NUSIKALTIMAI VIRTUALIOJE ERDVĖJE – ŠIUOLAIKINIAI IŠŠŪKIAI IR PREVENCIJOS GALIMYBĖS

Ugnė Grigaitytė, Miglė Mackevičiūtė

Vilniaus universiteto Teisės fakulteto
2–o kurso studentės
Saulėtekio al. 9, I rūmai, 10222 Vilnius
El. paštai: ugne.d.grigaityte@gmail.com; macmigle@gmail.com
Mokslinio straipsnio akademinis kuratorius Gintautas Sakalauskas
El. paštas: gintautas.sakalauskas@tf.vu.lt
Mokslinio straipsnio praktinis kuratorius Regimantas Žukauskas
El. paštas: regimantas.zukauskas@prokuraturos.lt

Straipsnyje pateikiama nusikaltimų virtualioje erdvėje analizė, aptariami probleminiai klausimai ir jų aktualumas šiomis dienomis.

The article analyzes virtual crimes, its issues and perspectives in relation to certain cybercrime questions.

Įvadas

Nusikalstamam elgesiui, kaip visuomenėje vykstančiam procesui, būdingas socialinis, kultūrinis, teisinis konstravimas. Nusikalstamumas ir jo formos nuolat keičiasi, vyksta nuolatinis kriminalizavimo ir dekriminalizavimo procesas. Jis priklauso nuo tam tikro laikotarpio ypatumų, taip pat nuo žmonijos vystymosi raidos etapo ir socialinės aplinkos. Sparti pastarųjų dešimtmečių technologijų raida kelia teisei naujus iššūkius ir atveria naujas tyrinėjimo kryptis, taip pat ir nusikaltimų virtualioje erdvėje kriminalizavimo srityje.

Informacinės technologijos vis labiau skverbiasi į įvairias gyvenimo sritis ir tampa visų mūsų kasdienybe. Materiali dokumentų forma vis dažniau konvertuojama į elektroninę, o ranka rašytus laiškus keičia žinutės socialiniuose tinkluose. Jei anksčiau dokumentai ar sutartys keliaudavo iš vienos valstybės į kitą per keletą savaičių, tai šiais laikais tai neužtrunka ilgiau nei keletą sekundžių. Laisva interneto prieiga lėmė ne tik perteklinį informacijos kiekį ir patogius būdus ją greitai susirasti ir gauti, tačiau – ir žalingą šios informacijos turinį bei kitas apsaugos nuo socialiai nepageidaujamo elgesio problemas. Nusikalstamas elgesys iš materialios erdvės iš dalies persikėlė į skaitmeninę. Sukčia-

Copyright © Ugnė Grigaitytė, Miglė Mackevičiūtė, 2020. Published by Vilnius University Press.
This is an Open Access article distributed under the terms of the Creative Commons Attribution License (CC BY), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

vimai, vagystės, pinigų plovimas, pornografija, šantažas bei specifiniai kompiuteriniai nusikaltimai, kurie atsirado kartu su internetu ir informacinėmis technologijomis, kaip antai įsilaužimas į kompiuterines sistemas, virusų atakos, kompiuterinės sistemos sutrikdymas – tik keli kompiuterinių technologijų vaidmens pavyzdžiai, iliustruojantys jo reikšmę.

Taigi, informacinėmis technologijoms keičiant mūsų kasdienybę, keitėsi ir būdai, kuriais vykdomi nusikaltimai. Ir tai yra opi šių dienų problema, kurią nors ir mėginama spręsti tarptautinėmis konvencijomis bei nacionaliniais teisės aktais, tačiau jos sprendimai vis dar turi savų niuansų ir spragų. Nusikaltimų elektroninėje erdvėje problematika vis aktualesnė teisinio reguliavimo srityje. Įvairios tarptautinės organizacijos, tokios kaip Europos ekonominio bendradarbiavimo ir plėtros organizacija (OECD), Europos Taryba, Jungtinių Tautos, Pasaulio prekybos organizacija siekia kovoti su plintančiais elektroniniais nusikaltimais.

Dėmesys elektroninių nusikaltimų problemai buvo skiriamas jau XX a. 9–ajame dešimtmetyje. 1983–1985 m. Ekonominio bendradarbiavimo ir plėtros organizacija atliko tyrimą apie su kompiuteriais susijusius nusikaltimus ir valstybėms narėms pateikė minimalius pavojingų veikų, susijusių su elektronine erdve, sąrašus. 1994 m. Jungtinės Tautos išleido „Su kompiuteriais susijusių nusikaltimų kontrolės ir prevencijos vadovą“, kuriame aprašomos kompiuterinių nusikaltimų tendencijos, teisinis reguliavimas, prevencija ir tarptautinis bendradarbiavimas šiuo klausimu. Europos Tarybos paskirtas su kompiuteriais susijusių nusikaltimų ekspertų komitetas nagrinėjo teisines kompiuterinių nusikaltimų problemas[1].

Pabrėždamos šios problemos aktualumą, jos fenomeną analizuojame šiame straipsnyje. Šio tyrimo **objektas** yra nusikaltimai elektroninėje erdvėje, jų rūšys, latentiškumas, specifika ir kompleksiškumas. Analizuojame ne tik Lietuvos Respublikos baudžiamojo kodekso (toliau vadinama – BK)[2] XXX skyriuje numatytus elektroninius nusikaltimus ir jų santykį su tarptautinės teisės aktais[3].

Darbo tikslas – apibrėžti elektroninių nusikaltimų sampratą, išanalizuoti elektroninius nusikaltimus, jų problematiką, atskleisti tarpusavio santykį ir jų rūšis, pateikti aktualiausių teisės aktų analizę, apžvelgti elektroninių nusikaltimų kriminalizavimo spragas ir šiuolaikinius jų kontrolės ir prevencijos iššūkius.

Darbe taikomi šie **metodai**: istorinis – apžvelgiamos aktų, kuriuose reglamentuojamos elektroninių nusikaltimų priėmimo priežastys, sąlygos, BK XXX skyriaus pakeitimai ir papildymai; sisteminis – tiriamos BK normos, susijusios su elektroniniais

---

1 KIŠKIS, M., PETRAUSKAS, R., ROTOMSKIS, I., ŠTITILIS, D. *Teisės informatika ir informatikos teisė*. Vilnius: Mykolo Romerio Universitetas, 2006, p. 249.

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

3 Lietuvos Respublikos prokuratūra. Nusikaltimai elektroninėje erdvėje. Prieiga per internetą: *https://www.prokuraturos.lt/lt/veiklos-sritys/baudziamasis-persekiojimas/nusikaltimai-elektronineje-erdveje/185*

nusikaltimais, duomenų analizės – tiriami statistikos duomenys ir teismų praktika; lyginamasis – nacionalinės teisės aktų nuostatų lyginimas su užsienio teisės aktais, ieškant tarp jų panašumų ir skirtumų.

1. Elektroninių nusikaltimų samprata

Šiuolaikinės informacinės technologijos sparčiai išplito daugelyje žmogaus veiklos sričių, siekiant kurti informacinę visuomenę. Išsivysčiusių šalių vyriausybės suinteresuotos kuo daugiau viešųjų paslaugų perkelti į elektroninę erdvę. Ūkinei, finansinei ir kitai veiklai persikeliant į elektroninę erdvę, įvykdomų nusikalstamų veikų skaičius bei įvairovė nuolat didėja – elektroninė erdvė suteikia galimybes naujų, iki tol teisinėje praktikoje nežinomų, nusikalstamų veikų atsiradimui bei įgyvendinimui. Su nusikalstamomis veikomis, kurios atliekamos panaudojant kompiuterinę įrangą, susiduria ir privatūs asmenys, ir verslo subjektai. Iki nusikalstamų veikų priskyrimo elektroniniams nusikaltimams, elektroniniai įsilaužėliai (angl. *hackers*) išvengdavo baudžiamosios atsakomybės, nes nusikaltimai elektroninėje erdvėje įstatymiškai nebuvo apibrėžti, tyrėjams trūkdavo kompetencijos arba teismai negalėjo įvertinti surinktų įkalčių tinkamumo[4].

Europos policijos biuro (Europolo) duomenimis, kai kuriose Europos Sąjungos šalyse elektroniniai nusikaltimai jau lenkia tradicinių nusikaltimų skaičių. Elektroninės erdvės naudojimas neišvengiamai tapo prieiga vykdyti nusikalstamas veikas, tokiu būdu užtikrinant laisvę veikti neatskleidžiant tapatybės, sudarė palankias sąlygas naudoti kompiuterinius puolimus teroristinėms grupuotėms bei atskirų šalių specialiosioms tarnyboms. Realybe tapo ir informacinis karas. Taigi, elektroninis nusikalstamumas tapo visuotiniu reiškiniu, šios veikos yra itin latentinės, o jų tyrimas ir atskleidimas yra itin sudėtingas. Nusikaltimų virtualioje erdvėje nagrinėjimas kelia daug iššūkių teisėsaugos institucijoms bei padaliniams, atsakingiems už informacijos saugos užtikrinimą.

Lietuvoje nėra bendros elektroninių nusikaltimų sąvokos. Pagrindiniai nacionaliniai įstatymai, kuriais vadovaujantis vykdomas elektroninis saugumas – Lietuvos Respublikos elektroninių ryšių įstatymas[5], Lietuvos Respublikos elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų įstatymas, Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas. Lietuva, ratifikavusi Konvenciją dėl elektroninių nusikaltimų, *de jure* įteisino elektroninio nusikaltimo terminą.

---

[4] GORANIN, N., MAŽEIKA, D. *Nusikaltimai elektroninėje erdvėje ir jų tyrimo metodikos.* Mokomoji knyga. KTU, GTU, UAB TEV, 2011, p. 11. Prieiga per internetą: *http://www.esparama.lt/documents/10157/490675/Nusikaltimai_elektronineje_erdveje_ir_ju_tyrimo_metodikos. pdf*

[5] Lietuvos Respublikos elektroninių ryšių įstatymas. *Valstybės žinios,* 2004, Nr. 69-2382 (su vėlesniais pakeitimais ir papildymais).

Remiantis Europos Bendrijų Komisijos komunikatu, Europos Parlamentui, Tarybai ir Europos Regionų Komitetui, jokia politika, skirta kovai su elektroniniais nusikaltimais, negali būti veiksminga, jei pastangos apsiriboja ES, nes informacijos tinklai yra pasaulinio pobūdžio. Svarbiausias Europos tarptautinis aktas šioje srityje yra 2001 m. Europos Tarybos konvencija dėl elektroninių nusikaltimų. 2004 m. įsigaliojusioje konvencijoje pateiktos bendros įvairių elektroninių nusikaltimų rūšių apibrėžtys ir nustatyti susitariančiųjų šalių teisinio bendradarbiavimo veikimo pagrindai[6]. Turime remtis galiojančiais tarptautiniais aktais, kadangi atakos prieš informacines sistemas gali būti ir yra rengiamos ne tik ES valstybėse narėse, bet ir už ES jurisdikcijos ribų, o šią konvenciją pasirašė visos ES valstybės narės, Jungtinės Amerikos Valstijos bei kitos ne Europos valstybės.

JAV teisingumo departamentas elektroninius nusikaltimus apibrėžia kaip neteisėtas veikas, kurių metu kompiuteris, atliekantis savo pirmines funkcijas, panaudojamas kaip tų veikų pagrindinė priemonė[7]. Prie neteisėtų veikų priskiriamas kompiuterinių virusų skleidimas, įsilaužimas į tinklą. Tapatybės vagystės, elektroninės patyčios, persekiojimas bei terorizmas. Europos Sąjungos kibernetinio saugumo strategijoje nurodoma, kad elektroniniai nusikaltimai reiškia įvairaus pobūdžio nusikalstamą veiką, kuriai kaip pirminės priemonės ar pirminis tikslas naudojami kompiuteriai ir informacinės sistemos[8]. Taigi, remiantis šiais dviem šaltiniais, galime teigti, kad elektroniniai nusikaltimai apima tiek įprastas nusikaltimų rūšis, pavyzdžiui, sukčiavimą, klastojimą, tiek specifinius nusikaltimus, pavyzdžiui, išpuolius prieš informacines sistemas, siekimą nutraukti sistemos veiklą ir kenkimo programinę įrangą.

JAV mokslininkas D. Parkeris pasiūlė naudoti *piktnaudžiavimo kompiuteriu* (angl. *computer abuse*) terminą, kuris elektroninį nusikalstamumą prilygino visoms tyčinėms veikoms, kurios vienaip ar kitaip susijusios su kompiuteriais ir dėl kurių asmuo patyrė ar galėjo patirti žalos, o nusikalstamumo subjektas turėjo ar galėjo gauti iš to naudos. Iš pažiūros sąvoka atrodanti pakankamai tiksli, visgi neapima neatsargumo ar veikų padarymo nesiekiant naudos. Europos Komisijos dokumentuose kompiuterinis nusikaltimas minimas kaip bet koks neteisėtas veiksmas, apimantis kompiuterį, jų sistemą arba programinę įrangą.

Ekspertų komitetas, sudarytas Ekonominio bendradarbiavimo ir plėtros organizacijos veiklai su kompiuteriais susijusių nusikaltimų problemai spręsti, kompiuterinius nusikaltimus apibrėžė kaip bet kokį neteisėtą, neetišką ar nesankcionuotą elgesį, susi-

---

6 Europos Bendrijų komisija. *Komisijos komunikatas Europos Parlamentui, Tarybai ir Europos Regionų Komitetui.* Briuselis, 2007. Prieiga per internetą: *https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:52007DC0267&from=EN*

7 The United States department of Justice. Prieiga per internetą: *https://www.justice.gov/*

8 Europos Komisijos Bendras komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir regionų komitetui. Briuselis, 2003. Prieiga per internetą: *https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:52013JC0001*

jusį su automatiniu kompiuterinės formos duomenų apdorojimu ir siuntimu[9]. Vertėtų pabrėžti, kad užsienio literatūroje samprata nėra išsamiai išnagrinėta. Tai be abejo, parodo, jog supratimas apie nusikaltimus elektroninėje erdvėje dar nėra iki galo susiformavęs, egzistuoja poreikis detalesniam problemos nagrinėjimui bei nusikaltimų elektroninėje erdvėje klasifikavimui[10].

Bendriausiu atveju nusikaltimai elektroninėje erdvėje skirstomi pagal sąsają su kompiuterine sistema:

- *Siaurąja prasme* nusikaltimai, tiesiogiai darantys įtaką pačiai kompiuterinei sistemai.
  Tai veikos, kurios tiesiogiai nurodytos baudžiamųjų įstatymų skirsniuose. Šiuo atveju, pati kompiuterinė sistema tampa nusikaltimo tikslu.
- *Plačiąja prasme* – nusikaltimui vykdyti vienaip ar kitaip panaudojamos kompiuterinės technologijos, kitais žodžiais tariant, pasikėsinimo dalykas – informacija, nusikaltimo įrankis – kompiuteris, o šių nusikaltimų tyrimo priemonės taikos nusikaltimo fakto įrodymui.

Esminis kriterijus, skiriantis įprastus, realybėje pasireiškiančius nusikaltimus nuo skaitmeninių – fizinis atstumas tarp nusikaltėlio ir aukos, kurio, šiuo atveju, išvis nėra. Mažai tikėtina rasti ir daiktinių įrodymų, kadangi nusikaltimas vyksta elektroninėje erdvėje – pėdsakai, kaip ir virtuali asmenybė, nesunkiai paslepiami ar sunaikinami. Vienas ryškiausių akcentų – nusikalstamos veikos atlikimas iš bet kurios pasaulio vietos; nusikaltėlis nėra saistomas buvimo tam tikroje teritorijoje. Tai leidžia kompiuteriniams nusikaltimams priskirti „vienas ir daugelis“ nusikaltimo schemą, kuri leidžia greitai bei operatyviai pasiekti daugelį aukų globaliu mastu, neapsiribojant konkrečia teritorija.

Taigi, nauja skaitmeninės erdvės realybė (pirmiausia panaikinti laiko ir erdvės ribojimai, anonimiškumas, plataus masto veikimo galimybės) leidžia naujus nelegalios veiklos formas ir būdus bei išskiria kompiuterinius nusikaltimus kaip ypatingus ir skirtingus nuo įprastų „žemiškojo pasaulio“ nusikaltimų.

2. Nusikaltimų virtualioje erdvėje rūšys

Atskirų valstybių nacionalinių įstatymų nepakanka kriminalizuojant nusikaltimus virtualioje erdvėje ir organizuojant jų prevenciją. Tam užtikrinti prireikė bendro, tarptautinio dokumento. Siekiant apsaugoti visuomenę nuo tokių nusikaltimų, *inter alia,* priimant tam tikrus norminius aktus bei skatinant tarptautinį bendradarbiavimą,

---

[9] ŠTITILIS, D., KIŠKIS, M., LIMBA, T. *Interneto ir technologijų teisė.* Registrų centras, 2016, p. 402–403.

[10] GORANIN, N., MAŽEIKA, D. *Nusikaltimai elektroninėje erdvėje ir jų tyrimo metodikos.* Mokomoji knyga. KTU, GTU, UAB TEV, 2011, p. 11. Prieiga per internetą: *http://www.esparama.lt/documents/10157/490675/Nusikaltimai_elektronineje_erdveje_ir_ju_tyrimo_metodikos. pdf*

2001 m. pasirašyta ir 2004 m. įsigaliojusi jau minėta Konvencija dėl elektroninių nusikaltimų[11]. Tai – pirmoji tarptautinė sutartis dėl kompiuterių sistemomis vykdomų nusikaltimų. Siekdama efektyviai kovoti su šiuolaikinių technologijų pagalba daromais nusikaltimais, Lietuva 2003 m. birželio 23 d. prisijungė prie šios Konvencijos. Ji įpareigoja ją pasirašiusias šalis pripažinti kriminaliniais nusikaltimais joje numatytas veikas bei nustatyti juridinių asmenų atsakomybę (Konvencijos 11, 12, 24, 35 straipsniai), taip siekiant kovoti su moderniųjų technologijų pagalba daromais nusikaltimais.

Remiantis Konvencijoje nurodytomis kriminalizuotinomis veikomis, materialioji baudžiamoji teisė susideda iš tokių virtualių nusikalstamų veikų, kurios priskirtinos nusikaltimams kompiuterinių duomenų ir sistemų konfidencialumui, vientisumui ir prieinamumui, kompiuteriniams nusikaltimams, turinio nusikaltimams, nusikaltimams, susijusiems su autorių teisių ir gretutinių teisių pažeidimais bei atitinkamai taikoma papildoma atsakomybė ir sankcijos.

2.1. Nusikaltimai, pažeidžiantys kompiuterinės informacijos ir kompiuterinių sistemų konfidencialumą, vientisumą ir prieinamumą

Elektroninių duomenų ir informacinių sistemų saugumo turinį atskleisti ir struktūrinti BK XXX skyriuje numatytas nusikalstamas veikas padeda *CIA triados modelis*[12]: elektroninių duomenų ir informacinių sistemų konfidencialumas (angl. *confidentiality)*, užtikrinantis, kad reikiama informacija bus prieinama tik tiems vartotojams, kuriems yra suteikta prieigos teisė, integralumas, (angl. *integrity)*, užtikrinantis, jog duomenų apdorojimo funkcijas atliekančios sistemos nebuvo neteisėtai keičiamos ar modifikuojamos, ir prieinamumas (angl. *availability)*, sukuriantis galimybę reikiamą informaciją be trukdžių pasiekti reikiamu metu. *CIA triados* modelis laikomas saugumo koncepcijos ištaka saugumo politikos ir saugumo modelių srityje, kuris taikomas ISO/IEC /27001 standarte, kuriant informacijos saugos valdymo sistemą. Informacija yra nemateriali vertybė, ją gali sudaryti duomenys, informacija ir žinios, turintys vertę informacijos valdytojui. Tačiau ši nemateriali vertybė turi materialų pagrindą, tai – informacijos saugojimo laikmenos, ryšio linijos, kuriomis informacija perduodama, taip pat informacinės sistemos, kuriose ta informacija yra apdorojama.

Neteisėta prieiga prie kompiuterių programų arba duomenų elektronine forma laikytina tokia veika, kuri pažeidžia laikomos informacijos slaptumą (t. y. kyla realios žalos grėsmė), o dėl neteisėtos prieigos vykdomas šnipinėjimas, neteisėtai kopijuojami

---

[11] Konvencija dėl elektroninių nusikaltimų. Budapeštas, 2001. Prieiga per internetą: *https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.228195*

[12] MARCINAUSKAITĖ, R. *Nusikalstamos veikos elektroninėje erdvėje*. Vilnius: Registrų centras, 2019, p. 31.

autorių teisėmis apsaugoti kūriniai, sabotažas, sukčiavimas naudojantis kompiuteriais ir pan. laikytini savarankiškomis pavojingomis veikomis. Direktyva[13], kuria buvo pakeistas Europos Tarybos pamatinis sprendimas dėl atakų prieš informacines sistemas siekiama priimti konsensusą dėl požiūrio į vykdomų nusikalstamų veikų sudėtį. Nusikalstamomis veikomis visuotinai laikoma neteisėta prieiga ir įsikišimas į informacinę sistemą, duomenis bei neteisėtas duomenų perėmimas. Neteisėta prieiga, perimtis, poveikis duomenims bei sistemai, taip pat kaip ir netinkamas įtaisų naudojimas sudaro kompiuterinių duomenų bei sistemų konfidencialumo, vientisumo bei prieinamumo pažeidimą.

Lietuvos nacionalinių teismų praktikoje neteisėtos prieigos problema atsispindi, pavyzdžiui, 2018 m. byloje 1-2411-917/2018[14], kurioje kaltinamasis neteisėtai prisijungė prie informacinės sistemos *„Facebook“*, siekdamas rasti atitinkamų įrodymų, tačiau tuo tik ir buvo apsiriboti. Taip pat buvo įvertintas ir dar 1985 m. vienos kompiuterinių mokslų srities studento įsilaužimas į finansinių institucijų kompiuterines sistemas nepadarant žalos. Mastu ir sudėtingumu situacijos skiriasi, tačiau jose tiesiogiai veikiama pasitelkiant neteisėtą prieigą. Neteisėta prieiga laikomas ne tik įsikišimas į kompiuterinės informacijos veikimo procesą, pasireiškiančiu neteisėtu informacijos ištrynimu, sunaikinimu, sugadinimu, pakeitimu, bet ir kompiuterinės informacijos vagystė, sietina su šnipinėjimu.

Elektroninėje erdvėje žalos padarymui populiariausia forma – kompiuterių virusai, kurie atitinkamai skirstomi į vykdomųjų bylų virusus (pavyzdžiui, CIH virusas, žinomas kaip „Černobylis“, taip pat „Windows“ operacinėje sistemoje gali būti .exe, .com, .scr ar kitos vykdomosios bylos), paleisties sektoriaus virusai (plinta užkrėsdami įvairių laikmenų pirmąjį sektorių, kuris naudojamas operacinei sistemai paleisti) bei mikrovirusai (parašyti naudojant rašyklių, skaičiuoklių, pavyzdžiui, „OpenOffice“ ar „Microsoft Office“, bei kitų programų mikrokomandas), taip pat tokios programos gali būti „Trojos arkliai“ (patenka į sistemą per spragas naršyklėse bei, priešingai nei virusai, paprastai nesidaugina), „kirminai“ (paprastai plinta el. pašto priedais) ir kt. Nacionalinio kibernetinio saugumo centro duomenimis[15], 2018 m. Lietuvoje užregistruota 53 tūkst. kibernetinių incidentų, kuriais pažeidžiamos interneto svetainės. Tiesa, 3 proc. mažiau nei 2017 m., tačiau išaugo kibernetinių incidentų sudėtingumas, atakos tapo vis labiau rafinuotos.

Pastaruoju metu pabrėžiamas kompiuterių sistemos darbo sutrikdymas, kai kompiuterių sistema per internetą „užverčiama“ daugybe žinučių (angl. *Denial of service attack (DoS).* DoS atakos vykdomos siekiant sutrikdyti normalią tinklalapio, serverio

---

[13] Europos Parlamento ir Tarybos direktyva 2013/40/ES. Prieiga per internetą: *https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:32013L0040*

[14] Kauno apylinkės teismo nuosprendis baudžiamojoje byloje 1-2411-917/2018.

[15] Nacionalinio kibernetinio saugumo būklės ataskaita, 2018. Prieiga per internetą: *https://www.nksc.lt/doc/NKSC_ataskaita_2018.pdf*

ar kitų tinklo išteklių veiklą. DdoS (angl. *Distributed Denial of Service)* veikimo principas – neteisėtas duomenų perėmimas ir panaudojimas; siekiama paveikti informacinę sistemą arba tinklą taip, kad kompiuterinės paslaugos taptų neprieinamos vartotojams. DdoS atakos dažnai neatsiejamos nuo botnet (virusų pagalba iš išorės neteisėtais tikslais valdomi kompiuterių tinklai) tinklų panaudojimo[16]. Priešingai nuo DoS, šiuo atveju užklausos į atakuojamą tinklo išteklių įrenginį siunčiamos iš daugelio kompiuterių. DdoS atakų pavyzdys – 2007 m. vykusiu įvykiu, kurio metu botnet tinklas, kurį sudarė apie 1 milijonas kompiuterių, buvo panaudotas atakuoti Estijos kompiuterius ir kompiuterinius tinklus ir taip buvo sutrikdytas šalies valstybių institucijų, parlamento bei daugumos bankų darbas[17]. Neteisėtas poveikis informacinei sistemai pasižymi DoS ir DdoS atakomis prieš internetinius puslapius (pavyzdžiui, Yahoo, CNN) bei tarnybines stotis.

Veikos pavojingumas sietinas su galimybe padaryti žalą. Neteisėtos prieigos priemonių, įrenginių platinimas, gaminimas, kaip ir kenkėjiškų programų sukūrimas, naudojimas ir platinimas taip pat laikomi nusikalstamomis veikomis. Kenkėjiškos programinės įrangos siekia įsitvirtinti kuo giliau kompiuterio operacinės sistemos viduje. Jomis sutrikdomas kompiuterinių sistemų darbas mažiausiai to tikintis, pavyzdžiui, perimant žiniatinklio naršyklės valdymą, rodant nepageidaujamą reklamą, stebint, kokiose žiniatinklio svetainėse lankomasi, pavagiant asmeninę informaciją, naudojant kompiuterį norint įsilaužti į kitus kompiuterius ir t. t. Dėl tokių programų kompiuterio veikimas gali sulėtėti arba tapti nestabiliu. Kenkėjiškomis programomis laikomi kompiuteriniai virusai, „loginės bombos“, „asinchroninės atakos“ ir kt.

BK numatyti keli straipsniai, pagal kuriuos taikoma baudžiamoji atsakomybė už neteisėtą prieigą prie kompiuterinių sistemų bei duomenų: neteisėtam elektroninių duomenų perėmimui ir panaudojimui (BK 198 str.), neteisėtam prisijungimui prie informacinės sistemos (BK 198[1] str.), neteisėtam disponavimui įrenginiais, programine įranga, slaptažodžiais, kodais bei kitokiais duomenimis (BK 198[2] str.).

2.2. Su kompiuterių naudojimu susiję nusikaltimai

Su technologijų raida atsirado platesnės galimybės tam tikriems ekonominiams nusikaltimams, pavyzdžiui, sukčiavimui. Elektroninė erdvė suteikė plotmę ir klastojimo veikoms atsirasti bei vystytis, todėl Lietuvos įstatymų leidėjas BK kriminalizavo sukčiavimo ir klastojimo veikas, vykdomas pasinaudojant elektronine erdve. Konvencijos dėl elektroninių nusikaltimų 7 ir 8 straipsniai pripažįsta kompiuterines klastotes bei kompiuterinius sukčiavimus neteisėtais bei ragina su jomis kovoti.

---

16 GRAHAM J. *Cyber Fraud: Tactics, Techniques and Procedures*. Taylor&Francis Group, 2009, p. 316.

17 KSHETRI, N. *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspective.* Springer-Verlag, 2010, p. 7.

Kompiuterinis sukčiavimas – kibernetinės apgaulės programų tipas. Pagal BK 182 straipsnį už sukčiavimą baudžiamojon atsakomybėn traukiamas „tas, kas apgaule savo ar kitų naudai įgijo svetimą turtą ar turtinę teisę, išvengė turtinės prievolės arba ją panaikino“. Vertėtų pabrėžti, jog sukčiavimas gali užtraukti atsakomybę ir pagal kitus BK straipsnius. 2017 m. byloje[18] E. R. išduotas Jungtinėms Amerikos Valstijoms kaltinamas apgaulės būdu iš „Google“ išviliojęs daugiau kaip 23 milijonus JAV dolerių, iš „Facebook“ – beveik 100 milijonų JAV dolerių, kurie buvo 2013–2015 m. įgyvendinto plano rezultatas. Anksčiau buvo skelbta, kad JAV teisėsauga pateikė kaltinimus dėl sukčiavimo, pinigų plovimo ir tapatybės vagystės. Taigi kompiuterinį sukčiavimą galima apibrėžti kaip pinigų ar kito turto pagrobimą naudojant kompiuterį. Tokios veikos apima nurodymus kompiuteriui pervesti pinigus į banko sąskaitą ir pan. Į Vokietijos baudžiamąjį kodeksą teisės reformos metu įtrauktos naujų nusikaltimų sudėtys, tarp kurių – kompiuterinis sukčiavimas (sukčiavimo veiką apibrėžia VFR BK 263 straipsnis)[19]. Tai rodo, jog atitinkamai su laiku sukčiavimo mastas nuolat augo ir atsirado būtinybė šią nusikalstamą veiką kriminalizuoti.

Kompiuterinis klastojimas – neteisėtas kompiuterinės informacijos sukūrimas arba pakeitimas. Pagal BK 300 str. už klastojimą baudžiamojon atsakomybėn traukiamas „tas, kas pagamino netikrą dokumentą, suklastojo tikrą dokumentą arba žinomai netikrą arba žinomai suklastotą dokumentą laiką, gabeno, siuntė, panaudojo ar realizavo“. Atsižvelgiant į tai, kad sukčiavimas negrynosiomis mokėjimo priemonėmis ir jų klastojimas vykdomas vis plačiau tarptautiniu mastu, kovai su klastojimu priimti bendresnio pobūdžio teisės aktai, taip pat apimantys kovos su elektroniniais nusikaltimais aspektus, pavyzdžiui, Europos Sąjungos Tarybos pamatinis sprendimas, skirtas kovai su sukčiavimu negrynosiomis priemonėmis ir jų klastojimu.

2.3. Su turiniu susiję elektroniniai nusikaltimai

Naudodamiesi paieškos sistemomis, vartotojai gali ištirti kibernetinę erdvę be visiško pasiklydimo. Informacijos gausa lėmė ir šios informacijos turinio žalingumą, netinkamumą. Internete apstu rasistinio pobūdžio medžiagos, smurtinių, žiaurių vaizdo įrašų, kur yra žalojami gyvūnai, žmonės, žalingą elgesį skatinančių pornografinių vaizdų ar kitos pavojingos informacijos[20].

---

[18] United States district court southern district of New York. *United States of America v. Evaldas Rimašauskas*. Form No. USA–33s–274. Prieiga per internetą: *https://www.justice.gov/usao-sdny/press-release/file/950556/download*

[19] Vokietijos Federacinės Respublikos baudžiamasis kodeksas. Prieiga per internetą: *https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html*

[20] Prieiga per internetą: *https://www.auguinternete.lt/lt/straipsniai/kok-zalinga-turin-internete-randajame-narsantys-paaugliai*

Tai kelia klausimus ir dėl baudžiamosios teisės vaidmens, kadangi baudžiamąją atsakomybę už tokio pobūdžio nusikaltimus yra sunkiau reglamentuoti, jie neapsiriboja konkrečiomis geografinėmis koordinatėmis ir apima daugiau nei vienos valstybės teisinės sistemos normas. Taip pat visos tokio pobūdžio ir kiekio informacijos neįmanoma surasti, ištrinti ar uždrausti. Pavyzdžiui, paieškos varikliai veikia nuskaitydami nuorodas internetinėje svetainėje. Jei svetainės savininkas nenori, kad svetainė būtų surasta, ji nebus įtraukta į tiesioginę nuorodą, o jei tinklalapyje nėra nuorodos, ji negali būti nuskaityta ar indeksuojama paieškos sistemoje, tad šis puslapis nebus rodomas[21].

Svetainės, kurios yra rodomos paieškos sistemoje kaip paieškos rezultatas, yra vadinamos „Surface web“ (paviršiaus tinklas), jos yra prieinamos ir lengvai pasiekiamos kiekvienam naudotojui, todėl tokios svetainėse esanti informacija gali būti lengvai sukontroliuojama, uždraudžiama ar ištrinama.

Kiek kitos „Deep web“ (giliojo interneto) principas – jis naudojamas prisijungiant prie savo banko paskyros, socialinių tinklų, internetinių parduotuvių, elektroninio pašto paskyrų. Šis turinys nebus rodomas paieškos sistemoje. Pavyzdžiui, jei įvestume asmens vardą ir pavardę paieškos sistemą, nebus rodoma jo asmeninė banko informacija ar elektroninio pašto susirašinėjimai. Ši informacija yra privati, todėl priešingai nei „Surface web“, nėra matoma kiekvienam interneto naudotojui, todėl daug neteisėtos ir žalingos informacijos, gali būti persiunčiama ir elektroniniu paštu, žinutėmis ir taip plisti internete.

Trečioji platforma – „Dark web/Darknet“ (tamsusis internetas), kuris naudoja užmaskuotą IP adresą, sąmoningai slepiant tinklalapius iš paieškos sistemos. Tam reikia specialios interneto naršyklės, kad vartotojai galėtų ją pasiekti. Pasak Andy Greenberg, tamsusis internetas sudaro mažiau nei 0,01 proc. giliojo interneto[22]. Vienas iš pavyzdžių – „Wikileaks“ svetainė, leidžianti pranešėjams anonimiškai įkelti pranešimus į spaudą ar įslaptintą informaciją. Įdomu tai, jog „Wikileaks“ įkūrėjui Julianui Assange nebuvo pateikti jokie kaltinimai[23].

Plačiai naudojamas socialinis tinklas „Facebook“ taip pat turi „Darknet“. Šis socialinis tinklas pradėjo „Tor“ paslėptą medžiagą, kad vartotojai galėtų išvengti stebėjimo ir cenzūros, tačiau anonimiškumas turi tamsią pusę – „Tor“[24] tinklas taip pat gali būti naudojamas paslėpti nusikalstamos veikos dalyvių tapatybę, kuo „Darkweb“ ir pasižymi. „Tor“ tinklas taip pat pasižymi šiais neteisėtos informacijos tipais – neteisėtų šaunamųjų ginklų pardavimas, vaikų pornografija, kenkėjiškų programų platinimas, narkotinių medžiagų pardavimas, asmens tapatybės ir pavogtų kreditinių kortelių pardavimas, lošimas, pinigų plovimas ir daug kitų.

---

21 https://quod.lib.umich.edu/cgi/t/text/text-idx?c=jep;view=text;rgn=main;idno=3336451.0007.104i

22 https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/

23 https://vpnoverview.com/privacy/anonymous-browsing/the-dark-web/

24 https://www.wired.com/2014/10/facebook-tor-dark-site/

Būtent „Dark web“ ir sudaro didžiąją dalį elektroninių nusikaltimų, kurių beveik neįmanoma išaiškinti, dėl specialiųjų naršyklių ir užmaskuotų kompiuterio vartotojo duomenų. Čia yra platinamos narkotinės medžiagos, vaikų pornografija, kaip prekę galima įsigyti organą ar uždraustą knygą[25]. Šalia šių žiaurių nusikaltimų galime paminėti ir prekybą žmonėmis. Keliamos negailestingos žmonių nuotraukos ar vaizdo įrašai, kurie vėliau yra pardavinėjami kaip objektai pasiūliusiems didžiausią sumą. Taip pat „Dark web“ kaip atsiskaitymo priemonę naudoja kriptovaliutas, tarkime, bitcoin[26].

Dėl interneto plėtros ir informacijos gausos elektroninė erdvė tapo pagrindiniu įrankiu, kuriuo platinama neteisėta informacija ar dalykai. Todėl ir baudžiamieji įstatymai turi atsižvelgti ne tik į materialaus pasaulio reiškinius ir nusikaltimus, bet ir plėstis į elektroninę erdvę. Taip pat šias problemas akcentuoja ir Europos Komisija savo ataskaitoje dėl Europos Sąjungos Tarybos ir Parlamento išleistos direktyvos 2011/93/ES[27] dėl kovos su seksualine prievarta prieš vaikus, jų seksualiniu išnaudojimu ir vaikų pornografija, kuria pakeičiamas Tarybos pamatinis sprendimas 2004/68/TVR.

Šioje ataskaitoje aptariamas pagalbos, paramos teikimas, nukentėjusiojo privatumo apsauga, reikalavimas, mechanizmai, kuriais galima užkirsti kelią nuteistiems asmenims vykdyti profesinę veiklą, susijusią su tiesioginiais ir reguliariais kontaktais su vaikais. Komisija ir toliau padės valstybėms narėms užtikrinti pakankamą perkėlimo ir įgyvendinimo lygį. Tai apima kontrolę, kad nacionalinėmis priemonėmis būtų vykdomos atitinkamos dalyvių nuostatos.

Lietuvos įstatymų leidėjas yra pasirinkęs tradicinį veikų, susijusių su vaikų pornografijos platinimu internetu, kriminalizavimo variantą. BK 309 straipsnis numato baudžiamąją atsakomybę už pornografinio turinio dalykų apie vaikus viešą demonstravimą, įsigijimą, platinimą, gaminimą ar net laikymą. Beje, šiuo straipsniu kriminalizuotos ir veikos platinant vadinamąsias „pseudofotografijas“, kuriose tam tikras asmuo pateikiamas kaip vaikas[28].

2.4. Su autorių ir gretutinėmis teisėmis susiję nusikaltimai

Intelektualios nuosavybės teisių pažeidimai, tokie kaip autoriaus darbo platinimas, naudojimas be jo sutikimo, kopijavimas taip pat yra aktualus elektroninių nusikaltimų kontekste. Apsaugos objektais laikomi literatūros darbai, muzikos, fotografijos, autovizualiniai ir kiti kūriniai, kurie gali būti platinami tiek jau aptartame „Surface web“, tiek per elektroninius laiškus, serverius, skelbimų portalu ir pan.

---

25 https://lifehacker.com/things-you-can-do-on-the-dark-web-that-arent-illegal-1819790298

26 https://www.thebalance.com/what-is-a-dark-market-391289

27 Europos Parlamento ir Tarybos direktyva 2011/92/ES. Prieiga per internetą: *https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A32011L0093*

28 Šiaulių apygardos teismo baudžiamoji byla 1A-11-519/2017.

Pagrindinis teisės aktas, reglamentuojantis autorių ir gretutinių teisių įgyvendinimą ir gynimą yra Lietuvos Respublikos autorių teisių ir gretutinių teisių įstatymo pakeitimo įstatymas. Šis įstatymas yra suderintas ir su Europos Sąjungos teisės aktais, o už autorių ir gretutinių teisių pažeidimą galima tiek civilinė, tiek administracinė, tiek baudžiamoji atsakomybė[29].

Baudžiamoji atsakomybė už autorinių teisių pažeidimą numatyta BK 192 straipsnyje: „tas, kas neteisėtai atgamino literatūros, mokslo, meno ar kitokį kūrinį ar jo dalį arba importavo, eksportavo, platino, gabeno ar laikė komercijos tikslais neteisėtas jų kopijas, jeigu kopijų bendra vertė pagal teisėtų kopijų mažmenines kainas viršijo 100 MGL dydžio sumą, baudžiamas viešaisiais darbais arba bauda, arba laisvės apribojimu, arba areštu, arba laisvės atėmimu iki dvejų metų". Atkreiptinas dėmesys, kad už šias veikas atsako ir juridinis asmuo.

Lietuvos Aukščiausiasis Teismas, aiškindamas BK 192 straipsnio dispozicijos turinį, ne vienoje nutartyje yra pasisakęs, kad neteisėtai atgamintas literatūros, mokslo, meno ar kitoks kūrinys, įskaitant kompiuterio programas, fonogramas bei audiovizualinius kūrinius, yra nusikaltimo, numatyto BK 192 straipsnyje, dalykas.

Taip pat pastaruoju metu vis dažniau plinta ir vadinamieji „Phishing" tipo elektroniniai nusikaltimai. Tai – asmens duomenų vagystė, susijusi su vartotojų teisių, informacijos saugumo, privatumo, taisyklių ir kitais pažeidimais. Ši problema ypatingai aktuali ir Lietuvai, kadangi net ir pažangios bankų sistemos, pasirodo nėra visiškai apsaugotos nuo elektroninių sukčių. Daugybę vartotojų dar visai neseniai gavo iš savo elektroninių bankų telefonines žinutes ar elektroninius laiškus, kurie pranešė apie banko internetinės programos atnaujinimą, ar nepavykusį pinigų pervedimą, o žmonės patikėje šia gudrybe, puolė atsinaujinti savo duomenis ar pakartotinai pervesti sumą, įvesdami savo duomenis, kurių įrašymas į sukčių sistemą jiems kainuodavo ne mažas pinigų sumas.

Autorių teisių ir gretutinių teisių pažeidimus elektroninėje erdvėje galima kvalifikuoti pagal BK XXIX skyriaus „Nusikaltimai intelektinei ir pramoninei nuosavybei" straipsnius. Šiame skyriuje kriminalizuoti tokie nusikaltimai: autorystės pasisavinimas (191 str.), literatūros, mokslo, meno ar kitokio kūrinio neteisėtas atgaminimas, neteisėtas kopijų platinimas, gabenimas ar laikymas (192 str.); informacijos apie autorių teisių ar gretutinių teisių valdymą sunaikinimas arba pakeitimas (193 str.) bei neteisėtas autorių teisių ar gretutinių teisių techninių apsaugos priemonių pašalinimas (194 str.).

---

[29] http://www.technologijos.lt/n/technologijos/it/straipsnis-7458/straipsnis/Teisininko-komentaras-Kas-*Lietuvoje-gresia-autoriniu-teisiu-pazeidejams?*

3. Elektroniniai įrodymai

Vis daugiau nusikaltimų yra padaroma kibernetinėje erdvėje. Įprastiems nusikaltimams, vykstantiems fizinėje erdvėje būdingi kitokie požymiai, lyginant su kompiuteriniais nusikaltimais, pavyzdžiui, nusikaltėlis ir auka dažnai turi tiesioginį kontaktą, nusikaltėlis tuo pačiu metu gali padaryti žalos vienam ar maksimaliai keliems asmenims, kai tuo tarpu kibernetiniai nusikaltimai turi tam tikrų ypatybių – čia nusikaltėlis jau gali pasiekti daugelį aukų ir sparčiai daryti šimtus ar net tūkstančius nusikaltimų. Viena iš ypatybių yra ir tokių nusikaltimų įrodinėjimas. Mažai tikėtina rasti fizinius (tarkime daiktinius) įrodymus, nes veika yra padaroma skaitmeninėje erdvėje, nusikaltimo pėdsakai gali būti lengvai sunaikinami, nusikaltėlis gali lengvai pakeisti savo virtualią asmenybę ar kompiuterio identifikavimo kodus.

Elektroninių įrodymų taikymas teismų sistemoje nuolat kito. Antai 1934 m. JAV Naujojo Džersio Aukščiausias teismas nagrinėjamoje byloje *State v. Simon*[30] atsisakė priimti kaip įrodymą fonografu įrašytą pokalbį. Tuo tarpu šiuolaikinė teisė leidžia kaip įrodymą naudoti įrašus, nuotraukas.

Lietuvos Respublikos baudžiamojo proceso kodekso 20 straipsnis įrodymus baudžiamojoje teisėje apibrėžia kaip įstatymų nustatyta tvarka gautus duomenis, kuriuos įvertina ir įrodymais pripažįsta atitinkamoje byloje paskirtas teisėjas ir kurie patvirtina ar paneigia bent vieną aplinkybę, turinčią reikšmės bylai išspręsti teisingai[31]. Į šią sąvoką taip pat patenka ir elektroninių duomenų apibrėžimas.

Pasitaiko atvejų, kai vykstant ginčui teisme, faktines aplinkybes galima įrodyti tik elektroniniais duomenimis, kurie yra kai kurių bylų įrodinėjimo pagrindas. Kaip pavyzdžius galima nurodyti bylas, susijusias su asmens privataus gyvenimo pažeidimu, tam tikros informacijos paskleidimu, kai informacija yra paskelbiama elektroninėje erdvėje (socialiniuose tinkluose, portaluose, persiunčiama tretiesiems asmenims ir kt.)[32] ir pan. Kai kuriais atvejais įstatymuose būna nustatyti tam tikri apribojimai rinkti duomenis arba informaciją, todėl vertinant surinktus duomenis būtina patikrinti, ar šių apribojimų buvo laikomasi[33]. Svarbi yra ir įrodymų sąsajumo taisyklė, pagal kurią teismas priima nagrinėti tik tuos įrodymus, kurie patvirtina arba paneigia reikšmės bylai turinčias aplinkybes. Įrodymai turi būti susiję su byla ir reikšmingi jai atskleisti.

Lietuvos Respublikos teismų įstatymo 37^1 str. 3 d. nustatyta, jog proceso dalyviai turi teisę visus procesinius dokumentus ir su teismo procesu susijusią informaciją

---

[30] *State v. Simon*, 174 A. 867 (N.J. 1934). Prieiga per internetą: *https://www.courtlistener.com/opinion/3585446/state-v-simon/?*

[31] Lietuvos Respublikos baudžiamojo proceso kodeksas. *Valstybės žinios,* 2000, Nr. 37-1341 (su vėlesniais pakeitimais ir papildymais).

[32] Šiaulių apygardos teismo nutartis civilinėje byloje Nr. 2A-120-124/2013.

[33] Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos nutartis Nr. 2K-281/2006.

teismams teikti elektroninės formos. Asmenys, teikiantys procesinius dokumentus elektroninių ryšių priemonėmis, turi juos pasirašyti saugiu e. parašu arba savo asmens tapatybę patvirtinti kitais būdais (per elektroninės bankininkystės sistemas ir pan.)[34]. Dokumentai elektroninių ryšių priemonėmis teismui teikiami naudojantis Lietuvos teismų informacijos sistemos (LITEKO) Viešųjų elektroninių paslaugų posistemiu (VEP). Problema ta, jog keliamų dokumentų ir jų priedų rinkmenos dydis yra ribotas (iki 200 MG), todėl proceso šalys, norinčios kaip įrodymus, pateikti nemažai nuotraukų, vaizdo įrašų, kurių bendras dydis viršija nustatytą, to negali padaryti LITEKO platformoje. Šalys dokumentus gali pateikti teismui materialioje laikmenoje (CD/DVD diske, atspausdinti ir pan.).

Elektroniniai įrodymai taip pat turi būt surinkti, ištirti, įvertinti laikantis įstatymo nustatytos tvarkos. Teisės doktrinoje yra minimas elektroninių įrodymų autentiškumas, pagal kurį duomenų turinys, kuriuo remiasi proceso šalis, išliko nepakitęs nuo sukūrimo momento, informacija gauta iš pirmojo šaltinio. Autentiškumas įrodinėjamas liudytojų parodymais, trečiųjų asmenų pateiktais dokumentais, specialisto išvadomis. Autentiškumui taip pat svarbus ir elektroninio parašo naudojimas[35]. Jei bylos šalis negalės pagrįsti elektroninių duomenų autentiškumo, teismas tokio įrodymo gali apskritai nevertinti[36].

Taigi, teismai prisitaikydami prie technologijų įtakos žmonėms, jų bendravimui dažnai taiko elektroninius įrodymus ir remiasi jais kaip turinčiais *prima facie* galią. Teismų praktikoje elektroniniai įrodymai, ypač kai nusikaltimas yra padarytas elektroninėje erdvėje, gali būti vieninteliai turimi, todėl teismai nevengia jais remtis. Kiekvienu konkrečiu atveju turi būti sprendžiama dėl byloje esančių įrodymų pakankamumo ir patikimumo. Ar įrodymus laikyti patikimais ar ne, kiekvienu atveju taip pat sprendžia teisėjas ar teismas, kurio žinioje yra byla[37].

4. Virtualios erdvės nusikaltimų latentiškumas ir daroma žala

Reikia pažymėti, kad nusikalstamos veikos, susijusios su virtualia erdve, ypač pavojingos tuo, kad oficiali teisėsaugos organų statistika neatspindi tikrosios jos padėties. Registruotas nusikalstamumas sudaro tik dalį nusikalstamo elgesio normos. Neišvengiamai kitą dalį tenka priskirti latentiniam nusikalstamumui, kuriuo (didesniu ar

---

[34] Lietuvos Respublikos teismų įstatymas. *Valstybės žinios,* 1994, Nr. 46-851 (su vėlesniais pakeitimais ir papildymais)

[35] Lietuvos Respublikos elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų įstatymas. *TAR*, 2018, Nr. 7474.

[36] Kauno miesto apylinkės teismo sprendimas civilinėje byloje Nr. 2-11525-877/2012.

[37] Prieiga per internetą: *https://www.teismai.lt/lt/naujienos/teismu-sistemos-naujienos/teiseja-j.-gaileviciene-ar-virtualus-susirasinejimai-gali-tapti-bylu-irodymais/3473*

mažesniu latentiškumo laipsniu) pasižymi visos nusikalstamos veikos. Nuostoliai dėl elektroninių nusikaltimų per metus viršija 300 mlrd. dolerių, o elektroninis nusikalstamumas laikomas viena latentiškiausių veikų. Žvelgiant į kibernetinio saugumo artimiausią ateitį, numatoma, kad kibernetinių nusikaltimų skaičius tik didės – iki 2021 m. kasmet atsieis apie 6 trilijonus JAV dolerių. Nusikaltimai virtualioje erdvėje pelningumu lenkia pasaulinę prekybą narkotikais[38].

2017 m. duomenimis, Symantec ataskaitoje atskleista, kad 17 mln. Didžiosios Britanijos vartotojų buvo paliesti kibernetinių nusikaltimų, o nuostoliai sudarė 4,6 mlrd. svarų[39]. FBI Nacionalinės kompiuterinių nusikaltimų tyrimų grupės teigimu, 85–97 proc. tokių nusikaltimų neiškyla į viešumą. JAV Gynybos departamento finansuotų tyrimų statistika gana stulbinanti – bandant įsibrauti į 8 932 informacines sistemas, dalyvavusias tyrime, 7 860 atvejų buvo sėkmingi[40]. 1995 m. organizuota Interpolo tarptautinė konferencija, po kurios Interpolas patvirtino, kad valstybių teisėsaugos institucijos, dalyvavusios konferencijoje, yra susirūpinusios dėl elektroninių nusikaltimų daromos žalos, nenuvaldomo plitimo ir latentiškumo. Aukštą elektroninių nusikaltimų latentiškumo laipsnį lemia keli faktoriai:

1. Didžioji dalis kompiuterinių nusikaltimų lieka nepastebėti. To priežastis – šiuos nusikaltimus sunkiau pastebėti nei įprastus nusikaltimus, kadangi visuomenė nėra pakankamai susipažinusi su jais, sunku juos atpažinti, sukčių profesionalumas, taip pat – gerai neišmanydami kompiuterinius nusikaltimus apibrėžiančių teisės aktų, nukentėjusieji gali ir nesuprasti, kad viena ar kita jų atžvilgiu vykdoma veika yra neteisėta[41].
2. Aukų vengimas informuoti kompiuterinius nusikaltimus, kai jie yra aptinkami. Taigi latentiškumui būdingas ir tiesioginių aukų nebuvimas, kuomet nei viena pusė, dalyvavusi nusikalstamoje veikoje, nėra suinteresuota pranešti teisėsaugos institucijoms. Prie tokių atvejų priskiriami ekonominiai, finansiniai nusikaltimai, narkotikų platinimas, kyšininkavimas ir kt. Verslo srityje šis nenoras susijęs su dviem dalykais:
   - kai kurios aukos nenori atskleisti informacijos apie savo darbą bijodamos viešumo arba prarasti gerą vardą;
   - kitos aukos bijo prarasti investuotoją, visuomenės pasitikėjimą.

---

38 https://www.bluebridge.lt/it-ziniu-centras/svarbiausios-kibernetines-gresmes-artimiausiu-metu-perspektyvoje/

39 https://www.itproportal.com/news/uk-consumers-lost-billions-to-cyber-crime-in-2017/

40 KIŠKIS, M., PETRAUSKAS, R., ROTOMSKIS, L., ŠTITILIS, D. *Teisės informatika ir informatikos teisė.* Vilnius: Mykolo Romerio universitetas, 2006, p. 240.

41 SAKALAUSKAS, G., DOBRYNINA, M., JUSTICKAJA, S., KALPOKAS, V., MALIŠAUSKAITĖ-SIMANAITIENĖ, S., NIKARTAS, S., POCIENĖ, A., ZAKSAITĖ, S. *Registruotas ir latentinis nusikalstamumas Lietuvoje: tendencijos, lyginamieji aspektai ir aplinkos veiksniai.* Vilnius, 2011, p. 175.

Latentiškumo problematika kyla ne tik dėl netinkamo kai kurių elektroninių nusikaltimų kriminalizavimo nacionaliniuose baudžiamuosiuose įstatymuose, tačiau ir dėl kvalifikacijos ar techninės įrangos stokos tiriant elektroninius nusikaltimus bei elektroninių įrodymo įtvirtinimo problemų[42].

5. Prevencijos galimybės

Kriminologine prasme prevencijos sąvoka išreikšta kaip viešų ir privačių pastangų, kuriomis siekiama užkirsti kelią nusikalstamoms veikoms, visuma. Tai visuomet yra tam tikra nusikalstamų veikų priemones taikančių subjektų veiklos paradigma[43].

Analizuojant specialiąją literatūrą[44], susijusią su elektroniniais nusikaltimais bei jų aspektais, galima būtų išskirti dvi pagrindines elektroninių nusikaltimų prevencijos priemones: teisines bei organizacines-technines. Prie teisinių priemonių galima priskirti teisinį elektroninių nusikaltimų reglamentavimą: teisės norminius aktus, taip pat minėtąją Europos Tarybos konvenciją dėl elektroninių nusikaltimų. Lietuvos elektroninės informacijos sauga reguliuojama daugelyje įstatymų, Vyriausybės nutarimų, ministrų ar atitinkamos įstaigos vadovų pasirašytų įsakymų. Būtų galima paminėti keletą svarbesnių įstatymų, kuriuose fragmentiškai reglamentuoti šie santykiai: Lietuvos Respublikos elektroninių ryšių įstatyme, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatyme, Lietuvos Respublikos autorių teisių ir gretutinių teisių įstatymo pakeitimo įstatyme, Lietuvos Respublikos elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų įstatyme, kuriuo 2018 m. gegužės 9 d. buvo pakeistas Lietuvos Respublikos elektroninio parašo įstatymas, ir kituose įstatymuose. Šių įstatymų pagrindu sudarytos sąlygos saugios informacinės visuomenės plėtrai, vartotojų pasitikėjimui informacine sistema didinimui.

Organizacinė pusė atskleidžia kompiuterinių sistemų funkcionavimą, jo konfidencialumą, techninį aprūpinimą, programinį aptarnavimą ir kt. Techninė pusė orientuojasi į kompiuterines programas ir į kompiuterio saugumo užtikrinimą.

Tarkime, viena iš labiausiai paplitusių šnipinėjimo programų yra „Spyware“, kitaip sakant, ji stebi vartotojo kompiuterį ir kontroliuoja jo sistemą. Ši šnipinėjimo programa įdiegiama žinant vartotojui, kai šis naudodamasis įprastine naršykle, tarkime, „Mozilla firefox“, bei ieškodamas informacijos gauna pasiūlymą įsidiegti „ActivX“ ar

---

42 KIŠKIS, M., PETRAUSKAS, R., ROTOMSKIS, I., ŠTITILIS, D. *Teisės informatika ir informatikos teisė.* Vilnius: Mykolo Romerio universitetas, 2006, p. 241.

43 TARASEVIČIUS, P. *Nusikalstamų veikų prevencijos kriminalinėje žvalgyboje samprata ir įgyvendinimo problemos.* Prieiga per internetą*: http://teise.org/wp-content/uploads/2017/07/Tarasevicius-2017-1.pdf*

44 ŠTITILIS, D. *Elektroniniai nusikaltimai: metodinė priemonė.* Vilnius: Mykolo Romerio universitetas, 2011, p. 91.

jo komponentą. Ši programa stebi vartotojo kompiuterį ir gali pasireikšti nepagrįstu automatiškai įsijungiančiais langais, svetainių registravimu. Vartotojas, norėdamas apsisaugoti nuo panašių šnipinėjimo programų, turėtų, visų pirma, atidžiau žiūrėti į „iššokančias" reklamas, su jomis nesutikti, įsidiegti ugniasienę[45], tarkime, „Microsoft" kompanijos sukurtą „Windows defender" programą.

Norint paslėpti failus, duomenis, registro raktus, branduolio taisykles, kuriamos atitinkamos programos, kaip antai „IceSwrod" ar „Rookit revealer", kurias reikia įdiegti, norint užsitikrinti šių failų apsaugą. Tai tvarkytuvės, kurios turi daug funkcijų aptinkant paslėptus failus, todėl vartotojas gali ne tik saugiai užsitikrinti naudojimąsi naršykle, tačiau ir nesunkiai surasti paslėptus failus.

Kalbant apie duomenų vagystę, jau minėta, jog pirmiausia internetiniai sukčiai veikia per elektroninius laiškus ar socialinius tinklus, prisidengdami tam tikrais asmenimis ar neatskleisdami savo tapatybės, todėl geriausia apsauga būtų nepasitikėti siunčiamais elektroniniais laiškais, jei jie bent minimaliai kelia įtarimą. Tokius laiškus galima atpažinti dėl nekorektiškos lietuvių kalbos gramatikos, pažadus apie laimėtą prizą, kurie atrodo lengvai gaunami, o reklama atsiranda vos tik puslapiui atsinaujinus. Taip pat derėtų atkreipti dėmesį į siuntėjo adresą, išanalizuoti laišką, jei patenkama į banko svetainę, kurios HTTPS sertifikatas neatitinka tikrojo, tai apgavystė.

Taip pat nuo kenksmingų programų galima apsisaugoti naudojant antivirusines ar kitokio pobūdžio kompiuterių apsaugos programas, perkant jų licencijas ar naudojant kitokio tipo aparatines ar programines programas.

Išvados

Apibendrinus atliktą tyrimą, galima padaryti tokias išvadas:

1. Išskiriamos dvi nusikalstamos veikos elektroninėje erdvėje sampratos kryptys – siaurąja ir plačiąja prasmėmis. Siaurąja prasme tai – nusikalstamos veikos, numatytos BK XXX skyriuje, pažeidžiančios elektroninių duomenų ir informacinių sistemų saugumą. Plačiąja – apimamos visos nusikalstamos veikos, kurioms įgyvendinti pasitelkiama informacinė sistema.
2. Elektroninio nusikaltimo tikslas – kompiuterinė sistema bei joje esantys duomenys, o duomenų perdavimo tinklai, kompiuterinė ar programinė įranga, skaitmeninė informacija tampa objektu ar įrankiu vykdyti nusikaltimus virtualioje erdvėje. T. y., išskiriamas elektroninių įrenginių abipusiškumas – jie gali būti nusikaltimo objektas arba priemonė, kuria vykdomi nusikaltimai, pavyzdžiui, DdoS atakos, įsilaužimai į informacinę sistemą, duomenų sunaikinimas ir kt.

---

[45] https://cert.litnet.lt/2015/05/asmeninio-kompiuterio-apsauga-4/4/

3. Nusikalstamų veikų skaičiaus didėjimą pastaraisiais metais lėmė ir viešųjų paslaugų persikėlimas į elektroninę erdvę, siekiant suteikti lengvesnį jų prieinamumą bei užtikrinti inovatyvumą.
4. 2001 m. lapkričio 23 d. Europos Tarybos priimta Konvencija dėl elektroninių nusikaltimų siekta sustabdyti veiksmus, nukreiptus prieš kompiuterinių duomenų konfidencialumą, vientisumą bei prieinamumą, dar žinomą kaip *CIA triados* modelį. Taip pat, šia Konvencija iki tol naudotas „kompiuterinių nusikaltimų" terminas pakeistas „elektroniniais nusikaltimais".
5. Baudžiamasis kodeksas, nustatydamas atsakomybę už neteisėtą poveikį elektroniniams duomenims bei informacinių sistemų saugumui, saugo kompiuterinių sistemų integralumo sritį.
6. Nusikalstamų veikų elektroninėje erdvėje problematika – nusikalstamos veikos atlikimas iš bet kurios pasaulio vietos neapsiribojant konkrečia teritorija – plataus masto veikimo galimybės bei anonimiškumas, sudarantis sąlygas nusikalstamų veikų latentiškumui.

Naudotų šaltinių sąrašas

1. Norminiai teisės aktai:

1.1. Lietuvos Respublikos teisės aktai:

1. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas. *TAR*, 2018. Nr. 11733.
2. Lietuvos Respublikos autorių teisių ir gretutinių teisių įstatymo pakeitimo įstatymas. *Valstybės žinios*, 2003, Nr. 28-1125.
3. Lietuvos Respublikos baudžiamasis kodeksas. *Valstybės žinios,* 2000, Nr. 89-2741 (su vėlesniais pakeitimais ir papildymais).
4. Lietuvos Respublikos baudžiamojo proceso kodeksas. *Valstybės žinios,* 2000, Nr. 37-1341 (su vėlesniais pakeitimais ir papildymais).
5. Lietuvos Respublikos elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų įstatymas. *TAR*, 2018, Nr. 7474.
6. Lietuvos Respublikos elektroninio parašo įstatymas. *Valstybės žinios,* 2000, Nr. 61-1827 (su vėlesniais pakeitimais ir papildymais, negalioja nuo 2018 m. gegužės 9 d.).
7. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas. *Valstybės žinios*, 2011, Nr. 163-7739 (su vėlesniais pakeitimais ir papildymais).
8. Lietuvos Respublikos elektroninių ryšių įstatymas. *Valstybės žinios,* 2004, Nr. 69-2382 (su vėlesniais pakeitimais ir papildymais).
9. Lietuvos Respublikos teismų įstatymas. *Valstybės žinios,* 1994, Nr. 46-851 (su vėlesniais pakeitimais ir papildymais).

1.2. Europos Sąjungos teisės aktai:

1. Europos Bendrijų komisija. *Komisijos komunikatas Europos Parlamentui, Tarybai ir Europos Regionų Komitetui.* Briuselis, 2007. Prieiga per internetą: *https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:52007DC0267&from=EN*

2. Europos Komisijos Bendras komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir regionų komitetui. Briuselis, 2003. Prieiga per internetą: *https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:52013JC0001*
3. Europos Parlamento ir Tarybos direktyva 2011/92/ES. Prieiga per internetą: *https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A32011L0093*
4. Europos Parlamento ir Tarybos direktyva 2013/40/ES. Prieiga per internetą: *https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:32013L0040*
5. Konvencija dėl elektroninių nusikaltimų. Budapeštas, 2001. Prieiga per internetą: *https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.228195*

1.3. Užsienio valstybių teisės aktai:

1. Vokietijos Federacinės Respublikos baudžiamasis kodeksas. Prieiga per internetą: *https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html*

2. Specialioji literatūra:

1. KIŠKIS, M., PETRAUSKAS, R., ROTOMSKIS, I., ŠTITILIS, D. *Teisės informatika ir informatikos teisė*. Vilnius: Mykolo Romerio Universitetas, 2006.
2. MARCINAUSKAITĖ, R. *Nusikalstamos veikos elektroninėje erdvėje*. Vilnius: Registrų centras, 2019.
3. SAKALAUSKAS, G., DOBRYNINA, M., JUSTICKAJA, S., KALPOKAS, V., MALIŠAUSKAITĖ-SIMANAITIENĖ, S., NIKARTAS, S., POCIENĖ, A., ZAKSAITĖ, S. *Registruotas ir latentinis nusikalstamumas Lietuvoje: tendencijos, lyginamieji aspektai ir aplinkos veiksniai.* Vilnius, 2011.
4. ŠTITILIS, D., KIŠKIS, M., LIMBA, T. *Interneto ir technologijų teisė.* Registrų centras, 2016.
5. ŠTITILIS, D. *Elektroniniai nusikaltimai: metodinė priemonė.* Vilnius: Mykolo Romerio universitetas, 2011.
6. GORANIN, N., MAŽEIKA, D. *Nusikaltimai elektroninėje erdvėje ir jų tyrimo metodikos.* Mokomoji knyga. KTU, GTU, UAB TEV, 2011, Prieiga per internetą: *http://www.esparama.lt/documents/10157/490675/Nusikaltimai_elektronineje_erdveje_ir _ju_tyrimo_metodikos.pdf*
7. GRAHAM, J. *Cyber Fraud: Tactics, Techniques and Procedures*. Taylor&Francis Group, 2009.
8. KSHETRI, N. *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspective*. Springer-Verlag, 2010.

3. Teismų praktika:

1. Kauno apylinkės teismo nuosprendis baudžiamojoje byloje 1-2411-917/2018.
2. Kauno miesto apylinkės teismo sprendimas civilinėje byloje Nr. 2-11525-877/2012.
3. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos nutartis Nr. 2K-281/2006.
4. *State v. Simon*, 174 A. 867 (N.J. 1934).
5. Šiaulių apygardos teismo baudžiamoji byla 1A-11-519/2017.
6. Šiaulių apygardos teismo nutartis civilinėje byloje Nr. 2A-120-124/2013.

7. United States district court southern district of New York. United States of America v. Evaldas Rimašauskas. Form No. USA–33s–274. Prieiga per internetą: *https://www.justice.gov/usao-sdny/press-release/file/950556/download*

4. Kita literatūra:

1. Asmeninio kompiuterio apsaugos būdai. Prieiga per internetą: *https://cert.litnet.lt/2015/05/asmeninio-kompiuterio-apsauga-4/4/*
2. Hacker lexicon: What is the Dark Web? Prieiga per internetą: *https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/*
3. Kokį žalingą turinį internete randa jame naršantys paaugliai? Prieiga per internetą: *https://www.auguinternete.lt/lt/straipsniai/kok-zalinga-turin-internete-randa-jame-narsantys-paaugliai*
4. Lietuvos Respublikos prokuratūra. Nusikaltimai elektroninėje erdvėje. Prieiga per internetą: *https://www.prokuraturos.lt/lt/veiklos-sritys/baudziamasis-persekiojimas/nusikaltimai-elektronineje-erdveje/185*
5. Nacionalinio kibernetinio saugumo būklės ataskaita, 2018. Prieiga per internetą: *https://www.nksc.lt/doc/NKSC_ataskaita_2018.pdf*
6. Svarbiausios kibernetinės grėsmės artimiausiu metu perspektyvos. Prieiga per internetą: *https://www.bluebridge.lt/it-ziniu-centras/svarbiausios-kibernetines-gresmes-artimiausiu-metu-perspektyvoje/*
7. Tarasevičius. P. Nusikalstamų veikų prevencijos kriminalinėje žvalgyboje samprata ir įgyvendinimo problemos. Prieiga per internetą *http://teise.org/wp-content/uploads/2017/07/Tarasevicius-2017-1.pdf*
8. Teisėja J. Gailevičienė: ar virtualūs susirašinėjimai gali tapti bylų įrodymais? Prieiga per internetą: *https://www.teismai.lt/lt/naujienos/teismu-sistemos-naujienos/teiseja-j.-gaileviciene-ar-virtualus-susirasinejimai-gali-tapti-bylu-irodymais/3473*
9. Teisininko komentaras. Kas Lietuvoje gresia autorinių teisių pažeidėjams? Prieiga per internetą: *http://www.technologijos.lt/n/technologijos/it/straipsnis-7458/straipsnis/Teisininko-komentaras-Kas-Lietuvoje-gresia-autoriniu-teisiu-pazeidejams?*
10. The Dark Web: What is it exactly and what can you find there? Prieiga per internetą: *https://vpnoverview.com/privacy/anonymous-browsing/the-dark-web/*
11. The Deep web: Surfacing hidden value. Prieiga per internetą: *https://quod.lib.umich.edu/cgi/t/text/text-idx?c=jep;view=text;rgn=main;idno=3336451.0007.104*
12. The Facebook just launched its own „Dark Web“ site. Prieiga per internetą: *https://www.wired.com/2014/10/facebook-tor-dark-site/*
13. The illicit world of bitcoin and the Dark Web. Prieiga per internetą: *https://www.thebalance.com/what-is-a-dark-market-391289*
14. The United States department of Justice. Prieiga per internetą: *https://www.justice.gov/*
15. Things you can do on the Dark Web that aren't illegal. Prieiga per internetą: *https://lifehacker.com/things-you-can-do-on-the-dark-web-that-arent-illegal-1819790298*
16. UK consumers lost billions to cyber-crime in 2017. Prieiga per internetą: *https://www.itproportal.com/news/uk-consumers-lost-billions-to-cyber-crime-in-2017/*

Santrauka

Šiame straipsnyje analizuojamos nusikalstamos veikos virtualioje erdvėje, jų problematiniai aspektai, aptariamos prevencijos galimybės. Apžvelgiamos elektroninių nusikaltimų rūšys, turinio aspektai šiuolaikinių iššūkių kontekste, nelegalios veiklos priemonės. Darbe pateikiama nacionalinio, ES ir tarptautinės teisės reglamentavimas, vertinamas kompetentingų institucijų, aktuali teismų praktika. Pristatoma 2001 m. priimta Konvencija dėl elektroninių nusikaltimų, plačiausiai apimanti ir teisiškai reguliuojanti nusikaltimus, daromus skaitmeninėje erdvėje, jos santykis su Lietuvos įstatymais, įskaitant BK. Moksliniame straipsnyje pabrėžiamas ir šių nusikaltimų ypatingas latentiškumas bei daromos žalos santykis su įprastais nusikaltimais.

Summary

The article presents an analysis of the virtual crimes, its problematic aspects, *inter alia*, prevention opportunities. Discussing types of virtual crimes, content aspects in the context of nowadays challenges, illegal acts' measures. Regulatory reviews at national, European Union and international level, considered by the competent intitutions, as well as case law. Convention on cybercrime, adopted in 2001, extensively covering and legally regulating crimes, commited through virtual space, a comparison with Lithuanian legislation, including criminal code. The work emphasizes latency of cybercrimes likewise the damages comparing with ordinary crimes.