ISSN 2029–2236 (print)
ISSN 2029–2244 (online)
SOCIALINIŲ MOKSLŲ STUDIJOS
SOCIETAL STUDIES
2011, 3(3), p. 897–914.

# NUSIKALSTAMOMIS VEIKOMIS ELEKTRONINĖJE ERDVĖJE PAŽEIDŽIAMOS PAGRINDINĖS BAUDŽIAMOJO ĮSTATYMO SAUGOMOS VERTYBĖS NUSTATYMO PROBLEMA

Renata Marcinauskaitė

Mykolo Romerio universiteto Teisės fakulteto
Baudžiamosios teisės ir kriminologijos katedra
Ateities g. 20, LT-08303 Vilnius, Lietuva
Telefonas (+370 5) 271 4584
Elektroninis paštas R.Marcinauskaite@lat.lt

Pateikta 2011 m. gegužės 6 d., parengta spausdinti 2011 m. rugsėjo 18 d.

***Anotacija***. *Straipsnyje nagrinėjamos pagrindinės baudžiamojo įstatymo saugomos vertybės, kuriai nusikalstamų veikų elektroninėje erdvėje padarymu sukeliama žala arba tokios žalos atsiradimo grėsmė, identifikavimo problemos. Šių problemų analizė leidžia pagrįsti, kad pagrindinio baudžiamosios teisės priemonėmis saugotino teisinio gėrio, svarbaus teisės technikos požiūriu kodifikuojant nusikalstamas veikas į vientisą sistemą, nustatymas yra neatsiejamas nuo elektroninių nusikalstamų veikų apibrėžties. Straipsnyje atlikta analizė leidžia teigti, kad vienos pagrindinės vertybės, į kurią pirmiausia būtų kėsinamasi minėtomis veikomis ir kuri leistų jas sujungti į savarankišką vienoda baudžiamojo įstatymo saugoma vertybe grindžiamą rūšį, konkretizuoti nebūtų įmanoma. Tačiau, autorės nuomone, viena iš šių nusikalstamų veikų sąsajų galėtų būti laikoma papildoma baudžiamojo įstatymo saugoma vertybė – elektroninės erdvės saugumas, kuriam minėtomis veikomis yra padaroma žala arba sukeliama tokios žalos kilimo grėsmė.*

***Reikšminiai žodžiai***: *nusikalstamos veikos elektroninėje erdvėje, nusikalstamos veikos elektroninių duomenų ir informacinių sistemų saugumui, baudžiamojo įstatymo saugoma vertybė (objektas), elektroninės erdvės saugumas, techninis kompiuterių saugumas, CIA triada, konfidencialumas, integralumas, prieinamumas.*

## Įvadas

Su baudžiamojo įstatymo saugomo teisinio gėrio nustatymo svarba siejamas ne tik praktinis baudžiamojo įstatymo taikymo lygmuo (saugomos vertybės parinkimas yra pirma preliminari sąlyga tinkamai kvalifikuoti padarytą nusikalstamą veiką), bet ir teisėkūros procesas, kai kriminalizuojamos įvairias pavojingos asmens elgsenos pasireiškimo formos bei giminingos nusikalstamos veikos baudžiamojo įstatymo saugomos vertybės pagrindu sisteminamos į atskiras grupes (rūšis).

Kad ir kokie būtų baudžiamosios teisės teorijoje suformuluoti pavojingi veikų kriminalizavimo kriterijai[1], neginčijama, kad turėtų išlikti saugotinos vertybės identifikavimas ir tokio ją apibūdinančio požymio kaip vertybės svarba visuomenėje (saugotino gėrio visuomeninė reikšmė) nustatymas. Šis požymis liudija pakankamą veikos pavojingumą, todėl galimą (atsižvelgiant į kriminalizavimo kriterijų visumą) pažeidžiamos vertybės saugotinumą baudžiamosios teisės priemonėmis. Ši pozicija taip pat akcentuojama Lietuvos Respublikos Konstitucinio Teismo 2003 m. birželio 10 d. nutarime, kuriame teigiama, kad *pagal Konstituciją įstatymų leidėjas baudžiamajame įstatyme nusikalstamomis gali įvardyti tik tas veikas, kurios yra iš tikrųjų pavojingos ir kuriomis daroma didelė žala asmens, visuomenės ir valstybės interesams*. Pasakytina, kad nusikalstamos veikos pavojingumo kaip materialaus nusikalstamą veiką apibūdinančio požymio tiesioginė sąsaja su teisinėmis vertybėmis pripažįstama ir teismų praktikoje, pavyzdžiui, Lietuvos Aukščiausiasis Teismas savo praktikoje formuoja nuostatą, kad *veikos pavojingumas reiškia, jog ja kėsinamasi į viešpataujančias visuomenės vertybes, veikos baudžiamumas – kad ji uždrausta ne bet kokiu, o būtent baudžiamuoju įstatymu*[2].

Pagrindinis šios analizės tikslas yra identifikuoti tą baudžiamojo įstatymo saugomą vertybę, kuri, kaip pagrindinis ar kaip papildomas baudžiamosios teisės priemonėmis saugomas teisinis gėris, leistų nustatyti elektroninių nusikalstamų veikų tarpusavio sąsają, taip pat atskleisti šios vertybės turinį.

Elektroninių nusikalstamų veikų sudėtys šiuo apsektu Lietuvos teisės ar kitų sričių mokslininkų darbuose iš esmės nėra nagrinėtos, tuo tarpu užsienio valstybių mokslininuose darbuose baudžiamojo įstatymo saugomos vertybės nustatymo ir jos turinio atskleidimo problematika plėtojama nuolat. Daugumos užsienio mokslininkų darbuose analizuojami įvairūs elektroninių nusikalstamų veikų doktrinoje suformuluotų pagrindinių saugumo koncepcijų aspektai – „*elektroninės erdvės saugumo*“ ir „*techninio kompiuterių saugumo*“ turinio nustatymo, jų turinį sudarančių elementų tarpusavio sąsajos problemos.

Tyrimas atliktas taikant sisteminės analizės, loginį-analitinį, istorinį, dokumentų analizės ir lyginamąjį metodus.

---

1 Plačiau Švedas, G. *Baudžiamosios politikos pagrindai ir tendencijos Lietuvos Respublikoje*. Vilnius: Teisinės informacijos centras, 2006, p. 27.

2 Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2006 m. balandžio 4 d. nutartis baudžiamojoje byloje Nr. 2K-281/2006.

## 1. Nusikalstamų veikų elektroninėje erdvėje apibrėžties įtaka pagrindinės baudžiamojo įstatymo saugomos vertybės nustatymui

Analizuojant nusikalstamų veikų elektroninėje erdvėje sudėtis, teigtina, kad pagrindinės baudžiamojo įstatymo saugomos vertybės, kuri yra pažeidžiama arba kuriai sukeliama žalos atsiradimo grėsmė, nustatymas tiesiogiai priklauso nuo minėtu terminu įvardijamų nusikalstamų veikų visumos[3]. Manytina, kad šių pavojingų ir baudžiamojo įstatymo uždraustų įvairių elgesio formų elektroninėje erdvėje apibrėžtis lemia ne tik nusikalstamų veikų elektroninėje erdvėje koncepcijos ypatumus, bet ir turi įtakos apibrėžiant galimas šiomis pavojingomis veikomis pažeidžiamų baudžiamojo įstatymo saugomų vertybių analizės ribas. Pasakytina, kad šis probleminis elektroninių nusikalstamų veikų doktrinos aspektas taip pat gali būti tiesiogiai siejamas su teisinėje literatūroje nurodoma technologijų ir terminologijos problema[4].

Detaliau analizuojant baudžiamojo įstatymo saugomo pagrindinio teisinio gėrio, kuriam nusikalstamomis veikomis elektroninėje erdvėje padaroma žala, nustatymo bei šios vertybės turinio atskleidimo problemas, pirmiausia iš elektroninių nusikalstamų veikų visumos išskirtinos tradicinės, tačiau pagal savo prigimtį skirtingoms rūšims priklausančios veikos, kurios pakito ta apimtimi, kiek informacinių technologijų panaudojimas praplėtė minėtų veikų padarymo būdų (bei nusikalstamų veikų padarymo vietų) sąrašą.

Atsižvelgiant į 2007 m. gegužės 22 d. Europos Komisijos Komunikato Europos Parlamentui, Tarybai ir Europos Regionų komitetui KOM (2007) galutinis Bendrosios politikos, skirtos kovai su elektroniniais nusikaltimais (toliau – Komunikatas KOM (2007)[5] nuostatas, autorės nuomone, prie šių nusikalstamų veikų plačiąja prasme galėtų

---

3 Autorė nori atkreipti dėmesį, kad šiame straipsnyje analizuojama problema nėra tiesiogiai siejama su nusikalstamų veikų elektroninėje erdvėje terminijos bei jas sudarančių nusikalstamų veikų visumos problemų analize, todėl autorė vadovavosi 2007 m. gegužės 22 d. Europos Komisijos Komunikatu Europos Parlamentui, Tarybai ir Europos Regionų komitetui KOM (2007) bendrosios politikos, skirtos kovai su elektroniniais nusikaltimais, linkme, kuriame pažymėta, jog terminas „*elektroniniai nusikaltimai*“ siejami su trimis nusikalstamų veikų rūšimis. Pirmoji apima įprastus nusikaltimus, padaromus naudojant elektroninių ryšių tinklus ir informacines sistemas (pavyzdžiui, sukčiavimas, klastojimas ir kita). Antroji rūšis siejama su neteisėto turinio informacijos skelbimu elektroninėje erdvėje (pavyzdžiui, rasinės neapykantos, terorizmo kurstymas, vaikų pornografijos platinimas ir kita), o trečioji rūšis apima išimtinai specifinius elektroninių tinklų nusikaltimus (pavyzdžiui, neteisėtas poveikis elektroniniams duomenims, neteisėtas prisijungimas prie informacinės sistemos ir kita). Todėl nusikalstamos veikos elektroninėje erdvėje negali būti tapatinamos tik su nusikalstamomis veikomis elektroninių duomenų ir informacinių sistemų saugumui, nes tokiu būdu dalį prilyginus visumai būtų nepagrįstai siaurinama šių nusikalstamų veikų apibrėžtis. Kaip alternatyvą „*elektroninių nusikaltimų*“ terminui autorė taip pat vartoja tikslesnį tokio pobūdžio nusikalstamas veikas įvardijantį „*nusikalstamų veikų elektroninėje erdvėje*“ terminą (plačiau Civilka, M., *et al*. *Informacinių technologijų teisė.* Vilnius: NVO Teisės institutas, 2004, p. 511).

4 Walden, I. *Computer Crimes and Digital Investigation*. Oxford: Oxford University Press, 2007, p. 15.

5 2007 m. gegužės 22 d. Europos Komisijos Komunikatas Europos Parlamentui, Tarybai ir Europos Regionų komitetui KOM (2007) galutinis Bendrosios politikos, skirtos kovai su elektroniniais nusikaltimais [interaktyvus]. [žiūrėta 2010-09-14]. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:LT:HTML>.

būti priskiriamos dvi Komunikate KOM (2007) nurodytos nusikalstamų veikų grupės – *elektroninėje erdvėje padarytos įprastinės nusikalstamos veikos*[6] bei *nusikalstamos veikos, susijusios su neteisėto turinio informacijos platinimu šioje erdvėje*[7]. Tokia pozicija gali būti grindžiama tuo, kad šias nusikalstamas veikas tarpusavyje sieja ne tik tai, kad jų padarymo procese naudojamos informacinės sistemos ir elektroninių ryšių tinklai, bet ir pats šių nusikalstamų veikų pobūdis. Nusikalstamos veikos, susijusios su neteisėto turinio medžiagos platinimu, padaromos nenaudojant elektroninės erdvės, būtų priskiriamos vadinamoms tradicinėms (lyginant su nusikalstamomis veikomis elektroninių duomenų ir informacinių sistemų saugumui) baudžiamajame įstatyme kriminalizuotoms pavojingoms veikoms, kaip, pavyzdžiui, sukčiavimas (BK 182 straipsnis), dokumentų suklastojimas arba suklastoto dokumento panaudojimas (BK 300 straipsnis), neteisėtas informacijos apie privatų asmens gyvenimą rinkimas (BK 167 straipsnis) ir kitos. Vienintelis kriterijus, kuris leido su neteisėto informacijos turinio platinimu susijusias nusikalstamas veikas išskirti iš tradicinių nusikalstamų veikų visumos, yra pačios gaminamos, įsigyjamos, laikomos, reklamuojamos ar kitaip platinamos informacijos pobūdis. Todėl teigtina, kad informacinių sistemų ir elektroninių ryšių tinklų panaudojimas visų tradicinių nusikalstamų veikų, ne išimtis ir su neteisėto turinio informacijos platinimu susijusių nusikalstamų veikų, atveju praplėtė šių nusikalstamų veikų padarymo būdų (bei padarymo vietų) sąrašą. Todėl analizuojant elektronines nusikalstamas veikas baudžiamojo įstatymo saugomos vertybės aspektu, siūlytina šias sudedamąsias elektroninių nusikalstamų veikų dalis vertinti kartu.

Kompleksiškai analizuojant baudžiamajame įstatyme įtvirtintas šių nusikalstamų veikų sudėtis, teigtina, kad vien tik elektroninės erdvės panaudojimo faktas neatitiko įstatymo leidėjo baudžiamojo įstatymo specialiojoje dalyje numatyto nusikalstamų veikų sisteminimo pagrindo, todėl nebuvo laikomas tuo lemiamu kriterijumi, kuris leistų minėtas nusikalstamas veikas sujungti į vieną, rūšine įstatymo saugoma vertybe grindžiamą, nusikalstamų veikų grupę (rūšį). Paminėtina, kad prasiplėtęs tradicinių nusikalstamų veikų padarymo būdų (bei padarymo vietų) sąrašas tiesioginės įtakos pagrindiniams bei anksčiau oficialiai baudžiamajame įstatyme įtvirtintiems teisiniams gėriams, į kuriuos būtų kėsinamasi tokio pobūdžio nusikalstamomis veikomis, neturėjo (saugomos teisinės vertybės liko pirminės – privataus gyvenimo neliečiamumas; nuosavybė, turtinės teisės ir turtiniai interesai; intelektinė ir pramoninė nuosavybė; visuomenės saugumas; dorovė ir kitos).

Atsižvelgiant į tai, kad informacinių technologijų panaudojimas nepakeitė tradicinių pavojingų bei baudžiamojo įstatymo uždraustų veikų esmę atskleidžiančio objektyvaus nusikalstamos veikos sudėties požymio, teigtina, kad tiek ta pati įprasta nusi-

6 Atitinkančios 2003 m. birželio 23 d. Konvencijos dėl elektroninių nusikaltimų II skyriaus 1 skirsnio 2 dalyje (kompiuterinės klastotės, kompiuterinis sukčiavimas) minimas nusikalstamas veikas. Manytina, kad šioms nusikalstamoms veikoms taip pat galėtų būti priskiriamos ir šios Konvencijos II skyriaus 1 skirsnio 4 dalyje minimi nusikaltimai, susiję su autorių teisių ir gretutinių teisių pažeidimais

7 Atitinkančios 2003 m. birželio 23 d. Konvencijos dėl elektroninių nusikaltimų II skyriaus 1 skirsnio 3 dalyje (nusikaltimai, susiję su vaikų pornografija) minimas nusikalstamas veikas. Pasakytina, kad nusikalstamos veikos, susijusios su neteisėto turinio informacijos platinimu elektroninėje erdvėje, neturėtų būti tapatinamos tik su pornografinio turinio informacijos platinimu, bet turėtų apimti ir kurstymą prieš bet kokios tautos, rasės, etninę, religinę ar kitokią žmonių grupę (BK 170 straipsnis), terorizmo kurstymą (BK $250^1$ straipsnis).

kalstama veika, padaryta fizinėje erdvėje (pavyzdžiui, sukčiavimas), tiek ir ši pavojinga veika, padaryta elektroninėje erdvėje (pavyzdžiui, sukčiavimas elektroninėje erdvėje) baudžiamąja teisine prasme pasižymi tuo pačiu pavojingumo pobūdžiu, nes yra priskirtos tai pačiai vienodos pagrindinės baudžiamojo įstatymo saugomos vertybės pagrindu sudarytai nusikalstamų veikų rūšiai (pavyzdžiui, nusikalstamos veikos nuosavybei, turtinėms teisėms ir turtiniams interesams). Vadovaujantis tuo, kad nusikalstamų veikų pavojingumo pobūdis leidžia tarpusavyje palyginti skirtingoms rūšims priklausančias nusikalstamas veikas, darytina išvada, kad tradicinės nusikalstamos veikos, padaromos elektroninėje erdvėje, pagal šį kriterijų tarpusavyje skirsis tik tuomet, jeigu jos bus įtrauktos į skirtingus baudžiamojo įstatymo specialiosios dalies skyrius (pavyzdžiui, sukčiavimas elektroninėje erdvėje yra laikomas pagal pavojingumo pobūdį pavojingesnis nei elektroninio dokumento suklastojimas ar disponavimas suklastotu elektroniniu dokumentu).

Šiuo aspektu nagrinėjant pagrindinės baudžiamojo įstatymo saugomos vertybės nustatymo problemą užsienio valstybių baudžiamuosiuose įstatymuose, pažymėtina, kad užsienio teisės specialistai[8], atskleisdami nusikalstamų veikų, *susijusių su neteisėto turinio informacijos skleidimu*, sudėties požymių turinį, nekelia abejonių, kad baudžiamajame įstatyme įtvirtintos tradicinių nusikalstamų veikų sudėtys net be pakeitimų galėtų būti pritaikomos kvalifikuojant kaltininko padarytas nusikalstamas veikas elektroninėje erdvėje. Daugumos užsienio valstybių baudžiamuosiuose įstatymuose įprastinių nusikalstamų veikų padarymo būdų (bei nusikalstamos veikos vietos) pokytis, kaip ir Lietuvos baudžiamajame įstatyme[9], neturėjo lemiamos reikšmės nustatant pagrindinę baudžiamojo įstatymo saugomą vertybę. Pavyzdžiui, Estijos baudžiamojo įstatymo 213 paragrafe[10], Vokietijos baudžiamojo įstatymo 184 skyriuje[11] ir Lenkijos baudžiamojo įstatymo 202 straipsnyje[12] numatytos nusikalstamos veikos, vienu ar kitu aspektu susijusios su pornografinio turinio medžiagos platinimu, nepriklausomai nuo šių nusikalstamų

8 Kunicka-Michalska, B. *Przestępstwa przeciwko wolności seksualnej i obyczajności popełniania za pośrednictwem systemu informatycznego*. Wrocław: Zakład Narodowy im. Ossolińskich, 2004, s. 84.

9 Pasirinkta įvairių nusikalstamų veikų (pavyzdžiui, BK 182 straipsnis (Sukčiavimas), 184 straipsnis (Turto iššvaistymas), 250[1] straipsnis (Terorizmo kurstymas), 309 straipsnis (Disponavimas pornografinio turinio dalykais) ir kitos) sudėčių konstrukcija bei gana abstraktus reikšmingų požymių aprašymo būdas leidžia teigti, jog įstatymų leidėjas, nedetalizuodamas tam tikrų nusikalstamų veikų padarymo būdų bei vietos (atsisakydamas kazuistinio nusikalstamos veikos požymių aprašymo), numatė ir tuos atvejus, kai šios nusikalstamos veikos gali būti padaromos elektroninėje erdvėje pasitelkiant informacinių technologijų teikiamas galimybes. Tokios nusikalstamų veikų sudėties požymių aiškinimo tendencijos matyti ir teismų praktikoje, pavyzdžiui, Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2010 m. rugsėjo 28 d. nutartyje baudžiamojoje byloje Nr. 2K-426/2010 nurodoma, kad „*Dokumentu gali būti pripažįstamas bet kokia forma ant popieriaus, elektroninėje erdvėje ar kompiuterinėje laikmenoje padarytas įrašas, tačiau keliami reikalavimai dokumento turiniui. Dokumentas turi suteikti informacijos apie įvykį, veiksmą ar asmenį. Dokumentas – tai tam tikra forma padarytas įrašas, kuris nustato, pakeičia ar panaikina teisiškai reikšmingą faktą* (*juridinį faktą*).“

10 Criminal Code of the Republic of Estonia [interaktyvus]. [žiūrėta 2010-09-05]. <http://www.legislationline.org/download/action/download/id/1280/file/4d16963509db70c09d23e52cb8df.htm/preview>.

11 Criminal Code of the Federal Republic of Germany [interaktyvus]. [žiūrėta 2010-09-05]. <http://www.legislationline.org/documents/action/popup/id/9015/preview>.

12 Criminal Code of the Republic of Poland [interaktyvus]. [žiūrėta 2010-09-05]. <http://www.legislationline.org/documents/section/criminal-codes>.

veikų padarymo būdų (ar vietos), kaip ir anksčiau yra laikomos nusikalstamų veikų, pažeidžiančių seksualinio apsisprendimo laisvę ir padorumą ar nepilnamečių teises, dalimi.

Skirtingai nei neteisėto turinio informacijos platinimo elektroninėje erdvėje kriminalizavimo atveju, užsienio valstybių baudžiamuosiuose įstatymuose pastebimos ir specialių normų, numatančių baudžiamąją atsakomybę *už kitų tradicinių nusikalstamų veikų, padaromų elektroninėje erdvėje*, išskyrimo tendencijos. Tačiau analogišką išvadą, kad informacinių technologijų panaudojimas nekeitė šių nusikalstamų veikų esmės apibūdinančio nusikalstamos veikos sudėties požymio − baudžiamojo įstatymo saugomos vertybės, galima daryti atsižvelgiant į tai, kad dėl elektroninės erdvės panaudojimo pakitusias nusikalstamas veikas įtvirtinančios specialiosios normos (pavyzdžiui, sukčiavimas elektroninėje erdvėje) buvo įtrauktos į tuos baudžiamojo įstatymo skyrius, kuriuose numatytos ir bendrosios normos (pavyzdžiui, sukčiavimas). Todėl darant Estijos baudžiamojo įstatymo 213 paragrafe, Vokietijos baudžiamojo įstatymo 263a skyriuje ir Lenkijos baudžiamojo įstatymo 287 straipsnyje aprašytas nusikalstamas veikas (sukčiavimą elektroninėje erdvėje) kėsinamasi į tą pačią rūšinę baudžiamojo įstatymo saugomą vertybę kaip ir numatytą bendrojoje sukčiavimo sudėtyje.

Analizuojant kitus nusikalstamų veikų, padaromų elektroninėje erdvėje, turinio elementus – specifines nusikalstamas veikas, kurias darant tiesiogiai pažeidžiamas elektroninių duomenų ir informacinių sistemų saugumas, pasakytina, kad šios rūšies veikos ilgą laiką Lietuvos baudžiamajame įstatyme kaip *delicta sui generis* nebuvo kriminalizuotos. Todėl teisinio gėrio, kuriam tokio pobūdžio nusikalstamomis veikomis padaroma žala arba jų padarymu sukeliama tokios žalos atsiradimo grėsmė, įvardijimo problema Lietuvos baudžiamosios teisės doktrinoje nebuvo nagrinėjama. Šios baudžiamojo įstatymo saugomos vertybės nustatymas ir įtvirtinimas baudžiamajame įstatyme pirmiausia buvo siejamas su įvairių pavojingų asmens elgesio elektroninėje erdvėje formų, pažeidžiančių elektroninių duomenų ir informacinių sistemų konfidencialumą, integralumą ir prieinamumą, tiesioginiu kriminalizavimu. Toks kriminalizavimas lėmė, kad šios nusikalstamos veikos nėra laikomos sudedamąja kitų veikų dalimi, o kiekviena atskirai turi savarankišką baudžiamąją teisinę reikšmę ir kartu su kitomis tos pačios rūšies nusikalstamomis veikomis yra sujungtos į atskirą baudžiamojo įstatymo specialiosios dalies skyrių[13].

Apibendrinus teigtina, kad, iš materialinės baudžiamosios teisės pozicijų analizuojant įvairias į elektroninių nusikalstamų veikų visumą įtrauktas pavojingas bei baudžiamojo įstatymo uždraustas veikas, vienos pagrindinės baudžiamosios teisės priemonėmis saugomos vertybės, į kurią pirmiausia būtų kėsinamasi darant šias nusikalstamas veikas ir kuri leistų jas sujungti į savarankišką vienoda baudžiamojo įstatymo saugoma vertybe grindžiamą rūšį, konkretizuoti nebūtų įmanoma. Todėl pritartina specialisto D. Štitilio teiginiui, kad „nusikaltimų elektroninėje erdvėje, kaip atskiros nusikaltimų grupės (pavyzdžiui, nusikaltimai nuosavybei, nusikaltimai informatikai (t. y. kompiuteriniai

13 Detaliau baudžiamojo įstatymo saugomos vertybės, kuriai specifinių nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui padarymu tiesiogiai yra sukeliama žala arba žalos atsiradimo grėsmė, nustatymo ir jos turinio konkretinimo problematika analizuojama tolesnėse šio straipsnio dalyse.

nusikaltimai) neegzistuoja <...>.“[14] Tačiau vis dėlto svarstytina, ar nusikalstamos veikos elektroninėje erdvėje į vieną visumą sujungtos tik informacinių technologijų bei elektroninės erdvės panaudojimo ar kompiuterinės informacijos kaip nusikaltimo dalyko kriterijumi[15].

Todėl būtina paminėti dar vieną aspektą – vienu ar kitu pasirinktu būdu baudžiamajame įstatyme kriminalizavus įvairias elektronines nusikalstamas veikas, tiesiogine šių nusikalstamų veikų sąsaja taip pat galėtų būti laikoma ir papildoma baudžiamojo įstatymo saugoma vertybė, kuriai minėtomis nusikalstamomis veikomis padaroma žala arba sukeliama tokios žalos kilimo grėsmė. Nustatant šį papildomą baudžiamosios teisės priemonėmis saugomą teisinį gėrį, atkreiptinas dėmesys, kad baudžiamajame įstatyme įtvirtintas naujas nusikalstamas veikas elektroninių duomenų ir informacinių sistemų saugumui į vieną visumą vienijantis pagrindinis teisinis gėris (elektroninių duomenų ir informacinių sistemų saugumas – elektroninių duomenų ir informacinių sistemų konfidencialumas, integralumas ir prieinamumas) negali būti laikomas pakankamu papildomai baudžiamojo įstatymo saugomai vertybei įvardyti. Šio teisinio gėrio pažeidimus ne visais atvejais būtų įmanoma nustatyti, kai elektroninėje erdvėje padaromos nusikalstamos veikos, susijusios su neteisėto turinio informacijos platinimu (pavyzdžiui, kurstymas prieš bet kokios tautos, rasės, etninę, religinę ar kitokią žmonių grupę (BK 170 straipsnis), terorizmo kurstymas (BK 250[1] straipsnis) ir kita). Todėl *papildoma baudžiamojo įstatymo saugoma vertybe* tais atvejais, kai nusikalstamų veikų padarymui yra pasitelkiamos informacinės technologijos bei elektroninė erdvė, galėtų būti laikomas plačiausią prasmę turintis *elektroninės erdvės saugumas*.

## 2. Pagrindinės baudžiamojo įstatymo saugomos vertybės, tiesiogiai pažeidžiamos specifinėmis nusikalstamomis veikomis elektroninių duomenų ir informacinių sistemų saugumui, kitimo baudžiamajame įstatyme analizė

Pagrindinių teisėkūros krypčių, pasirenkant nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui kriminalizavimo būdus, analizė leidžia teigti, kad baudžiamosios atsakomybės už šių nusikalstamų veikų padarymą nustatymo tendencijos yra dvejopos: pirma, bandoma pakankamai plačiai interpretuoti tradicinių nusikalstamų veikų sudėties požymius juos pritaikant naujoms nusikalstamoms veikoms pagal analogiją (pavyzdžiui, 1982 m. Olandijoje „*informacija*“ buvo pripažinta daiktu, taip išsprendžiant vagystės dalyko problemą)[16] arba, antra, baudžiamajame įstatyme formuluojant naujų nusikalstamų veikų sudėtis. Pastarasis teisėkūros būdas lemia pagrin-

14 Štitilis, D. *Teisinės atsakomybės pagrindų nustatymo už neteisėtas veikas elektroninėje erdvėje problemos.* Daktaro disertacija. Socialiniai mokslai, teise. Vilnius: LTU, 2002, p. 39.

15 *Ibid.,* p. 34.

16 Mazurov, V. A. *Kompjuternye prestuplenija* [Computer Crimes]. Moskva: Paleotip, 2002, s. 9.

dinės baudžiamojo įstatymo saugomos vertybės, kuri pažeidžiama, padarius minėtas nusikalstamas veikas, suformulavimo ir įtvirtinimo baudžiamajame įstatyme problemas.

Atkreiptinas dėmesys, kad dauguma tiek kontinentinės, tiek bendrosios teisės tradicijos šalių pasirinko antrąją minėtų nusikalstamų veikų elektroninėje erdvėje kriminalizavimo kryptį. Lietuvos Respublikos baudžiamųjų įstatymų ir jų kitimo analizė leidžia teigti, kad pagrindinė baudžiamosios atsakomybės už šias nusikalstamas veikas nustatymo tendencija yra susijusi su naujų teisės normų kūrimu, pripažįstant, kad baudžiamajame įstatyme numatytos tradicinės nusikalstamos veikos yra nepakankamos specifinėms elektroninių tinklų nusikalstamoms veikoms kvalifikuoti. Taip pat ir tradicinės baudžiamosios teisės doktrinos negali būti be išimčių taikomos nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui sudėties požymiams atskleisti.

Minėta, kad 1961 m. Lietuvos Respublikos baudžiamajame kodekse[17] (toliau – 1961 m. BK) nusikalstamos veikos, kuriomis pažeidžiamas elektroninių duomenų ir informacinių sistemų saugumas, kaip *delicta sui generis* nebuvo kriminalizuotos, todėl pagrindinės baudžiamojo įstatymo saugomos vertybės, kaip nusikalstamų veikų sisteminimo pagrindo, nustatymo ir tiesioginio įtvirtinimo baudžiamajame įstatyme problemos nebuvo analizuojamos. Taip pat kitos į elektroninių nusikalstamų veikų visumą įtrauktos nusikalstamos veikos buvo kriminalizuotos tik fragmentiškai, jas numatant kaip kvalifikuotas tradicinių nusikalstamų veikų sudėtis (pavyzdžiui, 1961 m. BK 274 straipsnio 2 dalis (Sukčiavimas), 1961 m. BK 277 straipsnio 2 dalis (Turtinės žalos padarymas apgaule arba piktnaudžiaujant pasitikėjimu). Šis pasirinktas teisėkūros būdas leido elektroninėje erdvėje padaromam sukčiavimui ar turtinės žalos padarymui apgaule arba piktnaudžiaujant pasitikėjimu nustatyti didesnį pavojingumo laipsnį, tačiau nepakeitė pagrindinės šiomis nusikalstamomis veikomis pažeidžiamos baudžiamojo įstatymo saugomos vertybės (ja anuomet baudžiamosios teisės doktrinoje buvo laikoma nuosavybė[18]).

Tuo tarpu 2003 m. gegužės 1 d. įsigaliojus naujajam Lietuvos Respublikos baudžiamajam kodeksui[19], daugelis naujų nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui buvo sujungtos į vieną BK XXX skyrių „*Nusikaltimai informatikai*“. Tačiau BK XXX skyriuje numatytos baudžiamojo įstatymo saugomos vertybės pavadinimas negalėjo būti laikomas tinkamu, nes įvairiomis pavojingomis asmens elgsenos formomis elektroninėje erdvėje buvo sukeliama grėsmė arba padaroma žala ne informatikai kaip mokslui bei technikos sričiai, nagrinėjančiai informacijos kaupimo, perdavimo ir apdorojimo dėsningumus, metodus ir technines priemones,[20] o pirmiausia kėsintasi į techninį kompiuterių[21] saugumą.

Vėlesni BK XXX skyriuje numatytų nusikalstamų veikų sudėčių keitimai buvo susiję su tarptautiniais Lietuvos Respublikos įsipareigojimais ratifikavus 2001 m. lapkričio 23 d. Budapešte priimtą Europos Tarybos konvenciją dėl elektroninių nusikaltimų (toliau – Konvencija dėl elektroninių nusikaltimų) bei Europos Sąjungos lygiu priėmus

17 Lietuvos Respublikos baudžiamasis kodeksas. *Valstybės žinios*. 1961, Nr. 18-147.

18 *Baudžiamoji teisė: specialioji dalis*. Pavilionis, V. (sud.). Vilnius: Eugrimas, 2000, p. 388.

19 Lietuvos Respublikos baudžiamasis kodeksas. *Valstybės žinios*. 2000, Nr. 89-2741.

20 Balčytienė, A., *et al*. *Informatikos įvadas*. Vilnius: Apyaušris, 1996, p. 7.

21 Įvairūs „techninio kompiuterių saugumo“ koncepcijos aspektai yra pateikiami tolesnėse šio straipsnio dalyse.

2005 m. vasario 24 d. Tarybos pamatinį sprendimą 2005/222/TVR dėl atakų prieš informacines sistemas (toliau − Tarybos pamatinis sprendimas 2005/222/TVR).

Siekiant suderinti Lietuvos Respublikos baudžiamuosius įstatymus su šiomis nuostatomis, 2004 m. sausio 29 d.[22] BK XXX skyrius papildytas dviem naujais $198^1$ ir $198^2$ straipsniais, kurie kriminalizavo neteisėtą prisijungimą prie kompiuterio ar kompiuterinio tinklo (BK $198^1$ straipsnis) ir neteisėtą disponavimą įrenginiais, kompiuterinėmis programomis, slaptažodžiais, prisijungimo kodais ir kitokiais duomenimis, skirtais nusikaltimams daryti (BK $198^2$ straipsnis). Kaip matyti, šie pakeitimai buvo susiję tik su baudžiamojo įstatymo spragų šalinimu, kriminalizuojant naujas nusikalstamas veikas, vienu ar kitu būdu pažeidžiančias elektroninių duomenų ar informacinių sistemų saugumą, tačiau ne su esamų nusikalstamų veikų sudėčių požymių koregavimu. Nors Konvencijos dėl elektroninių nusikaltimų preambulėje bei II skyriaus 1 skirsnio 1 dalyje, įtvirtinančioje įvairias su materialiąja baudžiamąja teise susijusias nuostatas, buvo pateiktas tikslesnis baudžiamojo įstatymo saugomos vertybės pavadinimas („*kompiuterinių duomenų ir sistemų konfidencialumas, vientisumas ir prieinamumas*“), tačiau šiuo aspektu baudžiamojo įstatymo nuostatos 2004 m. nebuvo pakeistos.

Pagrindinio baudžiamosios teisės priemonėmis saugomo teisinio gėrio netikama formuluotė buvo pakeista tik 2007 m. birželio 28 d.[23] į nacionalinę teisės sistemą perkėlus Tarybos pamatinio sprendimo 2005/222/TVR nuostatas ir taip su jomis suderinus įvairius baudžiamosios atsakomybės už nusikalstamų veikų elektroninėje erdvėje padarymą aspektus. Taip iš esmės pertvarkius BK XXX skyriuje įtvirtintas nusikalstamų veikų apibrėžtis, kartu pakeistas ir šias nusikalstamas veikas į savarankišką rūšį jungiančio teisinio gėrio pavadinimas, suformuluojant daug tikslesnį ir tinkamesnį „*elektroninių duomenų ir informacinių sistemų saugumo*“ pavadinimą.

Apibendrinus teigtina, kad pagrindinio baudžiamosios teisės priemonėmis saugotino teisinio gėrio, pažeidžiamo specifinėmis informacinių sistemų ir elektroninių tinklų nusikalstamomis veikomis, įvardijimo problema kilo tik tiesiogiai šias nusikalstamas veikas kriminalizavus ir jas laikant nebe sudėtine tradicinių nusikalstamų veikų dalimi, o savarankišką baudžiamąją teisinę reikšmę turinčiomis nusikalstamomis veikomis. Šių nusikalstamų veikų padarymu pažeidžiamas teisinis gėris kito nuo pirminio, laikytu ydingu „*informatikos kaip mokslo*“ iki daug tikslesnio šių nusikalstamų veikų esmę atskleidžiančio „*elektroninių duomenų ir informacinių sistemų saugumo*“.

---

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

23 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.

## 3. Elektroninių duomenų ir informacinių sistemų saugumo samprata

Analizuojant įvairius mokslinėje literatūroje minimus informacinių sistemų ir apskritai elektroninės erdvės saugumo aspektus, pasakytina, kad elektroninių nusikalstamų veikų doktrinoje egzistuoja dvi pagrindinės saugumo koncepcijos. Šių skirtingų savo apimtimi saugumo koncepcijų susiformavimui tiesioginės įtakos turėjo gana plati nusikalstamų veikų elektroninėje erdvėje apibrėžtis ir, atitinkamai, šiuo terminu įvardijamų skirtingų rūšių nusikalstamų veikų prevencijai taikytinų būdų ir priemonių parinkimo problemos.

„*Elektroninės erdvės saugumas*“ (angl. *Cybersecurity*), arba plačiausią prasmę saugumui suteikianti koncepcija, dažniausiai minima tais atvejais, kai akcentuojami įvairūs nacionalinio saugumo aspektai. Šiuo atveju saugumas atskleidžiamas per tris pagrindines grėsmių kategorijas: *grėsmės, susijusios su neteisėto informacijos turinio skleidimu elektroninėje erdvėje*, *atakų prieš strateginės svarbos infrastruktūras* (ar kitas svarbią reikšmę turinčias informacines sistemas) ir pačių *informacinių sistemų darbo sutrikdymo ar nutraukimo grėsmės*[24].

Nors ši koncepcija turėtų leisti saugumą traktuoti plačiąja prasme, kaip visos elektroninės erdvės saugumą, vis dėto joje palikti ją siaurinantys, todėl diskutuotini aspektai.

Pirmiausia atkreiptinas dėmesys į tai, kad sparti kompiuterinių informacinių technologijų, kurių materialų pagrindą sudaro kompiuterių technologijos,[25] bei kompiuterinių tinklų raida sudarė prielaidas didelės apimties įvairaus pobūdžio informacijos sklaidai, naujoms prieigos prie informacijos, taip pat informacijos apsikeitimo galimybėms atsirasti ne tik nacionaliniu lygiu. Toks vystymasis užtikrino ir transnacionalinius informacinius procesus, todėl dėl elektroninių nusikalstamų veikų pobūdžio baudžiamojo įstatymo saugomoms vertybėms kylančios grėsmės gali būti tiek lokalaus, tiek ir globalaus pobūdžio, trukdančios dėsningam informacinės infrastruktūros vystymuisi, pažeidžiančios elektroninių duomenų ir informacinių sistemų apsaugą bei saugumą. Todėl, autorės nuomone, „*elektroninės erdvės saugumo*“ koncepcijai būtina suteikti globalumo aspektą, atsisakant jo tiesioginės sąsajos tik su nacionaliniu saugumu.

Pažymėtina, kad pateikta „*elektroninės erdvės saugumo*“ samprata neatsiejama nuo atitinkamų elektroninėje erdvėje kylančių įvairių rūšių grėsmių identifikavimo, nes galimų grėsmių akcentavimas atskleidžia ne tik informacinės visuomenės pažeidžiamumo problemą, bet apibrėžia ir šios teorijos ribas. Todėl formuluojant „*elektroninės erdvės saugumo*“ sampratą būtina atsižvelgti į elektroninėje erdvėje kylančių grėsmių ir, atitinkamai, šioje erdvėje padaromų nusikalstamų veikų, sukeliančių minėtas grėsmes, įvairovę. Pernelyg siaurai apibrėžus „*elektroninės erdvės saugumą*“ ir į jo turinį neįtraukus dalies saugumui keliamų grėsmių būtų nepagrįstai apribojamas ir elektroninėje erdvėje padaromų nusikalstamų veikų sąrašas.

---

24 Balkin, J. M., *et al. Cybercrime: Digital Cops in the Networked Environment*. New York: New York University Press, 2007, p. 63.

25 Skyrius, R., *et al. Informacijos ir komunikacijos technologijos.* Vilnius: Vilniaus universiteto leidykla, 2008, p. 17.

Iš materialinės baudžiamosios teisės pozicijų analizuojant elektroninėje erdvėje baudžiamojo įstatymo saugomoms vertybėms kylančias grėsmes, siūlytina jas konkretizuoti nurodant, kokios nusikalstamo elgesio formos elektroninėje erdvėje nulemia šių grėsmių atsiradimą. „*Elektroninės erdvės saugumui*“ kenkiančių elektroninių nusikalstamų veikų ir jų sukeliamų grėsmių baudžiamojo įstatymo saugomoms vertybėms sąsajos nustatymas galėtų būti laikomas vienu iš būdų, leidžiančių išvengti pernelyg siauros „*elektroninės erdvės saugumo*“ sampratos. Todėl, autorės nuomone, „*elektroninės erdvės saugumas*“ pirmiausia galėtų būti laikomas ta baudžiamojo įstatymo saugoma vertybe, kuri yra pažeidžiama arba kuriai yra sukeliama žalos atsiradimo grėsmė bet kurios į elektroninių nusikalstamų veikų visumą įtrauktos veikos padarymu. Kadangi nusikalstamų veikų elektroninėje erdvėje terminas siejamas su trimis nusikalstamų veikų rūšimis, todėl, autorės nuomone, „elektroninės erdvės saugumui“ kylančios grėsmės pirmiausia gali būti siejamos su *grėsmėmis, kurias sukelia neteisėto turinio informacijos skleidimas elektroninėje erdvėje* (pavyzdžiui, rasinės neapykantos, terorizmo kurstymas, vaikų pornografijos platinimas). Antra, grėsmės, kurių atsiradimas siejamas su *specifinėmis nusikalstamomis veikomis, kuriomis tiesiogiai kėsinamasi į elektroninių duomenų ir informacinių sistemų konfidencialumą, integralumą arba autentiškumą* (pavyzdžiui, neteisėtas poveikis elektroniniams duomenims arba informacinei sistemai, neteisėtas elektroninių duomenų perėmimas ir panaudojimas). Ir trečia, galėtų būti skiriamos tos grėsmės, kurias *sukelia tradicinės, tačiau dėl elektroninės erdvės panaudojimo galimybių pakitusios, nusikalstamos veikos* (pavyzdžiui, sukčiavimas elektroninėje erdvėje).

Šiuo aspektu analizuojant anksčiau minėtas mokslinėje literatūroje pateikiamas tris grėsmių kategorijas[26], svarstytina, ar kai kurios jų turėtų būti siaurinamos iki grėsmių, sukeliamų strateginės svarbos infrastruktūroms ar kitoms svarbią reikšmę turinčioms informacinėms sistemoms, tai yra atskirai nurodant atakų prieš strateginės svarbos infrastruktūras (ar kitas svarbią reikšmę turinčias informacines sistemas) ir pačių informacinių sistemų darbo sutrikdymo ar nutraukimo grėsmes. Manytina, kad šiuo atveju vis dėlto svarbesniu turėtų būti laikomas pats žalos informacinėms sistemoms kilimo grėsmės ar žalos padarymo joms faktas, o ne informacinės sistemos didesnę svarbą liudijančių požymių akcentavimas. Tik šiuo požymiu grindžiamas grėsmių atskyrimas lemia, kad nurodytos grėsmės sutaps visais atvejais, kai nutraukiamas arba sutrikdomas strateginę ar kitą svarbią reikšmę turinčių informacinių sistemų darbas. Taip pat svarstytina, ar į pateiktą grėsmių sąrašą įtrauktos grėsmės ir elektroninių duomenų (o ne tik informacinių sistemų) saugumui. Kartu keltinas klausimas, kodėl pateiktos grėsmių kategorijos nėra siejamos ir su tokiomis dėl elektroninės erdvės panaudojimo pakitusiomis tradicinėmis nusikalstamomis veikomis kaip, pavyzdžiui, sukčiavimas elektroninėje erdvėje ar elektroninio dokumento suklastojimas.

Antrosios „*techniniu kompiuterių saugumu*“ (angl. *Technical computer security*) vadinamos koncepcijos ištakų turėtų būti ieškoma technikos srityje[27]. Nors termino

26 Balkin, J. M., *et al., supra* note 24, p. 63.

27 Dažnai įvairūs informacinių technologijų saugumo metodai įtvirtinti informacijos saugumo valdymo praktikos kodeksuose (pavyzdžiui, ISO/IEC 27002:2005, kuris anksčiau buvo žinomas kaip ISO/IEC 17799; ISO/IEC 27001:2005, kuris pakeitė BS7799-2:2002 ir kita).

„*saugumas*“ turinys nagrinėjamame kontekste galėtų būti atskleidžiamas pasitelkiant lingvistinį aiškinimą nurodant, kad elektroniniai duomenys ir informacinės sistemos saugios tuomet, kai joms nekeliamas pavojus arba jos yra apsaugotos nuo pavojų[28], tačiau tokio bendro pobūdžio samprata negali būti laikoma informatyvia bei pakankama. Todėl mokslinėje literatūroje „*techninio kompiuterių saugumo*“ samprata susiejama su trimis saugumą apibūdinančiomis kategorijomis: elektroninių duomenų ir informacinių sistemų konfidencialumas (angl. *Confidentiality*), integralumas (angl. *Integrity*) ir prieinamumas (angl. *Availability*). Pažymėtina, kad nors šie „techninį kompiuterių saugumą“ atskleidžiantys požymiai specialistų vadinami skirtingai − saugumo pagrindinėmis koncepcijomis[29], principais[30] ar siekiais[31], tačiau dažniausiai šie terminai siejami su konfidencialumo, integralumo ir prieinamumo triada, kuri mokslinėje literatūroje sutrumpintai vadinama *CIA triada*. Šie klasikiniais pripažįstami elektroninių duomenų ir informacinių sistemų saugumo aspektai minimi ir Konvencijos dėl elektroninių nusikaltimų[32] 1 skirsnio 1 dalyje, kurioje pateiktos specifinių elektroninių tinklų nusikalstamų veikų apibrėžtys.

Paminėtina, kad šią triadą sudaro savarankiški, turinio prasme nesutampantys ir vienas kito neapimantys elementai. Tačiau priklausomai nuo padarytos į elektroninių nusikalstamų veikų visumą įtrauktos nusikalstamos veikos pobūdžio, žalos kilimo grėsmė arba žala gali būti padaroma keliems nurodytiems saugumo elementams. Pavyzdžiui, neteisėtu elektroninių duomenų pakeitimo būdu nutraukiamas informacinės sistemos darbas, tokiu būdu pažeidžiant elektroninių duomenų ir informacinių sistemų integralumą ir jų prieinamumą. Bet galimi ir tokie atvejai, kai padaryta nusikalstama veika pažeidžiamas tik vienas *CIA triados* elementas. Pavyzdžiui, neteisėtas elektroninių duomenų paskleidimas, pažeidžiant šių duomenų konfidencialumą, tačiau nepakeičiant jų ar informacinių sistemų integralumo ir nedarant įtakos jų prieinamumui.

Atskirai analizuojant minėtas tris savarankiškas saugumo kategorijas, pasžymėtina, kad klasikinis požiūris į techninį elektroninių duomenų ir informacinių sistemų saugumą ilgą laiką buvo siejamas su konfidencialumo, integralumo ir prieinamumo užtikrinimu, tačiau mokslinėje literatūroje pastaruoju laikotarpiu matomi specialistų siekiai ne tik savaip interpretuoti *CIA triadą* sudarančius elementus[33], bet taip pat ir praplėsti jos turinį, įtraukiant daugiau elektroninių duomenų ir informacinių sistemų saugumą apibūdinančių požymių[34].

---

28 *Dabartinės lietuvių kalbos žodynas.* Keinys, S., *et al.* (red.). 4-oji laida. Lietuvių kalbos institutas, 2000, p. 677.

29 Sumit, K., *et al. Communication networks: principles and practice*. New York: McGraw-Hill, 2007, p. 336.

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

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

32 2003 m. Konvencija dėl elektroninių nusikaltimų [interaktyvus]. [žiūrėta 2010-09-27]. <http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=228195&p_query=&p_tr2=>.

33 Sumit, K., *et al., supra* note 29, p. 336.

34 *Computer security handbook*. 4th edition. Bosworth S., *et.al*. (eds.). New York, 2002.

Analizuojant minėtos triados pirmąjį požymį, apibūdinantį elektroninių duomenų ir informacinių sistemų saugumą − jų konfidencialumą, paminėtina, kad jis įvairių autorių moksliniuose straipsniuose suvokiamas panašiai ir apibrėžiamas kaip draudimas paskleisti elektroninius duomenis tiems vartotojams, kurie neturi prieigos prie šių duomenų teisės[35]. Atkreiptinas dėmesys, kad neteisėtas elektroninių duomenų perėmimas ir panaudojimas, kriminalizuotas BK 198 straipsnyje, galimas neteisėtai stebint, fiksuojant, perimant, įgyjant, laikant, pasisavinant, paskleidžiant ar kitaip panaudojant neviešus elektroninius duomenis, todėl, manytina, kad elektroninių duomenų konfidencialumo pažeidimo atvejai neturėtų būti apribojami tik elektroninių duomenų paskleidimu tiems vartotojams – asmenims ar informacinėms sistemoms,− kurie neturi teisėtos prieigos prie šių duomenų. Kartu pritartina tiems autoriams, kurie konfidencialumo užtikrinimo poreikį akcentuoja ne tik duomenų saugojimo, kaupimo, bet ir jų apdorojimo bei keitimosi (perdavimo) metu[36]. Taip pat būtina atkreipti dėmesį, kad konfidencialumas turėtų būti laikomas ne tik vienu iš elektroninių duomenų, bet taip pat ir informacinių sistemų saugumo aspektų, užtikrinant, kad informacinės sistemos, atliekančios duomenų apdorojimo procesus, prieinamos tik prieigos teisę prie šių sistemų turintiems vartotojams. Pavojingos veikos, neteisėtai prisijungus prie informacinės sistemos, tokiu būdu pažeidžiant informacinių sistemų konfidencialumą, kriminalizuotos BK 198[1] straipsnyje.

Antrasis pamatinis į *CIA triados* sudėtį įeinantis saugumo elementas yra elektroninių duomenų ir informacinių sistemų integralumas, patvirtinantis elektroninių duomenų ir informacinių sistemų vidinės struktūros užbaigtumą bei vientisumą. Elektroninių duomenų integralumas laikytinas duomenų savybe, liudijančia, kad saugojimo, apdorojimo ar duomenų keitimosi metu šie duomenys be atitinkamų teisėtų įgaliojimų nebuvo pakeisti. Pavyzdžiui, viena iš alternatyvių BK 196 straipsnio 1 dalyje kriminalizuotų veikų – neteisėtas elektroninių duomenų pakeitimas, kaltininkui gali būti inkriminuojamas ir tais atvejais, kai jis tyčiniais veiksmais pažeidžia elektroninių duomenų struktūrą, taip pažeisdamas ir šių duomenų integralumą. Informacinių sistemų integralumas rodo, kad sistema, atliekanti jai nurodytas funkcijas, saugi nuo neteisėtų manipuliacijų, įsikišimo į jos darbą[37]. Pažymėtina, kad mokslinėje literatūroje pateikiamos ir diskutuotinos nuomonės, kuriomis nepagrįstai siaurinamas integralumo turinys, jį laikant tik būtina elektroninių duomenų savybe, nepaisant taip pat ir informacinių sistemų vientisumo poreikio[38].

Elektroninių duomenų ir informacinių sistemų prieinamumas yra trečiasis elektroninių duomenų ir informacinių sistemų saugumo elementas. Dauguma mokslininkų šį saugumo elementą sieja tik su elektroninių duomenų prieinamumu, užtikrinančiu, kad turintiems atitinkamus įgaliojimus vartotojams – asmenims ar informacinėms sistemoms, elektroniniai duomenys yra prieinami be trukdžių ar kliūčių ir gaunami reikiamu

35 Whitman, M. E., *et al*. *Principles of information security*. 3rd edition. Boston: Thomson: Course Technology, 2009, p. 10; *Computer and Information security handbook*, *supra* note 30, p. 256.

36 Stoneburner, G., *supra* note 31, p. 2.

37 *Ibid*.

38 *Ibid*.

formatu[39]. Arba nurodoma, kad informacija turi būti prieinama bet kuriuo užklausos pateikimo metu[40]. Manytina, kad šios autorių pozicijos nepagrįstai iš *CIA triados* eliminuoja informacinių sistemų prieinamumą, kai neteisėtai sutrikdomas ar nutraukiamas informacinės sistemos darbas ir ji dėl to tampa laikinai arba nuolat neprieinama prieigos teisę turintiems vartotojams. Tokio pobūdžio pavojingos asmens elgsenos elektroninėje erdvėje pasireiškimo formos, nukreiptos prieš informacinių sistemų prieinamumą, kriminalizuotos BK 197 straipsnyje, jeigu informacinės sistemos darbo sutrikdymas arba nutraukimas sukėlė atitinkamo masto žalą.

Kaip buvo minėta anksčiau, mokslinėje literatūroje taip pat galima sutikti ir kitokių į *CIA triados* turinį įeinančių elementų interpretavimo atvejų, kai į triados sudėtį įtraukiami kiti nei pripažinti klasikiniai elektroninių duomenų ar informacinių sistemų saugumą apibūdinantys konfidencialumo, integralumo ir prieinamumo požymiai. Dalis autorių neginčija elektroninių duomenų ir informacinių sistemų konfidencialumo ir integralumo poreikio, tačiau vietoj elektroninių duomenų ir informacinių sistemų prieinamumo į *CIA triados* sudėtį įtraukia kitą elementą – jų autentiškumą (angl. *Authentication*). Susiejęs elektroninių duomenų autentiškumą su duomenų šaltinio tikrumo garantu, šie autoriai akcentuoja, kad autentiškumas tampa neatsiejamas nuo elektroninių duomenų integralumo, todėl abu sujungiami į vieną elektroninių duomenų autentiškumo elementą[41]. Atsižvelgus į tai, kad ši pozicija siaurina „techninio kompiuterių saugumo“ koncepciją, nepagrįstai iš jos turinio eliminuodama elektroninių duomenų ir informacinių sistemų prieinamumo apsaugą, bei neatitinka vieno pagrindinių *CIA triados* konstravimo principų, kad į visumą turėtų būti sujungtos savarankiškos ir savo turiniu nesutampančios įvairius saugumo aspektus atspindinčios kategorijos, jai nepritartina. Manytina, kad papildomi elektroninių duomenų ir informacinių sistemų saugumo elementus apibūdinantys požymiai galėtų būti naudojami siekiant išsamiau atskleisti konfidencialumo, integralumo ir prieinamumo turinį, tačiau šių papildomų požymių išskyrimas kaip pagrindinių laikytinas pertekliniu ir nesuteikiančiu *CIA triadai* pridėtinės vertės.

Bene radikaliausiu požiūriu į *CIA triados* elementų visumą gali būti laikoma specialisto D. Parkerio suformuluota šešių elementų sistema, kuri dažnai vadinama *D. Parkerio heksada*. Šioje naujoje techninio kompiuterių saugumo struktūroje skiriami tokie pamatiniai elementai kaip konfidencialumas, integralumas, prieinamumas, autentiškumas, naudingumas ir nuosavybės teisių išsaugojimas, kurie turėtų pakeisti klasikinę CIA triadą kaip nepakankamą užtikrinant elektroninių duomenų saugumą[42].

Išanalizavus pagrindines elektroninių nusikalstamų veikų doktrinoje susiformavusias saugumo koncepcijas, darytina išvada, kad „*elektroninės erdvės saugumas*“ galėtų būti laikomas ta baudžiamojo įstatymo saugoma vertybe, kuri pažeidžiama (arba kuriai yra sukeliama žalos kilimo grėsmė) bet kurios į elektroninių nusikalstamų veikų visumą įtrauktos veikos padarymu. Todėl ši kaip papildoma vertybė tarpusavyje jungia įvairias kriminalizuotas pavojingas asmens elgsenos elektroninėje erdvėje pasireiškimo formas.

---

39 Whitman, M. E., *et al*., *supra* note 35, p. 9.

40 *Computer and Information security handbook*, *supra* note 30, p. 256.

41 Sumit, K., *et al*., *supra* note 29, p. 336.

42 *Computer security handbook*, *supra* note 34.

Tuo tarpu „*techninis kompiuterių saugumas*“ yra ta pagrindinė baudžiamojo įstatymo saugoma vertybė, kuri leido tarpusavyje į vieną savarankišką nusikalstamų veikų rūšį sujungti BK XXX skyriuje kriminalizuotas nusikalstamas veikas. Todėl terminas „*techninis kompiuterių saugumas*“ galėtų būti vartojamas kaip elektroninių duomenų bei informacinių sistemų saugumo sinonimas.

## Išvados

Pagrindinės baudžiamojo įstatymo saugomos vertybės, tiesiogiai pažeidžiamos nusikalstamomis veikomis elektroninėje erdvėje, identifikavimas neatsiejamas nuo minėtu terminu įvardijamų nusikalstamų veikų visumos.

Atsižvelgiant į tai, kad terminas *„elektroniniai nusikaltimai“* siejami su trimis nusikalstamų veikų rūšimis – tradicinėmis nusikalstamomis veikomis, padaromomis naudojant elektroninių ryšių tinklus ir informacines sistemas, nusikalstamomis veikomis, susijusiomis su neteisėto turinio informacijos platinimu elektroninėje erdvėje, ir išimtinai specifinėmis elektroninių tinklų nusikalstamomis veikomis, vienos pagrindinės ir baudžiamosios teisės priemonėmis saugomos vertybės, į kurią pirmiausia būtų kėsinamasi šiomis nusikalstamomis veikomis ir kuri leistų jas sujungti į savarankišką vienoda baudžiamojo įstatymo saugoma vertybe grindžiamą rūšį, konkretizuoti nebūtų įmanoma.

Priėjus prie išvados, kad nusikalstamos veikos elektroninėje erdvėje į vieną visumą sujungtos vadovaujantis ne pažeidžiama pagrindine baudžiamojo įstatymo saugoma vertybe, vis dėlto abejotina, ar šių nusikalstamų veikų sąsaja galėtų būti laikomi tik informacinių technologijų bei elektroninės erdvės panaudojimo ar kompiuterinės informacijos kriterijai. Manytina, kad tiesiogine šių nusikalstamų veikų sąsaja taip pat yra ir papildoma baudžiamojo įstatymo saugoma vertybė – plačiausia prasme saugumą apibūdinantis elektroninės erdvės saugumas.

Analizuojant išimtinai teisinio gėrio, pažeidžiamo nusikalstamomis veikomis elektroninių duomenų ir informacinių sistemų saugumui, įvardijimo baudžiamajame įstatyme problemas, pastebėta, kad jos kilo tik tiesiogiai šias nusikalstamas veikas kriminalizavus baudžiamajame įstatyme ir jas laikant nebe sudėtine tradicinių nusikalstamų veikų dalimi, o savarankišką baudžiamąją teisinę reikšmę turinčiomis nusikalstamomis veikomis. Šiomis nusikalstamomis veikomis pažeidžiamas teisinis gėris kito nuo pirminio, laikyto ydingu, „*informatikos kaip mokslo*“, iki daug tikslesnio šių nusikalstamų veikų esmę atskleidžiančio „*elektroninių duomenų ir informacinių sistemų saugumo*“.

Atskleidžiant elektroninių duomenų ir informacinių sistemų saugumo sampratą pažymėta, kad elektroninių nusikalstamų veikų doktrinoje egzistuoja dvi pagrindinės saugumo koncepcijos – „*elektroninės erdvės saugumas*“ ir „*techninis kompiuterių saugumas*“.

„*Elektroninės erdvės saugumas*“ galėtų būti laikomas ta baudžiamojo įstatymo saugoma vertybe, kuri yra pažeidžiama (arba kuriai yra sukeliama žalos kilimo grėsmė) bet kurios į elektroninių nusikalstamų veikų visumą įtrauktos nusikalstamos veikos padarymu. Tuo tarpu „*techninis kompiuterių saugumas*“ – tai ta pagrindinė baudžiamo-

jo įstatymo saugoma vertybė, kuri leido tarpusavyje į vieną savarankišką rūšį sujungti BK XXX skyriuje kriminalizuotas nusikalstamas veikas. Todėl „*techninis kompiuterių saugumas*“ gali būti laikomas elektroninių duomenų ir informacinių sistemų saugumo sinonimu.

Siekiant atskleisti „*techninio kompiuterių saugumo*“ sampratos turinį turėtų būti vadovaujamasi konfidencialumo, integralumo ir prieinamumo triada, kuri mokslinėje literatūroje sutrumpintai vadinama *CIA triada.*

## Literatūra


2003 m. Konvencija dėl elektroninių nusikaltimų [interaktyvus]. [žiūrėta 2010-09-27]. <http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=228195&p_query=&p_tr2=>.

2007 m. gegužės 22 d. Europos Komisijos Komunikatas Europos Parlamentui, Tarybai ir Europos Regionų komitetui KOM (2007) galutinis Bendrosios politikos, skirtos kovai su elektroniniais nusikaltimais [interaktyvus]. [žiūrėta 2010-09-14]. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:LT:HTML>.

Balčytienė, A., *et al*. *Informatikos įvadas*. Vilnius: Apyaušris, 1996.

Balkin, J. M., *et al. Cybercrime: Digital Cops in the Networked Environment*. New York: New York University Press, 2007.

*Baudžiamoji teisė: specialioji dalis*. Pavilionis, V. (sud.). Vilnius: Eugrimas, 2000.

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

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

*Computer Security Handbook*. 4th edition. Bosworth, S. *et.al*. (eds.). New York, 2002. Criminal Code of the Federal Republic of Germany [interaktyvus]. [žiūrėta 2010-09-05]. <http://www.legislationline.org/documents/action/popup/id/9015/preview>.

Criminal Code of the Republic of Estonia [interaktyvus]. [žiūrėta 2010-09-05]. <http://www.legislationline.org/download/action/download/id/1280/file/4d16963509db70c09d23e52cb8df.htm/preview>.

Criminal Code of the Republic of Poland [interaktyvus]. [žiūrėta 2010-09-05]. <http://www.legislationline.org/documents/section/criminal-codes>.

*Dabartinės lietuvių kalbos žodynas*. Keinys, S., *et al.* (red.). 4-oji laida. Lietuvių kalbos institutas, 2000.

Kunicka-Michalska, B. *Przestępstwa przeciwko wolności seksualnej i obyczajności popełniania za pośrednictwem systemu informatycznego*. Wrocław: Zakład Narodowy im. Ossolińskich, 2004.

Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2010 m. rugsėjo 28 d. nutartis baudžiamojoje byloje Nr. 2K-426/2010.

Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2006 m. balandžio 4 d. nutartis baudžiamojoje byloje Nr. 2K-281/2006.

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

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.

Lietuvos Respublikos Konstitucinio Teismo 2003 m. birželio 10 d. nutarimas. *Valstybės žinios*. 2003, Nr. 57-2552.

Mazurov, V. A. *Kompjuternye prestuplenija* [Computer Crimes]. Moskva: Paleotip, 2002.

Skyrius, R., *et al*. *Informacijos ir komunikacijos technologijos*. Vilnius: Vilniaus universiteto leidykla, 2008.

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

Sumit, K., *et al. Communication Networks*: *Principles and Practice*. New York: McGraw-Hill, 2007.

Štitilis, D. *Teisinės atsakomybės pagrindų nustatymo už neteisėtas veikas elektroninėje erdvėje problemos*. Daktaro disertacija. Socialiniai mokslai, teisė. Vilnius: LTU, 2002.

Švedas, G. *Baudžiamosios politikos pagrindai ir tendencijos Lietuvos Respublikoje*. Vilnius: Teisinės informacijos centras, 2006.

Walden, I. *Computer Crimes and Digital Investigation*. Oxford: Oxford University Press, 2007.

Whitman, M. E., *et al*. *Principles of Information Security*. 3rd edition. Boston: Thomson: Course Technology, 2009.

# THE PROBLEMS OF INDENTIFICATION OF THE MAIN OBJECT OF CYBER OFFENCES

Renata Marcinauskaitė

Mykolas Romeris University, Lithuania

***Summary.*** *The article deals with the problems of identifying the main object* (*the principal value*), *that is protected by criminal law and suffers a damage caused by cyber crime acts. An analysis of the said problems enabled the authors to substantiate the identification of the main object* (*the principal value*) *protected by ultima ratio measures and its importance for a legal technician on codification of criminal acts in an integral system, its inseparability from identification of criminal acts included in the cyber crimes as a whole. So, it should be supposed that the definition of these various dangerous forms of behavior in cyber space prohibited by the criminal law not only predetermines the peculiarities of the conception of cyber crime acts but also affects the determination of the possible limits of analysis of the main objects* (*the principal values*) *protected by the criminal law that are damaged by such dangerous acts.*

*It is stated in the article that it is impossible to identify the single main object (the principal value) protected by criminal law measures that is mostly encroached by the said criminal acts and that would enable to unite them into an independent uniform type based on the object protected by criminal law. However, in the opinion of the author, one of the links between such criminal acts may be considered an additional object* (*additional value*)

*protected by criminal law, i.e. Cybernetic security that identifies cyber safety in a broad sense and that suffers a damage caused by the above–mentioned criminal acts or a threat of appearance of such damage.*

*Through the analysis of exclusively specific criminal acts in electronic nets, it was found that two principal concepts are formulated in the doctrine of cyber crime acts, namely, Cybernetic security and Technical computer security. Cybernetic security is considered a concept of safety in a broad sense, so this term can be used for identification of the said additional object (additional value) that is protected by criminal law and that is affected by any criminal act included in the cyber crime as a whole. Technical computer security may be identified as an object* (*value*) *protected by criminal law that enables uniting criminalized acts into an independent type of criminal acts in the Chapter XXX of the Criminal Code and can be considered as a synonym of the security of electronic data and information systems.*

*In the article, an analysis of the contents of Technical computer security is carried out using the confidentiality, integrity and availability triad that in scientific references is shortly referred to as CIA triad.*

***Keywords***: *cyber crime, offences against security of electronic data and information systems, the object of the offence, cybernetic security, technical computer security, CIA triad, confidentiality, integrity, availability.*

---

**Renata Marcinauskaitė**, Mykolo Romerio universiteto Baudžiamosios teisės ir krimonologijos katedros lektorė. Mokslinių tyrimų kryptys: nusikalstamos veikos elektroninėje erdvėje.

**Renata Marcinauskaitė**, Mykolas Romeris University, Faculty of Law, Department of Criminal Law and Criminology, Lecturer. Research interests: cybercrime, i.e. criminal offences against the confidentiality, integrity and availability of electronic data and information systems, computer–related offences, content–related offences.