

c. poveikis duomenims – neteisėtas kompiuterinių duomenų sugadinimas, sunaikinimas, apgadinimas, pakeitimas arba galimybės naudotis panaikinimas;
d. poveikis sistemai – neteisėtas didelis kompiuterinės sistemos darbo trukdymas įvedant, perduodant, sugadinant, sunaikinant, apgadinant, pakeičiant kompiuterinius duomenis arba panaikinant galimybe jais naudotis;
e. netinkamas įtaisų naudojimas – įtaisų, kompiuterinės programos, slaptažodžio, prieigos kodo ar panašių duomenų gaminimas, pardavimas, įsigijimas naudoti, įvežimas, platinimas arba kitoks galimybės naudotis suteikimas. Šie įtaisai, duomenys turi būti skirti daryti a–d punktuose paminėtoms veikoms.

2. Kompiuteriniai nusikaltimai – kompiuterinės klastotės (sąmoningas ir neteisėtas kompiuterių duomenų įvedimas, pakeitimas, sunaikinimas arba galimybės naudotis tokia informacija panaikinimas, kurių pasekmė yra neautentiški duomenys, turint tikslą, kad jie būtų laikomi autentiškais, ar jais būtų naudojamasi teisėtiems tikslams, nepriklausomai nuo to, ar šie duomenys yra tiesiogiai skaitomi ir suprantami), kompiuterinis sukčiavimas (sąmoningas, neteisėtas veiksmas sąlygojęs kito asmens nuosavybės praradimą įvedant, pakeičiant, sunaikinant kompiuterinius duomenis arba panaikinant galimybę naudotis tokiais duomenimis arba paveikiant kompiuterinės sistemos darbą nesąžiningai arba nedorai ketinant gauti neteisėtos ekonominės naudos sau arba kitam asmeniui);
3. Turinio nusikaltimai – nusikaltimai, susiję su vaikų pornografija t. y. pornografinio turinio produkcijos, kurioje atvaizduotas vaikas, gaminimas, siūlymas, platinimas, įsigijimas, laikymas kompiuterinėje sistemoje;
4. Nusikaltimai, susiję su autorių teisių ir gretutinių teisių pažeidimais.

Ar tikrai visos šios išvardintos nusikalstamos veikos priskirtinos kibernetiniams nusikaltimams? Verta paminėti, jog pati Budapešto konvencija susilaukė nemažai kritikos, dėl nusikaltimų, susijusių su autorinių teisių ir gretutinių teisių pažeidimais bei pornografinio turinio nusikaltimų priskyrimu kibernetiniams nusikaltimams[68]. Pastebėtina, kad nors ir kalbant apie kompiuterinius nusikaltimus, dažnu atveju apie juos kalbama plačiąja prasme, mokslininkai pažymi, kad tikrieji kibernetiniai nusikaltimai yra padaryti kompiuterinių duomenų ir sistemų konfidencialumui, vientisumui ir prieinamumui, būtent tuos, kuriuos apibūdina Budapešto konvencijos 2–6 straipsniai t. y. pirmoji minėta kategorija (pvz., I. Walden[69], D. Wall[70]). Taigi, kuo gi skiriasi šie

[68] SCHJOLBERG, S. The history of global harmonization on cybercrime legislation – the road to Gevena [interaktyvus; žiūrėta 2017 m. sausio 1 d.]. Prieiga per internetą: <http://www.cybercrimelaw.net/documents/cybercrime_history.pdf>.
[69] WALDEN, I. *Computer Crimes and Digital Investigation*. Oxford: Oxford university press, 2007, p. 24.

nusikaltimai nuo jau įvardintų sukčiavimų pasinaudojant kompiuteriu, kibernetinio persekiojimo arba šmeižto, neleistino turinio informacijos platinimo ir kitų nusikalstamų veikų, kurių padarymui yra pasitelkiamas kompiuteris, kompiuterių tinklas ar internetas? Šiam klausimui atsakyti, galima išskirti tris bruožus, požymius, kurie manytina, geriausiai atspindi „grynuosius“ kibernetinius nusikaltimus, taip pat būtinus tikslios sąvokos formavimui.

1.2.3. Kibernetinių nusikaltimų požymiai

1. Kibernetinė erdvė

Turbūt vienas iš labiausiai kibernetinius nusikaltimus išskiriančių požymių nuo „tradicinių“ nusikalstamų veikų yra kibernetinė erdvė. Įdomu tai, kad šis terminas kilo ne iš kompiuterių mokslo ar inžinerijos, bet iš W. Gibson parašytos mokslinės fantastikos novelės „Neuromantikas“ (angl. „*Neuromancer“*). Kaip teigiama, pats autorius, rašydamas mokslinės fantastikos kūrinį, vartodamas šį terminą, nevisiškai įžvelgė, kokią konkrečią semantinę prasmę šis žodis apėmė[71]. Šis terminas, kilęs iš mokslinės fantastikos srities, ne tik, kad tapo visuotinai vartojamas, tačiau įgavo ir juridinę prasmę, kadangi tapo naudojamas įstatymuose, kituose teisės aktuose. Šiandien kibernetinę erdvę galima suprasti keliomis prasmėmis: kaip techninį kompiuterių tinklą arba kaip virtualią aplinką. Techninis supratimas remiasi tuo, kad kompiuteriai, kaip atskiri vienetai, yra sujunti į globalų elektroninį kompiuterių tinklą (įskaitant internetą). Šiuo kibernetiniu erdvės supratimu remiasi M. Gercke, kuris kibernetinius nusikaltimus išimtinai sieja su jų padarymu tinkle, internete[72]. Atkreiptinas dėmesys, kad tokiu atveju, veikos, kaip virusų panaudojimas kompiuteryje, kuris nėra prijungtas prie interneto ar kitokio tinklo, iškristų iš M. Gercke siūlomo kibernetinės erdvės, tuo pačiu ir kibernetinių nusikaltimų, apibrėžimo, nors yra iš esmės pripažįstami tikraisiais kibernetiniais nusikaltimais. Tačiau, kaip ir minėta, kibernetinę erdvę galima suprasti ir kaip virtualią aplinką t. y. kibernetinį pasaulį, kuris būtų visiška priešingybė ir atsvara fiziniam, materialiniam pasauliui. Taip iš esmės kibernetine erdve yra laikomas ne tik internetas ir jo sukuriami informacijos duomenų keitimosi srautai, ryšiai tarp kelių kompiuterių, bet ir pavienio kompiuterio sukuriama skaitmenizuota aplinka. Tokia kibernetinės erdvės samprata įtvirtinta ir Lietuvos teisės aktuose. Lietuvos Respublikos kibernetinio saugumo įstatymo 2 straipsnio 3 dalyje kibernetinė erdvė yra apibrėžiama, kaip aplinka, kurioje pavieniuose

[70] WALL, D. What are cybercrimes? *Criminal Justice Matters,* 2008, Vol. 58:1, p. 20–21.
[71] JEWKES, Y.; YAR. M. *Handbook of Internet Crime.* New York: Routledge, 2011, p. 149–152.
[72] GERCKE, M. Understanding Cybercrime: Phenomena, challenges and legal response [interaktyvus; žiūrėta 2017 m. vasario 2 d.]. Prieiga per internetą: <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf>.

kompiuteriuose ar kitoje informacinėje ir ryšių technologijų įrangoje sukuriama elektroninė informacija ir (arba) perduodama per elektroninių ryšių tinklu sujungtus kompiuterius ar kitą informacinių ir ryšių technologijų įrangą[73]. Vadovaujantis šia įstatymo norma, manytina, jog kibernetinė erdvė turėtų būti suprantama plačiau nei teigia M. Gercke. Priešingu atveju nebūtų aišku, kokiems nusikaltimams tektų priskirti tas veikas, kurios taikosi į kompiuterius ar juose esančius duomenis, nors analogiškas atakas prieš kompiuterius, prijungtus prie tinklo, laikytumėme kibernetiniais nusikaltimais.

Aptarus, kas yra kibernetinė erdvė, derėtų pažymėti, kaip ji padeda atskirti tikrus kibernetinius nusikaltimus nuo netikrų. Šiuo momentu svarbu identifikuoti nusikalstamas veikas, kurios *naudoja* kibernetinę erdvę ir tas, kurios *priklauso* nuo kibernetinės erdvės. Pavyzdžiui, poveikis sistemai, kaip sąmoningas ir neteisėtas galimybės naudotis kompiuteriniais duomenimis panaikinimas gali pasireikšti DoS ataka. Savaime suprantama, DoS ataką galima atlikti tik kibernetinėje erdvėje. Panaikinus kibernetinę erdvę, nelieka ir neteisėto žalingo veikimo. Analogiškai tai taikytina, pavyzdžiui, ir neteisėtam kompiuterinių duomenų perimčiai, poveikiui. Visi kompiuteriniai virusai, skirti naikinti, keisti, nutekinti duomenis ar informaciją, netenka prasmės, kadangi nelieka terpės, kurioje jie veikia. To paties nebūtų galima pasakyti apie „tradicinius“ nusikaltimus, kurie tik *naudoja* kibernetinę erdvę. Pavyzdžiui, šmeižto skleidimas internete – tikrovės neatitinkanti informacija gali būti skelbiama tiek socialiniuose tinklalapiuose, tiek internetinėse svetainėse, tačiau panaikinus kibernetinę erdvę, savaime toks žalingas elgesys niekur nedingtų. Tokią informaciją, kuria būtų siekiama pažeminti arba paniekinti asmenį, būtų galima skleisti ir pasitelkiant kitas visuomenės informavimo priemones, pavyzdžiui, spaudą, televiziją. Žinoma, kibernetinėje erdvėje informacija sklinda gerokai sparčiau bei didesniu mastu, tačiau vien tik tai, jog kibernetinė erdvė didina nusikalstama veika padaromą žalą, sukeliamus neigiamus padarinius, nesudaro prielaidos šių nusikalstamų veikų priskirti kibernetinių nusikaltimų kategorijai. Dėl šios priežasties vaikų pornografija, taip pat D. L. Shinder priskiriamos net tokios veikos, kaip prostitucijos reklamavimas, azartinių žaidimų lošimas internete, narkotinių medžiagų pardavimas internete, kibernetinis neteisėtai įgytų pinigų legalizavimas, be abejonės neturėtų būti laikytinos kibernetiniais nusikaltimais. Šioms veikoms inkriminuoti ir baudžiamajai atsakomybei kilti nereikia naujų nusikalstamų veikų sudėčių. Ypatingai tokių veikų, kaip prostitucijos propagavimas, priskyrimas kibernetinių nusikaltimų kategorijai, yra absoliučiai nepagrįstas.

[73] Lietuvos Respublikos kibernetinio saugumo įstatymas. *Teisės aktų registras*, 2014, Nr. XII-1428.

Atkreiptinas dėmesys, kad ir Budapešto konvencijos 2–6 straipsniuose pateikiamos nusikalstamos veikos ne visais atvejais gali būti padarytos kibernetinėje erdvėje. Pavyzdžiui, neteisėtam poveikiui elektroniniams duomenims ištrinant juos kibernetinėje erdvėje prilyginamas materialiems objektams t. y. elektroninių duomenų laikmenoms padaromas fizinis poveikis, kuriuo sunaikinama tiek laikmena, tiek joje esantys elektroniniai duomenys[74]. Tarkime, slaptažodžio įgijimas gali pasireikšti nebūtinai jį išgaunant kibernetinėje erdvėje pasitelkiant kenkėjiškas programas, bet paperkant asmenį, kuris teisėtai disponuoja slaptažodžiais ar kitais prisijungimo duomenimis. Tokiu atveju nors ir nusikalstama veika nukreipta į elektroninius duomenis ar IS, yra prarandamas esminis kibernetinės erdvės elementas, dėl kurio skiriasi šių nusikaltimų tyrimo metodai, susiduriama su specifine problematika.

Remiantis tuo, kas išdėstyta, kibernetiniais nusikaltimais pripažintini tik tie nusikaltimai, kurie *priklauso* nuo kibernetinės erdvės egzistavimo. Visos kitos veikos laikytinos su kompiuteriais susijusios nusikalstamos veikos – savaime galinčios egzistuoti ir be kibernetinės erdvės, tačiau ją pasitelkiančios kaip alternatyvų objektyviosios pusės įgyvendinimo būdą.

2. Naudojimasis kompiuteriais ar kitomis informacinėmis technologijomis

Atrodytų, šis požymis jau buvo kritikuotas, teigiant, kad nusikaltimų padarymas vienaip ar kitaip pasitelkiant kompiuterį apima plačias kategorijas kitų nusikalstamų rūšių ir nebūtinai siejasi su kibernetiniais nusikaltimais. Tačiau čia yra reikalingas platesnis paaiškinimas, nurodant, dėl ko yra pasitelkiamas kompiuteris ir kuo kompiuterio naudojimas kibernetinių nusikaltimų atžvilgiu skiriasi nuo nusikaltimų susijusių su kompiuteriais.

Paminėtina, kad tam tikrais atvejais vien pirmojo išskirto požymio t. y. priklausomumo nuo kibernetinės erdvės nepakanka. Esti ribinių atvejų, kuriuos D. Wall įvardija kaip hibridinius nusikaltimus[75]. Vienas iš tokių pavyzdžių yra tapatybės vagystė. Antai kaltininkas naudoja vieną iš apgaulės formų, taip vadinamą slaptažodžio „žvejybą“ (angl. *phishing*). Šia tapatybės vagystės forma yra siekiama išvilioti konfidencialius duomenis, naudojant internetinius adresus, panašius į tikrą, egzistuojančios institucijos adresą. Standartinė šios apgaulės pasireiškimo schema būtų tokia – kaltininkas nusiunčia el. paštu aukai laišką, kuriame apsimeta tam tikros institucijos, įstaigos ar organizacijos

[74] 2001 m. lapkričio 8 d. Europos Tarybos Ministrų komiteto Konvencijos dėl kibernetinių nusikaltimų aiškinamasis pranešimas Nr. 185 (Explanatory Report to the Convection on Cybercrime No. 185, adopted on 8 November 2001 by the Committee of Ministers of the Council of Europe) [interaktyvus; žiūrėta 2017 m. vasario 15 d.]. Prieiga per internetą: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b>.

[75] WALL, D. What are cybercrimes? *Criminal Justice Matters,* 2008, Vol. 58:1, p. 20–21.

atstovu (pvz., banko), įtikina auką paspausti el. laiške esančią nuorodą, kuri nukreipia sukčiavimo auką į neva oficialų tos įstaigos tinklalapį. Auka, suklaidinta internetinio tinklalapio panašumo į tikrąjį analogą, dažnu atveju, nieko neįtardama suveda savo asmeninius prisijungimo ar kitus duomenis, kurie, savaime suprantama, patenka kaltininkams į rankas. Toks tapatybės vagystės būdas, lygiai taip pat priklauso nuo kibernetinės erdvės egzistavimo. Nėra kibernetinės erdvės – nėra ir „*phishing'o*“. Tačiau atkreiptinas dėmesys, kad priešingai nei kibernetinių nusikaltimų atveju, esminis tokios kompiuterinės apgaulės požymis išlieka veikimo būdas t. y. apgaulė, nepaisant to, kad turėjo būti panaudotos ir informatikos mokslo žinios, kuriant atitinkamus tinklalapius ir pan. Bet kuriuo atveju, toks nusikaltimas yra grįstas, N. Kshetri vadinamu, „socialinės inžinerijos elementu“[76]. Kitaip tariant šis terminas reiškia tarp dviejų ar daugiau asmenų užmezgamą dialogą, tačiau verta pažymėti, kad šis terminas dažniausiai siejamas su paties įvairiausio tipo kenkėjiška veikla, naudojant manipuliacijos žmogaus psichologija būdus. Kaltininkai pasinaudoja potencialių aukų emocijomis tokiomis kaip jauduliu, baime, sukuria pasitikėjimo ar įsipareigojimo jausmą.

Tokių socialinių inžinerijos arba manipuliacijos schemų nerasime kibernetinių nusikaltimų atveju. Diegiant „loginę bombą“, atliekant DoS ataką, užkrečiant kompiuterį virusu, „nulaužiant“ apsaugos sistemas nėra būtinas kontaktas su auka. Kibernetinių nusikaltimų atžvilgiu naudojama „apgaulė“ yra taikoma ne fiziniam asmeniui, o elektroninei sistemai „suklaidinti“. Visais šiais atvejais socialinį elementą pakeičia kompiuterio arba kitų informacinių technologijų naudojimas. Šiuo aspektu terminas kompiuteris turėtų būti suprantamas plečiamai, apimant ir kompiuterines programas. Esminis taikomas kriterijus kompiuteriui ar kitoms naudojamoms informacinėms technologijoms yra gebėjimas apdoroti duomenis. Apdorojimo funkcija reiškia kompiuterio veiksmus ar veiksmų serijas, operacijas, kurias jis atlieka su pateiktais jam duomenimis: šių organizacija, adaptacija, pakeitimas, išgavimas, atskleidimas, skleidimas, sulygiavimas, kombinavimas, blokavimas, ištrynimas, sunaikinimas ir pan[77]. Būtent kompiuteris ar informacinės technologijos kibernetiniuose nusikaltimuose naudojamos dėl gebėjimo atlikti logines, aritmetines funkcijas, sekti griežtai numatytais algoritmais siekiant atitinkamo rezultato.

[76] KSHETRI, N. The Global Cybercrime Industry. Economic, Institutional and Strategic Perspectives. Berlin: Springer, 2010, p. 10.
[77] WALDEN, I. *Computer Crimes and Digital Investigation*. Oxford: Oxford university press, 2007, p. 13–26.

3. Elektroniniai duomenys ir informacija bei kompiuterinės sistemos

Galiausiai paskutinis kibernetinių nusikaltimų požymis parodo kibernetinių nusikaltimų kryptį – šios nusikalstamos veikos visada nutaikytos į elektroninius duomenis arba informaciją, arba elektronines sistemas. Akcentuotina, kad elektroniniai duomenys ir elektroninė informacija nėra tas pats. Duomenys, tai tarsi potenciali informacija. Tai kompiuterinė kalba kompiuteriui, kuris apdorojęs konvertuoja juos į informaciją. Informacija laikoma tai, kas yra suprantama žmogui kaip kompiuterio vartotojui. I. Walden pažymi, jog teisė turėtų įsiterpti ir saugoti būtent kompiuterinius duomenis, kaip dar neapdorotą informaciją, kadangi svarbu apsaugoti pradinį „produktą“, tiesiogiai nulemiantį informaciją, kaip galutinį kompiuterio pateikiamą rezultatą vartotojui[78]. Akcentuotina, kad poveikiu kompiuteriniams duomenims, informacijai ar kompiuterinei sistemai yra pažeidžiamas konfidencialumas, vientisumas ir prieinamumas, taip išskiriant kibernetinius nusikaltimus nuo kitų nusikaltimų, kurie gali būti nukreipti į kompiuterinius duomenis, tačiau pažeidžia kitą teisinį gėrį, pvz., nusikaltimai, susiję su autorių teisių ir gretutinių teisių pažeidimais.

1.2.4. Terminai ir sąvoka

Prieš galutinai pateikiant kibernetinių nusikaltimų apibrėžimą, verta pažymėti, kad ir pats terminas vartojamas šiam reiškiniui nusakyti yra įvairus. Skaitant literatūrą šia tematika galima rasti tokius vartojamus terminus kaip: kompiuteriniai nusikaltimai (angl. *computer crime*), aukštųjų technologijų nusikaltimai (angl. *high-tech crime*), skaitmeniniai nusikaltimai (angl. *digital crime*), elektroniniai nusikaltimai (angl. *electronic crime*), virtualūs nusikaltimai (angl. *virtual crime*), kibernetiniai nusikaltimai (angl. *cybercrime*), tinklo nusikaltimai (angl. *net-crime*), informacinių ir komunikacinių technologijų nusikaltimai (angl. *Information and communications technology crime*) (toliau – ICT) ir kt. Tačiau visi jie iš esmės apibūdina vieną ir tą patį reiškinį. Taigi, kuris iš jų tinkamiausias?

Pastebėtina, kad terminas kito ir atitinkamai nuo istorinio laikmečio – terminas kompiuteriniai nusikaltimai plačiai buvo vartojamas šių nusikaltimų pradžios tarpsnyje 1970 m., 1980 m.[79]. XXI a. didėjant įvairių prietaisų galimybėms ir supratus, kad ir kiti įrenginiai gali prilygti kompiuteriui funkcinėmis savybėmis (pvz. telefonai), pradėti vartoti ICT, kibernetinių, elektroninių, virtualių nusikaltimų terminai. Toks terminas kaip

[78] WALDEN, I. *Computer Crimes and Digital Investigation*. Oxford: Oxford university press, 2007, p. 13–26.

[79] SIEBER, U. *Legal Aspects of Computer-Related Crime in the Information Society –COMCRIME- study* [interaktyvus; žiūrėta 2017 m. vasario 15 d.]. Prieiga per internetą: <http://www.oas.org/juridico/english/COMCRIME%20Study.pdf>.

informacinių ir komunikacinių technologijų nusikaltimai kritikuotinas dėl to, jog jis pats savaime persidengia, kadangi komunikacinės technologijos iš esmės yra informacinių technologijų dalis. Be to ICT gali būti vartojamas ir kitoms disciplinoms – finansų, marketingo, žmogiškųjų išteklių valdymo sritims[80]. Aukštųjų technologijų terminas nepalengvina šios užduoties, kadangi net ir šių dienų visuomenėje yra sudėtinga nusakyti, kas yra aukštosios technologijos, kuo gi jos skiriasi nuo neaukštųjų technologijų, taip dar labiau komplikuojant termino aiškumą[81]. Pabrėžtina, kad elektroniniai nusikaltimai, taip pat nėra tiksliausia sąvoka, kadangi šie nusikaltimai būdingi ne vien elektronikos sričiai, elektronikos mokslui, o informatikos inžinerijai, kompiuterijos mokslams. Elektronika, elektroniniai signalai, įtaisai, plačiai vartojami televizijoje, radijuje, automobiliuose, pramonėje ir kt[82]. Terminai, tokie kaip skaitmeniniai, virtualūs, tinklo, kibernetiniai nusikaltimai iš esmės yra siejami su kibernetine erdve, tačiau labiausiai iš šių paminėtų tinkamiausiu laikytinas terminas kibernetiniai nusikaltimai. Šis terminas ne tik tiesiogiai kilęs iš kibernetinės erdvės sąvokos, bet ir apima kibernetikos, kaip mokslo tiriančio įvairių sistemų bendruosius valdymo procesus, kurie vyksta renkant, perduodant, laikant ir perdirbant informaciją, sampratą. Taip kibernetinių nusikaltimų terminas atspindi ne tik šių nusikaltimų pirmąjį požymį (priklausomumą nuo kibernetinės erdvės), bet ir antrąjį – kompiuterių ir kitų technologijų naudojimas dėl duomenų, informacijos apdorojimo.

Apibendrinant šiame skyriuje analizuotą kibernetinių nusikaltimų sampratą, siūlytina tokia kibernetinių nusikaltimų sąvoka: **Kibernetiniai nusikaltimai – tai nuo kibernetinės erdvės priklausomos, duomenų ar informacijos apdorojimo pagrindu pagrįstos nusikalstamos veikos, nukreiptos į elektroninių duomenų ir sistemų konfidencialumą, vientisumą ir prieinamumą.**

[80] KLEVE, P., *et al*. The definition of ICT crime. *Computer law & security review*, 2011, Vol. 27, p. 162–167.
[81] *Ibid.*
[82] SAULIŪNAS, D., ŠTITILIS, D., TOLIUŠIS, S. *et al. Informacinių technologijų teisė*. Vilnius: NVO Teisės institutas, 2004, p. 508–513.

2. Nusikaltimų elektroninių duomenų ir informacinių sistemų saugumui sistema, probleminiai inkriminavimo aspektai

2.1. Lietuvos Respublikos baudžiamojo kodekso XXX skyriaus sistema

Lietuvos Respublikos Konstitucinis Teismas (toliau – Konstitucinis Teismas) aiškindamas Lietuvos Respublikos Konstitucijos[83] (toliau – Konstitucija) 31 straipsnį, ne kartą yra pažymėjęs, kad valstybės, kaip visos visuomenės politinės organizacijos, paskirtis – užtikrinti žmogaus teises ir laisves, garantuoti viešąjį interesą, todėl vykdydama savo funkcijas ir veikdama visos visuomenės interesais valstybė turi priedermę užtikrinti žmogaus teisių ir laisvių, kitų Konstitucijos saugomų ir ginamų vertybių, kiekvieno asmens ir visos visuomenės veiksmingą apsaugą *inter alia* nuo nusikalstamų kėsinimųsi[84]. Taigi įstatymų leidėjas, vykdydamas savo pareigą, privalo uždrausti pavojingas veikas nacionaliniuose baudžiamuosiuose įstatymuose. Vykdant šią pareigą įstatymų leidėjas, reaguojant į naujai kylančias kibernetines grėsmes, Lietuvos Respublikos baudžiamojo kodekso[85] XXX skyriuje numatė nusikalstamas veikas elektroninių duomenų ir informacinių sistemų saugumui. Išnagrinėjus kibernetinių nusikaltimų sampratą, nustačius konkretų šių veikų apibrėžimą ir identifikavus kibernetinius nusikaltimus, kaip atskirą nuo „tradicinių nusikaltimų“ fenomeną, verta išanalizuoti, ar BK XXX skyriuje numatytos nusikalstamos veikos atitinka kibernetinių nusikaltimų apibrėžties rėmus, kaip yra baudžiama už kibernetinius nusikaltimus Lietuvoje, kuo pasižymi teisinis reglamentavimas šių nusikalstamų veikų atžvilgiu.

2.1.1. Nusikaltimų elektroninių duomenų ir informacinių sistemų saugumui objektas

Konstitucinis Teismas yra konstatavęs, kad įstatymų leidėjas baudžiamajame įstatyme nusikalstamomis veikomis gali įvardinti tik tas veikas, kurios iš tikrųjų yra pavojingos ir kuriomis daroma esminė žala asmenų, visuomenės ar valstybės interesams arba keliama grėsmė, kad tokia žala atsiras, kadangi nusikaltimai – tai teisės pažeidimai, kuriais itin

[83] Lietuvos Respublikos Konstitucija. *Valstybės žinios*, 1992 m. lapkričio 30 d., Nr. 33-1014.

[84] Lietuvos Respublikos Konstitucinis Teismas. *2006 m. sausio 16 d. nutarimas byloje 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 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 straipsnis (2002 m. kovo 14 d. redakcija) neprieštarauja Lietuvos Respublikos Konstitucijai, Nr. 7/03-41/03-40/04-46/04-5/05-7/05-17/05.*

[85] Lietuvos Respublikos baudžiamasis kodeksas (su pakeitimais ir papildymais). *Valstybės žinios,* 2000, Nr. 89-2741.

šiurkščiai pažeidžiamos žmogaus teisės ir laisvės, kitos Konstitucijos saugomos ir ginamos vertybės, daromas neigiamas poveikis gyvenimo sąlygoms, žmonių gyvenimo lygiui, kėsinamasi į valstybės ir visuomenės gyvenimo pagrindus[86].

Atsižvelgiant į Konstitucinio Teismo konstitucinės doktrinos nuostatas, kyla diskusijos, koks yra XXX BK skyriaus objektas, t. y. baudžiamojo įstatymo ginamos teisinės vertybės. Kadangi BK specialiosios dalies nusikalstamų veikų sudėtys yra skirstomos pagal rūšinį objektą, būtina identifikuoti XXX BK skyriuje numatytų nusikalstamas veikas vienijančius vienarūšius ar tapačius teisinius gėrius[87].

Dar 2000 m. literatūroje buvo teigiama, kad kompiuterinių nusikaltimų objektas iš esmės yra kompiuterinė informacija, todėl šiomis nusikalstamomis veikomis yra padaroma žala informaciniams visuomeniniams santykiams[88]. Kiek vėliau, buvo išreikšta nuomonė, kad BK XXX skyriaus nusikalstamų veikų objektu laikytinas kompiuterinės informacijos saugumas[89]. Matyti, jog teisinį gėrį buvo siūloma sieti išimtinai tik su kompiuterine informacija. Tai keltų tam tikrų keblumų, kadangi susiaurinant šių veikų objektą iki kompiuterinės informacijos saugumo arba visuomeninių santykių susijusių su kompiuterine informacija, nebūtų apimtos tokios ir anuo metu BK redakcijoje numatytos veikos kaip, pavyzdžiui, BK 197 straipsnyje kriminalizuotas kompiuterinio tinklo, duomenų banko ar informacinės sistemos darbo pakeitimas, sutrikdymas, mat informacinė sistema yra žymiai platesnė sąvoka nei kompiuterinė informacija, nors iš pirmo žvilgsnio galėtų pasirodyti, jog kompiuterinė informacija apima ir informacinę sistemą. Toks požiūris teisingas tik iš dalies. „Informacinė sistema – tai techninių ir programinių priemonių visuma, naudojama informacijai kurti, siųsti, priimti, išsaugoti ar kitaip tvarkyti elektroniniu būdu“[90]. Europos Parlamento ir Tarybos 2013 m. rugpjūčio 12 d. direktyvos[91] (toliau – ir Direktyva) 2 straipsnyje a) punkte yra nurodoma, kad informacinė sistema – tai prietaisas arba tarpusavyje sujungtų ar susijusių prietaisų grupė, iš kurių vienas arba daugiau pagal programą vykdo automatinį kompiuterinių duomenų

---

[86] Lietuvos Respublikos Konstitucinis Teismas. *2009 m. birželio 8 d. nutarimas byloje dėl Lietuvos Respublikos baudžiamojo kodekso 20 straipsnio 1,2,3 dalių (2000 m. rugsėjo 26 d. redakcija), 20 straipsnio 5 dalies (2004 m. liepos 5 d. redakcija), 43 straipsnio 4 dalies (2000 m. rugsėjo 26 d. redakcija) atitikties Lietuvos Respublikos Konstitucijai, Nr. 34/2008-36/2008-40/2008-1/2009-4/2009-5/2009-6/2009-7/2009-9/2009-12/2009-13/2009-14/2009-17/2009-18/2009-19/2009-20/2009-22/2009.*

[87] ABRAMAVIČIUS, A., *et al. Baudžiamoji teisė: Vadovėlis*. Vilnius: Eugrimas, 1998, p. 155–160.

[88] PETRAUSKAS, R., ŠTITILIS, D. *Kompiuteriniai nusikaltimai ir jų prevencija*. Vilnius: Lietuvos teisės akademijos Leidybos centras, 2000, p. 7.

[89] SAULIŪNAS, D., ŠTITILIS, D., TOLIUŠIS, S. *et al. Informacinių technologijų teisė*. Vilnius: NVO Teisės institutas, 2004, p. 508–513.

[90] MOCKEVIČIUS, R., VALATKEVIČIUS, D., *et al. Lietuvos Respublikos baudžiamojo kodekso komentaras. Specialioji dalis (99–212 straipsniai).* Vilnius: VĮ Registrų centras, 2009, p. 426.

[91] 2013 m. rugpjūčio 12 d. Europos Parlamento ir Tarybos direktyva 2013/40/ES dėl atakų prieš informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR (OL 2013 L 218, p. 8).

tvarkymą, taip pat kompiuteriniai duomenys, saugomi, tvarkomi, išrenkami arba perduodami to prietaiso ar grupės prietaisų jo ar jų eksploatacijos, naudojimo, apsaugojimo ir priežiūros tikslais. Tuo tarpu elektroniniai duomenys, kaip juos apibrėžia Lietuvos Respublikos elektroninio parašo įstatymas[92] yra duomenys, kurie tvarkomi informacinių technologijų priemonėmis. Direktyva savo ruožtu dar labiau detalizuoja šią sąvoką nurodydama, kad tai – faktai, informacija ar sąvokos, pateiktos tokia forma, kuri tinkama tvarkyti informacinėje sistemoje, įskaitant programą, tinkamą tam, kad informacinė sistema atliktų funkciją. Taigi, matyti, kad informacinė sistema apima ne tik kompiuterinius duomenis, bet ir technologinius prietaisus, intranetą, ekstranetą, tinklus ir serverius bei kitą interneto infrastruktūrą. Šių nusikalstamų veikų objektą suprantant tik kaip kompiuterinę informaciją, BK 197 numatyta veika paprasčiausiai išsiskirtų iš BK XXX skyriaus konteksto.

Tiesa, pats BK XXX skyriaus pavadinimas taip pat nebuvo itin tikslus – „Nusikaltimai informatikai“. Informatika suprantama kaip mokslo šaka, tirianti visų rūšių informacijos struktūrą, organizaciją, funkcijas, genezę, sąveiką su kitais materijos elementais[93]. Taigi pavadinus baudžiamojo įstatymo skyrių nusikaltimais informatikai suponavo tai, kad tame skyriuje numatytos nusikalstamos veikos daro žalą pačiai informatikai. Tačiau, tapo aišku, kad įsilaužus į privataus kompiuterio sistemą, ar pasisavinus neteisėtai elektroninius duomenis, veikiau yra padaroma žala konkrečiam informacinės sistemos vartotojui, ar konkrečia elektronine informacija disponuojančiam asmeniui, bet ne informatikai kaip mokslo šakai. Priešingai, informatikai, kaip mokslui nagrinėjančiam informacijos apdorojimą, kitus su tuo susijusius procesus, kibernetiniai nusikaltimai gali tapti tyrimo dalimi. Juolab, kad ir vykdant kibernetinį nusikaltimą neretai, o kai kuriais atvejais, būtinai turi būti naudojamos informatikos žinios. Šis akivaizdus pavadinimo ir saugomo teisinio gėrio ne atitikmuo 2007 m. paskatino įstatymų leidėją pakeisti BK XXX skyriaus pavadinimą ir pervadinti jį taip – „Nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui“[94]. Matyti, kad šis skyriaus pavadinimas jau pamini ne tik elektroninius duomenis, bet ir atskirai išskiria informacinę sistemą.

---

[92] Lietuvos Respublikos elektroninio parašo įstatymas (su pakeitimais ir papildymais). *Valstybės žinios*, 2000, Nr. VIII-182.

[93] Tarptautinis žodžių žodynas [interaktyvus; žiūrėta 2017 m. vasario 7 d.]. Prieiga per internetą: <http://www.zodziai.lt/reiksme&word=informatika&wid=8519>.

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

R. Marcinauskaitė analizuodama dabartinio BK XXX skyriaus objektą nurodo, kad elektroninių nusikaltimų teisiniu gėriu gali būti įvardijamas elektroninės erdvės saugumas, kuris, autorės nuomone, galėtų būti susijęs su grėsmėmis, kurias sukelia neteisėto turinio informacijos skleidimas elektroninėje erdvėje (neapykantos, terorizmo kurstymas), grėsmėmis, kurias sukelia tradicinės, tačiau dėl elektroninės erdvės panaudojimo galimybių pakitusios, nusikalstamos veikos (sukčiavimas elektroninėje erdvėje), galiausia grėsmėmis, kurių atsiradimas siejamas su pačiais kibernetiniais nusikaltimais[95]. Šiuo momentu atskleistina kibernetinių nusikaltimų, kuri buvo išvesta pirmoje šioje darbo dalyje, apibrėžimo nauda. Suprantant plačiai kibernetinius nusikaltimus, matoma, kad elektroninės erdvės saugumo objektas yra pernelyg platus, persidengia su kitomis baudžiamojo įstatymo saugomomis vertybėmis, todėl tokių veikų išskyrimas į atskirą BK skyrių taptų problemiškas, ką iš esmės pažymi ir pati straipsnio autorė. Atsižvelgus į tai, laikytina, jog tokia pozicija nėra tinkama. R. Marcinauskaitė, taip pat pažymėjo, jog galima ir „techninė kompiuterių saugumo“ koncepcijos atitiktis BK XXX skyriaus saugomam teisiniam gėriui, kuri vartojama kaip elektroninių duomenų ir informacinių sistemų saugumo sinonimas[96]. Techninis kompiuterių saugumas apima „CIA triadą“[97], kurią sudaro elektroninių duomenų ir informacinių sistemų konfidencialumas (angl. *Confidentiality*) – duomenys nėra atskleidžiami ar pasiekiami vartotojams bei procesams, kuriems nesuteikta tokia teisė, integralumas (angl. *Integrity*) – duomenų savybė reiškianti, kad jie nebuvo pakeisti ar sunaikinti neteisėtu būdu ir prieinamumas (angl. *Availability*) – garantuoja, kad duomenys ir informacinės sistemos reikiamu metu yra prieinami sankcionuotam vartotojui. R. Mockevičius ir D. Valatkevičius išskiria dar ir ketvirtą elementą – autentiškumą (tapatumą), kuris reiškia savybę, garantuojančią duomenų neiškraipymą, jų saugojimo, kaupimo, apdorojimo, perdavimo metu[98]. Pastebėtina, kad minėtas ketvirtasis elementas gali būti tapatinamas su integralumu. Ši autorės įvardijama techninė kompiuterių saugumo koncepcija, matyti, kur kas labiau detalesnė ir apčiuopiama nei prieš tai įvardinta elektroninės erdvės saugumo koncepcija. CIA sandaros trys elementai apima visas BK XXX skyriuje numatytų nusikalstamų veikų, kuriais kėsinamasi į teisinį gėrį, sritis, šie elementai yra aiškiai

[95] MARCINAUSKAITĖ, R. Nusikalstamomis veikomis elektroninėje erdvėje pažeidžiamos pagrindinės baudžiamojo įstatymo saugomos vertybės nustatymo problema. *Socialinių mokslų studijos*, 2011, Nr. 3(3), p. 897–914.
[96] *Ibid.*
[97] CIA triadą sudaro 3 elementai: konfidencialumas, integralumas ir prieinamumas *(angl. Confidentiality, Integrity, Availability)*.
[98] MOCKEVIČIUS, R., VALATKEVIČIUS, D., *et al. Lietuvos Respublikos baudžiamojo kodekso komentaras. Specialioji dalis (99–212 straipsniai).* Vilnius: VĮ Registrų centras, 2009, p. 416–442.

apibrėžiami, išreiškiami. Pastebėtina, kad tokia CIA triada minima ir Budapešto konvencijoje.

Taigi, apžvelgus vyraujančias nuomones šiuo klausimu, matyti, kad BK XXX skyriumi saugomas duomenų ir informacinių sistemų konfidencialumas, integralumas, prieinamumas. Šių elementų turinys yra pakankamai aiškus – jie visi atspindi asmens ryšį su duomenimis ar IS. Būtų klaidinga manyti, kad šių nusikalstamų veikų objektas yra duomenys ar informacinės sistemos, kadangi tai yra šių veikų dalykas. Nėra tikslu objektu laikyti ir patį elektroninių duomenų ar IS saugumą, kadangi pats savaime saugumas savyje netalpina aiškaus, apibrėžiamo turinio, kuris būtinas teisiniam gėriui nusakyti (kaip pavyzdžiui, BK XVII skyriaus – gyvybė, kuri ginama nuo sunaikinimo). Todėl šių BK XXX skyriuje numatytų nusikalstamų veikų objektas laikytinas asmens santykis su duomenimis ar informacinėmis sistemomis, kaip galimybė ir laisvė tokį gėrį valdyti, disponuoti, naudotis juo. Tokį patį teisinio gėrio principą galima įžvelgti ir nusikalstamų veikų nuosavybei, turtinėms teisėms ir turtiniams interesams atveju, kai teisiniu gėriu yra laikomas ne turtas ar jo saugumas, o būtent asmens ir turto ar turtinės teisės (intereso) ryšys. Todėl BK XXX skyriaus objektu laikomas ne elektroninių duomenų ar informacinių sistemų saugumas, o elektroninių duomenų ar informacinių sistemų valdytojo, turėtojo interesai, kurie yra susiję su duomenų ar IS vientisumu, konfidencialumu ir prieinamumu.

2.1.2. Nusikaltimų elektroninių duomenų ir informacinių sistemų saugumui sistema

Verta pažymėti, kad BK XXX skyriuje apibrėžtas nusikalstamas veikas galima būtų laikyti kibernetiniais nusikaltimais, laikantis pirmoje dalyje pateikto apibrėžimo, išskyrus išimtinius atvejus, kai BK XXX skyriuje numatytos veikos yra padaromos materialioje erdvėje (pavyzdžiui, sunaikinami duomenys pažeidžiant ar sunaikinant fiziškai laikmeną, kurioje jie yra įrašyti, neteisėtai išgaunant informacinės sistemos slaptažodį tiesiogiai iš asmens, kuris jį žino – tokiais atvejais asmenį bus galima patraukti baudžiamojon atsakomybėn pagal BK XXX skyriuje numatytas sudėtis, tačiau tokios veikos nebus laikomos kibernetiniais nusikaltimais tikrąja prasme, kadangi neapima kibernetinės erdvės ir duomenų ar informacijos apdorojimo pagrindo išskirtų požymių).

Analizuojant BK 196 – 198[2] straipsnius neabejotinai pastebėtina, jog ypač didelę įtaką tiek jų atsiradimui, tiek pakeitimams turėjo Lietuvos prisijungimas prie Budapešto konvencijos. Dar net neįsigaliojus 2000 m. BK, mokslininkų dėmesys krypo link

Konvencijos teikiamų rekomendacijų[99]. Kitaip tariant, Budapešto konvencija suteikė pagrindines gaires kibernetinių nusikaltimų srityje tobulinant BK nuostatas, kadangi iki tol galiojęs BK numatė tik tris nusikalstamų veikų sudėtis – kompiuterinės informacijos sunaikinimą ir pakeitimą, kompiuterinės programos sunaikinimą ar pakeitimą, kompiuterinės informacijos pasisavinimą ir skleidimą. Prieš konvencijos ratifikavimą BK buvo papildytas dviem straipsniais, t. y. BK 198^1 ir BK 198^2. Kito ir BK 196 ir 197 dispozicijos papildant jas alternatyviu požymiu – pašalinimu, taip pat įtrauktas neteisėtumo požymis[100]. Nepaisant šių pastangų, nevisiška apimtimi buvo įgyvendintos Budapešto konvencijos nuostatos. Trūkumu buvo laikoma tai, kad BK 196 ir BK 197 straipsniai numatė atsakomybę už poveikį iš esmės tapačiam dalykui[101]. Tuometinis BK 197 straipsnis „Kompiuterinės programos sunaikinimas ar pakeitimas ir kompiuterinio tinklo, duomenų banko ar informacinės sistemos darbo sutrikdymas“ (BK redakcija galiojusi iki 2007 m. liepos 21 d.) numatė atsakomybę už poveikį kompiuterinei programai, o 196 straipsnis „Kompiuterinės informacijos sunaikinimas ar pakeitimas“ (BK redakcija galiojusi iki 2007 m. liepos 21 d.) – kompiuterinei informacijai, taip iš esmės dubliuojant kompiuterinę programą ir kompiuterinę informaciją, nors kompiuterinė programa tam tikra prasme ir yra kompiuterinės informacijos paketas, kadangi vadovaujantis Lietuvos Respublikos autorių teisių ir gretutinių teisių įstatymo[102] 2 straipsnio 28 punkto pateikiama sąvoka, kompiuterių programa iš esmės suprantama, kaip duomenų, teikiančių tam tikras instrukcijas, kurios sudaro galimybę kompiuteriui atlikti tam tikrą užduotį, visuma. Vis dėlto didžiausia to meto reguliavimo yda laikyta nepaisant Konvencijos – terminų „duomenų“ ir „informacijos“ tapatinimas[103]. Šie trūkumai ištaisyti po 2007 metų vykusių pakeitimų įgyvendinant 2005 m. vasario 24 d. Tarybos pamatinį sprendimą dėl atakų prieš informacines sistemas[104].

Neseniai BK XXX skyrius sulaukė dar vienos pakeitimų bangos. 2015 m. birželio 19 d. įsigaliojusiais pakeitimais[105] atsižvelgiama į Europos Parlamento ir Tarybos 2013

[99] PETRAUSKAS, R., ŠTITILIS, D. Lietuvos Respublikos baudžiamasis kodeksas nusikaltimų elektroninėje erdvėje konvencijos kontekste. *Jurisprudencija*, 2002, t. 24(16), p. 79–86.
[100] Lietuvos Respublikos baudžiamojo kodekso 13, 162, 191, 196, 197, 203, 206, 216, 219, 221, 309 straipsnių pakeitimo ir papildymo bei kodekso papildymo 198-1 ir 198-2 straipsniais įstatymas. *Valstybės žinios*, 2004, Nr. 25-760.
[101] SAULIŪNAS, D. Legislation on cybercrime in Lithuania: development and legal gaps in comparison with the convention on cybercrime. *Jurisprudencija*, 2010, Nr. 4(122), p. 203–219.
[102] Lietuvos Respublikos autorių teisių ir gretutinių teisių įstatymas. *Valstybės žinios*, 1999, Nr. 50-1598.
[103] SAULIŪNAS, D. Legislation on cybercrime in Lithuania: development and legal gaps in comparison with the convention on cybercrime. *Jurisprudencija*, 2010, Nr. 4(122), p. 203–219.
[104] 2005 m. vasario 24 d. Tarybos pagrindų sprendimas 2005/222/TVR dėl atakų prieš informacines sistemas (OL 2005 L 69, p. 67).
[105] Lietuvos Respublikos baudžiamojo kodekso 7, 196, 197, 198^1, 198^2 straipsnių ir priedo pakeitimo ir kodekso papildymo 270^3 straipsniu įstatymas. *Teisės aktų registras*, 2015, Nr. 2015-09697.

m. rugpjūčio 12 d. direktyvą[106], kuria keičiamas 2005 m. vasario 24 d. Tarybos pamatinis sprendimas. Šiais pakeitimais BK XXX skyrius buvo koreguojamas keturiais aspektais. Pirma, pakeistos sankcijos ribos. Antai BK 196 ir 197 straipsnių 1 dalyse laisvės atėmimo ribos sumažintos nuo 4 m. iki 2 m., o BK 198^1 straipsnio 1 dalyje laisvės atėmimo terminas padidintas nuo 1 m. iki 2 m. Tiesa, BK 198^2 straipsnis tik nuo 2016 m. birželio 28 d. įsigaliojusių BK pakeitimų sulaukė sankcijos griežtinimo – vietoje trejų metų nuo šiol galima skirti ketverius metus laisvės atėmimo[107]. Antra, buvo modifikuotas BK 198^2 straipsnis numatant papildomus alternatyviuosius objektyviosios pusės požymius „importavo“ bei „suteikė prieigą“, taip pat pakeista 1 dalies konstrukcija. Trečia, atsakomybė diferencijuojama pagal nusikalstama veika padarytą žalą. Tačiau įdomiausias ir atidesnio dėmesio vertas pakeitimas susijęs su BK 196 ir BK 197 straipsnių kvalifikuojančių sudėčių numatymu t. y. veika padaryta daugeliui informacinių sistemų (BK 196 str. 2 d., 197 str. 2 d.) arba veika padaryta pasinaudojant svetimais asmens duomenimis (BK 197 str. 2 d.).

Pasinaudojimas svetimais asmens duomenimis iš esmės atspindi tapatybės vagystės inkriminavimą. Tapatybės vagystė suprantama, kaip asmens duomenų išgavimas ir jų panaudojimas paveikti elektroninių duomenų ar informacinių sistemų konfidencialumui, prieinamumui, vientisumui. Tapatybės vagystė gali būti padaroma įvairiais būdais: minėtu *phising'u, farming'u,* naudojant kenkėjiškas programas ir pan[108]. Direktyvoje numatyta, kad valstybės narės turi imtis priemonių užtikrinant, kad neteisėtas įsikišimas į duomenis ar sistemą piktnaudžiaujant kito asmens duomenimis siekiant įgyti trečiosios šalies pasitikėjimą, tokiu būdu padarant žalą teisėtam tapatybės turėtojui, būtų laikoma sunkinančiomis aplinkybėmis, išskyrus tuo atveju, jei tos aplinkybės jau yra taikomos kitai nusikalstamai veikai, už kurią baudžiama pagal nacionalinę teisę. Matyti, kad Direktyvos nuostata nurodžius svetimų asmens duomenų panaudojimą BK 196 ir 197 straipsniuose buvo įgyvendinta tiesiogiai. Nepaisant to, galima kelti diskusiją ar tikrai šis požymis atspindi didesnį nusikalstamos veikos pavojingumą? Hipotetiškai modeliuojant, galima tokia situacija, kai asmuo A panaudodamas kenkėjišką programą išgauna aukos tapatybės identifikavimo duomenis, kuriuos perduoda kaltininkui B. Pastarasis pasinaudodamas šiais duomenimis prisijungia prie aukos paskyros ir sunaikina joje

[106] 2013 m. rugpjūčio 12 d. Europos Parlamento ir Tarybos direktyva 2013/40/ES dėl atakų prieš informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR (OL 2013 L 218, p. 8).
[107] Lietuvos Respublikos baudžiamojo kodekso 198^2, 309 straipsnių ir priedo pakeitimo įstatymas. *Teisės aktų registras*, 2016, Nr. 2016-17730.
[108] KALPOKAS, V., MARCINAUSKAITĖ, R. Tapatybės vagystė elektroninėje erdvėje: technologiniai aspektai ir baudžiamasis teisinis vertinimas. *Teisės problemos*, 2012, Nr. 3(77), p. 30–52.

esančius duomenis, taip padarydamas BK 196 straipsnio 1 dalyje numatytą veiką. Kitu atveju kaltininkas C pats įveikia saugos sistemą prisijungia prie aukos paskyros ir sunaikina lygiai tuos pačius duomenis, kaip ir asmuo B. Įvertinant B ir C veikas – B asmeniui būtų inkriminuojami BK 196 straipsnio 2 dalis (už duomenų sunaikinimą) bei 198^2 straipsnio 1 dalis (už prisijungimo duomenų įgijimą), tuo tarpu C veika kvalifikuotina, kaip BK 196 straipsnio 1 dalis (už duomenų sunaikinimą) bei 198^1 straipsnio 1 dalis (už neteisėtą prisijungimą prie informacinės sistemos). Galiausiai rezultatą turime tokį patį – tiek B, tiek C sunaikino tuos pačius elektroninius duomenis, tačiau B taikoma kvalifikuota sudėtis. Svarstytina ar asmuo C, kuris sugeba savarankiškai patekti į aukos informacinę sistemą, pasižymi didesne informatikos bei kibernetikos išmone, nekelia didesnės grėsmės nei asmuo B, kuris geba iš esmės atlikti tik pusę to, ką padarė pats C. Todėl tokį požymio nustatymą būtų galima kritikuoti, kaip nevisiškai tiksliai atspindinčio nusikalstamos veikos pavojingumą.

Kiek kitaip vertintinas požymis – veika padaryta daugeliui informacinių sistemų. Savaime suprantama, šis požymis siejamas su kibernetinės atakos padariniais. Ką laikyti dideliu skaičiumi informacinių sistemų, įstatymų leidėjas paliko nustatyti teismų praktikai. Tiesa, prieš priimant pataisas buvo teiktas kitas BK pakeitimo įstatymo projektas, kuriame siūloma vietoje neapibrėžto „daugelio informacinių sistemų“ numatyti konkretų tokių informacinių sistemų skaičių t. y. dešimt ir daugiau[109]. Lietuvos Respublikos Vyriausybės kanceliarijos teisės departamentas išvadoje pažymėjo, kad BK 196 ir 197 straipsnių formuluotės „daugelio informacinių sistemų“ nevisiškai atitinka aiškumo teisėkūroje principą, kuris reiškia, kad teisinis reguliavimas, *inter alia*, turi būti tikslus, aiškus ir nedviprasmiškas[110]. Tačiau šio projekto lydimojoje medžiagoje taip ir nepavyko surasti paaiškinimo, kokiu kriterijumi buvo remtasi siūlant šį konkretų atskaitos tašką. Kita vertus, vertinamojo kriterijaus pateikimas, nėra savaime ydingas dalykas. Tai suteikia teismui galimybę taikyti įstatymą dinamiškai.

Nepaisant to, šio požymio įtvirtinimas gali būti tikslinamas. Atkreiptinas dėmesys į šiais pakeitimais įgyvendinamą Direktyvą. Akcentuotina, jog apie poveikį daugeliui informacinių sistemų yra kalbama šios Direktyvos preambulės 13 punkte, kuriame sakoma, kad: „tikslinga numatyti griežtesnes sankcijas tais atvejais, kai ataka prieš informacinę sistemą padaryta nusikalstamos organizacijos <...>, kai elektroninė ataka vykdoma plačiu mastu ir todėl dėl jos daromas poveikis daugeliui informacinių sistemų,

[109] Lietuvos Respublikos baudžiamojo kodekso 7, 196, 197, 198^1, 198^2 straipsnių ir priedo pakeitimo bei kodekso papildymo 270^3 straipsniu įstatymo projektas, 2014, Nr. XIIP-2617.
[110] Lietuvos Respublikos Vyriausybės kanceliarijos teisės departamento išvada dėl Lietuvos Respublikos baudžiamojo kodekso 7, 196, 197, 198^1, 198^2 straipsnių ir priedo pakeitimo bei kodekso papildymo 270^3 straipsniu įstatymo projekto, 2014, Nr. NV-3278.

įskaitant tuos atvejus, kai ataka siekiama sukurti *botnetą*[111] arba kai ji vykdoma naudojant *botnetą* ir tokiu būdu padaroma didelė žala, įskaitant atvejus, kai ataka vykdoma per *botnetą*“. Matyti, kad poveikis daugeliui informacinių sistemų čia yra minimas, tačiau išsakyto Direktyvoje siekio esmė yra ne tik griežtesnės sankcijos už paveiktų informacinių sistemų skaičių, o ir griežtesnės sankcijos už naujo kibernetinio nusikaltimo būdo panaudojimą – atakos vykdymas per „botnetą“. Tą parodo į pasiūlyme dėl Europos Parlamento ir Tarybos direktyvos dėl atakų prieš informacines sistemas ir dėl Tarybos pamatinio sprendimo 2005/222/TVR panaikinimo išsakytas susirūpinimas[112]. Būtent siūlyme dėl Direktyvos atkreipiamas dėmesys į „botnetų“ panaudojimą, jog jo pagalba rengiamos atakos dažnai būna didelio masto. Čia pat paaiškinama, kas yra didelio masto ataka: „atakos, kurios rengiamos pasitelkiant priemones, dėl kurių nukenčia daug informacinių sistemų (kompiuterių), arba tokios atakos, dėl kurių patiriama didelė žala“. Pasiūlyme pabrėžiama, kad „botnetų“ dydis gali siekti net nuo 40 000 iki 100 000 užkrėstų kompiuterių per 24 valandas. Europos ekonomikos ir socialinių reikalų komiteto nuomonėje[113] taip pat neapsiribojama tik pažeidžiamų informacinių sistemų kriterijumi. Čia nurodoma, kad organizuoti nusikaltėliai ir priešiškų valstybių vyriausybės naudojasi destruktyviomis atakų prieš informacines sistemas galimybėmis, tokiomis kaip „botnetas“. Kaip pavyzdys pateikiamas išpuolio prieš Estiją 2007 m. balandžio – gegužės mėnesiais atvejis, kai dėl didelio atakų masto informacinių sistemų sutrikdymas tęsėsi keletą dienų ir padarė nuostolių už 19–28 milijonus eurų, taip pat nemažą politinę žalą. Išvadoje taip pat siūloma įtraukti tokias nuostatas dėl sunkinančių aplinkybių – didelio masto atakų rengimo, „botneto“ kūrimas arba panašių priemonių naudojimas darant pamatiniame sprendime išvardytus nusikaltimus. Žinoma, sprendimas įstatymo normose

[111] Sąvoka „*botnetas*“ reiškia kompiuterių, kuriuose įdiegta kenkimo programinė įranga (kompiuterio virusai), tinklą. Toks užkrėstų kompiuterių („zombių“) tinklas gali būti naudojamas konkretiems veiksmams atlikti, pavyzdžiui, atakoms prieš informacines sistemas (t. y. kibernetinėms atakoms) rengti. Šie „zombiai“ gali būti kontroliuojami iš kito kompiuterio, dažnai užkrėstų kompiuterių naudotojams visiškai nieko nežinant. Šis kontroliuojantis kompiuteris dar vadinamas komandų ir kontrolės centru. Šį centrą kontroliuojantys asmenys yra pažeidėjai, nes jie naudojasi užkrėstais kompiuteriais atakoms prieš informacines sistemas rengti. Nusikaltėlius susekti labai sunku, nes *botnetui* priklausantys kompiuteriai, naudojami atakoms rengti, gali būti visai kitoje vietoje nei pažeidėjas.

[112] 2010 m. rugsėjo 30 d. Europos Komisijos COM/2010/0517 galutinis – COD 2010/0273 pasiūlymas dėl Europos Parlamento ir Tarybos direktyvos dėl atakų prieš informacines sistemas ir dėl Tarybos pamatinio sprendimo 2005/222/TVR panaikinimo {SEC(2010) 1122 galutinis}{SEC(2010) 1123 galutinis} (COM/2010/0517 final – COD 2010/0273 proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA {SEC(2010) final} {SEC(2010) 1123 final}.

[113] 2011 m. liepos 23 d. Europos ekonomikos ir socialinių reikalų komiteto nuomonė dėl pasiūlymo dėl Europos Parlamento ir Tarybos direktyvos dėl atakų prieš informacines sistemas ir Tarybos pamatinio sprendimo 2005/222/TVR panaikinimo (OL 2011 C 218, p. 130).

tiesiogiai numatyti būtent „botneto“ panaudojimą būtų neracionalus, nes neatitiktų techninio neutralumo principo[114].

Taigi, matyti, kad siekiant Direktyvos išleidimo vienas paskatinusių veiksnių buvo didelio masto atakų sparčiai kylanti grėsmė. Atsižvelgiant į tai, manytina, kad įgyvendinant Direktyvos nuostatą dėl poveikio dideliam informacinių sistemų kiekiui, būtų tikslinga neapsiriboti vien šiuo požymiu. Tokiu atveju siūlytinas „didelio masto atakos“ kaip kvalifikuojančios nusikalstamą veiką sudėties požymis, kuris būtų įvairiapusiškesnis, kadangi apimtų ne tik poveikį dideliam skaičiui informacinių atakų, bet ir didelio kiekio informacinių technologijų panaudojimą, kalbant apie informacinių sistemų sutrikdymą – laiko tarpą, kuriuo informacinių sistemų veikla buvo sutrikdyta ir pan. Šiuo atveju, tik pažodžiui perkėlus Direktyvos tekstą dėl poveikio dideliam informacinių sistemų kiekiui, minėti kriterijai, rodantys atakos destruktyvumą ir pavojingumą, lieka nuošalyje.

Apibendrinant, galima teigti, kad BK XXX skyriaus nusikaltimų elektroninių duomenų ir informacinių sistemų saugumui nuostatos yra intensyviai derinamos įgyvendinant Konvencijos bei Direktyvos nuostatas. Kaip bebūtų, harmonizuojant nacionalinę teisę ir Europos Sąjungos teisę galima įžvelgti ir vietas, kurios reikalauja tobulinimo.

2.2. Nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui teismų praktikoje

2.2.1. Atribojimas nuo kitų nusikalstamų veikų

Lietuvos Aukščiausiojo Teismo (toliau – LAT) apžvalgoje yra pažymėta, kad teismai nemažai susiduria su probleminiais baudžiamojo įstatymo normų konkurencijos sprendimo klausimais nustatydami dviejų – bendrosios ir specialiosios – normų santykį bei kvalifikuodami veiką. Neteisingai nustačius konkuruojančių normų pobūdį, nepagrįstai gali būti nustatoma reali arba ideali nusikalstamų veikų sutaptis. Kaip antai, netinkamai išsprendus klausimą ar tradicinę nusikalstamą veiką numatanti norma gali būti pritaikoma ir kibernetinėje erdvėje padarytai nusikalstamai veikai kvalifikuoti, gali būti nepagrįstai inkriminuojama keletas idealią sutaptį sudarančių nusikalstamų veikų[115].

[114] MARCINAUSKAITĖ, R. Technologinio neutralumo principas ir jo reikšmė formuluojant ir aiškinant nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui sudėtis. *Socialinių mokslų studijos*, 2013, Nr. 5(1), p. 367–379.

[115] Lietuvos Aukščiausiojo Teismas. 2016 m. rugpjūčio 23 d. Teismų praktikos nagrinėjant baudžiamąsias bylas dėl sudėtingų pavienių nusikalstamų veikų ir nusikalstamų veikų sutapčių apžvalga Nr. AB-44-1. *Teismų praktika*, 2016, Nr. 44, p. 570–626.

Pavyzdžiui, kaltinamasis L. B. buvo nuteistas už tai, kad pasinaudodamas nešiojamu kompiuteriu bei pamatytais ir įsimintais prisijungimo prie D. J. naudojamos el. pašto paskyros vardu ir slaptažodžiu, prisijungė prie D. J. el. pašto paskyros bei nukopijavo į nešiojamojo kompiuterio standųjį diską neviešus elektroninius duomenis – informaciją apie D. J. privatų gyvenimą, susirašinėjimą el. paštu. Šią informaciją kaltinamasis vėliau išplatino šešiais el. pašto adresais, taip viešai paskleisdamas neviešus elektroninius duomenis[116]. L. B. veika kvalifikuota ir pagal BK 198, ir pagal BK 168 (neteisėtas informacijos apie asmens privatų gyvenimą atskleidimas ar panaudojimas) straipsnius. Taigi žemesnės instancijos teismai neatsižvelgė, kad BK 168 straipsnyje kriminalizuotas asmens privataus gyvenimo pažeidimas ne tik fizinėje, bet taip pat ir elektroninėje erdvėje. LAT nurodė, kad BK 168 straipsnyje įtvirtinti neteisėto informacijos apie asmens privatų gyvenimą atskleidimo ar panaudojimo veiksmai, palyginus su BK 198 straipsnyje numatytaisiais, yra konkretesni, tiesiogiai susiję būtent su asmens privataus gyvenimo neliečiamumo pažeidimais. BK 168 straipsnio 1 dalyje numatyta norma turi ir visus bendrojoje normoje (BK 198 str. 1 d.) nurodytus požymius, tačiau reguliuoja įstatymo leidėjo specialiai išskirtus privataus gyvenimo neliečiamumo pažeidimo atvejus. Todėl BK 168 straipsnio 1 dalyje nurodyta norma laikytina specialiąja, o BK 198 straipsnio 1 dalyje esanti – bendrąja. Svarbu yra tai, kad viešas informacijos apie kito žmogaus privatų gyvenimą paskelbimas galimas ne tik fizinėje, bet ir elektroninėje erdvėje, todėl šioje erdvėje (pvz., elektroniniu paštu) paskelbta informacija turi ir visus elektroninių duomenų požymius. Dėl šių priežasčių LAT pažymėjo, kad BK 198 straipsnio inkriminavimas yra perteklinis – pakanka tik BK 168 straipsnio taikymo.

Panašiai situacija galėtų būti vertinama ir kitoje Vilniaus apygardos teismo byloje. Joje V. Š. nurodė prekybos salono konsultantei R. G. neteisėtai iš įmonės vidinės sistemos įgyti klientų mobilaus telefono ryšio abonentinių numerių detalias sąskaitas, informaciją apie įmonės darbuotojų atostogas ir šiuos neviešus elektroninius duomenis atspausdinti popieriuje[117]. Teisėjų kolegija pažymėjo, kad BK 198 straipsnio objektas yra neviešų elektroninių duomenų konfidencialumas. Būtent remdamasis tuo, kad duomenis, kuriuos išgavo kaltininkas, buvo patalpinti elektroninėje erdvėje ir tuo, kad šie atitiko konfidencialių duomenų reikalavimus, kvalifikavo V. Š. veiką pagal BK 198 straipsnio 1 dalį. Tačiau, pastebėtina, kad informaciją, kurią neteisėtai perėmė V. Š. taip pat galėjo

[116] Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2015 m. sausio 6 d. nutartis baudžiamojoje byloje, Nr. 2K-138/2015.*

[117] Vilniaus apygardos teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2014 m. gegužės 15 d. nutartis baudžiamojoje byloje, Nr. 1A-338-312-2014.*

būti laikoma ir komercine paslaptimi, kaip tą nustato Lietuvos Respublikos civilinio kodekso[118] 1.116 straipsnis. Pati teisėjų kolegija pateikdama motyvus nurodė, kad iš bylos duomenų matoma, jog šioje įmonėje buvo numatyta komercinę ir technologinę paslaptį sudarančių žinių apsaugos tvarka, kurioje nurodyta, kas sudaro bendrovės komercinę (technologinę) paslaptį. Į šį sąrašą pateko ir kaltininko pasisavintos detaliosios klientų sąskaitos. Taip pat buvo nustatyta, kad kaltininkas neabejotinai buvo supažindintas su minėtu sąrašu, kadangi anksčiau dirbo toje įmonėje ir tą žinojo. Matyti, kad buvo dėtos pastangos išsaugoti tokios informacijos slaptumą, kadangi ji talpinta informacinėje sistemoje, kuri buvo prieinama tik jos darbuotojams. Dėl šių priežasčių kaltininko veika galėjo būti kvalifikuojama kaip komercinis šnipinėjimas (BK 210 str.). Žinoma, vien šių aplinkybių nepakanka – teismas turi patikrinti, ar tokia informacija turi tikrą ar bent potencialią komercinę vertę. Tačiau teismo nuosprendyje tas apskritai nebuvo svarstyta. O vis dėlto, pripažinus klientų sąskaitas kaip komercinę paslaptį, būtų galima teigti, kad veika kvalifikuotina pagal BK 210 straipsnį, jį vertinant kaip specialų, BK 198 atžvilgiu, nes pasisavinta informacija yra detalesnio pobūdžio, apimanti ne tik duomenų konfidencialumą, bet ir sąžiningo ūkininkavimo principus.

Iš pateiktų pavyzdžių matyti, kad teismas nagrinėdamas bylas pervertina duomenų formos elementą – jei duomenys yra elektroninės formos, teismas taiko BK XXX skyriuje esančius straipsnius, taip nepagrįstai neatsižvelgdamas į bendrosios ir specialiosios normų konkurencijos taisykles. Kadangi elektroniniai duomenys gali būti ir kitų nusikalstamų veikų dalyku, būtina spręsti konkurencijos klausimą, kitu atveju gaunamas jau iliustruotas rezultatas – neteisingai kvalifikuojama kaltininko veika arba nepagrįstai nustatomas veikų daugetas. Pažymėtina, kad BK 168, 210 normos apima ne tik elektroninius duomenis, tačiau be bendrų požymių BK 198 straipsnio atžvilgiu, jos išsiskiria joms specifiškai būdingais požymiais – žinios apie privatų gyvenimą, komercinę paslaptį sudarantis turinys, elektroninės mokėjimo priemonės identifikaciją patvirtinantys duomenys. Todėl minėtos normos neabejotinai turi prioritetą prieš BK 198 straipsnyje įtvirtintą normą.

Pastebėtina, kad taip pat nemažai neaiškumų teismams yra iškilę atribojant BK XXX skyriuje numatytus nusikaltimus nuo nusikaltimų finansų sistemai, konkrečiai BK 214, 215 straipsnių.

Štai vienoje byloje T. S. siekdamas apgaule savo naudai įgyti svetimą turtą neteisėtai panaudodamas uždarosios akcinės bendrovės (toliau – UAB) priklausančio el. bankininkystės sąskaitų generatoriaus duomenis, įgytus iš direktoriaus D. V., neturėdamas teisėto elektroninės bankininkystės sąskaitų generatoriaus duomenų

[118] Lietuvos Respublikos civilinis kodeksas. *Valstybės žinios,* 2000, Nr. 74-2262.

valdytojo leidimo, neteisėtai prisijungė prie UAB sąskaitos ir taip veikdamas iš UAB į savo sąskaitą, be UAB žinios pervedė apie 27 000 Lt sumą[119]. Kaltininko veika kvalifikuota pagal BK 198 ir 182 straipsnius. Apeliacinis teismas pažymėjo, kad neteisėtas elektroninių duomenų panaudojimas, atliekant finansinę operaciją (vykdant finansinę operaciją) atitinka BK 198 straipsnio dispoziciją. Teisėjų kolegija nurodė, kad šiuo atveju panaudotas kodų generatorius nėra laikytinas el. mokėjimo instrumentu BK 215 straipsnio prasme, nes jo pagalba tik generuojami kodai, bet nevykdomi atsiskaitymai ne grynaisiais pinigais. Suprantama, kad teismas tokius generatoriaus išgaunamus kodus priskyrė el. duomenims atitinkančius BK 198 dispoziciją. Pažymėtina, jog ši byla pasiekė LAT, kuris nurodė, kad baudžiamasis įstatymas buvo taikytas netinkamai[120]. Pagal savo prasmę sugeneruoti slaptažodžiai, atpažinimo kodai ir pan. atitinka naudotojo tapatybės patvirtinimo priemonių duomenų požymį (BK 215 str.). Neteisėtas tokių duomenų panaudojimas atliekant mokėjimo pavedimą visiškai atitinka BK 215 straipsnyje numatytos veikos požymius ir vertintinas kaip neteisėtas finansinės operacijos atlikimas panaudojant svetimos mokėtojo priemonės naudotojo tapatybės patvirtinimo priemonės duomenis. Taigi elektroninės mokėjimo priemonės duomenys negali būti laikomi BK 198 straipsnio dalyku[121].

Tokia situacija yra susiklosčiusi ir atskiriant BK 215 bei 198^2 straipsnio dalykus, kadangi pastarasis taip pat numato atsakomybę už slaptažodžių, prisijungimo kodų ar kitokių duomenų disponavimą, turint tikslą panaudoti nusikalstamoje veikoje. Kalbant apie tikslą, galima paminėti tik tai, kad šiame straipsnyje numatytos priemonės ar kodai, neturėtų būti tapatinami tik su specialiai pritaikytomis priemonėmis ar kodais – dalyko požymius atitinka ir dvigubo naudojimo (angl. *dual-use*) priemonės, kurios gali būti naudojamos ir teisėtiems tikslams[122], nes pasitaiko atvejų, kai teismas siekdamas atskirti BK 215 ir 198^2 aiškina, jog elektroninės bankininkystės slaptažodžiai ir prisijungimo kodai yra BK 215 dalyku tik dėl to, kad nėra skirti ar specialiai pagaminti, ar pritaikyti nusikalstamoms veikoms daryti (Panevėžio apygardos teismo 2013 m. lapkričio 29 d. nuosprendis[123]; 2014 m. balandžio 18 d. nuosprendis[124]). Toks aiškinimas lemia tai, kad

[119] Vilniaus apygardos teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2011 m. gruodžio 23 d. nuosprendis baudžiamojoje byloje, Nr. 1A-977-92-2011.*
[120] Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2012 m. birželio 26 d. nutartis baudžiamojoje byloje, Nr. 2K-375/2012.*
[121] Klaipėdos apygardos teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2013 m. spalio 24 d. nutartis baudžiamojoje byloje, Nr. 1A-695-380-2013.*
[122] Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2015 m. gegužės 12 d. nutartis baudžiamojoje byloje, Nr. 2K-188-489/2015.*
[123] Panevėžio apygardos teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2013 m. lapkričio 29 d. nuosprendis baudžiamojoje byloje, Nr. 1A-767-350-2013.*

BK 198[2] veikos dalyku gali būti tik specialiai skirti nusikalstamoms veikoms daryti įrenginiai ir pan., kas nėra teisinga. Tiesa, atkreiptinas dėmesys, kad kartais teismuose tikslas, kaip atribojimo kriterijus nuo BK 215 yra pasitelkiamas ne tik BK 198[2], bet ir BK 198[1] atveju, aiškinant, jog nenustačius tikslo pamatyti informacinėje sistemoje laikomas duomenų bylas, susipažinti su duomenų turiniu, atlikti kitus veiksmus (juos keisti, trinti, kopijuoti ir t. t.) negalima veikos kvalifikuoti pagal BK 198[1] straipsnį[125]. Tokios išvados taip pat nėra pagrįstos, kadangi BK 198 ir 198[1] straipsnių fakultatyvieji subjektyvieji sudėčių požymiai (motyvai ir tikslai) gali būti įvairūs ir reikšmės kvalifikavimui neturi[126]. Apie tikslą galima kalbėti tik BK 198[2] atžvilgiu. Kaip bebūtų, tikslas ir šiuo atveju nėra esminis kriterijus pagal kurį galėtumėme atriboti BK 198[2] ir BK 214 taikymą, kadangi BK 198[2] straipsnyje jis yra bendro pobūdžio t. y. nusikalstamoms veikoms daryti, o BK 214 ir 215 straipsniuose numatytose sudėtyse tikslas nėra būtinasis požymis, taigi tikslas savaime nenusako skirtumo tarp BK 198[2] ir BK 214, 215 straipsnių.

Grįžtant prie BK 215 ir 198[2] pagrindinio skiriančio elemento, paminėtina kita LAT byla, kurioje kaltinamoji V. A. susipažinusi su A. Č. ir sužinojusi apie jos problemas skyrybų ir turto pasidalijimo su sutuoktiniu byloje, apsimetusi advokato padėjėja ir įgavusi A. Č. pasitikėjimą, gavo pastarosios el. bankininkystės identifikacinius duomenis, kuriais pasinaudojusi V. A. imdavo kreditus ir pervesdavo pinigų sumas sau į sąskaitą[127]. V. A. veika kvalifikuota pagal BK 198[2] ir 182 straipsnius. LAT dėl tokios kvalifikacijos nepasisakė ir paliko galioti apeliacinės instancijos teismo nuosprendį. Vis dėl to manytina, jog ir šiuo atveju turėtų būti išlaikyta tokia pati logika, kuria remtasi atskiriant BK 168 ir 198 straipsnius. BK 198[2] numatyti slaptažodžiai, prisijungimo kodai ir kiti panašūs duomenys yra daugiau bendresnio pobūdžio, priešingai nei BK 214 ir 215 straipsniuose įvardijami tapatybės patvirtinimo priemonių duomenys, kurie būtent skirti finansinėms operacijoms atlikti ar inicijuoti, be to taip pat gali būti ir elektroninės formos. Įvertinus tai ir BK 214, 215 straipsniai yra specialieji BK 198[2] straipsnio atžvilgiu.

Matyti, kad ir šiais atvejais teismas ne visada įvertina bendrosios ir specialiosios normų konkurenciją, būtent BK 214, 215 straipsnių specifiškumą BK XXX skyriuje numatytų veikų atžvilgiu, o kai kuriais atvejais net yra bandoma atskirti šias veikas pasitelkiant požymius, kurie neturi reikšmės kvalifikuojant veiką (pvz. tikslas – BK 198[1]

---

[124] Panevėžio apygardos teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2014 m. balandžio 18 d. nuosprendis baudžiamojoje byloje, Nr. 1A-117-581-2014.*

[125] Šiaulių apygardos teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2014 m. gegužės 7 d. nuosprendis baudžiamojoje byloje, Nr. 1A-388-309-2014.*

[126] Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2015 m. sausio 20 d. nutartis baudžiamojoje byloje, Nr. 2K-93-489/2015.*

[127] Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2012 m. kovo 27 d. nutartis baudžiamojoje byloje, Nr. 2K-117/2012.*

straipsnio atveju). Neabejotinai darytina išvada, kad tuo atveju, kai kaltininkas neteisėtai disponuoja elektroninės mokėjimo kortelės duomenimis, jam turi būti inkriminuojamos atitinkamai BK 214 ar 215 straipsnių normos.

2.2.2. Sudėties požymių aiškinimo problemos

Turbūt vienas iš dažniausiai pasitaikančių vertinamųjų požymių baudžiamajame įstatyme yra siejamas su žala. Šiame skyriuje žalos kriterijus yra šiek tiek specifinis dėl kai kurių techninių aspektų.

Pirmiausiai paminėtina, kad vertinant ar šiomis veikomis buvo sukelta didelė žala nedera vadovautis BK 212 straipsnio 1 dalimi, kuris didelę žalą sieja su 150 MGL. Dera nepamiršti principo, jog analogija baudžiamojoje teisėje negalima, todėl taikyti kitame skyriuje numatytus straipsnius taip pat nėra tinkamas variantas. Tą pažymėjo ir LAT, kadangi tokių atvejų pasitaikė ir teismų praktikoje. LAT nurodė, kad apeliacinės instancijos teismas, spręsdamas dėl patirtos turtinės žalos dydžio, klaidingai vadovavosi BK 212 straipsnio 1 dalimi, nepagrįstai didelę turtinę žalą siejo su 150 MGL dydžio sumą viršijančia žala. Šiame straipsnyje nurodytas 150 MGL dydžio kriterijus yra suformuluotas ir taikomas didelei turtinei žalai nustatyti nusikalstamose veikose ekonomikai ir verslo tvarkai. BK 212 straipsnio 1 dalyje tiesiogiai nurodyta, kad toks didelės turtinės žalos aiškinimas yra taikomas tik BK XXXI skyriuje nurodytai didelei žalai nustatyti, todėl buvo prieita netinkama išvada[128].

Antra, atsižvelgtina, kad šiomis nusikalstamomis veikomis gali būti padaryta ne tik turtinė, bet ir neturtinė žala kaip, pavyzdžiui, reputacijos pablogėjimas. Įdomu tai, kad ne visais atvejais gali kilti realiai patiriama žala, tačiau kaltininkas nuo baudžiamosios atsakomybės nėra atleidžiamas. Turima omenyje tie atvejai, kai duomenys yra sunaikinami (Kauno apygardos teismo 2012 m. spalio 22 d. nutartis[129]; Vilniaus apygardos teismo 2014 m. balandžio 16 d. nutartis[130]). Antai pirmojoje byloje A. A. nuteistas pagal BK 196 straipsnio 1 dalį dėl to, kad padarė neteisėtą poveikį elektroniniams duomenims, o būtent, pasinaudodamas kompiuteriu, panaudodamas programinę įrangą, neteisėtai sunaikino elektroninius duomenis, patalpintus internetinėje svetainėje, pakeitė juos kitais. Atrodytų, jog patiriama žala, tokiu atveju, kai duomenys yra ištrinami, turėtų sukelti mažiau problemų, nei tarkime kai ji yra nutekinama, nes

[128] Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2015 m. gegužės 12 d. nutartis baudžiamojoje byloje, Nr. 2K-188-489/2015.*
[129] Kauno apygardos teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2012 m. spalio 22 d. nutartis baudžiamojoje byloje, Nr. 1A-94-175-2012.*
[130] Vilniaus apygardos teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2014 m. balandžio 16 d. nutartis baudžiamojoje byloje, Nr. 1A-303-256-2014.*

apytikriai galima nustatyti tos informacijos vertę, kuri ir bus pagrindinis atskaitos taškas sprendžiant apie žalą. Tačiau šioje byloje kaltinamasis iškėlė pakankamai įdomų klausimą, teigdamas, kad ištrindamas elektroninius duomenis, jų visiškai nesunaikino, todėl juos galima atkurti. Teismas, atsakydamas į šį apeliacinio skundo argumentą, akcentavo ir tai, jog esanti galimybė specialios programinės įrangos pagalba atstatyti, atkurti sunaikintus, sugadintus, pakeistus ar pašalintus duomenis nepašalina baudžiamosios atsakomybės. Jos nepašalina ir tas faktas, kad nukentėjusysis turi tokių duomenų kopiją. Kaltinamojo argumentuose taip pat galima įžvelgti racijos – žvelgiant iš techninės pusės pavykus atkurti ištrintus duomenis, arba tais atvejais, kai auka turi duomenų kopiją, būtų galima teigti, kad nekilo padariniai, kaip būtinas materialiosios sudėties požymis. Kaip bebūtų, net ir objektyviai nekilus padariniams, kaltininko siekis ištrinti duomenis laikytinas pavojingu, kadangi tai rodo kaltininko nukreiptą tyčią žalos sukėlimui todėl, pavyzdžiui, likus tų duomenų kopijoms, tai turėtų būti vertinama, kaip nuo kaltininko nepriklausanti aplinkybė, o veiką kvalifikuoti kaip pasikėsinimą į neteisėtą poveikį asmens duomenims (BK 196 str.).

Kitas, nemažai dėmesio sulaukęs, požymis – BK 198[1] straipsnio 1 dalyje numatytas prisijungimas „pažeidžiant informacines sistemos apsaugos priemones“. Neteisėtumo kriterijus didesnių problemų nekelia – ar teisėtai jungiamasi prie IS, ar ne, spręstina pagal pareigines funkcijas[131], tai ar turimas teisėto valdytojo leidimas ir pan. Tačiau kas yra laikytina IS apsaugos priemonių pažeidimu? Čia paminėtina ir Direktyva. Iki jos priėmimo Budapešto konvencijos 2 straipsnyje buvo nustatyta, kad turi būti priimtas teisės aktas, kuriuo būtų numatyta baudžiamoji atsakomybė už sąmoningą ir neteisėtą prieigą prie visos kompiuterinės sistemos ar jos dalies. Konvencija taip pat numatė ir fakultatyviuosius požymius (tokius kaip kompiuterinės sistemos apsaugos priemonių pažeidimas ir kt.), kurie valstybių, prisijungusių prie Konvencijos, galėjo būti papildomai pripažinti kaip privalomi. Direktyva savo ruožtu 3 straipsnyje įtvirtino, kad už neteisėtą prieigą turi kilti baudžiamoji atsakomybė, jei tai neteisėtas, tyčinis prisijungimas, kai tai padaroma pažeidžiant apsaugos priemonę. Tuo Direktyva susilaukė kritikos, kadangi nustatydama požymį neteisėtam prisijungimui prie IS, nepateikė sąvokų, kas laikytina saugos priemone, kas prilygintina saugos priemonės pažeidimui[132]. Kita vertus, tai buvo palikta spręsti nacionalinei teisei ir teismų praktikai. Savo ruožtu, Lietuvos teismų praktika šiuo klausimu išsiskiria, ypatingai tais atvejais, kai yra vertinamas neteisėtas

[131] Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2014 m. liepos 1 d. nutartis baudžiamojoje byloje, Nr. 2K-345/2014.*

[132] FREITAS, P. M. F., GONÇALVES, N. Illegal access to information systems and the Directive 2013/40/EU. *International Review of Law, Computers & Technology*, 2015, Vol. 29:1, p. 50–62.

prisijungimas prie el. bankininkystės pasinaudojant svetimais tapatybės identifikavimo duomenimis.

Antai vienoje byloje kaltininkas neteisėtai prisijungė prie informacinės sistemos, neteisėtai įgijęs R. V. elektroninės bankininkystės sistemos vartotojo nuolatinį atpažinimo kodą, prisijungimo slaptažodį bei kiekvienam teisėtam vartotojui išduodamą identifikavimo kodų kortelę ir panaudodamas R. V. tapatybės patvirtinimo priemonių duomenis prisijungė prie AB banko „Snoras“ elektroninės bankininkystės sistemos inicijuoti ir atlikti finansines operacijas su jos sąskaitoje esančiomis lėšomis[133]. Teismas R. V. tapatybės duomenų panaudojimą pripažino kaip IS apsaugos priemonių pažeidimą ir kaltininkui inkriminavo BK 198[1] straipsnį. Visiškai priešingos pozicijos buvo laikytasi kitose analogiškose bylose, kai būdavo prisidengiant kito asmens tapatybe prisijungiama prie el. banko IS (Šiaulių apygardos teismo 2014 m. kovo 31 d. nuosprendis[134]; Kauno apygardos teismo 2014 m. sausio 21 d. nuosprendis[135]; 2015 m. gegužės 7 d. nutartis[136]). Šiose nutartyse teismas pažymėjo, kad kaltinamieji, įgyvendindami savo nusikalstamus sumanymus, teikdami paraiškas juridiniams asmenims dėl kreditų, prisijungdami prie bankų informacinės sistemos – elektroninės bankininkystės, atlikdami kitas nurodytas finansines operacijas, nėra pažeidę jokių informacinės sistemos apsaugos priemonių, jų sugadinę, pakenkę apsaugos priemonių režimui, sutrikdę informacinės sistemos darbą ir pan. Kaltininkai prie informacinių sistemų neteisėtai jungėsi naudodamiesi tikrais, nors ir neteisėtai gautais elektroninių mokėjimo priemonių naudotojų tapatybės patvirtinimo priemonių duomenimis ir informacinių sistemų apsaugos priemonių nepažeidė.

Galiausiai LAT yra suformavęs teismų praktiką bei aiškią savo poziciją šiuo klausimu, kadangi dėl šio požymio pasisakė keliose nutartyse (LAT 2012 m. birželio 26 d. nutartis[137]; 2015 m. sausio 6 d. nutartis[138]; 2015 m. gruodžio 8 d. nutartis[139]; 2016 m. sausio 26 d. nutartis[140]). Jose pažymima, kad: 1) vartotoją informacinėje

[133] Vilniaus apygardos teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2014 m. gegužės 12 d. nuosprendis baudžiamojoje byloje, Nr. 1A-294-195-2014.*
[134] Šiaulių apygardos teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2014 m. kovo 31 d. nuosprendis baudžiamojoje byloje, Nr. 1A-169-354-2014.*
[135] Kauno apygardos teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2014 m. sausio 21 d. nuosprendis baudžiamojoje byloje, Nr. 1A-82-327-2014.*
[136] Kauno apygardos teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2015 m. gegužės 7 d. nutartis baudžiamojoje byloje, Nr. 1A-432-594/2015.*
[137] Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2012 m. birželio 26 d. nutartis baudžiamojoje byloje, Nr. 2K-375/2012.*
[138] Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2015 m. sausio 6 d. nutartis baudžiamojoje byloje, Nr. 2K-138/2015.*
[139] Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2015 m. gruodžio 8 d. nutartis baudžiamojoje byloje, Nr. 2K-555-788/2015.*
[140] Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2016 m. sausio 26 d. nutartis baudžiamojoje byloje, Nr. 2K-4-507/2016.*

sistemoje leidžianti nustatyti autentiškumo patvirtinimo procedūra gali būti laikoma viena iš šios sistemos saugumo (taip pat ir konfidencialumo) užtikrinimo priemonių, 2) teisėto vartotojo tapatybę patvirtinančių duomenų neteisėtas įvedimas, suklaidinant sistemą, laikytinas šios sistemos apsaugos priemonių pažeidimu ir 3) neteisėtas prisijungimas prie informacinės sistemos (internetinės bankininkystės sistemos) pažeidžiant autentifikavimo priemonėmis nustatytų prisijungimo prie informacinės sistemos apribojimus (reikalavimus) paprastai negali būti laikomas nereikšmingu, vertinant jį iš baudžiamosios teisės pozicijų, ypač jei tai leido padaryti kitus neteisėtus veiksmus sistemoje. Dėl to teisėto vartotojo tapatybę patvirtinančių duomenų neteisėtas įvedimas, suklaidinant sistemą, laikytinas šios sistemos apsaugos priemonių pažeidimu ir atitinka neteisėto prisijungimo prie informacinės sistemos veikos padarymo būdą. BK 198[1] straipsnis gali būti taikomas kartu su BK 215 straipsniu. Niekam nekils abejonių, kad sistemos reikalavimas suvesti slaptažodį laikytinas apsaugos priemone, kadangi taip užtikrinamas tos sistemos konfidencialumas ir prieinamumas tik sankcionuotiems asmenims. LAT minėtose bylose palaikė idėją, kad slaptažodžio suvedimas ne to asmens, kuriam priklauso el. bankininkystės paskyra laikytina pažeidimu, kadangi žiūrint iš baudžiamosios teisės pozicijų tokia veika laikytina pavojinga. Tik 2016 metų byloje LAT nurodė, kaip pasireiškė pažeidimas: „E. J., pažeisdamas, t. y. suklaidindamas, <...> informacinės sistemos apsaugos priemones, įvesdamas neteisėtai įgytus nukentėjusiosios D. B. vardu išduotus internetinės prieigos duomenis[141]“. Trumpai tariant LAT teigimu – informacinės sistemos apsaugos priemonė yra pažeidžiama, jei ji yra suklaidinama, apsimetant kitu asmeniu.

Bet ar tikrai tokiu būdu pažeidžiama apsaugos sistema, suklaidinama pati IS? Galima ginčytis. Minėtų bylų atvejais, kaltininkai tik suvesdavo kito asmens prisijungimo kodus. Būtent tokius, kurių prašė ir reikalavo informacinė sistema. Jei IS reikalauja slaptažodžio X ir mes suvedame slaptažodį X, viskas veikia įprastine tvarka – saugos sistema sulygina jai pateiktus duomenis su jau turimais duomenimis duomenų bazėje ir jei randa visišką atitikimą, leidžia patekti į IS. Jei tais atvejais kaltininkai būtų suvedę vietoje prašomo slaptažodžio X, slaptažodį Y, apsaugos sistema būtų atmetusi vartotojo reikalavimą patekti į IS. Vadinasi pati saugos sistema veikia 100 proc. teisingai, taip kaip ir jai pridera veikti, todėl savaime nėra pažeista. Pažeidimą būtų galima konstatuoti tuo atveju, jei kaltininkas būtų paveikęs slaptažodžio saugos sistemą taip, kad ji visiškai neveiktų arba veiktų, tačiau netinkamai, pavyzdžiui, apsaugos sistema priimtų bet kokią

[141] Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2016 m. sausio 26 d. nutartis baudžiamojoje byloje, Nr. 2K-4-507/2016.*

skaičių ar raidžių kombinaciją, tarkim, kad ir „000“. Šiais atvejais aiškiai matomas tinkamas apsaugos veikimo funkcijų sutrikimas ir neabejotinai būtų laikoma minėto BK 198^1 požymio atitikimu. LAT argumentai dėl apsaugos sistemos pažeidimo, kaip IS suklaidinimo, taip pat yra abejotini. Ar kaltininkas tikrai suklaidina informacinę sistemą pateikdamas būtent tuos duomenis, kurių ji prašo? Žiūrint iš techninės pusės, pačiai informacinei sistemai nėra svarbu, kas fiziškai suveda reikalaujamus slaptažodžius, koks asmuo atlieką duomenų įvestį. Jai rūpi tik pateiktų duomenų tikslumas. Priešingu atveju, jei laikytume, kad suvesti duomenis neklaidindamas sistemos gali tik tas asmuo, prie kurio el. banko sistemos yra jungiamasi, gaunama situacija, kai pažeidimui konstatuoti užtenka, jog vietoje asmens A, duomenis suvestų asmuo B. Net jei ir B tai daro teisėtai t. y. su A leidimu ar priežiūra, B pažeistų IS apsaugos priemones, nes esą IS tikėjosi, jog duomenis suves asmuo A. Tokiu atveju matomas visiškas BK 198^1 straipsnio antrojo požymio t. y. IS apsaugos priemonių pažeidimo priklausomumas nuo pirmojo – neteisėtumo. Vadovaujantis LAT išaiškinimu, iš esmės užtenka tik to, kad asmuo ketintų prisijungti prie IS neteisėtai ir automatiškai bus pripažintas apsaugos priemonių pažeidimo požymis. Matyti, kad pagal aprašymo būdą BK 198^1 straipsnyje įtvirtinta sudėtinga nusikalstamos veikos sudėtis t. y. sudėtis su dviem veiksmais – neteisėtai prisijungė ir pažeidė IS apsaugos priemones. Darytina išvada, kad šie du veiksmai privalo būti išpildyti, nes jie nėra alternatyvūs. Atsižvelgiant į tai, BK 198^1 straipsnio taikymas minėtais atvejais, kai prie el. bankininkystės neteisėtai prisijungiama naudojant tinkamus slaptažodžius, nebūtų galimas.

Žinoma, suprantama ir teismo pozicija šiuo atveju, siekiant apsaugoti aukos teises bei teisėtus interesus, siekiant užtikrinti, jog iš baudžiamosios teisės pozicijų liktų įvertintas pats neteisėto prisijungimo prie paskyros veiksmas. Tačiau nedera pamiršti ir *nullum crimen sine lege* principo, kuris bendriausiu požiūriu reiškia, kad nusikalstamos veikos požymiai baudžiamajame įstatyme turi būti tiksliai (apibrėžimo tiksli formuluotė) ir aiškiai (turinio suvokimas) apibrėžti. LAT išaiškinimas leidžia abu atskirus požymius apjungti ir aiškinti kaip vieną, kadangi neteisėtumas BK 198^1 straipsnio atžvilgiu nulemia ir apsaugos priemonių pažeidimą. Vis dėlto tokia situacija prasilenkia su minėtuoju principu, kadangi įstatymų leidėjas aiškiai ir nedviprasmiškai kelis požymius išskyrė į savarankišką norminį krūvį turinčius minimumus.

3. Kibernetiniai nusikaltimai užsienio šalyse, tendencijos tarptautiniu mastu

3.1. Užsienio šalių teisinis reglamentavimas

Aptariant Lietuvos BK, nemažai buvo kalbėta apie jo XXX skyrių. Nepaisant tam tikrų išimčių, kai BK 196–198[2] straipsniuose numatytos veikos gali būti padaromos fizinėje erdvėje, remiantis pirmoje šio darbo dalyje išvestu apibrėžimu, BK XXX skyrių galima vertinti, kaip skyrių iš esmės kriminalizuojančiu kibernetinius nusikaltimus.

Dėl to pakankamai įdomu išanalizuoti kitų valstybių baudžiamuosius kodeksus, pažvelgti, kokią vietą baudžiamuosiuose įstatymuose užima kibernetiniai nusikaltimai.

Visgi pastebėta, kad nemažai valstybių tam tikrus kibernetinius nusikaltimus išskaido pagal jų keliamą grėsmę teisiniam gėriui. Tačiau šie nusikaltimai ne visada įvardijami, kaip pažeidžiantys elektroninių duomenų ar informacinių sistemų saugumą. Štai Estijos Respublikos baudžiamajame kodekse[142] (toliau – Estijos BK) poveikis kompiuteriniams duomenims ir poveikis informacinėms sistemoms yra priskirti prie nusikaltimų darančių žalą nuosavybei. Kita dalis jų, t. y. neteisėtas prisijungimas, disponavimas įrenginiais, programine įranga ir kt. numatyta skyriuje pavadinimu „neteisėtas naudojimas“. Latvijos Respublikos baudžiamajame kodekse[143] (toliau – Latvijos BK) nusikaltimai informacinėms sistemoms bei elektroniniams duomenims numatyti nusikaltimų prieš bendrąjį saugumą ir viešąją tvarką, kartu su tokiomis veikomis kaip masinės riaušės, kapų ir palaikų išniekinimas, žiaurus elgesys su gyvūnais ir pan. Šveicarijos Konfederacija neteisėtą elektroninių duomenų perėmimą, prisijungimą prie duomenų apdorojimo sistemos pasitelkiant duomenų persiuntimo priemones, ar žalingą poveikį duomenims priskiria nusikaltimų nuosavybei skyriui, šalia plėšimo, vagystės, sukčiavimo sudėčių[144]. Štai Kanados baudžiamajame kodekse[145] (toliau – Kanados BK) kompiuterinių duomenų (Kanados BK 430(1.1) str.) sunaikinimas priskiriamas prie pogrupio nusikalstamų veikų, kuriomis niokojamos kultūrinės vertybės, religinės vertybės, kariniai memorialai ir pan. Prie šių valstybių grupės priskirtina ir Suomijos

[142] Estijos Respublikos baudžiamasis kodeksas [interaktyvus; žiūrėta 2017 m. vasario 20 d.]. Prieiga per internetą: <http://www.legislationline.org/documents/section/criminal-codes>.
[143] Latvijos Respublikos baudžiamasis kodeksas [interaktyvus; žiūrėta 2017 m. vasario 20 d.]. Prieiga per internetą: <http://www.legislationline.org/documents/section/criminal-codes>.
[144] Šveicarijos Konfederacijos baudžiamasis kodeksas [interaktyvus; žiūrėta 2017 m. vasario 20 d.]. Prieiga per internetą: <http://www.legislationline.org/documents/section/criminal-codes>.
[145] Kanados baudžiamasis kodeksas [interaktyvus; žiūrėta 2017 m. vasario 20 d.]. Prieiga per internetą: <http://www.legislationline.org/documents/section/criminal-codes>.

Respublika. Suomijos Respublikos baudžiamasis kodeksas[146] (toliau – Suomijos BK) tokias veikas kaip poveikį elektroniniams duomenims ir poveikį informacinėms sistemoms išskiria į du atskirus skyrius: pirmąjį – prie nusikaltimų, kuriais keliama kriminalinė žala, antrąjį – prie duomenų ir komunikacijos nusikaltimų skyriaus.

Egzistuoja ir valstybės, kurios „neišbarsto“ kibernetinių nusikaltimų keliuose baudžiamojo kodekso skyriuose. Maltos Respublikos baudžiamasis kodeksas[147] turi atskirą poskyrį tokioms nusikalstamoms veikoms, kuris vadinasi „piktnaudžiavimas kompiuteriu“. Jame ne tik išvardinamos nusikalstamų veikų sudėtys, bet ir paaiškinamos specifinės vartojamos sąvokos, pavyzdžiui, kompiuteris, kompiuteriniai duomenys, kompiuterių tinklas ir pan. O štai Gruzijos[148] ir Bulgarijos Respublikos[149] baudžiamuosiuose kodeksuose išskirti skyriai juos taip ir pavadinant – kibernetiniai nusikaltimai.

Matyti, kad požiūris į kibernetinius nusikaltimus nėra vienodas. Vienos valstybės kompiuterinius duomenis priskiria nuosavybei taip priskirdamos dalį veikų prie nusikaltimų nuosavybei, kitos neteisėtas veikas kibernetinėje erdvėje sulygina su nusikaltimais viešajai tvarkai, galiausiai pateikti atvejai rodo, kad ir pats kibernetinių nusikaltimų terminas kai kurių valstybių teisinėje sistemoje, išskiriant tokias veikas į atskirus skyrius, nėra svetimas.

Kita vertus, vertinant patį turinį pastebima tendencija, jog branduolys kibernetinių nusikaltimų išlieka daugmaž toks pat – kriminalizuotos veikos, kuriomis neteisėtai paveikiami kompiuteriniai duomenys, informacinės sistemos, neteisėtai prie jų prisijungiama ar disponuojama neleistina programine įranga ir pan. Žinoma, šios veikos nėra apibrėžtos visiškai vienodai. Antai Estijos BK 206^1 straipsnis numato ir neteisėtą galinių įrenginių identifikacinių priemonių pakeitimą ar panaikinimą. Bosnijos ir Hercegovinos baudžiamojo kodekso 394 straipsnis apibrėžia kompiuterio duomenų ar programų padirbimą[150]. Vokietijos Federacinės Respublikos baudžiamojo kodekso[151] 303b straipsnio 2 dalis, draudžianti neteisėtą poveikį duomenų apdorojimo operacijoms, numato didesnę atsakomybę ne tik už poveikį tokioms operacijoms, kurios svarbios

[146] Suomijos Respublikos baudžiamasis kodeksas [interaktyvus; žiūrėta 2017 m. vasario 20 d.]. Prieiga per internetą: <http://www.legislationline.org/documents/section/criminal-codes>.
[147] Maltos Respublikos baudžiamasis kodeksas [interaktyvus; žiūrėta 2017 m. vasario 20 d.]. Prieiga per internetą: <http://www.legislationline.org/documents/section/criminal-codes>.
[148] Gruzijos baudžiamasis kodeksas [interaktyvus; žiūrėta 2017 m. vasario 20 d.]. Prieiga per internetą: <http://www.legislationline.org/documents/section/criminal-codes>.
[149] Bulgarijos Respublikos baudžiamasis kodeksas [interaktyvus; žiūrėta 2017 m. vasario 20 d.]. Prieiga per internetą: <http://www.legislationline.org/documents/section/criminal-codes>.
[150] Bosnija ir Hercegovinos baudžiamasis kodeksas [interaktyvus; žiūrėta 2017 m. vasario 20 d.]. Prieiga per internetą: <http://www.legislationline.org/documents/section/criminal-codes>.
[151] Vokietijos Federacinės Respublikos baudžiamasis kodeksas [interaktyvus; žiūrėta 2017 m. vasario 20 d.]. Prieiga per internetą: <http://www.legislationline.org/documents/section/criminal-codes>.

nacionaliniam saugumui, bet ir įmonei ar verslui, taip saugant ne tik visuomeninį, bet ir privatų verslo sektorių. Suomijos BK taip pat galima aptikti ne mažiau įdomių nusikalstamų veikų sudėties požymių, tarkime, kaip neteisėto poveikio IS, sunkinančią aplinkybę išskiria nusikaltimo padarymo būdą, kai poveikis IS sistemai yra padarytas itin planingu metodu. Taip pat galime rasti ir tokių įdomių veikų, kurios tikrąją prasme nebūtų laikomos kibernetiniais nusikaltimais, tačiau saugo el. duomenis ar IS. Pavyzdžiui, Maltos BK 337D straipsniu draudžiamas kompiuterinės įrangos ar jos aprūpinimo resursų, kuriuos naudoja kompiuteris, modifikavimas ar gadinimas. Tokiu atveju pakanka paveikti IS, net ir nutraukiant elektros energijos tiekimą techninei įrangai, kuri ją palaiko. Kai kurios valstybės savo ruožtu išsiskiria ne kitokiu sudėčių ar požymių numatymu, o skiriamomis sankcijomis. Pavyzdžiui, Albanijos Respublikos baudžiamajame kodekse už tokias veikas kaip poveikis el. duomenims ar IS, neteisėtu disponavimu įrenginiais, slaptažodžiais, nėra skiriamos alternatyvios bausmės apart laisvės atėmimo. O ir ribos ganėtinai įstabios. Štai už antroje Albanijos BK 293/b straipsnio dalyje (poveikis el. duomenims), numatančioje kvalifikuojančią sudėtį, kai tai liečia valstybės saugumą, viešąją tvarką, sveikatos apsaugą ir pan. skiriama nuo 3 iki 10 m. laisvės atėmimo bausmė. Už poveikį IS Albanijos BK 293/c straipsnio pirma dalis numato nuo 3 iki 7 m. laisvės atėmimą, o štai kvalifikuotoje sudėtyje – net nuo 5 iki 15 m. laisvės atėmimo laikotarpį. Lietuvos BK rėmuose, tokia sankcija beveik atitinka už nužudymą skiriamą bausmę. Net pačios Albanijos BK 76 straipsnis už nužudymą numato nuo 10 iki 20 m. laisvės atėmimo. Taigi matyti, kokios griežtos sankcijos gali būti taikomos už kibernetinius nusikaltimus.

Galiausiai palyginus Lietuvos BK su kitų šalių baudžiamaisiais įstatymais, nepaisant minimalių skirtumų, pastebėtina, kad nemažai šalių yra perėmusios ir Konvencijoje numatytą kibernetinį nusikaltimą – kompiuterinį sukčiavimą. Šią sudėtį numato tokios valstybės kaip Vokietija, Šveicarija, Austrija[152], Estija, Latvija, Bosnija ir Hercegovina, Albanija. Pasikartotina, kad kompiuterinis sukčiavimas tai – sąmoningas, neteisėtas veiksmas sąlygojęs kito asmens nuosavybės praradimą įvedant, pakeičiant, sunaikinant kompiuterinius duomenis arba panaikinant galimybę naudotis tokiais duomenimis arba paveikiant kompiuterinės sistemos darbą nesąžiningai arba nedorai ketinant gauti neteisėtos ekonominės naudos sau arba kitam asmeniui. Lietuvos BK šios sudėties nenumato. Kaip bebūtų, 2007 m. gegužės 30 d. Budapešto konvencijos

[152] Austrijos Respublikos baudžiamasis kodeksas [interaktyvus; žiūrėta 2017 m. vasario 20 d.]. Prieiga per internetą: <http://www.legislationline.org/documents/section/criminal-codes>.

įgyvendinimo apybraižoje[153] nurodyta, kad Budapešto konvencijos 8 straipsnis dėl kompiuterinio sukčiavimo įgyvendintas trimis BK straipsniais: 196, 197 ir 182. Taigi, matoma, kad Lietuvos atveju, vietoje naujos nusikalstamos veikos sudėties, pasitelkiama sukčiavimo (BK 182 str.) sudėtis. Tačiau toks Budapešto konvencijos 8 straipsnio įgyvendinimas yra problemiškas.

Pastebėtina, kad tiek kitų šalių baudžiamuosiuose įstatymuose, tiek Budapešto konvencijos 8 straipsnyje ekonominės naudos gavimas pasireiškia paveikiant kompiuterinius duomenis ar IS. BK 182 straipsnio objektyviosios pusės veikos požymį iš esmės apibrėžia apgaulės panaudojimas. Skirtumas tas, kad Lietuvos atveju, siekiant įvertinti ekonominės naudos gavimą baudžiamosios teisės atžvilgiu, būtinas BK 182 straipsnio inkriminavimas, taigi ir apgaulės konstatavimas. Probleminis klausimas šiuo atveju – ar galima apgaulė kibernetinių nusikaltimų atveju? Viena vertus, analizuojant kibernetinių nusikaltimų koncepciją, šio darbo pirmojoje dalyje išsiaiškinta, kad tokioms nusikalstamoms veikoms nėra būdingas socialinis manipuliacijos dialogas tarp subjekto ir aukos. Kita vertus, LAT praktikoje pasisakoma, kad gali būti suklaidinta, t. y. panaudota apgaulė, ir elektroninė sistema (LAT 2001 m. spalio 9 d. nutartis[154], 2005 m. lapkričio 15 d. nutartis[155], 2012 m. birželio 26 d. nutartis[156]). Nuo šio klausimo priklausytų tai, ar galimas BK 182 straipsnio taikymas kibernetinių nusikaltimų atžvilgiu, ar nebūtų pažeidžiamas teisėtumo principas.

Minėtose nutartyse LAT, kalbėdamas apie elektroninės sistemos suklaidinimą, pažymėjo, kad el. sistema sudaryta tokiu būdu, jog ji priima komandą ir atlieka operaciją, jei surinkti tinkami sąskaitų turėtojų identifikaciniai kodai. Būtent kodas pagal programos veikimo principus identifikuoja asmens, kaip sąskaitos turėtojo, tapatybę ir pažymi teisę atlikti operacijas su sąskaitoje esančiomis piniginėmis lėšomis. Jei kodą surenka ir komandą duoda asmuo, neturintis teisės atlikti operacijų su sąskaitoje esančiomis piniginėmis lėšomis, jis pateikia operacinei sistemai ir bankui save kaip kitą asmenį, turintį tokią teisę, ir taip suklaidina elektroninę sistemą. Tačiau šiuose teismo argumentuose nėra gilinamasi į pačią apgaulės esmę. Apgaulė – tai dėl kaltininko

---

[153] 2007 m. gegužės 30 d. Europos Tarybos projekto dėl kibernetinių nusikaltimų, Lietuvos teisinio reglamentavimo profilis (30 May 2007 Cybercrime legislation – country profile (Lithuania) of the Council of Europe's Project on Cybercrime) [interaktyvus; žiūrėta 2017 m. kovo 23 d.]. Prieiga per internetą: <http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/CountryProfiles/567-LEG-country%20profile%20Lithuania%20_30%20May%2007_En.pdf>.

[154] Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2001 m. spalio 9 d. nutartis baudžiamojoje byloje, Nr. 2K-682/2001.*

[155] Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2005 m. lapkričio 15 d. nutartis baudžiamojoje byloje Nr. 2K-587/2005.*

[156] Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2012 m. birželio 26 d. nutartis baudžiamojoje byloje, Nr. 2K-375/2012.*

objektyviosios tiesos iškraipymo nukentėjusiojo sąmonėje susiformavęs klaidingas įsivaizdavimas objektyviai egzistuojančių faktų, kurie nukentėjusįjį paskatina nenaudingai disponuoti turtu[157]. Taigi, apgaulė pasireiškia tuo, kad objektyvios tiesos iškraipymas nukentėjusįjį turi paskatinti priimti jam nenaudingą sprendimą. Tą pažymi ir LAT teismų praktikoje pabrėždamas, kad apgaulė turi būti esminė, t. y. nukentėjusiojo suklaidinimas dėl kaltininko ketinimų turi turėti lemiamą įtaką asmens apsisprendimui dėl turto ar turtinės teisės perdavimo kitam asmeniui[158]. Be to, teismas atsižvelgia ir į nukentėjusiojo apdairumo kriterijų – naudojama apgaulė turi įveikti bent minimalų protingo nukentėjusiojo elgesio lygį[159]. Atsižvelgus į šią teismų praktiką, kyla klausimas kaip galima panaudoti apgaulę prieš informacinę sistemą, jei ši tiesiog mechaniškai seka numatytais veikimo algoritmais? Pati informacinė sistema negeba priimti savarankiškų sprendimų, todėl minimalaus nukentėjusiojo apdairumo kriterijaus taikymas nėra galimas, lygiai taip pat, kaip nebūtų galima teigti, kad iškreipta tiesa suformavo kitokią informacinės sistemos sąmonėje egzistuojantį įsivaizdavimą. Tai yra subjektyvūs kriterijai, kurie nedera kibernetinių nusikaltimų kontekste, nes juose subjektas veiką nukreipia ne prieš kitą asmenį, o elektroninius duomenis ar IS. Pavyzdžiui, kaltininkas paveikdamas elektroninius duomenis ar IS iš banke esančių sąskaitų ar bankinių pavedimų metu perveda dalį lėšų į kitą turimą sąskaitą ir taip neteisėtai pasipelno. Šiuo atveju galima inkriminuoti atitinkamai BK 196, 197 straipsnius, tačiau BK 182 straipsnio inkriminavimas prieštarautų teisėtumo principui, kadangi nėra galimas apgaulės požymio konstatavimas. Susidaro situacija, kai subjekto nusikalstama veika baudžiamosios teisės aspektu lieka įvertinta tik iš dalies – įvertinamas poveikis el. duomenims ar IS, bet ne materialinės naudos gavimas.

Atsižvelgiant į tai, ir sekant kitų šalių praktika bei Budapešto konvencijos reglamentavimu, darytina išvada, jog būtų pravartu numatyti naują sudėtį, kuri numatytų baudžiamąją atsakomybę tam, kuris neteisėtai paveikdamas el. duomenis, programinę įrangą ar IS savo ar trečiųjų asmenų naudai įgijo turtinę naudą. Tokia sudėtis leistų visapusiškai įvertinti baudžiamosios teisės prasme kaltininkų veiksmus.

[157] Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2017 m. sausio 10 d. nutartis baudžiamojoje byloje, Nr. 2K-33-303/2017*.
[158] Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2014 m. birželio 19 d. nutartis baudžiamojoje byloje, Nr. 2K-327/2014*.
[159] Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2011 m. sausio 18 d. nutartis baudžiamojoje byloje, Nr. 2K-81/2011*.

3.2. Kibernetiniai nusikaltimai ir Tarptautinis baudžiamasis teismas

3.2.1. Tarptautinio baudžiamojo persekiojimo idėja

Kibernetiniai nusikaltimai neretai padaromi tarptautiniu mastu ir net gali būti taikomi kaip spaudimo darymo priemonė valstybių tarptautiniuose santykiuose, todėl visiškai nenuostabu, jog šiuos nusikaltimus siekiama „perkelti“ į tarptautinį lygmenį. 2012 m. teisėjas S. Schjolberg Hagoje vykusioje tarptautinės baudžiamosios teisės konferencijoje pristatė Tarptautinio baudžiamojo tribunolo (toliau – Tribunolas) kibernetiniams nusikaltimams įkūrimo idėją[160]. Teisėjas išdėstė tarptautinio baudžiamojo persekiojimo svarbą tais atvejais, kai kibernetinės atakos atliekamos prieš vyriausybių ar privačios pramonės infrastruktūrą, kelia grėsmę visuotinei taikai ir apima globalius kibernetinių nusikaltimų atvejus[161]. Dar 2011 m. buvo įžvelgtas Tribunolo poreikis ir galima nauda įgyvendinant tarptautinius standartus kovoje su šiais nusikaltimais[162]. S. Schjolberg pristatė šią idėją, numatant Tribunolo galimą struktūrą, jį sudarančias darbo bei tyrėjų grupes, statuto, kurio pagrindu būtų kuriama ir apibrėžta Tribunolo veikla, turinį. Teisėjas kaip alternatyvą Tribunolui, užsimena ir apie galimybę praplėsti Tarptautinio baudžiamojo teismo (toliau – TBT) jurisdikciją. Tačiau siekdamas visiško globalaus poveikio, argumentuodamas tuo, kad didžiosios valstybės kaip Kinija, Rusija, JAV nėra ratifikavusios Tarptautinio baudžiamojo teismo Romos Statuto[163] (toliau – ir Statutas), mano jog, veiksmingesnis būtų Tribunolo įkūrimas pasinaudojant Jungtinių Tautų Chartijos[164] (toliau – ir Chartija) 7 straipsnio 2 dalyje numatyta galimybe steigti reikalingas pagalbines institucijas, taip iš esmės apimant visas valstybes, kurias saisto Chartija[165].

Žinoma, tokio Tribunolo poveikis būtų nepalyginamai didesnis, tačiau nedera pamiršti, kad ir sukūrimo procesas nėra lengvas. Nepaisant to, galima įvertinti jau turimų priemonių išnaudojimo galimybes – išanalizuoti ar kibernetiniai nusikaltimai galėtų

---

[160] SCHJOLBERG, S. Peace and Justice in Cyberspace. Potential new international legal mechanisms against global cyberattacks and other global cybercrime [interaktyvus; žiūrėta 2017 m. vasario 23 d.]. Prieiga per internetą: <http://www.cybercrimelaw.net/documents/ICLNSummary.pdf>.

[161] *Ibid.*

[162] STAHL, W. M. The Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity. *Georgia Journal of International and Comparative Law*, 2011 m., Vol. 40, Issue. 1, p. 247–273.

[163] Tarptautinio baudžiamojo teismo Romos Statutas, priimtas 1998 m. liepos 17 d. Jungtinių Tautų diplomatinėje įgaliotųjų atstovų konferencijoje, skirtoje Tarptautinio baudžiamojo teismo įsteigimui. *Valstybės žinios*, 2003, Nr. 49-2165.

[164] Jungtinių Tautų Chartija. *Valstybės žinios*, 2002, Nr. 15-557.

[165] SCHJOLBERG, S. Peace and Justice in Cyberspace. Potential new international legal mechanisms against global cyberattacks and other global cybercrime [interaktyvus; žiūrėta 2017 m. vasario 23 d.]. Prieiga per internetą: <http://www.cybercrimelaw.net/documents/ICLNSummary.pdf>.

patekti į TBT jurisdikciją. Vis dėlto Statutą yra ratifikavusios 124 valstybės[166], taigi kibernetinių nusikaltimų priskyrimas TBT taip pat turėtų nemažai įtakos.

3.2.2. Romos Statuto pataisos

Statuto 5 straipsnio 1 dalis numato TBT jurisdikcijai priklausančius nusikaltimus: genocidas, nusikaltimai žmoniškumui, karo bei agresijos nusikaltimai. Pirmosios dvi kategorijos neabejotinai netinka. Kibernetiniai nusikaltimai taip pat negalėtų būti prilyginami karo nusikaltimams, nors literatūroje pakankamai dažnai randama kibernetinio karo sąvoka[167]. Tačiau kaip dėl agresijos nusikaltimų?

Ilgą laiką Statute nebuvo apibrėžta agresijos nusikaltimų sąvoka. Tai nebuvo padaryta iki 2010 m. priimtų Statuto, dar vadinamų, Kampalos pataisų[168]. Kampalos pataisose numatyta, kad TBT galės vykdyti jurisdikciją šiems nusikaltimams jei juos priims ar ratifikuos bent 30 Statuto šalių, taip pat jei po 2017 m. sausio 1 d. dviejų trečdalių Statuto šalių balsų daugumos sprendimu bus priimtos šios pataisos. Pataisos sulaukė kitų tarptautinių institucijų palaikymo, buvo rekomenduojama ratifikuoti šias pataisas (jas rekomendavo priimti Europos Parlamentas[169]). Šiai dienai tai padariusios yra 32 valstybės, tarp kurių yra ir Lietuva[170].

Kampalos pataisų 8*bis* straipsnį, apibrėžiantį agresijos nusikaltimus, galima suskirstyti į 3 segmentus. 1) 8*bis* straipsnio 1 dalis numato, kad agresijos nusikaltimas – asmens, galinčio veiksmingai kontroliuoti valstybės politinius ar karinius veiksmus ar jiems vadovauti, planuojamas, rengiamas, inicijuojamas ar vykdomas agresijos aktas, kuris savo pobūdžiu, sunkumu ir mastu akivaizdžiai pažeidžia Jungtinių Tautų Chartiją. 2) 8*bis* straipsnio 2 dalyje numatyta agresijos akto sąvoka. 3) 8*bis* straipsnio 2 dalyje

---

[166] Romos statuto valstybės narės – chronologinė seka [interaktyvus; žiūrėta 2017 m. vasario 23 d.]. Prieiga per internetą: <https://asp.icc-cpi.int/en_menus/asp/states%20parties/Pages/states%20parties%20_%20chronological%20list.aspx>.

[167] HOLLIS, D., B. Why States Need an International Law for Information Operations. *Lewis & Clark Law Review*, 2007, Vol. 11, Issue 4, p. 1023–1061.

[168] 2010 m. birželio 11 d. Romos Statuto Peržiūros konferencijos rezoliucija Nr. RC/Res.6 (Resolution RC/Res.6, adopted on 11 June 2010 by the Review Conference of the Rome Statute) [interaktyvus; žiūrėta 2014 m. vasario 23 d.]. Prieiga per internetą: <https://asp.icc-cpi.int/iccdocs/asp_docs/Resolutions/RC-Res.6-ENG.pdf>.

[169] 2010 m. gegužės 19 d. Europos Parlamento rezoliucija P7_TA(2010)0185 dėl Tarptautinio baudžiamojo teismo Romos statuto peržiūros konferencijos Kampaloje, Uganda (European Parliament resolution P7_TA(2010)0185 of 19 May 2010 on the Review Conference on the Rome Statute of the International Criminal Court, in Kampala, Uganda) (OL 2010 CE 161, p. 78).

[170] Tarptautinio baudžiamojo teismo Romos statuto pataisas dėl agresijos nusikaltimų priėmusios/ratifikavusios valstybės: <https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-10-b&chapter=18&clang=_en>.

numatytas pavyzdinis sąrašas agresijos aktui prilygstančių veiksmų, kurie tiesiogiai yra perimti iš JT Generalinės Asamblėjos rezoliucijos[171].

Nagrinėjant 8*bis* 1 dalį pažymėtina, kad agresijos nusikaltimai, priešingai nei karo nusikaltimai, reguliuoja *jus ad bellum* pažeidimus. Pabrėžtina, kad už agresijos nusikaltimus atsakomybė yra keliama specialius požymius turinčiam subjektui t. y. asmeniui, kuris turi įgaliojimus koordinuoti veiksmus valstybės mastu. Taip užtikrinama, kad baudžiamojon atsakomybėn nebūtų traukiamas kiekvienas individualus karys, o patys pavojingiausi asmenys, tam tikra prasme organizatoriai, koordinuojantys ir nukreipiantys individų veiką. Tai suteikia šiems nusikaltimams išskirtinumo, kadangi lyginant su kitais Statute numatytais nusikaltimais šie koncentruojami ne ties individų ar jų grupės, o visos valstybės apsauga nuo kitos šalies agresorės. Ši specialius požymius turinčio subjekto sąvoka apima vyriausybių vadovus, gynybos ministrus ir kitus kariuomenės struktūrų lyderius, aukšto rango pareigūnus. Šiuo atveju svarbu ar toks subjektas efektyviai gali daryti poveikį, organizuoti ir koordinuoti kitų veiksmus, bet ne jo užimamos pareigos[172]. Be to, atsakomybė iškyla ne tik už padarytą agresijos aktą, bet ir už jo planavimą, rengimą, inicijavimą. Tai turi būti konkretūs veiksmai, parodantys aiškias intencijas įvykdyti patį agresijos aktą. Atkreiptinas dėmesys, jog vien šių veiksmų nepakanka baudžiamajai atsakomybei kilti – privalo būti atliktas ir pats agresijos aktas[173]. 8*bis* straipsnio 1 dalis taip pat daro nuorodą į Chartiją, taigi siekiant veiksmą pripažinti agresijos nusikaltimu, turi būti pažeistos ir Chartijos nuostatos. Statuto kontekste labiausiai išskirtina būtų Chartijos 2 straipsnio 4 dalis, kurioje įtvirtinta, kad visos narės tarptautiniuose santykiuose susilaiko nuo grasinimo jėga ir jos panaudojimo tiek prieš kurios nors valstybės teritorinį vientisumą arba politinę nepriklausomybę, tiek kuriuo kitu būdu, nesuderinamu su Jungtinių Tautų tikslais. Žinoma, sprendžiant dėl Chartijos pažeidimo reikia turėti omenyje ir Chartijos numatomas jėgos panaudojimo išlygas t. y. tuos atvejus, kada galimas teisėtas jėgos panaudojimas: jėgos panaudojimą savigynos tikslais arba jėgos panaudojimą sankcionavus Jungtinių Tautų Saugumo Tarybai. Galiausiai dera pasakyti, kad teismas turi įvertinti pažeidimo pobūdį, sunkumą, mastą ir akivaizdumą. Šie vertinamieji elementai – tarsi riba skirianti agresijos nusikaltimą nuo

[171] 1974 m. gruodžio 14 d. Jungtinių Tautų Generalinės Asamblėjos rezoliucija Nr. 3314 (XXIX) (United Nations General Assembly 14 December 1974 resolution No. 3314 (XXIX)) [interaktyvus; žiūrėta 2017 m. vasario 23 d.]. Prieiga per internetą: <http://www.mefacts.com/cached.asp?x_id=10378>.

[172] TRIFFTERER, O.; AMBOS, K. *The Rome Statute of the International Criminal Court. A Commentary Third Edition.* Oxford: Hart, 2016, p. 580–617.

[173] 2010 m. birželio 11 d. Romos Statuto Peržiūros konferencijos rezoliucija Nr. RC/Res.6 (Resolution RC/Res.6, adopted on 11 June 2010 by the Review Conference of the Rome Statute) [interaktyvus; žiūrėta 2014 m. vasario 23 d.]. Prieiga per internetą: <https://asp.icc-cpi.int/iccdocs/asp_docs/Resolutions/RC-Res.6-ENG.pdf>.

kitų nusikaltimų. Baudžiamajai atsakomybei taikyti reikalingi visi šie elementai[174]. Be abejonės būtinas ir pats agresijos aktas. Pataisų 8*bis* straipsnio 2 dalyje yra detalizuojama, jog agresijos aktas tai vienos valstybės ginkluotųjų pajėgų panaudojimas prieš kitos valstybės suverenitetą, teritorinį vientisumą ar politinę nepriklausomybę arba bet kokiu kitu Chartijai prieštaraujančiu būdu. Akcentuotina, kad 2 dalyje numatytas pavyzdinis agresijos *aktų*, bet ne *nusikaltimų* sąrašas – visais atvejais, siekiant tokius aktus pripažinti nusikaltimais juos turi įvertinti TBT.

3.2.3. Kibernetiniai nusikaltimai – agresijos nusikaltimai?

Dauguma apibūdintų požymių, kurie priskirtini agresijos nusikaltimams, yra aktualūs ir kibernetinių nusikaltimų kategorijai. Dažnai kibernetinės atakos vykdomos ne karinio konflikto metu, kas atitiktų *jus ad bellum* sritį. Žinoma ir tai, kad jau dabar kai kurios valstybės (pvz.: Kinija, Šiaurės Korėja, Sirija[175]) savo karinėse struktūrose turi padalinius besispecializuojančius kibernetinių atakų srityse, todėl tai ne vien tik pavienių asmenų ar grupių rengiamos atakos, o visos valstybės mastu koordinuojamos operacijos. Kibernetinių nusikaltimų padaroma tiek ekonominė, tiek politinė žala taip pat yra aiškiai jaučiama, kaip tarkime Estijos 2007 m. išpuolio atveju. Bet ar kibernetinė ataka gali būti prilyginta ginkluotos jėgos panaudojimui? Būtent šis požymis iš esmės ir nulemtų ar kibernetiniai nusikaltimai gali būti prilyginti agresijos nusikaltimams. Šiuo klausimu buvo keliama daugybė diskusijų, kurios neabejotinai yra aktualios ir šiandien.

Priimant Kampalos pataisas buvo teiktas projektas, kuriuo buvo išreikštas susirūpinimas dėl ginkluotos jėgos panaudojimo termino, taip atsiribojant nuo neįprastų, kariavimo priemonių. Minėtas projektas buvo atmestas. Specialioji darbo grupė savo ataskaitoje pažymėjo, jog agresijos nusikaltimai neapima netradicinių kovojimo priemonių tokių kaip kibernetinės atakos ar ekonominiai embargai[176]. Pataisų kūrėjų valia aiški. Juolab, kad ir Statuto pataisų 8*bis* straipsnio 2 dalyje pateikiamas agresijos aktų pavyzdinis sąrašas nurodo tik „tradicinius“ ginkluotus agresijos būdus. Dėl šių priežasčių Kampalos pataisų 8*bis* straipsnyje, kitaip nei Chartijoje, atsirado būtent *ginkluotos* jėgos panaudojimo terminas. M. Gillett pabrėžia, kad 8*bis* straipsnyje pateikiamas sąrašas nėra baigtinis, tačiau jį būtina interpretuoti siaurai, jog nebūtų pažeidžiamas *nullum crimen*

[174] TRIFFTERER, O.; AMBOS, K. *The Rome Statute of the International Criminal Court. A Commentary Third Edition.* Oxford: Hart, 2016, p. 580-617.
[175] WARF, B.; FEKETE, E. Relational geographies of cyberterrorism and cyberwar. *Space and Polity,* 2016, Vol. 20:2, p. 143–157.
[176] 2008 m. birželio 6 d. agresijos nusikaltimų Specialiosios darbo grupės ataskaitos II priedas Nr. ICC-ASP/6/20/Add.1 (6 June 2008 Annex II ICC- ASP/6/20/Add.1 Report of the Special Working Group on the Crime of Aggression) [interaktyvus; žiūrėta 2017 m. vasario 23 d.]. Prieiga per internetą: <http://www.iccnow.org/documents/ICC-ASP-6-20-Add1-AnnexII-ENG.pdf>.

sine lege principas. Todėl, M. Gillett manymu, interpretuoti elektronines priemones kaip ginklus 8*bis* straipsnio 2 dalies prasme būtų itin sudėtinga, kadangi kibernetinės atakos pristinga tradicinių kinetinio poveikio charakteristikų, kurios asocijuojamos ginkluotos jėgos prasme[177]. Tokiam teiginiui iliustruoti, kaip pavyzdys tiktų jau ne kartą minėtas 2007 m. atvejis Estijoje, kai po Taline panaikintų sovietinių statulų, kurios buvo skirtos sovietų pergalei prieš nacistinę Vokietiją atminti, DDoS atakomis iš Rusijos buvo paveiktos Estijos prezidento, parlamento, kai kurių ministerijų, didžiųjų žiniasklaidos organizacijų ir dviejų didžiųjų bankų elektroninės sistemos. Estija pirmąkart Šiaurės Atlando Sutarties Organizacijos (toliau – NATO) istorijoje prašė NATO aljanso narių pagalbos ginkluotos atakos atveju. Tąsyk NATO nepripažino tokio išpuolio, kaip ginkluotos jėgos panaudojimo[178].

Tačiau įdomu tai, kad kibernetinių atakų poveikis fiziniams objektams išryškėjo dar tais pačiais 2007 m. Idaho nacionalinėje laboratorijoje atlikto „Auroros testo“ metu. JAV vyriausybė davė leidimą „hakeriams“, esantiems dideliu nuotoliu, įsibrauti į 1 milijono dolerių vertės, 27 tonų dyzelino generatoriaus sistemą. „Hakeriams“ pavyko prisijungti prie generatoriaus sistemos ir paveikti srovės pertraukiklius, kurių greitas atidarymas ir uždarymas kėlė didelę įtampą generatoriaus mechaninėms detalėms. Šios savo ruožtu pradėjo lūžti, iš paties generatoriaus pasipylė dūmai, kol galiausiai generatorius nustojo veikti dėl mechaninių trikdžių[179]. Eksperimento rezultatai buvo filmuojami, dar ir šiandien vaizdo medžiaga yra pasiekiama internete[180]. Taigi kyla klausimas, kodėl nebuvo atsižvelgta į ryškėjančias kibernetinių nusikaltimų kinetines charakteristikas priimant Kampalos pataisas, nors eksperimento pavyzdžiai rodė realias kibernetinių atakų galimybes? Galbūt dėl to, jog tai atrodė daugiau kaip teorinė, suprojektuota kontroliuojamoje aplinkoje galimybė.

Teorinės abejonės buvo išsklaidytos 2010 m. ir virto realybe, kai Irane buvo aptiktas „Stuxnet“ virusas. Šis virusas buvo panaudotas Irano branduolinėje infrastruktūroje. Skelbiama, kad „Stuxnet“ buvo sukurtas sutrikdyti būtent Irano urano sodrinimo programą, paveikiant šiame procese naudojamas dujines aliuminines centrifugas. Virusas specialiai buvo nutaikytas į sistemos programuojamus loginius

[177] GILLETT, M. The Anatomy of an International Crime: Aggression at the International Criminal Court. *International Criminal Law Review*, 2013, Vol. 13, Issue 4, p. 829–864.
[178] STAHL, W. M. The Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity. *Georgia Journal of International and Comparative Law*, 2011 m., Vol. 40, Issue 1, p. 247–273.
[179] WARF, B.; FEKETE, E. Relational geographies of cyberterrorism and cyberwar. *Space and Polity*, 2016, Vol. 20:2, p. 143–157.
[180] Vaizdo įrašas [interaktyvus; žiūrėta 2017 m. vasario 23 d.]. Prieiga per internetą: <https://www.youtube.com/watch?v=fJyWngDco3g>.

valdiklius, kurie ir valdė centrifugų sukimosi greičius. Sukeliant pernelyg didelius greičius, jautrios centrifugos buvo gadinamos. Per visą viruso veikimo laikotarpį iki tol, kol kenkėjiška programa buvo aptikta, buvo sunaikinta per 2000 centrifugų, o dėl šių nuostolių branduolinės programos veikla truko kelerius metus ilgiau nei buvo numatyta. Analitikai vėliau tyrinėję šį virusą tikino, jog ši ataka itin ilgo ir kruopštaus projekto rezultatas. Tvirtinama, kad tai ne grupės, bet valstybės ar kelių valstybių, politiškai motyvuota ataka. Šias prielaidas leido kelti tai, kad programos kodas parašytas itin sudėtingai, virusas, kuris vėliau užkrėtė ir daugybę kitų valstybių kompiuterius, buvo sukurtas paveikti tik vienam specifiniam taikiniui. Programa pati skanavo ir ieškojo vienintelio taikinio, o jei jo nerasdavo toje informacinėje sistemoje – susinaikindavo[181]. „Stuxnet“ laikomas ginkluotos agresijos sąvokos kitimo lūžio tašku. A. C. Foltz „Stuxnet“ pavadino pirmąja preciziškai valdoma amunicija[182]. Pasitelkęs „Schmito“ analizės modelį autorius konstatuoja, jog ši ataka atitinka jėgos panaudojimą Chartijos 2 straipsnio 4 dalies prasme. K. Finklea ir C. A. Theohary „Stuxnet“ prilygina ginklo kategorijai, kadangi ši programa sukurta ne informacijai rinkti, bet fiziniam objektui naikinti[183]. 2014 m. patirtas dar vienas kibernetinis-fizinis smūgis. Šį kartą Vokietijoje plieno gamykloje. Virusu per sistemos programuojamus loginius valdiklius paveiktas gamyklos žaizdras. Teigiama, kad buvo patirta didelė fizinio pobūdžio žala[184].

Šie realūs pavyzdžiai, ypatingai „Stuxnet“, sukėlė tarptautinės teisės specialistų diskusijas, dėl ginkluotos jėgos panaudojimo koncepcijos. M. N. Schmitt pažymėjo, jog ne visos kibernetinės atakos prilygsta jėgos panaudojimui, tačiau tvirtai teigia, kad veiksmai, kuriais sužalojami ar nužudomi žmonės, žalojami ar naikinami objektai vienareikšmiškai yra jėgos panaudojimas. M. N. Schmitt ragina tarptautinę bendruomenę labai jautriai vertinti kiekvieną kibernetinės operacijos atvejį jėgos panaudojimo rėmuose ir jokiu būdu nenuvertinti kibernetinių atakų ir jomis padaromų nusikaltimų[185]. Kita pozicijos pusė kritikuoja kibernetinės atakos pripažinimą kaip jėgos panaudojimą, dėl jų plataus spektro padarinių. Dalis kibernetinių atakų prilygtų Chartijos 2 straipsnio 4 daliai, dalis – ne, todėl apibendrintai visas galimas kibernetines atakas lyginti kaip jėgos

[181] FOLTZ, A. C. Stuxnet, Schmitt Analysis, and the Cyber „Use-of-Force“ Debate [interaktyvus; žiūrėta 2017 m. vasario 23 d.]. Prieiga per internetą: <http://www.au.af.mil/au/awc/awcgate/jfq/foltz_stuxnet_schmitt_oct2012.pdf>.
[182] *Ibid.*
[183] FINKLEA, K.; THEOHARY, C., A. Cybercrime: Conceptual Issues for Congress and U. S. Law Enforcement [interaktyvus; žiūrėta 2017 m. vasario 23 d.]. Prieiga per internetą: <https://fas.org/sgp/crs/misc/R42547.pdf>.
[184] LEE, R., M.; ASSANTE, M., J.; CONWAY, T. German Steel Mill Cyber Attack [interaktyvus; žiūrėta 2017 m. vasario 23 d.]. Prieiga per internetą: <https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf>.
[185] SCHMITT, M. N.; *et al. Tallinn manual on the international law applicable to cyber warfare*. Cambridge: Cambridge university press, 2013, p. 29–42.

panaudojimą yra netikslu. L. J. M. Boer teigia, kad abi – tiek kibernetinės priemonės, tiek ekonominės priemonės kelia labai panašią žalą, tačiau leidus kibernetines atakas pripažinti patenkančias į Chartijos 2 straipsnio 4 dalies sritį, lieka neaišku, kodėl užribyje lieka ekonominės priemonės[186].

Vis dėlto, iš aptartų pavyzdžių matyti, kad iš esmės kibernetinė ataka gali turėti labai aiškų, apibrėžtą kinetinį poveikį, lygiai taip pat kaip ir ginkluota ataka. Žinoma, sutinkama ir su pozicijomis, kurios teigia, kad kibernetinė ataka negali būti pripažįstama ginkluotos jėgos panaudojimui, ypatingai tais atvejais, kai ji sukelia ekonominio pobūdžio padarinius. Tačiau darytina išvada, kad pati jėgos panaudojimo doktrina turi kisti – būtent jei anksčiau ginkluotos jėgos panaudojimas buvo siejamas išimtinai su fizinėje erdvėje vykstančiomis atakomis panaudojant „tradicinius“ puolimo metodus t. y. tokiais atvejais kaip numato Statuto pataisų 8*bis* straipsnio 2 dalis, minėti „Auroros eksperimento“, Vokietijos plieno gamyklos, ypatingai „Stuxnet“ atvejai parodo, kad sukelti padariniai savo mastu ir pobūdžiu nenusileidžia, kad ir svetimos valstybės tam tikro objekto bombardavimui. „Stuxnet“ atveju, jei kibernetinė ataka būtų nukreipta ne į aliuminių centrifugų gadinimą, o visišką branduolinės infrastruktūros sunaikinimą, neatmetama ir ten dirbusių žmonių sužalojimo galimybė. Tai dar labiau priartina kibernetinių atakų keliamą grėsmę prie tradicinės ginkluotos jėgos atakos keliamos grėsmės. Žinoma, kibernetinė ataka, kaip agresijos aktas nebus nukreipta prieš valstybės teritorinį vientisumą, priešingai nei tai būtų tradicinio ginkluoto puolimo metu, tačiau remiantis Statuto pataisų 8*bis* straipsnio 2 dalimi, ginkluotos jėgos panaudojimas gali būti nukreiptas ir prieš valstybės suverenitetą. Valstybės suverenitetas iš esmės apima pareigą kitoms valstybėms nesikišti į tos valstybės suverenių teisių apsaugą, vidaus ir išorės reikalus. Pagal JT Generalinės Asamblėjos deklaraciją dėl neleistinos intervencijos ir kišimosi į valstybių vidaus reikalus[187] kiekvienos valstybės teisė laisvai, be kišimosi tvarkyti savo vidaus ir išorės reikalus apima valstybių teisę nevaržomai ir nepriklausomai nuspręsti savo politinę, ekonominę, kultūrinę ir socialinę sistemą, laisvai ir nevaržomai naudotis savais ištekliais, derinant tai su piliečių valia be jokios išorinės intervencijos, prievartos ar grasinimų ją panaudoti. Kibernetinės atakos, tokios kaip „Stuxnet“ neabejotinai patenka į minėtą kišimosi į valstybės suverenitetą sritį, taigi kibernetiniai

[186] BOER, L. J. M. Echoes of Times Past: On the Paradoxical Nature of Article 2(4). *Journal of Conflict & Security Law*, 2015, Vol. 20, Issue 1, p. 5–26.
[187] 1981 m. gruodžio 9 d. Jungtinių Tautų Generalinės Asamblėjos deklaracija dėl neleistinos intervencijos ir kišimosi į valstybių vidaus reikalus Nr. A/RES/36/103 (United Nations General Assembly 9 December 1981 Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States No. A/RES/36/103) [interaktyvus; žiūrėta 2017 m. kovo 26 d.]. Prieiga per internetą: <http://www.un.org/documents/ga/res/36/a36r103.htm>.

nusikaltimai, pakoregavus ginkluotos jėgos suvokimą, iš esmės galėtų atitikti 8*bis* straipsnio 2 dalies agresijos aktui keliamus reikalavimus.

Taip pat nereikėtų pamiršti ir Kampalos pataisų 8*bis* straipsnyje numatytos baudžiamosios atsakomybės už agresijos akto planavimą, rengimą ir inicijavimą. Rengiant ar sudarant prielaidas agresijos aktui, net ir tos kibernetinės atakos, kurios neturi tiesioginio poveikio realiam pasauliui galėtų būti vertinamos TBT kaip inkorporuota nusikalstama veika, kartu su agresijos nusikaltimu. Pavyzdžiui, 2008 m. Gruzijoje vykusio, Pietų Osetijos konflikto metu, buvo aiškiai pademonstruota, kaip kibernetinės priemonės gali būti efektyviai suderinamos su tradicinėmis, ginkluotame konflikte – DDoS atakomis išjungiant informacines sistemas, kurios skirtos komunikacijai palaikyti, taip žymiai apsunkinant gynybos priemonių koordinavimą, skubių žinių visuomenei perdavimą ir apskritai ryšį su likusiu pasauliu[188]. Taigi, jei rengiamas kitos valstybės karinio objekto bombardavimas (agresijos aktas), o jam įvykdyti prieš tai pasitelkiama kibernetinė ataka, kuria sutrikdoma puolamos valstybės priešlėktuvinė gynybinė sistema, radarai, taip leidžiant bombonešiams pasiekti taikinius nepastebėtiems, baudžiamoji atsakomybė pagal Statuto Kampalos pataisas turėtų kilti ir asmenims, kurie koordinavo ir teikė nurodymus įvykdyti kibernetines atakas.

Apibendrinus minėtus pavyzdžius bei teisinį reglamentavimą, konstatuotina, kad Statuto pataisos, 8*bis* straipsnyje apibrėžiančios agresijos nusikaltimus, neužkardo galimybės į agresijos nusikaltimų sritį įtraukti ir kibernetines atakas. Kitaip išaiškinus jėgos panaudojimo doktriną, ją pritaikius prie šiandieninės modernaus pasaulio realijų, t. y. ginkluotos jėgos panaudojimu pripažįstant ir kibernetinėje erdvėje daromas atakas, vykdomi vienos valstybės prieš kitą kibernetiniai nusikaltimai, galėtų būti pripažinti agresijos aktu Statuto pakeitimų 8*bis* straipsnio prasme. Žinoma, kiekvienu konkrečiu atveju, kaip ir įprastinės ginkluotos jėgos panaudojimo atveju, teismas turėtų įvertinti tokio agresijos akto pobūdį, sunkumą ir mastą. Neabejotinai tokios kibernetinės atakos, kaip 2007 m. Estijos atveju, kėlusios ekonominius padarinius šių kriterijų negalėtų atitikti, tačiau atakos, kurios naikina objektus, kelia grėsmę žmonių gyvybei, būtų vertos detalesnio įvertinimo ir atitikus pakankamo masto, pobūdžio, sunkumo kriterijus, galėtų būti savarankiškai pripažintos agresijos nusikaltimu.

[188] STAHL, W. M. The Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity. *Georgia Journal of International and Comparative Law*, 2011 m., Vol. 40, Issue 1, p. 247–273.

Išvados

1. Kibernetiniai nusikaltimai – tai nuo kibernetinės erdvės priklausomos, duomenų ar informacijos apdorojimo pagrindu pagrįstos nusikalstamos veikos, nukreiptos į elektroninių duomenų ir sistemų konfidencialumą, vientisumą ir prieinamumą.

2.1. Lietuvos Respublikos baudžiamojo kodekso XXX skyriuje numatytų nusikalstamų veikų objektu laikytinas asmens santykis su duomenimis ar informacinėmis sistemomis, kaip galimybė ir laisvė tokį gėrį valdyti, disponuoti, naudotis juo. Taigi, minėto skyriaus objektas tikslintinas t. y. juo laikytinas ne elektroninių duomenų ar informacinių sistemų saugumas, o elektroninių duomenų ar informacinių sistemų valdytojo, turėtojo interesai, kurie susiję su duomenų ar informacinių sistemų vientisumu, konfidencialumu ir prieinamumu.

2.2. Lietuvos Respublikos baudžiamojo kodekso XXX skyriaus nuostatų turinį lėmė poreikis harmonizuoti baudžiamojo įstatymo turinį su 2001 m. Konvencija dėl elektroninių nusikaltimų bei Europos Parlamento ir Tarybos 2013 m. rugpjūčio 12 d. direktyva. Dauguma šių teisės aktų nuostatų Lietuvos Respublikos baudžiamajame kodekse įgyvendinta tinkamai, tačiau pastebima, jog nacionalinis reguliavimas galėtų būti tobulinamas, pavyzdžiui, tikslinamas BK 197 straipsnio 2 dalies poveikio daugeliui informacinių sistemų požymis.

2.3. Pasitaikantys teismų praktikos, taikant Lietuvos Respublikos baudžiamojo kodekso XXX skyriaus normas, trūkumai ir klaidos yra susiję su bendrosios ir specialiosios normų konkurencijos santykio nustatymo klausimu. Prioritetas tūrėtų būti teikiamas normoms, kurios išskiria elektroninių duomenų ar dalyko specifiką specialiais požymiais (pvz., informacija apie asmens privatų gyvenimą, komercinė paslaptis, su elektroninėmis mokėjimo priemonėmis susiję duomenys), t. y. vietoje BK 198 ar 198^2 straipsnių taikyti, pavyzdžiui, BK 168, 210, 214, 215 straipsnius.

2.4. Kritikuotina ir Lietuvos Aukščiausiojo Teismo praktika bylose dėl neteisėto prisijungimo prie elektroninės bankininkystės paskiros, aiškinant BK 198^1 straipsnio informacinės sistemos apsaugos priemonių pažeidimo požymį. Šios nusikalstamos veikos sudėties požymis turėtų būti inkriminuojamas tik tada, kai yra sutrikdomos apsaugos priemonių veikimo funkcijos.

3.1. Kompiuterinio sukčiavimo atveju, įvertinant kaltininko turtinę naudą, gautą dėl poveikio elektroniniams duomenims ar informacinėms sistemoms, BK 182 straipsnio inkriminavimas nėra tinkamas dėl apgaulės požymio pritaikymo negalimumo. Atsižvelgiant į užsienio šalių baudžiamuosius įstatymus bei 2001 m.

Konvencijos dėl elektroninių nusikaltimų nuostatas konstatuotina, jog tikslinga numatyti atskirą nusikalstamos veikos sudėtį, numatančią atsakomybę už ekonominės naudos gavimą paveikus elektroninius duomenis ar informacines sistemas nesant apgaulės požymio.

3.2. Kibernetinių nusikaltimų priskyrimas prie Tarptautinio baudžiamojo teismo jurisdikcijos neišvengiamai yra susijęs su nekonvencinių jėgos priemonių panaudojimo prilyginimo ginkluotos jėgos panaudojimo sąvokai klausimu. Atsižvelgiant į teisinį reglamentavimą bei aktualius kibernetinių atakų poveikio atvejus darytina išvada, kad kibernetiniai nusikaltimai galėtų būti laikomi agresijos nusikaltimų dalimi pasirengimo stadijoje. Taip pat agresijos nusikaltimais galėtų būti pripažinti ir savarankiškai, tačiau tam turi būti pakeistas ginkluotos jėgos panaudojimo doktrinos aiškinimas, prie šių priskiriant ir netradicines agresijos apraiškas – kibernetines atakas.

Šaltinių sąrašas

Norminiai teisės aktai

Tarptautiniai teisės aktai:

1. Jungtinių Tautų Chartija. *Valstybės žinios*, 2002, Nr. 15-557.
2. Tarptautinio baudžiamojo teismo Romos Statutas, priimtas 1998 m. liepos 17 d. Jungtinių Tautų diplomatinėje įgaliotųjų atstovų konferencijoje, skirtoje Tarptautinio baudžiamojo teismo įsteigimui. *Valstybės žinios*, 2003, Nr. 49-2165.
3. 2001 m. lapkričio 23 d. Konvencija dėl elektroninių nusikaltimų. *Valstybės žinios*, 2004, Nr. 36-1188.
4. 1981 m. gruodžio 9 d. Jungtinių Tautų Generalinės Asamblėjos deklaracija dėl neleistinos intervencijos ir kišimosi į valstybių vidaus reikalus Nr. A/RES/36/103 (United Nations General Assembly 9 December 1981 Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States No. A/RES/36/103) [interaktyvus; žiūrėta 2017 m. kovo 26 d.]. Prieiga per internetą: <http://www.un.org/documents/ga/res/36/a36r103.htm>.
5. 1974 m. gruodžio 14 d. Jungtinių Tautų Generalinės Asamblėjos rezoliucija Nr. 3314 (XXIX) (United Nations General Assembly 14 December 1974 resolution No. 3 314 (XXIX)) [interaktyvus; žiūrėta 2017 m. vasario 23 d.]. Prieiga per internetą: <http://www.mefacts.com/cached.asp?x_id=10378>.
6. 1989 m. rugsėjo 13 d. Europos Tarybos Ministrų komiteto rekomendacija valstybėms narėms Nr. R(89) 9 dėl su kompiuteriais susijusių nusikaltimų [interaktyvus; žiūrėta 2017 m. sausio 3 d.]. Prieiga per internetą: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804f1094>.
7. 1995 m. rugsėjo 11 d. Europos Tarybos Ministrų komiteto rekomendacija valstybėms narėms Nr. R(95) 13 dėl baudžiamojo proceso teisės problemų, susijusių su informacinėmis technologijomis [interaktyvus; žiūrėta 2017 m. sausio 3 d.]. Prieiga per internetą: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804f6e76>.

Europos Sąjungos teisės aktai:

1. 2013 m. rugpjūčio 12 d. Europos Parlamento ir Tarybos direktyva 2013/40/ES dėl atakų prieš informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR (OL 2013 L 218, p. 8).
2. 2010 m. gegužės 19 d. Europos Parlamento rezoliucija P7_TA(2010)0185 dėl Tarptautinio baudžiamojo teismo Romos statuto peržiūros konferencijos Kampaloje,

Uganda (European Parliament resolution P7_TA(2010)0185 of 19 May 2010 on the Review Conference on the Rome Statute of the International Criminal Court, in Kampala, Uganda) (OL 2010 CE 161, p. 78).

3. 2005 m. vasario 24 d. Tarybos pagrindų sprendimas 2005/222/TVR dėl atakų prieš informacines sistemas (OL 2005 L 69, p. 67).

Lietuvos Respublikos teisės aktai:

1. Lietuvos Respublikos Konstitucija. *Valstybės žinios*. 1992 m. lapkričio 30 d., Nr. 33-1014.
2. Lietuvos Respublikos Konstitucinis Teismas. *2006 m. sausio 16 d. nutarimas byloje 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 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 straipsnis (2002 m. kovo 14 d. redakcija) neprieštarauja Lietuvos Respublikos Konstitucijai, Nr. 7/03-41/03-40/04-46/04-5/05-7/05-17/05.*
3. Lietuvos Respublikos Konstitucinis Teismas. *2009 m. birželio 8 d. nutarimas byloje dėl Lietuvos Respublikos baudžiamojo kodekso 20 straipsnio 1,2,3 dalių (2000 m. rugsėjo 26 d. redakcija), 20 straipsnio 5 dalies (2004 m. liepos 5 d. redakcija), 43 straipsnio 4 dalies (2000 m. rugsėjo 26 d. redakcija) atitikties Lietuvos Respublikos Konstitucijai, Nr. 34/2008-36/2008-40/2008-1/2009-4/2009-5/2009-6/2009-7/2009-9/2009-12/2009-13/2009-14/2009-17/2009-18/2009-19/2009-20/2009-22/2009.*
4. Lietuvos Respublikos baudžiamasis kodeksas. *Valstybės žinios,* 2000, Nr. 89-2741.
5. Lietuvos Respublikos civilinis kodeksas. *Valstybės žinios,* 2000, Nr. 74-2262.
6. Lietuvos Respublikos kibernetinio saugumo įstatymas. *Teisės aktų registras*, 2014, Nr. XII-1428.
7. Lietuvos Respublikos elektroninio parašo įstatymas. *Valstybės žinios*, 2000, Nr. VIII-182.
8. Lietuvos Respublikos autorių teisių ir gretutinių teisių įstatymas. *Valstybės žinios*, 1999, Nr. 50-1598.

9. Lietuvos Respublikos baudžiamojo kodekso 7, 38, 47, 63, 66, 70, 75, 82, 93, 129, 166, 167, 172, 178, 180, 181, 182, 183, 184, 185, 189, 194, 196, 197, 198, 198^1, 198^2, 199, 202, 213, 214, 215, 225, 227, 228, 231, 233, 235, 252, 256, 257, 262, 284, 285, 312 straipsnių, priedo pakeitimo ir papildymo, XXVI, XXX skyrių pavadinimų pakeitimo ir kodekso papildymo 256^1, 257^1 straipsniais įstatymas. *Valstybės žinios.* 2007, Nr. 81-3309.
10. Lietuvos Respublikos baudžiamojo kodekso 13, 162, 191, 196, 197, 203, 206, 216, 219, 221, 309 straipsnių pakeitimo ir papildymo bei kodekso papildymo 198-1 ir 198-2 straipsniais įstatymas. *Valstybės žinios*, 2004, Nr. 25-760.
11. Lietuvos Respublikos baudžiamojo kodekso 7, 196, 197, 198^1, 198^2 straipsnių ir priedo pakeitimo ir kodekso papildymo 270^3 straipsniu įstatymas. *Teisės aktų registras*, 2015, Nr. 2015-09697.
12. Lietuvos Respublikos baudžiamojo kodekso 198^2, 309 straipsnių ir priedo pakeitimo įstatymas. *Teisės aktų registras*, 2016, Nr. 2016-17730.

Užsienio valstybių teisės aktai:

1. Estijos Respublikos baudžiamasis kodeksas [interaktyvus; žiūrėta 2017 m. vasario 20 d.]. Prieiga per internetą: <http://www.legislationline.org/documents/section/criminal-codes>.
2. Latvijos Respublikos baudžiamasis kodeksas [interaktyvus; žiūrėta 2017 m. vasario 20 d.]. Prieiga per internetą: <http://www.legislationline.org/documents/section/criminal-codes>.
3. Šveicarijos Konfederacijos baudžiamasis kodeksas [interaktyvus; žiūrėta 2017 m. vasario 20 d.]. Prieiga per internetą: <http://www.legislationline.org/documents/section/criminal-codes>.
4. Kanados baudžiamasis kodeksas [interaktyvus; žiūrėta 2017 m. vasario 20 d.]. Prieiga per internetą: <http://www.legislationline.org/documents/section/criminal-codes>.
5. Suomijos Respublikos baudžiamasis kodeksas [interaktyvus; žiūrėta 2017 m. vasario d. Prieiga per internetą: <http://www.legislationline.org/documents/section/criminal-codes>.
6. Maltos Respublikos baudžiamasis kodeksas [interaktyvus; žiūrėta 2017 m. vasario 20 d.]. Prieiga per internetą <http://www.legislationline.org/documents/section/criminal-codes>.
7. Gruzijos baudžiamasis kodeksas [interaktyvus; žiūrėta 2017 m. vasario 20 d.]. Prieiga per internetą: <http://www.legislationline.org/documents/section/criminal-codes>.

8. Bulgarijos Respublikos baudžiamasis kodeksas [interaktyvus; žiūrėta 2017 m. vasario 20 d.]. Prieiga per internetą: <http://www.legislationline.org/documents/section/criminal-codes>.
9. Bosnijos ir Hercegovinos baudžiamasis kodeksas [interaktyvus; žiūrėta 2017 m. vasario 20 d.]. Prieiga per internetą: <http://www.legislationline.org/documents/section/criminal-codes>.
10. Vokietijos Federacinės Respublikos baudžiamasis kodeksas [interaktyvus; žiūrėta 2017 m. vasario 20 d.]. Prieiga per internetą: <http://www.legislationline.org/documents/section/criminal-codes>.
11. Austrijos Respublikos baudžiamasis kodeksas [interaktyvus; žiūrėta 2017 m. vasario 20 d.]. Prieiga per internetą: <http://www.legislationline.org/documents/section/criminal-codes>.

Travaux préparatoires:

1. 2010 m. birželio 11 d. Romos Statuto Peržiūros konferencijos rezoliucija Nr. RC/Res.6 (Resolution RC/Res.6, adopted on 11 June 2010 by the Review Conference of the Rome Statute) [interaktyvus; žiūrėta 2014 m. vasario 23 d.]. Prieiga per internetą: <https://asp.icc-cpi.int/iccdocs/asp_docs/Resolutions/RC-Res.6-ENG.pdf>.
2. 2008 m. birželio 6 d. agresijos nusikaltimų Specialiosios darbo grupės ataskaitos II priedas Nr. ICC-ASP/6/20/Add.1 (6 June 2008 Annex II ICC- ASP/6/20/Add.1 Report of the Special Working Group on the Crime of Aggression) [interaktyvus; žiūrėta 2017 m. vasario 23 d.]. Prieiga per internetą: <http://www.iccnow.org/documents/ICC-ASP-6-20-Add1-AnnexII-ENG.pdf>.
3. 2001 m. lapkričio 8 d. Europos Tarybos Ministrų komiteto Konvencijos dėl kibernetinių nusikaltimų aiškinamasis pranešimas Nr. 185 (Explanatory Report to the Convection on Cybercrime No. 185, adopted on 8 November 2001 by the Committee of Ministers of the Council of Europe) [interaktyvus; žiūrėta 2017 m. vasario 15 d.]. Prieiga per internetą: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b>.
4. 2010 m. rugsėjo 30 d. Europos Komisijos COM/2010/0517 galutinis – COD 2010/0273 pasiūlymas dėl Europos Parlamento ir Tarybos direktyvos dėl atakų prieš informacines sistemas ir dėl Tarybos pamatinio sprendimo 2005/222/TVR panaikinimo {SEC(2010) 1122 galutinis}{SEC(2010) 1123 galutinis} (COM/2010/0517 final – COD 2010/0273 proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing

Council Framework Decision 2005/222/JHA {SEC(2010) final} {SEC(2010) 1123 final}.

5. 1989 m. rugsėjo 13 d. Europos Tarybos Ministrų komiteto rekomendacija valstybėms narėms Nr. R(89) 9 dėl su kompiuteriais susijusių nusikaltimų ir Europos Tarybos Europos nusikalstamumo problemų komiteto galutinė atskaita. (Recommendation No. R (89) 9 on computer-related crime and final report of the European Committee on Crime Problems). Strasbūras: Publishing and Documentation Service, 1990 [interaktyvus; 2017 m. sausio 3 d.]. Prieiga per internetą: <http://www.oas.org/juridico/english/89-9&final%20report.pdf>.
6. 2011 m. liepos 23 d. Europos ekonomikos ir socialinių reikalų komiteto nuomonė dėl pasiūlymo dėl Europos Parlamento ir Tarybos direktyvos dėl atakų prieš informacines sistemas ir Tarybos pamatinio sprendimo 2005/222/TVR panaikinimo (OL 2011 C 218, p. 130).
7. 2007 m. gegužės 30 d. Europos Tarybos projekto dėl kibernetinių nusikaltimų, Lietuvos teisinio reglamentavimo profilis (30 May 2007 Cybercrime legislation – country profile (Lithuania) of the Council of Europe‘s Project on Cybercrime) [interaktyvus; žiūrėta 2017 m. kovo 23 d.]. Prieiga per internetą: <http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/CountryProfiles/567-LEG-country%20profile%20Lithuania%20_30%20May%2007_En.pdf>.
8. Lietuvos Respublikos baudžiamojo kodekso 7, 196, 197, 198^1, 198^2 straipsnių ir priedo pakeitimo bei kodekso papildymo 270^3 straipsniu įstatymo projektas, 2014, Nr. XIIP-2617.
9. Lietuvos Respublikos Vyriausybės kanceliarijos teisės departamento išvada dėl Lietuvos Respublikos baudžiamojo kodekso 7, 196, 197, 198^1, 198^2 straipsnių ir priedo pakeitimo bei kodekso papildymo 270^3 straipsniu įstatymo projekto, 2014, Nr. NV-3278.

Specialioji literatūra

Komentarai, vadovėliai ir kitos knygos:

1. ABRAMAVIČIUS, A., *et al. Baudžiamoji teisė: Vadovėlis.* Vilnius: Eugrimas, 1998.
2. BILEVIČIŪTĖ, E., *et al. Kriminalistika. Taktika ir metodika*: Vadovėlis. Vilnius: Mykolo Romerio universitetas, 2013.
3. MOCKEVIČIUS, R., VALATKEVIČIUS, D., *et al. Lietuvos Respublikos baudžiamojo kodekso komentaras. Specialioji dalis (99–212 straipsniai).* Vilnius: VĮ Registrų centras, 2009.

4. PETRAUSKAS, R., ŠTITILIS, D. *Kompiuteriniai nusikaltimai ir jų prevencija*. Vilnius: Lietuvos teisės akademijos Leidybos centras, 2000.
5. SAULIŪNAS, D., ŠTITILIS, D., TOLIUŠIS, S. *et al. Informacinių technologijų teisė*. Vilnius: NVO Teisės institutas, 2004.
6. ŠTITILIS, D., *et al. Interneto ir technologijų teisė*. Vilnius: Mykolo Romerio universitetas, 2016.
7. BOYLE, R., *et al. Corporate computer security*. Essex: Person, 2014.
8. GERCKE, M. Understanding Cybercrime: Phenomena, challenges and legal response [interaktyvus; žiūrėta 2017 m. vasario 2 d.]. Prieiga per internetą: <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf>.
9. GOLLMANN, D. *Computer security*. West Sussex: John Wiley & Sons, Ltd, 2011.
10. GRIFFIN, R. C. Cybercrime. *Journal of International Commercial Law and Technology*, 2012, Vol. 7 (2).
11. HIGGINS, G. E. *Cybercrime. An introduction to an Emerging Phenomenon.* New York: McGraw-Hill, 2010.
12. YAR, M. *Cybercrime and Society.* London: SAGE Publications Inc., 2013.
13. JEWKES, Y.; YAR, M., *et al. Handbook of internet crime*. New York: Routledge, 2011.
14. PARKER D. B. Computer Crime. Criminal Justice Resource Manual [interaktyvus; žiūrėta 2017 m. sausio 25 d.]. Prieiga per internetą: <https://www.ncjrs.gov/pdffiles1/Digitization/118214NCJRS.pdf>.
15. PFLEEGER, C., *et al. Security in computing*. New Jersey: Prentice hall, 2002.
16. SCHJOLBERG, S. *The history of cybercrime – 1976-2014*. Norderstedt: Books on demand, 2014.
17. SCHMITT, M. N.; *et al. Tallinn manual on the international law applicable to cyber warfare*. Cambridge: Cambridge university press, 2013.
18. SHINDER, D. L. *Scene of the cybercrime. Computer forensics handbook.* Rockland: Syngress Publishing Inc., 2002.
19. STREET, F. L. *Law of the Internet*. Charlottesville: Lexis law publishing, 1998.
20. TRIFFTERER, O.; AMBOS, K. *The Rome Statute of the International Criminal Court. A Commentary Third Edition.* Oxford: Hart, 2016.
21. WALDEN, I. *Computer Crimes and Digital Investigation*. Oxford: Oxford university press, 2007.
22. WELLS, T. J. *et al. Internet fraud casebook. The world wide web of deceit*. Hoboken, New Jersey: John Wiley & Sons, Inc., 2010.

Straipsniai:

1. BILEVIČIENĖ, T. Dynamics of crimes against the security of electronic data and information systems, and its influence on the development of electronic business in Lithuania. *Jurisprudencija*, 2011, Nr. 18(2), p. 689–702.
2. KALPOKAS, V., MARCINAUSKAITĖ, R. Tapatybės vagystė elektroninėje erdvėje: technologiniai aspektai ir baudžiamasis teisinis vertinimas. *Teisės problemos*, 2012, Nr. 3(77), p. 30–52.
3. MARCINAUSKAITĖ, R. Nusikalstamomis veikomis elektroninėje erdvėje pažeidžiamos pagrindinės baudžiamojo įstatymo saugomos vertybės nustatymo problema. *Socialinių mokslų studijos*, 2011, Nr. 3(3), p. 897–914.
4. MARCINAUSKAITĖ, R. Technologinio neutralumo principas ir jo reikšmė formuluojant ir aiškinant nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui sudėtis. *Socialinių mokslų studijos*, 2013, Nr. 5(1), p. 367–379.
5. PETRAUSKAS, R., ŠTITILIS, D. Lietuvos Respublikos baudžiamasis kodeksas nusikaltimų elektroninėje erdvėje konvencijos kontekste. *Jurisprudencija*, 2002, t. 24(16), p. 79–86.
6. SAULIŪNAS, D. Legislation on cybercrime in Lithuania: development and legal gaps in comparison with the convention on cybercrime. *Jurisprudencija*, 2010, Nr. 4(122), p. 203–219.
7. BOER, L. J. M. Echoes of Times Past: On the Paradoxical Nature of Article 2(4). *Journal of Conflict & Security Law*, 2015, Vol. 20, Issue 1, p. 5–26.
8. CLOUGH, J. Cybercrime. *Commonwealth law bulletin*, 2011, Vol. 37, Issue 4, p. 671–680.
9. FINKLEA, K.; THEOHARY, C., A. Cybercrime: Conceptual Issues for Congress and U. S. Law Enforcement [interaktyvus; žiūrėta 2017 m. vasario 23 d.]. Prieiga per internetą: <https://fas.org/sgp/crs/misc/R42547.pdf>.
10. FOLTZ, A. C. Stuxnet, Schmitt Analysis, and the Cyber „Use-of-Force“ Debate [interaktyvus; žiūrėta 2017 m. vasario 23 d.]. Prieiga per internetą: <http://www.au.af.mil/au/awc/awcgate/jfq/foltz_stuxnet_schmitt_oct2012.pdf>.
11. FREITAS, P. M. F., GONÇALVES, N. Illegal access to information systems and the Directive 2013/40/EU. *International Review of Law, Computers & Technology*, 2015, Vol. 29:1, p. 50–62.
12. GILLETT, M. The Anatomy of an International Crime: Aggression at the International Criminal Court. *International Criminal Law Review*, 2013, Vol. 13, Issue 4, p. 829–864.

13. GRABOSKY, P. N. Virtual Criminality: old wine in new bottles? *Social & legal studies*, 2001, Vol. 10(2), p. 243–249.
14. KLEVE, P., *et al*. The definition of ICT crime. *Computer law & security review*, 2011, Vol. 27, p. 162–167.
15. HOLLIS, D., B. Why States Need an International Law for Information Operations. *Lewis & Clark Law Review*, 2007, Vol. 11, Issue 4, p. 1023–1061.
16. HUNTON, P. The growing phenomenon of crime and the internet: A cybercrime execution and analysis model. *Computer law & security review*, 2009, Vol. 25, p. 528–535.
17. KSHETRI, N. Positive externality, increasing returns, and the rise in cybercrimes. *Communications of the ACM*, 2009, Vol. 52, Issue 12, p. 141–144.
18. LEE, R., M.; ASSANTE, M., J.; CONWAY, T. German Steel Mill Cyber Attack [interaktyvus; žiūrėta 2017 m. vasario 23 d.]. Prieiga per internetą: <https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf>.
19. RHO, J. J. Blackbeards of the Twenty-First Century: Holding Cybercriminals Liable under the Alien Tort Statute. *Chicago Journal of International Law*, 2007, Vol. 7, Issue 2, p. 695–718.
20. SCHJOLBERG, S. Peace and Justice in Cyberspace. Potential new international legal mechanisms against global cyberattacks and other global cybercrime [interaktyvus; žiūrėta 2017 m. vasario 23 d.]. Prieiga per internetą: <http://www.cybercrimelaw.net/documents/ICLNSummary.pdf>.
21. SCHJOLBERG, S. The history of global harmonization on cybercrime legislation – the road to Geneva [interaktyvus; žiūrėta 2017 m. sausio 1 d.]. Prieiga per internetą: <http://www.cybercrimelaw.net/documents/cybercrime_history.pdf>.
22. SIEBER, U. *Legal Aspects of Computer-Related Crime in the Information Society – COMCRIME-study* [interaktyvus; žiūrėta 2017 m. vasario 15 d.]. Prieiga per internetą: <http://www.oas.org/juridico/english/COMCRIME%20Study.pdf>.
23. SIMION, R. Cybercrime and its challenges between reality and fiction. Where do we actually stand? *The Criminology, Victimology and Security Review*, 2010, Vol. 4, Issue 1, p. 296–312.
24. STAHL, W. M. The Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity. *Georgia Journal of International and Comparative Law*, 2011 m., Vol. 40, Issue 1, p. 247–273.
25. URBAS G., Cybercrime Legislation in the Asia-Pacific Region [interaktyvus; žiūrėta 2017 m. vasario 1 d.]. Prieiga per internetą: <https://www.google.lt/url?sa=t&rct=j&q

=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwjEzMTJ5e7RAhXqHpoKHZ_iDgEQFggcMAE&url=http%3A%2F%2Fwww.ibrarian.net%2Fnavon%2Fpaper%2FCybercrime_Legislation_in_the_Asia_Pacific_Region.pdf%3Fpaperid%3D3127647&usg=AFQjCNGqkQ9XZ09aHw7bl9EGAvdx7Z7m4Q>.

26. WALL, D. What are cybercrimes? *Criminal Justice Matters,* 2008, Vol. 58:1, p. 20–21.
27. WARF, B.; FEKETE, E. Relational geographies of cyberterrorism and cyberwar. *Space and Polity*, 2016, Vol. 20:2, p. 143–157.
28. WILSON, C. Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. CRS report for congress [interaktyvus; žiūrėta 2017 m. vasario 1 d.]. Prieiga per internetą: <https://fas.org/sgp/crs/terror/RL32114.pdf>.
29. White-Collar crime: Second Annual Survey of Law: Substantive Crimes. The American criminal law review. *American Bar Association, section of criminal just*, 1981, Vol. 2, p. 499–509.

Teismų praktika

1. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2017 m. sausio 10 d. nutartis baudžiamojoje byloje, Nr. 2K-33-303/2017*.
2. Lietuvos Aukščiausiojo Teismas. 2016 m. rugpjūčio 23 d. Teismų praktikos nagrinėjant baudžiamąsias bylas dėl sudėtingų pavienių nusikalstamų veikų ir nusikalstamų veikų sutapčių apžvalga Nr. AB-44-1. *Teismų praktika*, 2016, Nr. 44, p. 570–626.
3. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2016 m. sausio 26 d. nutartis baudžiamojoje byloje, Nr. 2K-4-507/2016.*
4. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2015 m. gruodžio 8 d. nutartis baudžiamojoje byloje, Nr. 2K-555-788/2015.*
5. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2015 m. gegužės 12 d. nutartis baudžiamojoje byloje, Nr. 2K-188-489/2015.*
6. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2015 m. sausio 20 d. nutartis baudžiamojoje byloje, Nr. 2K-93-489/2015.*
7. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2015 m. sausio 6 d. nutartis baudžiamojoje byloje, Nr. 2K-138/2015.*
8. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2014 m. liepos 1 d. nutartis baudžiamojoje byloje, Nr. 2K-345/2014.*

9. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2014 m. birželio 19 d. nutartis baudžiamojoje byloje, Nr. 2K-327/2014*.
10. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2012 m. birželio 26 d. nutartis baudžiamojoje byloje, Nr. 2K-375/2012.*
11. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2012 m. kovo 27 d. nutartis baudžiamojoje byloje, Nr. 2K-117/2012.*
12. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2011 m. sausio 18 d. nutartis baudžiamojoje byloje, Nr. 2K-81/2011*.
13. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2005 m. lapkričio 15 d. nutartis baudžiamojoje byloje Nr. 2K-587/2005*.
14. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2001 m. spalio 9 d. nutartis baudžiamojoje byloje, Nr. 2K-682/2001.*
15. Kauno apygardos teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2015 m. gegužės 7 d. nutartis baudžiamojoje byloje, Nr. 1A-432-594/2015.*
16. Vilniaus apygardos teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2014 m. gegužės 15 d. nutartis baudžiamojoje byloje, Nr. 1A-338-312-2014.*
17. Vilniaus apygardos teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2014 m. gegužės 12 d. nuosprendis baudžiamojoje byloje, Nr. 1A-294-195-2014.*
18. Šiaulių apygardos teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2014 m. gegužės 7 d. nuosprendis baudžiamojoje byloje, Nr. 1A-388-309-2014.*
19. Panevėžio apygardos teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2014 m. balandžio 18 d. nuosprendis baudžiamojoje byloje, Nr. 1A-117-581-2014.*
20. Vilniaus apygardos teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2014 m. balandžio 16 d. nutartis baudžiamojoje byloje, Nr. 1A-303-256-2014.*
21. Šiaulių apygardos teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2014 m. kovo 31 d. nuosprendis baudžiamojoje byloje, Nr. 1A-169-354-2014.*
22. Kauno apygardos teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2014 m. sausio 21 d. nuosprendis baudžiamojoje byloje, Nr. 1A-82-327-2014.*
23. Panevėžio apygardos teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2013 m. lapkričio 29 d. nuosprendis baudžiamojoje byloje, Nr. 1A-767-350-2013.*
24. Klaipėdos apygardos teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2013 m. spalio 24 d. nutartis baudžiamojoje byloje, Nr. 1A-695-380-2013*
25. Kauno apygardos teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2012 m. spalio 22 d. nutartis baudžiamojoje byloje, Nr. 1A-94-175-2012*

26. Vilniaus apygardos teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2011 m. gruodžio 23 d. nuosprendis baudžiamojoje byloje, Nr. 1A-977-92-2011*.

Kiti šaltiniai

1. O‘Brien, S. A. Widespread cyber attack takes down sites worldwide [interaktyvus; žiūrėta 2017 m. vasario 27 d.]. Prieiga per internetą: <http://money.cnn.com/2016/10/21/technology/ddos-attack-popular-sites/>.
2. NATO Review. The history of cyber attacks – a timeline [interaktyvus; žiūrėta 2017 m. vasario 27 d.]. Prieiga per internetą: <http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm>.
3. BNS. Atakos prie Lietuvą dažnėja [interaktyvus; žiūrėta 2017 m. vasario 27 d.]. Prieiga per internetą <http://www.delfi.lt/news/daily/lithuania/vsd-vadovas-atakos-pries-lietuva-dazneja.d?id=73396080>.
4. 2001 m. lapkričio 23 d. Konvencijos dėl elektroninių nusikaltimų pasirašymo ir ratifikavimo lentelė [interaktyvus; žiūrėta 2017 m. sausio 3 d.]. Prieiga per internetą: <http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures>.
5. Tarptautinis žodžių žodynas [interaktyvus; žiūrėta 2017 m. vasario 7 d.]. Prieiga per internetą: <http://www.zodziai.lt/reiksme&word=informatika&wid=8519>.
6. Romos statuto valstybės narės – chronologinė seka [interaktyvus; žiūrėta 2017 m. vasario 23 d.]. Prieiga per internetą: <https://asp.icc-cpi.int/en_menus/asp/states%20parties/Pages/states%20parties%20_%20chronological%20list.aspx>.
7. Tarptautinio baudžiamojo teismo Romos statuto pataisas dėl agresijos nusikaltimų priėmusios/ratifikavusios valstybės: <https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-10-b&chapter=18&clang=_en>.
8. Vaizdo įrašas [interaktyvus; žiūrėta 2017 m. vasario 23 d.]. Prieiga per internetą: <https://www.youtube.com/watch?v=fJyWngDco3g>.

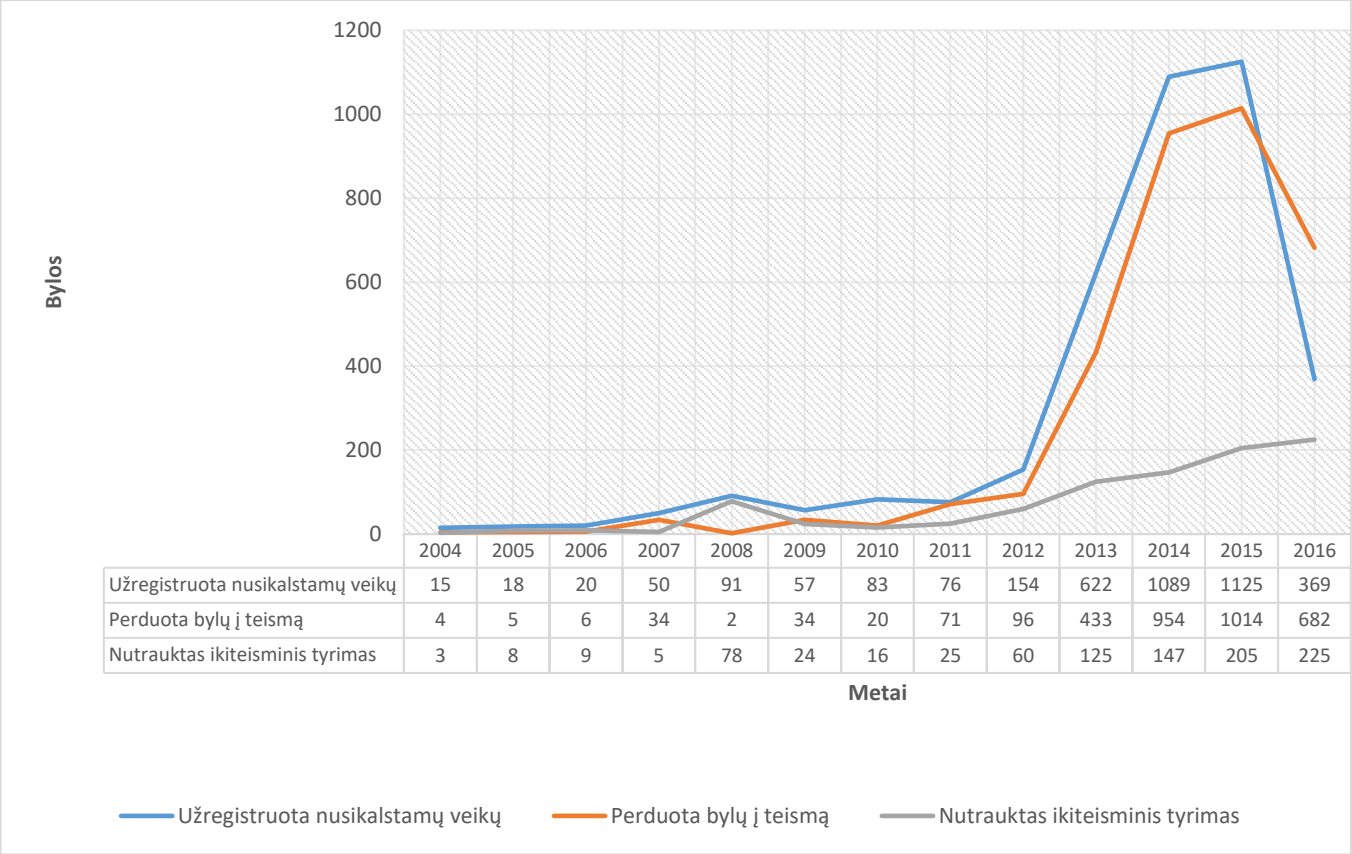
Santrauka

Šiame magistro darbe analizuojama kibernetinių nusikaltimų sąvoka bei sistema, įtvirtinta Lietuvos Respublikos baudžiamojo kodekso XXX skyriuje. Darbą sudaro trys dalys. Pirmoji darbo dalis skirta kibernetinių nusikaltimų koncepcijos detalizavimui – aptariama istorinė raida, pateikiamos skirtingos autorių nuomonės, šios nusikalstamų veikų rūšies klasifikavimas. Iškėlus teorinę kibernetinių nusikaltimų sąvokos ir termino problematiką, darbe pateikiama šiai nusikaltimų sričiai būdingų požymių visuma, kuria remiantis sudaroma siūlytina kibernetinių nusikaltimų sąvoka. Antroje struktūrinėje darbo dalyje apžvelgiamos Lietuvos Respublikos baudžiamojo kodekso XXX skyriuje įtvirtintos nusikalstamų veikų sudėtys, gilinamasi į kai kurių straipsnių dispozicijų vertinamųjų požymių aiškinimą, rūšinio objekto tikslinimą, nacionalinio teisinio reglamentavimo harmonizavimą su tarptautiniais bei Europos Sąjungos teisės aktais. Taip pat dėmesys skiriamas Lietuvos Aukščiausiojo Teismo bei žemesnės instancijos teismų praktikoje kylantiems probleminiams klausimams, aptariami teismų praktikoje pasitaikantys trūkumai bei klaidos. Moksliniame darbe daroma išvada, jog tiek Lietuvos Respublikos baudžiamojo kodekso XXX skyriaus teisinis reglamentavimas, tiek teismų praktika tūrėtų būti tikslinama ir koreguojama. Paskutinioji magistrinio darbo dalis skirta užsienio šalių teisinio reglamentavimo (taip pat lyginimo su Lietuvos reglamentavimu) bei polemikos, kylančios dėl kibernetinių nusikaltimų ir jėgos panaudojimo santykio, analizei. Atsižvelgiant į šių dienų tarptautines aktualijas bei tendencijas, darbe yra nagrinėjama kibernetinių nusikaltimų pripažinimo agresijos nusikaltimais, priklausančiais Tarptautinio baudžiamojo teismo jurisdikcijai, galimybė. Šio skyriaus rezultatu laikomas poreikio naujai nusikalstamos veikos t. y. kompiuterinio sukčiavimo sudėčiai Lietuvos Respublikos baudžiamajame kodekse bei kibernetinių nusikaltimų agresijos nusikaltimais pripažinimo galimumo konstatavimas.

Summary

The master thesis analyzes the concept and system of cybercrime, which is established in Criminal Code of Lithuania chapter XXX. The thesis is composed of three sections. Section one is based on characterizing the cybercrime concept – it discusses historical aspects of cybercrime, considers different author's opinions as well as different cybercrime classifications on that matter. Bearing in mind the tendency to regard almost any offence that involves a computer as a 'cybercrime', the lack of consensus as to what they actually are, and the terminology issue, study examines and highlights specific reference points inherent to the cybercrime nature. In addition, cybercrime definition is given in section one. Section two analyses the *corpus delicti* of crimes described in Criminal Code of Lithuania chapter XXX, likewise some evaluative features of *corpus delicti*, compares national and international, European Union legislation in terms of harmonization of legal frameworks. This section also provides an outline of relevant rulings, decisions of Supreme Court of Lithuania and other lower instance courts, analyses case law flaws and mistakes. Section Two recommends changes to be made in legislation along with the case law. Finally, Section Three focuses on criminal codes of foreign countries (in comparison with Criminal Code of Lithuania), also concentrates on problems regarding dispute over relation between cybercrime and use of force doctrine. Concerning international incidents and tendencies, thesis points out and analyzes possibility of acknowledging cybercrime as crime of aggression, which belong to the International Criminal Courts jurisdiction. Conclusions are drawn in section three that there is a demand for adoption of a new crime (computer-related fraud) in Criminal Code of Lithuania, furthermore thesis states, that cybercrime meets the traits of crime of aggression.

Priedai



Užregistruotų nusikalstamų veikų skaičius													
BK 196 str.	4	1	2	4	10	8	7	5	7	32	11	26	14
BK 197 str.	2	0	2	3	7	1	7	2	11	6	6	4	11
BK 198 str.	7	6	10	11	72	32	55	41	64	88	235	136	48
BK 198[1] str.	1	10	6	30	2	9	10	26	38	435	820	930	283
BK 198[2] str.	1	1	0	2	0	7	4	2	34	61	17	29	21
Metai	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016

Priedas Nr. 1 – Grafikas ir lentelė. **Duomenys apie Lietuvos Respublikos baudžiamojo kodekso XXX skyriaus uždraustas veikas, padarytas Lietuvos Respublikoje 2004 m. – 2016 m. laikotarpiu.**

Šaltinis: Sudaryta remiantis: Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos duomenimis. Prieiga per internetą: <http://www.ird.lt/>.