Vilnius University Press

Contents lists available at Vilnius University Press

Kriminologijos studijos
2021, vol. 9, pp. 8–46

ISSN 2351-6097 eISSN 2538-8754
DOI: https://doi.org/10.15388/CrimLithuan.2021.9.1

Socialiniai tyrimai apie elektroninius nusikaltimus: globalus temų diapazonas ir Lietuvoje atliktų tyrimų sisteminė analizė

Maryja Šupa

Vilniaus universitetas, Filosofijos fakultetas
Sociologijos ir socialinio darbo institutas
Kriminologijos katedra
Vilnius University, Faculty of Philosophy
Institute of Sociology and Social Work
Department of Criminology
Universiteto g. 9, LT-01513 Vilnius
tel. (8 5) 266 7600
maryja.supa@fsf.vu.lt

Santrauka. Socialiniai tyrimai apie elektroninius nusikaltimus sudaro lauką, apimantį platų temų diapazoną ir jungiantį įvairias disciplinas. Straipsnyje, remiantis išsamia literatūros analize ir egzistuojančiuose apžvalginiuose straipsniuose (Holt, Bossler 2014; Stratton, Powell, Cameron 2017; Maimon, Louderback 2019) identifikuotais trūkumais, išskirta 41 elektroninių nusikaltimų socialinių tyrimų tema, suklasifikuota į keturias kategorijas: 1) tyrimai, charakterizuojantys atskirus nusikaltimų tipus; 2) tyrimai, sutelkti į pažeidėjus, nukentėjusiuosius ir teisėsaugą; 3) tyrimai apie elektroninių nusikaltimų diskursus; 4) tyrimai apie lokalius ir globalius elektroninių nusikaltimų ypatumus. Remiantis sudaryta temų schema, buvo atlikta sisteminė publikacijų apžvalga apie Lietuvoje įgyvendintus socialinių mokslų empirinius tyrimus apie elektroninius nusikaltimus. Rezultatai parodė, kad Lietuvoje tokių tyrimų atliekama mažai. Nuo 2004 m. iki 2020 m. iš viso rastos 26 publikacijos, iš kurių 10 yra teorinio pobūdžio, o

Received: 13/07/2021. **Accepted:** 24/08/2021

16 pristato atliktus empirinius tyrimus. Iš 41 išskirtos temos 14 temų turėjo teorinių arba empirinių publikacijų, o 27, arba du trečdaliai visų temų, Lietuvoje buvo nenagrinėtos. Kaupiant savalaikes, pagrįstas, kritinį mąstymą skatinančias, krizinėse situacijose reikalingas žinias apie elektroninius nusikaltimus, būtina plėtoti šią tyrimų sritį, didinti joje nagrinėjamų temų įvairovę ir skirtingų disciplinų indėlį, pildyti susikaupusias spragas, ypatingą dėmesį skiriant išsamiems, kompleksiniams ir validžiais empiriniais duomenimis pagrįstiems tyrimams plėtoti.
Pagrindiniai žodžiai: elektroniniai nusikaltimai, technologijos ir nusikaltimai, technologijų diskursai, interneto tyrimai, sisteminė apžvalga.

Social Research about Online Crime: Global Range of Topics and a Systematic Analysis of Research in Lithuania

Summary. Social research about online crime is a multi-disciplinary field addressing a wide array of topics since its inception in the 1980s. Based on a broad review of state-of-the-art literature and gaps identified in review publications (Holt, Bossler 2014; Stratton, Powell, Cameron 2017; Maimon, Louderback 2019, and others), in this paper I outline 41 key topic in social research about online crime, classified into four broad categories: 1) research focusing on specific types of online crime, 2) research about perpetrators, victims, and law enforcement, 3) research about online crime discourses and public perceptions, 4) research putting the local and global specifics of online crime into perspective. Based on the topic map, I undertook a systematic review of literature on research about online crime published in Lithuania from the empirical social scientific perspective. The results show that very few such studies are carried out in Lithuania. From 2004 to 2020, 26 publications have been found in total. 10 of them were theoretical briefs, while 16 were based on empirical data. Out of the 41 key topic, 14 were covered in the publications, while 29 or roughly two thirds remained unaddressed. The dominant contributors were legal scholars writing about the social aspects of online crime across a variety of topics, and mostly focusing on specific crime types. The most developed topic was cyberbullying, with contributions by scholars mostly from the fields of psychology and education. To fill in these glaring gaps, it is vital to develop this field of research with an emphasis on both wider and deeper research agendas, complex, valid and reliable research data and critical theoretical approaches, inviting systematic contributions from criminology, sociology, communication and media studies, and political science.
Keywords: technology and crime, online crime, technological discourses, internet research, systematic review.

Įvadas

Elektroniniai nusikaltimai – platus, aktualus, nuolat atsinaujinantis, tarpdalykinis tyrimų laukas. Tematiškai socialinius tyrimus apie elektroninius nusikaltimus galima skirstyti pagal pagrindinį tyrimo objektą, nuo mikrolygmens iki makrolygmens: nusikaltimų tipus, proceso dalyvius, sąsajas tarp nusikaltimų ir jų socialinio bei politinio konteksto. Šio tyrimų lauko apžvalgos paprastai pateikia dalinius pjūvius. Jose pristatoma tik pozityvistinė, kiekybinė paradigma iš elektroninio nusikaltimo proceso dalyvių perspektyvos (žr. Maimon, Louderback 2019) arba susitelkiama į tyrimus, skirtus konkrečiam elektroninių nusikaltimų tipui (žr. Holt, Bossler 2014), arba labai bendrai apžvelgiamas galimų tyrimų spektras ir koncentruojamasi į spragų išryškinimą (žr. Stratton, Powell, Cameron 2017). Šios apžvalgos pateikia vertingų dalinių įžvalgų apie elektroninių nusikaltimų tyrimus, tačiau neaprėpia tematinės lauko įvairovės ir sudėtingumo arba pristato tik siauras potemes.

Atlikto tyrimo tikslas – apibrėžti pasaulyje ir Lietuvoje atliekamų socialinių tyrimų apie elektroninius nusikaltimus tematinį gylį bei plotį. Tikslas įgyvendinamas, atsižvelgiant į nurodytus teorinius trūkumus ir pildant esamų žinių spragas, siekiant:

1) įtraukti su elektroniniais nusikaltimais susijusias temas, kurios iki šiol nepakliuvo į minėtų didesnių apžvalgų akiratį;
2) parodyti, kad kai kurie klausimai, kuriuos dalinės apžvalgos nurodo kaip neatsakytus ar dar netiriamus, iš tiesų yra tiriami;
3) išskleisti tiriamojo lauko temų kompleksiškumą, pabrėžiant klaidingų generalizacijų problemą, pavyzdžiui, kad elektroninius nusikaltimus darančių pažeidėjų ir nukentėjusiųjų charakteristikos nėra universalios, jos gali skirtis priklausomai nuo nusikaltimo tipo, naudojamų įrankių, globalių ir lokalių sąlygų nusikaltimui padaryti.

Tad šiame straipsnyje pristatoma elektroninių nusikaltimų socialinių tyrimų temų schema, atspindinti mikrolygmens ir makrolygmens temų aprėptį ir įvairovę užsienio autorių tyrimuose. Schema atskleidžia, kad siekiant suprasti elektroninius nusikaltimus kaip technosocialinį reiškinį yra svarbūs ne tik atskirų nusikaltimų tipų, pažeidėjų ir nukentėjusiųjų tyrimai, bet ir su elektroniniais nusikaltimais siejami technologiniai diskursai, masinėse medi-

jose publikuojami elektroninių nusikaltimų naratyvai, tarpkultūriniai ir transnacionaliniai šių nusikaltimų vyksmo ir poveikio skirtumai.

Remiantis sudaryta temų schema, buvo atlikta sisteminė publikacijų apžvalga apie Lietuvoje įgyvendintus socialinių mokslų, išskyrus teisę, tyrimus, patenkančius į elektroninių nusikaltimų tematinį lauką. Rezultatai leidžia įvertinti, kokios globaliai aktualizuojamos temos yra tiriamos ir Lietuvoje, o kurios priklauso dar netirtai, mokslininkų dėmesio ir įdirbio reikalaujančiai sričiai.

Interneto technologijų raidos įtaka socialiniams tyrimams apie elektroninius nusikaltimus

Vienoje išsamiausių elektroninių nusikaltimų socialinių tyrimų lauko apžvalgų Stratton'as, Powell ir Cameron'as dalija elektroninių nusikaltimų mokslinių tyrimų istoriją į tris laikotarpius (2017, p. 19):

1. **1980–1990 m. laikotarpis iki globalaus interneto paplitimo.** Dalyje pasaulio valstybių augo darbo vietų kompiuterizavimas, taigi ir galimybė pasiekti jas per išorinius komunikacijos tinklus. Pagrindinės tyrimų temos, dažniausiai nagrinėjamos kaip baltųjų apykaklių nusikaltimai, tuo metu buvo: kompiuteriniai ekonominiai nusikaltimai, konfidencialios informacijos atskleidimas, nelegalus programinės įrangos platinimas, informacijos saugumas ir privatumas, pirmieji elektroninių nusikaltimų teisinio reglamentavimo bandymai (Stratton, Powell, Cameron 2017, p. 19). Šiuose tyrimuose elektroniniai nusikaltimai buvo tiriami kaip išskirtiniai įvykiai. Atlikti kiekybiniai tyrimai atskleidė elektroninių nusikaltimų skaičiaus augimą, atspindėjo mokslininkų reakcijas į pirmus šios srities teisinio reguliavimo bandymus ir poreikį geriau suprasti tuo metu dar nišiniu laikomą reiškinį. Taigi radosi susidomėjimas skirtingais naujaisiais elektroninių nusikaltimų tipais ir juos darančiais naujaisiais nusikaltėliais bei jų motyvais.

2. **1990–2000 m. globaliojo interneto ir namų ūkių įsitinklinimo laikotarpis.** Mokslininkai įtvirtino skirtį tarp kompiuterinių sistemų *kaip nusikaltimo taikinio* (angl. *computer-focused crime*) ir kompiuterinių sistemų *kaip nusikaltimo įrankio* (angl. *computer-assisted crime*), internetas tapo komunikacijos platforma nusikaltimų organizavimui ir rinkoms. Pagrindines tyrimų temas papildė į žmones nukreiptų nusikaltimų formos: finansinis sukčiavimas, duomenų vagystės, informacijos privatumo pažeidimai, tapatybės pasisavinimas,

vaikų seksualinis išnaudojimas internete, taip pat įprastų valdysenos ir galios taikymo principų negaliojimas internete (Stratton, Powell, Cameron 2017, p. 19–20). Šiam laikotarpiui būdinga auganti nusikaltimų tyrimų įvairovė: anksčiau buvę unikalia veiklos sfera, reikalaujančia gilių technologinių žinių, vis daugiau elektroninių nusikaltimų ėmė sudaryti tradiciniai nusikaltimai, padaromi internete. Kartu mažėjo atvejų, kai elektroniniai nusikaltimai buvo nusikaltimais be aukų (angl. *victimless crime*) ir daugėjo tiesiogiai paveiktų individų ir organizacijų, pavyzdžiui, įmonių, kurių verslas patyrė nuostolių, augo teisėsaugos ir teisėkūros institucijų įsitraukimas į elektroninių nusikaltimų reglamentavimą ir kontrolę, elektroniniai nusikaltimai tapo populiariosios kultūros dalimi. Socialinių tyrimų tematikos plėtėsi ir dažniau skyrė dėmesį ne tik nusikaltimams bei pažeidėjams, bet ir kitiems šio proceso dalyviams – nukentėjusiesiems ir teisėsaugai.

3. **Nuo 2000 m. socialinės tinklaveikos internetas (angl. *the social web*)**. Visuomenėse, kuriose išplito socialinės tinklaveikos paslaugos ir internetinės masinės medijos, į internetą persikėlė didesnė dalis komunikavimo praktikų, taigi ir jų sąlygojamų asmeninių ir socialinių konfliktų. Augo giliojo interneto (angl. *deep web*), nepasiekiamo per standartines paieškos svetaines, apimtys, daugėjo ir įvairėjo išmaniųjų telefonų, mobiliojo interneto, nešiojamųjų įrenginių, vystėsi didžiųjų duomenų verslai. Tyrėjai aiškinosi, kaip naujomis komunikacijos priemonėmis skleidžiama informacija gali būti naudojama nusikaltimams daryti, taip pat skyrė dėmesio teisėsaugos institucijų veiklos analizei, matematiniam elgesio modeliavimui (Stratton, Powell, Cameron 2017, p. 21).

Masinio vartojimo rinkoje ir toliau įsitvirtinant naujoms ir naujai vystomoms technologijoms, jos integruojamos į egzistuojančius skaitmeninės komunikacijos tinklus ir kasdienio gyvenimo socialines praktikas. Apžvalgų autoriai akcentuoja poreikį daugiau tyrėjų dėmesio skirti socialinės tinklaveikos priemonių, didžiųjų duomenų ir daiktų interneto kriminologinei analizei (Stratton, Powell, Cameron 2017, p. 18). Išnykus griežtai perskyrai tarp fizinės erdvės ir interneto, informacijos ir komunikacijos technologijoms įsitvirtinus kasdieniame gyvenime tarp daugelio socialinių grupių visame pasaulyje, kilo poreikis nuodugniai suprasti politinį, socialinį, ekonominį elektroninių nusikaltimų poveikį, jų globalumo ir lokalumo dermes.

Pateikta chronologija reikšminga (ir dėl to detaliau pristatyta) dėl dviejų priežasčių. Pirma, ji leidžia susieti informacijos ir komunikacijos technologijų

raidą su mokslinių tyrimų temomis ir apimtimi. Nuo nusikaltimų apibrėžimo ir individualių veikėjų supratimo tyrimų temos plečiasi ir juda prie kompleksinių socialinių procesų analizės. Antra, minėtos datos neuniversalios. Jos taikomos toms pasaulio valstybėms (pavyzdžiui, JAV, Vokietijai, Didžiajai Britanijai), kuriose anksčiau prasidėjo kompiuterinių technologijų taikymas ir masinis vartojimas. Pritaikant šią chronologiją Lietuvai, pirmasis etapas prasidėjo 10 metų vėliau – 1990–2000 m., atsiradus pirmiesiems interneto ryšio kanalams; antrasis datuojamas 2000–2010 m., kai namų ūkių, turinčių kompiuterį ir prieigą prie interneto, skaičius išaugo nuo 5,3 % 2000 m. iki 57,8 % 2010 m.[1]; trečiasis – nuo 2010 m., nes aktyvaus dalyvavimo socialinėje tinklaveikoje prielaida yra masinis interneto prieigos įsitvirtinimas. Nepaisant vėlesnės pradžios, dabartinė Lietuva yra perėjusi visus tris laikotarpius. O tai reiškia, kad yra tokios pačios sąlygos kaip ir kitose valstybėse vykdyti tyrimus apie elektroninius nusikaltimus aprėpiant tiek mikro-, tiek makrolygmens problemas.

Pastaruoju metu elektroniniai nusikaltimai pozicionuojami bendresniame kontekste ne kaip atskira, išskirtinė nusikaltimų rūšis, o kaip viena iš globalios ir transnacionalinės kriminologijos interesų sričių (Lee 2018, p. 223). Ji nagrinėjama šalia kitų šiuolaikinių problemų, kurios peržengia atskirų valstybių jurisdikcijas ir pasižymi naujais pažeidėjų veikimo būdais – organizuotos nusikalstamos grupės, aplinkosauginiai nusikaltimai, transnacionaliniai nusikaltimai. Kai kurie autoriai pabrėžia, kad būtent technologinius pokyčius nagrinėjantys mokslininkai turi galimybę svariai prisidėti prie teorinių ir metodinių pokyčių socialinių mokslų tyrimuose apie nusikaltimus (Stratton, Powell, Cameron 2017, p. 18). Elektroninių nusikaltimų nagrinėjimas globaliame kontekste turi potencialo atskleisti ne tik nusikaltimų tipus, pažeidėjų, aukų ir teisėsaugos veikimo būdus, bet ir apibrėžti platesnes socialines, politines, ekonomines problemas, pavyzdžiui, lokalūs ir globalūs skaitmeniniai sklastai (angl. *digital divides*), globalios Šiaurės ir globalių Pietų galios santykiai, transnacionalinis socialinių institutų veikimas ir jų tarpkultūriniai skirtumai.

[1] Lietuvos statistikos departamentas. Oficialiosios statistikos portalas. „Namų ūkiai, turintys asmeninį kompiuterį, interneto prieigą 2000–2020“. Vilnius: Lietuvos statistikos departamentas. Prieiga per internetą: https://osp.stat.gov.lt/statistiniu-rodikliu-analize [žiūrėta 2021 m. kovo 21 d.].

Elektroninių nusikaltimų tyrimai pagal nusikaltimo tipą

Elektroniniai nusikaltimai paprastai skirstomi į dvi pagrindines sritis (žr. Wall 2001; Wall 2017, p. 8; Maimon, Louderback 2019, p. 192; Stratton, Powell, Cameron 2017, p. 20). Pirma kategorija – technologijos kaip nusikaltimo taikinys, kai neegzistuojant konkrečiai technologijai toks nusikaltimas būtų neįmanomas. Antra – kai technologijos yra nusikaltimo įrankis, kuris panaudojamas įprastiems nusikaltimams daryti. Toliau pateikiamas šių sričių išskirstymas į konkrečius nusikaltimus ir pažeidimus kartu su naujausių tyrimų arba sisteminių literatūros apžvalgų pavyzdžiais.

1) Nusikaltimai, kuriuose technologijos yra nusikaltimo taikinys:
   - neautorizuota prieiga ir neteisėti veiksmai su informacinėmis sistemomis (Wang ir kiti 2019; Khan ir kiti 2020; Lallie ir kiti 2020);
   - sistemų veiklos trikdymai (Leverett ir Kaplan 2017; Abhishta 2019; Abhishta ir kiti 2020; Holt, Leukfeldt ir de Weijer 2020; Holt ir kiti 2020);
   - infrastruktūros pažeidimai (Argaw ir kiti 2019; Alladi, Chamola ir Zeadally 2020; Blythe ir Johnson 2021).
2) Nusikaltimai, kuriuose technologijos yra nusikaltimo įrankis – daromi pasitelkus kompiuterius ir internetą:
   - finansiniai nusikaltimai (Tcherni ir kiti 2016; Jose ir kiti 2017; Levi 2017; Lee ir Choi 2021);
   - sukčiavimai, nelegali prekyba (Leukfeldt, Kleemans ir Stol 2017; Broadhurst ir kiti 2018; Wu ir kiti 2020; Cross ir Layt 2021; Ghazi-Tehrani ir Pontell 2021);
   - intelektinės nuosavybės teisių pažeidimai (Chavarria ir kiti 2016; Fleming ir kiti 2017; Hou ir Wang 2020; Tyrowicz, Krawczyk ir Hardy 2020);
   - viešosios informacijos sklaidos įstatymų pažeidimai (Choi, Lee ir Cadigan 2018; Westerlund 2019);
   - draudžiamos pornografijos vartojimas (Popović 2018; Steele ir kiti 2020; Kusz ir Bouchard 2020);
   - nepageidaujamos reklamos platinimas (Kaur, Singh, Kumar 2018; Ferrara 2018; Perkins ir kiti 2020);

- persekiojimas (Clevenger, Navarro ir Gilliam 2018; Messing ir kiti 2020);
- seksualiniai nusikaltimai (Walker ir Sleath 2017; Broome, Izura ir Lorenzo-Dus 2018; Madigan ir kiti 2018; Koops, Dekker ir Briken 2018; Maas ir kiti 2019);
- patyčios (Jenaro ir kiti 2018; Chun ir kiti 2020);
- neapykantos sklaida (Bliuc ir kiti 2018);
- tapatybės pasisavinimas (Gies ir kiti 2020; Lee 2020);
- asmens duomenų apsaugos pažeidimai (Hutchings ir Holt 2017; Hall ir Wright 2018);
- grėsmės fiziniam saugumui sukėlimas (Heartfield ir kiti 2018).

Šios ir daugybė kitų studijų pateikia įvairius konkrečių elektroninių nusikaltimų formų pjūvius – jų apibrėžimus ir panašumą į kitus nusikaltimų tipus, klasifikacijos schemas, struktūrą ir vyksmą, skirtumus nuo netechnologinių tų pačių nusikaltimų versijų. Svarbi analizės kryptis – nustatymas, ką naujo konkrečiam nusikaltimui reiškia naujųjų technologijų taikymas, kokie išlieka seni bruožai ir atsiranda naujų, kas yra arba nėra unikalu būtent elektroninėms nusikaltimų versijoms. Kitų tyrimų autoriai aiškinasi atskirų nusikaltimų tipų įvairovę, paplitimą, socialinį, ekonominį ir kultūrinį poveikį bei intervencijos arba prevencijos galimybes.

Įvairių elektroninių nusikaltimų tipų tyrimai leidžia išryškinti ir jų vyksmo, struktūros, įrankių pasikeitimus bėgant laikui, kurie savo ruožtu parodo, kaip lėtai, bet nuolat keičiasi visa elektroninių nusikaltimų struktūra. Įrankiai, įgalinantys padaryti elektroninį nusikaltimą, tampa vis lengviau prieinami ir paprastesni. Internetiniai nusikaltimai tampa nebe aukštos kvalifikacijos ir patirties reikalaujančiu užsiėmimu, o rinkoje parduodama paslauga (angl. *cybercrime–as–service*). Kai technologijos yra nusikaltimo taikinys, šio proceso pavyzdys – lengvai modifikuojamos ir valdomos kenkėjiškos programos, išnuomojami nuotolinės prieigos trikdymo tinklai, nutekinamos slaptažodžių duomenų bazės. Kai technologijos yra nusikaltimo įrankis, šio proceso pavyzdys – nelegaliose rinkose santykinai pigiai parduodamos kreditinių kortelių duomenų bazės, asmens tapatybės duomenys, galimybės automatiniu būdu masiškai siųsti pranešimus į elektroninius paštus ir socialinės tinklaveikos priemones, turint tikslą skleisti neapykantos arba nepageidaujamos rinkodaros žinutes.

Tad „internetas gana ciniškai <...> demokratizavo tokius nusikaltimus kaip sukčiavimas, anksčiau laikomus galingų ir privilegijuotų grupių nusikaltimais“ (Wall 2017, p. 5). Kita vertus, patys įrankiai tampa vis sudėtingesni – apimantys daugiau funkcijų, sunkiau aptinkami, automatizuoti, jie jungiami į stambias sistemas, o tai reiškia, kad juos programuojantys ir palaikantys individai, kurie tarpusavyje konkuruoja, turi veikti vis profesionaliau (Wall 2015, p. 73), o „pasibaigus elektroninių chuliganų laikams, pažeidėjai nebenori būti žinomi ar siekti pripažinimo kaip kadaise“ (Wall 2017, p. 6).

Elektroninių nusikaltimų tyrimo patirtis yra svarbus pagrindas teoretizuoti ir potencialiai pritaikyti žinias kitose srityse, kur naujųjų technologijų atsiradimas sąlygoja ir naujų nusikaltimų formų atsiradimą, pavyzdžiui, išmaniųjų miestų arba biotechnologijų.

Elektroninių nusikaltimų tyrimai pagal proceso dalyvius

Individai, susiduriantys su elektroniniais nusikaltimais, paprastai suskaidomi pagal klasikinę kriminologinę schemą: pažeidėjai, nukentėjusieji ir teisėsauga (arba privatūs informacinio saugumo paslaugų teikėjai) (Maimon, Louderback 2019, p. 193). Elektroninių nusikaltimų socialiniuose tyrimuose mokslininkai susitelkia į vieną arba daugiau iš šių grupių, kartais susiaurina tyrimo objektą iki grupių, susijusių su konkrečiu nusikaltimo tipu.

1. *Pažeidėjų* tyrimuose daugiausia dėmesio skiriama „nusikaltėlių motyvacijai, dažnai pasitelkiant individualizuotas „racionalaus pažeidėjo“ teorijas, kurios technologijas traktuoja kaip paprastą įrankį daryti pažįstamus nusikaltimus“ (Stratton, Powell, Cameron 2017, p. 18). Pažeidėjų motyvų modeliavimas dažnai remiasi studentų arba organizacijų darbuotojų kiekybiniais tyrimais (Maimon, Louderback 2019, p. 195), taigi labai specifinėmis ir nereprezentatyviomis potencialius pažeidėjus turinčiomis grupėmis. Tokiu būdu tiriami ne pažeidėjai kaip socialinė grupė, o kitos socialinės grupės, ieškant jose išskirtinių atvejų – realių arba potencialių pažeidėjų. Tai sukelia abejonių apibendrinimo pagrįstumu, tokių tyrimų rezultatų pritaikomumo ribomis. Be to, besikeičiančiame elektroninių nusikaltimų lauke veiksniai ir modeliai, kurie tinkamai aiškino pažeidėjų motyvaciją prieš 20 metų, šiuo metu gali būti nebeaktualūs.

Autoriai, kurie nagrinėja elektroninių nusikaltimų pažeidėjus kaip heterogenišką, o ne homogenišką grupę, pabrėžia jų įvairovę ir išskaido juos į kategorijas (Broadhead 2018, p. 1183): a) individai ir mažos grupės, paprastai oportunistai arba profesionalai, o dažniausias jų veiklos motyvas – finansinis pelnas; b) organizacijų darbuotojai ir kiti veikėjai, iš vidaus prieinantys prie kompiuterinių sistemų arba duomenų, galintys veikti tikslingai (dalis tokių nusikaltimų – baltųjų apykaklių nusikaltimai), atmestinai arba per klaidą; c) organizuotos nusikalstamos grupuotės – tradicinės, diversifikuojančios savo veiklą, arba specializuotos, darančios tik elektroninius nusikaltimus; d) valstybės ir su valstybėmis susiję veikėjai, žvalgybos, nacionalinio saugumo institucijos, valstybių samdomi profesionalai, kurie elektroninę komunikaciją naudoja kaip geopolitinių interesų užtikrinimo priemonę; e) politiškai motyvuoti, finansinio pelno nesiekiantys haktyvistai; f) internete veikiančios teroristinės grupės, galinčios siekti įbauginimo, taikytis į kritinę infrastruktūrą; g) jauni, paprastai mažai techninių žinių turintys individai (angl. *script kiddies*), eksperimentuojantys su lengvai prieinamais elektroninių nusikaltimų įrankiais.

Būtent skirtingų pažeidėjų tipų išskyrimas leidžia suprasti „ne tik grėsmių sukėlėjų tapatybes ir sąsajas su grupėmis ar institucijomis, jeigu jie tokių turi, bet ir jų galimybes bei, kiek tai įmanoma, motyvaciją“ (Broadhead 2018, p. 1184). Afiliacijos klausimas susijęs su kita dažnai tyrimuose iškeliama problema – elektroninių nusikaltimų veiklos organizavimo modeliais. Skirtingi autoriai pabrėžia, kad šie modeliai remiasi tinkliniais veiklos principais ir decentralizacija, darbo pasidalijimu, derinant įgūdžius ir galimybes, automatizacija (Maimon, Louderback 2019, p. 194–195). Asmenines elektroninių pažeidėjų charakteristikas, jų formuojamus tinklus atspindi besikeičiantis elektroninių nusikaltimo įrankių pobūdis, „kriminalinis įdirbis <...> dėl tinklo ir skaitmeninių technologijų sparčiai tampa nebereikalaujantis aukštos kvalifikacijos ir tuo pat metu reikalauja vis aukštesnės kvalifikacijos“ (Wall 2017, p. 4). Taip įvedama skirtis tarp elektroninių nusikaltimo įrankių kūrėjų bei vartotojų, kurie tais įrankiais pasinaudodami padaro nusikaltimus. Pažeidėjų afiliacija ir technologijų kaita – labai svarbūs aspektai tiriant ne tik pažeidėjų motyvus, bet ir *modus operandi*, socialines sąveikas tarp skirtingo tipo pažeidėjų ir jiems pasiekiamas galimybes nusikalsti.

Mokslinio nesutarimo objektas – pažeidėjų ryšys su organizuotomis nusikalstamomis grupėmis. Vieni autoriai teigia, kad sąsajų yra mažai. Jiems

trūksta įrodymų, kad tradicinės organizuotos nusikalstamos grupės perkelia savo veiklą į elektroninę sferą (Wall 2017, p. 17; Lavorgna 2015), išskyrus kai kuriuos elektroninių nusikaltimų tipus (Broadhead 2018, p. 1182). Jie mano, kad elektroninių nusikaltimų atlikėjai priklauso kitoms socioekonominėms grupėms nei organizuotų nusikalstamų grupių atstovai, o elektroninių nusikaltimų organizavimo būdai per daug skiriasi nuo hierarchija ir autoritetu paremtų kriminalinių grupių organizacinės struktūros (Wall 2015, p. 72). Kiti autoriai argumentuoja, kad kai kurios organizuotos nusikalstamos grupės veikiant globalizacijai keičiasi į tinklines struktūras (arba iš pat pradžių tokiomis remiasi), primenančias būtent tuos modelius, kuriais paremta ir internetinių grupių veikla (Nguyen ir Luong 2020). Tuo tarpu tradicinės nusikalstamos grupės diversifikuoja savo veiklą ir įtraukia elektroninius nusikaltimus šalia kitų savo veiklų (Broadhead 2018, p. 1183). Tokiu atveju diskusijos apie elektroninių nusikaltimų sąsajas su organizuotomis nusikalstamomis grupėmis referuoja į bendresnę problemą – nusikaltimų kaitą globalizacijos sąlygomis: lokalių ir globalių praktikų derinimą nusikalstamų grupių veikloje, socialinės kontrolės ir teisinio reguliavimo veikimą globalioje tinklaveikoje.

Ateityje gali tapti aktualios nežmogiškųjų veikėjų ir sprendimo priėmimo sistemų keliamos grėsmės (Broadhead 2018, p. 1183), pavyzdžiui, pažeidimai, kuriuos padaro mašininio mokymosi algoritmai, apmokyti nuo pradžių iki galo padaryti nusikaltimą. Pastarasis pavyzdys – atvejis, reikalaujantis visai kitokios teorinės prieigos, negu racionalaus pasirinkimo teorija – čia išryškėja veiksniatinklio teorijos potencialūs privalumai.

2. *Nukentėjusieji nuo elektroninių nusikaltimų*, palyginus su pažeidėjais, tyrėjams yra lengviau prieinama tiriamųjų grupė, todėl ir jų tyrimai labiau pažengę nei pažeidėjų tyrimai (Holtfreter, Meyers 2015, p. 58). Tačiau šie tyrimai turi savo konceptualių problemų. Tam, kad nukentėjusieji suvoktų savo viktimizacinę patirtį ir ja dalintųsi, jie turi visų pirma suprasti, kad tapo nusikaltimo auka (Holtfreter, Meyers 2015, p. 57–58).

Būtent todėl yra dvi atskiros elektroninių nusikaltimų nukentėjusiųjų tyrimų kryptys. Viena – tai reprezentatyvios kiekybinės apklausos: klausimai apie elektroninius nusikaltimus įtraukiami į stambesnes viktimologines apklausas tose valstybėse, kur tokios apklausos atliekamos reguliariai. Taip pat gali būti atliekamos specifinės viktimologinės apklausos tik apie elektroninius nusikaltimus, į jas įtraukiama daugiau klausimų apie tyrimo dalyvių elgesį in-

ternete (žr. Jones, Mitchell, Finkelhor 2012; Junger, Montoya, Hartel, Heydari 2017; Näsi, Oksanen, Keipi, Räsänen 2015; viktimologines apklausas apie elektroninius nusikaltimus apžvelgia Reep-van den Bergh, Junger 2018; rutininių veiksmų teorija paremtus viktimologinius tyrimus apžvelgia Reyns 2015, p. 399–400; Arntfield 2015). Šiais tyrimais mokslininkai siekia išsiaiškinti, kiek žmonių patiria elektroninius nusikaltimus, tikėdamiesi, kad apklausų dalyviai praneš ir apie tuos atvejus, kai susidūrė su nusikaltimais, tačiau jų nepranešė teisėsaugos institucijoms. Tačiau šis rodiklis parodo ne realius susidūrimus su elektroniniais nusikaltimais ir pažeidimais, o atvejus, kuomet apklausų dalyviai suprato susidūrę su elektroniniais nusikaltimais. Neužfiksuota lieka ta dalis atvejų, kai nukentėjusieji taip ir nesužinojo, kad tapo aukomis.

Viktimologinių apklausų duomenys naudojami, ieškant veiksnių, kurie padidina tikimybę tapti elektroninio nusikaltimo auka: sociodemografinių charakteristikų, vartotojų veiklos internete, koreliacijų tarp aukų susidūrimų su skirtingų tipų nusikaltimais internete ir už jo ribų, tačiau rezultatai kol kas prieštaringi (žr. Maimon, Louderback 2019, p. 199–200). Kai kurie tyrimai tarp kitų rezultatų parodo ir tai, kad aukų ir pažeidėjų grupės ne visada idealiai atskirtos (Maimon, Louderback 2019, p. 200): deviantinis elgesys internete yra vienas iš veiksnių, kuris didina tikimybę tapti auka (pavyzdžiui, siųsdamiesi nelegalų turinį, vartotojai netyčia pasileidžia savo kompiuteriuose kenkėjiškų programų). Kartais viktimologinių apklausų analizėse tyrėjai susitelkia į konkretaus nusikaltimo tipo veiksnius, pavyzdžiui, sukčiavimo užmezgant romantinius santykius (Whitty 2018) arba elektronines patyčias tarp moksleivių (Holt, Fitzgerald, Bossler, Chee, Ng 2016).

Antra viktimologinių tyrimų kryptis susitelkia į asmenines viktimologines patirtis, nukentėjusiųjų poreikius. Išsamesnių studijų apie aukų perspektyvą, prisitaikymo ir išgyvenimo strategijas, elgesio pasikeitimus šiuo metu dar trūksta (Jansen, Leukfeld 2018, p. 206). Pasitelkę kokybinę metodologiją, mokslininkai tiria finansines, psichologines, emocines elektroninių nusikaltimų pasekmes, antrinę viktimizaciją – neigiamą nukentėjusiųjų patirtį po kreipimosi į teisėsaugos institucijas (žr. Jansen, Leukfeld 2018; Cross 2018a; Cross, Richards, Smith 2016).

Kokybiniai tyrimai atskleidžia, kad nukentėjusiųjų patirtis gali būti labai įvairi (Jansen, Leukfeld 2018, p. 223–224), taip pat ir tais atvejais, kai jie nukenčia nuo to paties tipo nusikaltimo, pavyzdžiui, sukčiavimo (Cross 2019;

Cross, Richards, Smith 2016). Todėl reikia daugiau studijų, kurios aprašytų ne tik aukų charakteristikas, bet ir jų patirtis (Jansen, Leukfeld 2018, p. 206). Aptartas temas papildo studijos, kurios traktuoja elektroninių nusikaltimų poveikį ne kaip individualią vienos aukos problemą, nes nukenčia ne (tik) konkretus individas, bet visas tinklas žmogiškųjų ir techninių veikėjų (Wagen, Pieters 2020) – taigi traktuoja viktimologinę patirtį kaip kolektyvinę. Viena iš kolektyvinių viktimologinių patirčių – nuo elektroninių nusikaltimų nukentėjusios organizacijos, tačiau kol kas būtent viktimologinę perspektyvą taikančių tyrimų apie organizacijas taip pat trūksta (Holtfreter, Meyers 2015, p. 58).

Viktimologiniai tyrimai gali suteikti informacijos ne tik apie nukentėjusiuosius, bet ir apie teisėsaugos institucijų veiklą. Atskira viktimologinių tyrimų potemė, tiriama ir kiekybiniais, ir kokybiniais metodais, – nukentėjusiųjų motyvacija pranešti apie elektroninius nusikaltimus (Cross 2018b; Weijer, Leukfeldt, Bernasco 2019), jų patirtys bendraujant su teisėsauga (Cross 2019, 2018a) ir kitomis atsakingomis valstybės institucijomis arba pagalbą teikiančiomis organizacijomis, paprastai iš nevyriausybinio sektoriaus. Be tiesioginės aukų patirties, šios studijos gali atskleisti nukentėjusiųjų ir teisėsaugos institucijų santykį: tarpusavio pasitikėjimą arba nepasitikėjimą, institucijų kompetencijas reaguoti į elektroninius nusikaltimus. Galiausiai pačios informacijos ir komunikacijos technologijos tampa įrankiu, įgalinančiu naujas nukentėjusiųjų praktikas: savipagalbos bendruomenes internete, aukų aktyvizmo ir skaitmeninės savisaugos (angl. *digilantism*) grupes, neformalaus teisingumo vykdymo praktikas (žr. Chang 2018s), kurios taip pat yra prieštaringa ir praktiškai netirta tema (Stratton, Powell, Cameron 2017, p. 25–26).

3. Į *teisėsaugą bei elektroninio saugumo industriją* nukreipti elektroninių nusikaltimų tyrimai dažnai skirti skaitmeninei kriminalistikai (angl. *digital forensics*) ir elektroninių nusikaltimų prevencijai. Tyrimai, teikiantys pirmenybę socialinei dimensijai, koncentruojasi į individualias ir organizacines praktikas, kurios gali paaiškinti, kaip teisėsaugos, baudžiamojo teisingumo sistemos atstovai, privatūs elektroninio saugumo paslaugų teikėjai reaguoja į elektroninius nusikaltimus.

Rutininių veiksmų teorijos atstovai, taikydami apklausas, tiria teisėsaugos atstovų požiūrį į elektroninių nusikaltimų tyrimą, asmenines ir organizacines kompetencijas, žmogiškųjų ir finansinių resursų skyrimą reakcijai į elektroninius nusikaltimus, alternatyviai policijos veiklai internete (pavyzdžiui, interne-

tinių bendruomenių socialinei kontrolei), tarptautiniam bendradarbiavimui tarp skirtingų valstybių teisėsaugos institucijų, siekiant išsiaiškinti tarptautinius nusikaltimus internete (tokias studijas apžvelgia Maimon, Louderback 2019, p. 202–203; Holt 2018; taip pat žr. Holt, Burruss, Bossler 2018). Minėtus tyrimus papildo kokybinės studijos, nagrinėjančios tuos pačius klausimus (žr. Nouh, Nurse, Webb, Goldsmith 2019; Powell, Henry 2018; Hadlington, Lumsden, Black, Ferra 2018; Black, Lumsden, Hadlington 2019).

Elektroninių nusikaltimų diskursai

Politinį ir socialinį elektroninių nusikaltimų kontekstą atskleidžia elektroninių nusikaltimų percepcijos ir diskursai, kurie formuojasi masinėse medijose ir viešojoje vaizduotėje. Elektroninių nusikaltimų diskursai yra socialiai konstruojami sankirtoje tarp kriminologinių ir technologinių diskursų. Kriminologinių diskursų dėmuo apima elektroninių nusikaltimų vietą tarp kitų masinėse medijose vaizduojamų nusikaltimų, jų pateikimo būdus, moralinės panikos, moralinės antreprenerystės, žalos vertinimo, nusikaltimų suvokimo ir nusikaltimų baimės formavimo procesus. Technologiniai diskursai atspindi, kaip visuomenėje ir politinių sprendimų priėmimo darbotvarkėje pateikiamos informacijos ir komunikacijos technologijos: kaip grėsmė ir rizikos šaltinis ar kaip universali problemų sprendimo priemonė[2]. Kriminologinis ir technologinis elektroninių nusikaltimų diskursų dėmuo lemia argumentus, priimant politinius sprendimus, nustatant prioritetus valstybės institucijose, formuojant formalią ir neformalią socialinę kontrolę, skirtą elektroniniams nusikaltimams.

Elektroninių nusikaltimų tikrovės, pateikimo masinėse medijose ir viešųjų sprendimų priėmimo tyrimai atskleidžia esminę prieštarą: elektroninių nusikaltimų baimės yra daug, o realių viktimizacijos patirčių mažai (Wall 2017, p. 15). Viešojoje erdvėje ir politinėje retorikoje elektroniniai nusikaltimai dažnai pateikiami kaip didelė grėsmė visuomenei, tačiau jie labai silpnai atsispindi registruojamų nusikaltimų statistikoje, jų socialinė kontrolė dažnai iš teisėsau-

[2] Šie du kraštutiniai požiūriai atspindi dominuojančias technologinio pesimizmo arba technologinio optimizmo nuostatas. Detalią filosofinių nuostatų apie technologijas apžvalgą pateikia Kerschner ir Ehlers (2016). Filosofijos vaidmenį, formuojant technologines praktikas, nagrinėja Brey (2016).

gos lauko perduodama kitoms valstybės institucijoms ir nevalstybiniam sektoriui, taip tarsi išskiriant reakciją į elektroninius nusikaltimus nuo kitų nusikaltimų (Wall 2017, p. 16). Elektroninių nusikaltimų recepciją visuomenėje mokslininkai tyrinėja atlikdami apklausas (Dimc, Dobovšek 2010; Mesko, Bernik 2011; Kamruzzaman ir kiti 2016), kokybinius interviu bei diskusijų grupes (Conway, Hadlington 2018; Ghazali, Gnai 2018).

Wall'as pabrėžia, kad vien techninių žinių nepakanka adekvačiai reakcijai ir sprendimų priėmimui, o elektroninių nusikaltimų baimė tampa rinkodaros priemone elektroninio saugumo pramonės produktams (Wall 2017, p. 2). Tai reiškia, kad elektroninių nusikaltimų politikos formavimas reikalauja pagrįstos prieigos, viena vertus, suprantančios viešąją nuomonę, vertybines nuostatas ir jų kilmę, antra vertus, gebančios vertinti jas kritiškai ir formuluoti adekvačias reakcijos priemones. Priešingu atveju, socialinė kontrolė ir teisėsaugos veikla, nukreipta į elektroninius nusikaltimus, tampa reakcija į moralinę paniką bei mokslinę fantastiką, o ne teisingumo užtikrinimu (Wall 2017, p. 15). Šiai temai atskleisti tyrėjai atlieka kiekybinius nusikaltimų baimės ir su ja koreliuojančių kintamųjų vertinimus (Brands, Wilsem 2019; Virtanen 2017), nagrinėja elektroninių nusikaltimų konstravimą politinėje retorikoje (Hill, Marion 2016).

Susiformavę viktimologiniai elektroninių nusikaltimų diskursai taip skatinti arba švelninti antrinės viktimizacijos patyrimus, suvoktą atsakomybės, kaltės ir žalos paskirstymą tarp pažeidėjų, nukentėjusiųjų ir teisėsaugos. Todėl yra aktualūs tyrimai apie elektroninių nusikaltimų pateikimą naujienose (pavyzdžiui, Lavorgna 2018; 3–7 p. autorė pateikia išsamią, kritišką kitų šios srities tyrimų apžvalgą), šių naujienų recepciją tarp skirtingų valstybių masinių medijų auditorijų (Levi 2008), elektroninių nusikaltimų vaizdavimą ir mitologizavimą pramogų industrijoje (Wall 2008a) bei viešųjų sprendimų priėmimo procese (Wall 2008b), apie medijų poveikį, vertinant riziką tapti elektroninio nusikaltimo auka (Wei, Liu, Liu 2019), skaitmeninių algoritmų indėlį į nusikaltimų amplifikaciją – perdėtą sureikšminimą socialinės tinklaveikos priemonėse (Wood 2016), nukentėjusiųjų grupių pateikimo masinėse medijose specifiką (Cross, Parker ir Sansom 2019).

Viešas elektroninių nusikaltimų supratimas ir vertinimas apibrėžia lūkesčius, kuriuos individai ir organizacijos turi valstybei. Valstybė gali formuoti tam tikrą elektroninių nusikaltimų socialinės kontrolės kultūrą ir įsijungti į elektroninių nusikaltimų diskurso formavimą šalia masinių medijų, prisidėti

prie technologinės edukacijos ir bendro visuomenės sutarimo dėl technologinio saugumo poreikių.

Globalios ir lokalios elektroninių nusikaltimų dimensijos

Elektroninių nusikaltimų paplitimui, jų pobūdžiui, proceso dalyvių tarpusavio sąveikoms daro įtaką globalioji tinklaveika – informacijos ir komunikacijos technologijos, kurios sujungia arba atskiria skirtingame laike ir skirtinguose pasaulio taškuose esančius tinklaveikos dalyvius.

Vieni autoriai teigia, kad būtent globalus komunikacijos tinklų paplitimas lemia unikalias elektroninių nusikaltimų savybes, mastą, pasiekiamumą, greitį (pavyzdžiui, Wall 2017, p. 4), matydami internetą kaip *jungiantį* tinklą. Kiti autoriai, priešingai, telkia dėmesį į socialinės *nelygybės bei atskirties* formas, būdingas tinklaveikos technologijoms (Stratton, Powell, Cameron 2017, p. 26), kurios išlaiko ir atkartoja kasdienio gyvenimo socialines struktūras.

Makrolygmens elektroninių nusikaltimų analizė yra iš principo problemiška. Tarptautinės organizacijos, atsakingos už telekomunikaciją, renka palyginamus duomenis skirtingose pasaulio valstybėse, pavyzdžiui, Tarptautinės telekomunikacijos sąjungos Globalus elektroninio saugumo indeksas (ITU 2018), tačiau tokių atvejų yra mažai. Skirtingose valstybėse ir regionuose renkamus kiekybinius duomenis yra sudėtinga lyginti tarpusavyje ir pateikti pagrįstus apibendrinimus apie padėtį regione ar visame pasaulyje.

Pozityvistinę paradigmą pasirinkę tyrėjai remiasi pavienių valstybių lygmens duomenimis, kartu siekdami kurti universalias elektroninių nusikaltimų teorijas taip, tarsi elektroniniai nusikaltimai kaip globalus reiškinys vienodai veiktų skirtinguose socialiniuose, politiniuose ir kultūriniuose kontekstuose visame pasaulyje. Tačiau, vertinant elektroninių nusikaltimų poveikį, būtina atsižvelgti į socialinį kontekstą, kaip pabrėžia kritinei kultūrinei paradigmai atstovaujantys autoriai (pavyzdžiui, Diamond, Bachmann 2015, p. 30). Kartu kiekybiniai tyrimai gali būti kompleksiniai, tyrėjai siekia atrasti ir pasiūlyti metodikas, kurios apima šio reiškinio sudėtingumą ir daugiaveiksniškumą (pavyzdžiui, Hall ir kiti 2020).

Nors elektroniniai nusikaltimai, lyginant su kitomis nusikaltimų formomis, dažniau pasižymi globaliomis savybėmis, jų poveikis yra lokalus (Wall

2015, p. 74). Jie susieja individus ir organizacijas (tai gali būti ir pažeidėjai, ir nukentėjusieji, ir teisėsaugos institucijos), veikiančius konkrečioje geografinėje vietoje ir kultūriniame kontekste, lokalizuojančiame jų kasdienes patirtis ir patiriamą žalą. Skirtumus tarp išvadų, kurias gauna universalizuojančių ir į vietinį kontekstą susitelkiančių tyrimų autoriai, iliustruoja skirtingi tipinių pažeidėjų portretai.

Pozityvistinių tyrimų autoriai teigia, kad elektroniniai nusikaltimai yra artimi baltųjų apykaklių nusikaltimams: daugumą jų padaro jauni išsilavinę vyrai, priklausantys vidurinei ir aukštesniajai ekonominei klasei. Šiuo faktu grindžiamas teiginys, kad etninės mažumos, nepasiturinčiosios klasės atstovai „pasitelkus kainas ir reikiamus įgūdžius atribojami nuo nusikaltimų, susijusių su nusikaltimais“ (Diamond, Bachmann 2015, p. 28). Tačiau pasaulyje yra valstybių, kur kaip tik finansinės naudos siekis ir priklausymas žemesnei ekonominei klasei yra pagrindinė paskata daryti nusikaltimus panaudojant informacijos ir komunikacijos technologijas. Technologinė galimybė per atstumą pasiekti aukštesnes ekonomines klases kitose valstybėse gali paskatinti imtis elektroninių nusikaltimų, o juos darant – kurti ir tam tikras lokalias kultūrines reikšmes bei tradicijas. Tokių atvejų pavyzdžiai – Veleso miestelio paaugliai Makedonijoje, kuriantys melagingas naujienas ir užsidirbantys iš reklamos (Alcott, Getzkow 2017, p. 217; Vian, McStay 2018, p. 5); Nigerijos elektroninių nusikaltėlių subkultūros (Olayemi 2014).

Lokalių elektroninių nusikaltimų ypatybių tyrimai[3], nagrinėjantys juos specifiniuose kontekstuose, tarp kitų aprėpia šias šalis: Australija (Hutchings 2014), Ekvadoras (Ron, Fuertes, Bonilla, Toulkeridis, Díaz 2018), Gana (Ennin, Mensah 2019), Indija (Gupta, Agrawal 2018; Kumar 2016; Kshetri 2017; Arora, Mendhekar 2017), Nigerija (Lazarus, Okolorie 2019; Olayemi 2014; Whitty, Ng 2017), Nyderlandai (Odinot, Verhoeven, Pool, Poot C. J. 2017), Rumunija (Lusthaus, Varese 2017), Saudo Arabija (Alotaibi, Furnell, Stengel, Papadaki 2016), Tanzanija (Mshana), Vietnamas (Nguyen 2019), kelių šalių

[3] Išvardyti keli tyrimų pavyzdžiai, prieinami anglų kalba tarptautinėse mokslinėse duomenų bazėse. Tarp jų yra ir kiekybinių, ir kokybinių studijų, besiremiančių skirtingomis šiame straipsnyje minėtomis teorinėmis prieigomis. Sąrašas nėra nei išsamus, nei baigtinis – juo siekiama iliustruoti, kokia egzistuoja lokalių patirčių tyrimų įvairovė. Ji itin aktuali vengiant perdėm universalizuojančių išvadų, formuluojant regionines strategijas ir transnacionalinio bendradarbiavimo taktikas. Išsami lokalių tyrimų apie elektroninius nusikaltimus analizė reikalauja atskiro tyrimo.

patirtis sisteminančios apžvalgos (pavyzdžiui, Olatunbosun, Edwards, Martineau 2018; Broadhurst, Chang 2013; Kshetri 2015, 2019; Bakhsh, Mahmood, Awan 2016; Chang 2017). Jų perspektyvų ir išvadų įvairovė parodo reiškinio sudėtingumą ir universalios teorijos paieškų problemiškumą, tai pažymi ir tyrėjai, siekiantys sisteminti tokių tyrimų patirtį (Kranenbarg 2020). Augant lokalių studijų skaičiui, jų pagrindu galima formuluoti tarpkultūrines elektroninių nusikaltimų teorijas, ieškoti panašumų ir skirtumų, remiantis ne iš anksto suformuluotomis ir galimai reiškinį per daug supaprastinančiomis hipotezėmis, o realiais, tirštais lauko tyrimų rezultatais.

Elektroninių nusikaltimų socialinių tyrimų laukas Lietuvoje

Tyrimo metodika. Siekiant nustatyti, koks temų spektras yra atskleistas Lietuvos autorių atliktuose socialiniuose tyrimuose apie elektroninius nusikaltimus ir kokia jų dalis pateikia empirinių tyrimų rezultatus, buvo atlikta sisteminė apžvalga šios srities mokslinių publikacijų, viešai prieinamų internete.

Straipsnių buvo ieškoma naudojant „Google Scholar“ sistemą, kurioje yra indeksuojama dauguma lietuvių kalba leidžiamų mokslo žurnalų, ir vedant paieškos terminus, susijusius su elektroniniais nusikaltimais. Didžioji dalis straipsnių buvo rasta, įvedus paieškos terminą „elektroniniai nusikaltimai“ ir jo sinonimus („kibernetiniai nusikaltimai“, „nusikaltimai internete“, „informacinio saugumo pažeidimai“, „deviacijos internete“). Šis paieškos terminas leido rasti ir straipsnius, apžvelgiančius elektroninių nusikaltimų diskursus, vietinius ypatumus. Nedidelė dalis straipsnių buvo atrasta įvedant paieškos žodžius, nusakančius konkrečius nusikaltimų tipus („neautorizuota prieiga“, „neteisėtas turinys“, „piratavimas“, „torrent svetainės“, „patyčios internete“, „pornografija internete“, „persekiojimas internete“, „neapykanta internete“, „vagystės internete“, „sukčiavimas internete“, „finansiniai nusikaltimai internete“, „seksualiniai nusikaltimai internete“, „lošimai internete“, „lažybos internete“, „nelegali prekyba internete“, „tapatybės pasisavinimas“, „narkotikų prekyba internete“). Taip pat buvo naudoti raktiniai žodžiai, susiję su konkrečiais veikėjais ir jų savybėmis („hakeriai“, „interneto piratai“, „programišiai“, „elektroninių nusikaltimų aukos“, „rizikingas elgesys internete“, „probleminis interneto naudojimas“). Paieška su dauguma šių specifinių terminų nepateikė

jokių rezultatų. Į tyrimą buvo įtraukti visi rasti straipsniai, neribojant publikavimo metų bei žurnalų.

Svarbu paminėti, kad Lietuvoje moksliniame elektroninių nusikaltimų diskurse kiekiu ir temų įvairove dominuoja teisininkų darbai. Naujausi moksliniai straipsniai ir disertacijos apima tokias temas kaip elektroninių nusikaltimų ir saugumo teisinis reglamentavimas (Marcinauskaitė 2021; Marcinauskaitė, Pukanasytė, Šukytė 2019; Štitilis et al. 2017a; Marcinauskaitė 2016), asmens duomenų apsaugos ir privatumo teisinis reglamentavimas (Stankevičiūtė 2020; Štitilis, Laurinaitis 2017; Malinauskaitė-van de Castel 2017; Meškauskaitė, Lankauskas 2016), finansinių technologijų teisinis reglamentavimas (Marcinauskaitė, Girdenis, Laurinaitis 2020; Bučiūnas 2016). Pavieniai autoriai yra nagrinėję specifinius elektroninių nusikaltimų aspektus iš kriminalistikos ir kompiuterių inžinerijos perspektyvų (Grigaliūnas, Toldinas 2020; Grigaliūnas 2020; Grigaliūnas, Venčkauskas 2017; Barkauskas, Spiečiūtė, Juodkaitė-Granskienė 2016; Venčkauskas et al. 2015).

Tačiau šio straipsnio tikslas – išnagrinėti elektroninius nusikaltimus socialiniame teoriniame ir empiriniame socialinių tyrimų lauke. Todėl į tyrimą nebuvo įtrauktos publikacijos, kuriose apie elektroninius nusikaltimus rašoma iš inžinerinės, teisinės, kriminalistinės perspektyvos, išskyrus atvejus, kai šių sričių publikacijose autoriai reikšmingą dėmesį suteikia ir socialiniam dėmeniui – nusikaltimo pobūdžiui ir atlikimo sąlygoms, priežastims ir pasekmėms, sąsajoms su socialinėmis institucijomis, socialiniams sąryšiams.

Taip pat į analizę nebuvo įtrauktos dvi publikacijos, kurios nagrinėjo elektroninius nusikaltimus bendrai kaip teorinę sampratą (Kalpokas 2009; Kuklytė, Ūsas 2017) – tai svarbi tema, tačiau jos neįmanoma sutalpinti į didesnio konkretumo reikalaujančią klasifikacijos schemą.

Atrinkus tiriamas publikacijas, jos visų pirma pagal savo pagrindinę temą buvo priskirtos vienai iš keturių kategorijų, nustatytų teorinėje straipsnio dalyje: nusikaltimų tipologijos, proceso dalyvių, diskursų, globalių bei lokalių dimensijų. Siekiant nustatyti šių temų tyrinėjimo Lietuvoje ypatumus, buvo analizuojamas publikacijų chronologinis išsidėstymas, o siekiant nustatyti, kokių disciplinų akiratyje nagrinėjamos šios temos, buvo fiksuojami žurnalai arba leidyklos. Siekiant nustatyti, kokia yra sukaupta empirinių tyrimų patirtis, buvo fiksuojama, ar publikacijoje aprašomas tyrimas, kurio metu autoriai patys rinko ir analizavo duomenis.

Tyrimo rezultatai. Tyrimo rezultatai apibendrinti *1 lentelėje*. Lentelę sudaro išanalizuotos literatūros pagrindu sudarytas temų sąrašas, išskaidytas į keturias pagrindines kategorijas (nusikaltimų tipai, proceso dalyviai, elektroninių nusikaltimų diskursai ir globalios bei lokalios elektroninių nusikaltimų dimensijos). Rausva spalva pažymėtos tos temos, kuriomis lietuviškų publikacijų nėra, gelsvai – publikacijos be empirinių tyrimų ir temos, kuriose didesnę dalį sudaro publikacijos be empirinių tyrimų, žalsvai – publikacijos, aprašančios autorių atliktus empirinius tyrimus, ir temos, kuriose didesnę dalį sudaro publikacijos su empiriniais tyrimais.

1 LENTELĖ. Lietuviškų socialinių tyrimų apie elektroninius nusikaltimus sisteminės tematikos ir empirinė aprėptis

Tematinės sritys ir temos	Lietuvos autorių publikacijos ir jų temos	Leidėjas (žurnalas arba leidykla)	Ar atliktas empirinis tyrimas?
I. Nusikaltimų tipai			
Technologijos kaip nusikaltimo taikinys			
Neautorizuota prieiga			
Neteisėti veiksmai su informacinėmis sistemomis			
Sistemų veiklos trikdymai			
Infrastruktūros pažeidimai			
Technologijos kaip nusikaltimo įrankis (finansai ir ekonomika)			
Finansiniai nusikaltimai			
Sukčiavimas	Šidlauskas, Ungurytė-Ragauskienė (2020), socialinės inžinerijos apibrėžimai ir tipai	Visuomenės saugumas ir viešoji tvarka	Ne
Nelegali prekyba	Gasparėnienė, Remeikienė, Sadeckas, Ginevičius (2016), skaitmeninės šešėlinės ekonomikos (angl. *digital shadow economy*) modeliavimas ir modelių pritaikymas Lietuvos atvejui	Entrepreneurship and Sustainability Issues	Taip
	Gasparėnienė, Remeikienė, Ginevičius, Schieg (2018), tas pats	Technological and Economic Development of Economy	Taip

Tematinės sritys ir temos	Lietuvos autorių publikacijos ir jų temos	Leidėjas (žurnalas arba leidykla)	Ar atliktas empirinis tyrimas?
Technologijos kaip nusikaltimo įrankis (turinys)			
Intelektinės nuosavybės teisių pažeidimai	Kiškis, Petrauskas (2006), trumpa techninių priemonių apžvalga kartu su teisiniu reguliavimu	Jurisprudencija	Ne
	Kiškis, Krikščionaitis (2008), tarptautinių intelektinės nuosavybės pažeidimų studijų palyginimas	Teisė	Ne
	Rekis, Rekienė (2016), socialinio dalyvavimo *Torrent* svetainėje ypatumai	Tiltai	Taip
Viešosios informacijos sklaidos pažeidimai	Amilevičius (2011), kalbos technologijų potencialas, kontroliuojant interneto turinį	Visuomenės saugumas ir viešoji tvarka	Ne
Draudžiamos pornografijos formos			
Technologijos kaip nusikaltimo įrankis prieš asmenis ir grupes			
Nepageidaujama reklama			
Persekiojimas			
Seksualiniai nusikaltimai	Kuklytė (2018), teorinių apibrėžimų apžvalga	European Journal of Business Science and Technology	Ne
Patyčios	Pilkauskaitė-Valickienė, Raižienė, Žukauskienė (2009), moksleivių patiriamos elektroninių patyčių formos	Socialinis darbas	Taip
	Valeckienė (2011), moksleivių ir pedagogų visoje Lietuvoje požiūris į elektroninių patyčių prevenciją	Tiltai	Taip
	Grigutytė, Raižienė, Pakalniškienė (2019), elektroninių patyčių pasekmės	Psichologija	Taip
Neapykantos sklaida	Auškalnienė (2006), etninis nepakantumas delfi.lt straipsnių komentaruose	Etniškumo studijos	Taip

Tematinės sritys ir temos	Lietuvos autorių publikacijos ir jų temos	Leidėjas (žurnalas arba leidykla)	Ar atliktas empirinis tyrimas?
Tapatybės pasisavinimas	Štitilis, Laurinaitis (2009), trumpa techninių priemonių ir teisinio reguliavimo apžvalga	Informacijos mokslai	Ne
	Štitilis ir kiti (2011), socialinius ir teisinius aspektus nagrinėjanti monografija	MRU	Taip
	Kalpokas, Marcinauskaitė (2012), naujesnė, daugiau aspektų įtraukianti apžvalginio pobūdžio publikacija	Teisės problemos	Ne
Asmens duomenų apsaugos pažeidimai			
Grėsmė fiziniam saugumui			
II. Proceso dalyviai			
Pažeidėjai			
Motyvacija, įsitraukimo veiksniai	Jokubaitė (2014), paauglių rizikingą elgesį internete didinančių ir mažinančių veiksnių tyrimų apžvalga	Tiltai	Ne
	Paluckaitė, Žardeckaitė-Matulaitienė (2015), rizikingo elgesio internete tyrimų apžvalga	Visuomenės sveikata	Ne
Sociodemografinės charakteristikos	Balsevičienė, Ruibytė (2015), pažeidėjų profiliavimo metodų apžvalga	Visuomenės saugumas ir viešoji tvarka	Ne
Priklausymas nusikalstamoms grupėms			
Nusikalstamos veiklos organizavimo modeliai			
Nežmogiškieji veikėjai			
Nukentėjusieji			
Individualios viktimologinės patirtys	Ruškus, Žvirdauskas, Kačenauskaitė (2010), moksleivių viktimizacijos internete prielaidos	Socialinis darbas	Taip
	Gedutienė, Šimulionienė, Čepienė, Rugevičius (2012), jaunesniojo amžiaus paauglių elektroninių ir tradicinių patyčių patirtis	Tiltai	Taip

Tematinės sritys ir temos	Lietuvos autorių publikacijos ir jų temos	Leidėjas (žurnalas arba leidykla)	Ar atliktas empirinis tyrimas?
Kolektyvinės viktimologinės patirtys			
Veiksniai, lemiantys tapimą auka			
Prisitaikymo ir išgyvenimo strategijos			
Antrinė viktimizacija			
Santykis su teisėsaugos institucijomis			
Savipagalba, aktyvizmas, savisauga			
Teisėsaugos ir informacinio saugumo industrijos atstovai			
Požiūris į elektroninius nusikaltimus	Butrimė, Zuzevičiūtė (2017), teisėsaugos studentų nuostatos	Informacijos mokslai	Taip
Asmeninės ir organizacinės kompetencijos			
Resursų optimizavimas			
Tarptautinis bendradarbiavimas			
III. Elektroninių nusikaltimų diskursai			
Elektroninių nusikaltimų pateikimas masinėse medijose, pramogų industrijoje			
Technologinių diskursų įtaka politinių sprendimų priėmimui			
Elektroninių nusikaltimų recepcija visuomenėje ir atskirose tikslinėse grupėse	Čepinskis, Rakevičienė, Rudytė (2004), internetinės bankininkystės vartotojų požiūris į duomenų saugumą	Organizacijų vadyba: sisteminiai tyrimai	Taip
	Žibėnienė, Brasienė (2013), moksleivių požiūris į grėsmes internete	Socialinės technologijos	Taip
	Skališienė, Žukauskienė (2018), dienos centrų darbuotojų požiūris į paauglių mergaičių rizikingą dalyvavimą socialiniuose tinkluose	Pedagogika	Taip
	Gasparėnienė, Remeikienė, Ginevičius (2018), požiūrių į skaitmeninę šešėlinę ekonomiką palyginimas Lietuvoje ir Ispanijoje	Acta Polytechnica Hungarica	Taip
Medijų efektų ryšys su viktimizacija			
Elektroninių nusikaltimų algoritminė amplifikacija socialinės tinklaveikos priemonėse			

Tematinės sritys ir temos	Lietuvos autorių publikacijos ir jų temos	Leidėjas (žurnalas arba leidykla)	Ar atliktas empirinis tyrimas?
IV. Globalios ir lokalios elektroninių nusikaltimų dimensijos			
Lokalūs elektroninių nusikaltimų ypatumai	Bilevičienė, Bilevičiūtė (2011), elektroninių nusikaltimų dinamika Lietuvoje 2003–2010 m.	Jurisprudencija	Taip
Tarptautiniai palyginimai			

Pagal nustatytus paieškos kriterijus į tyrimą iš viso pakliuvo 26 publikacijos, išleistos per pastaruosius 16 metų, t. y. nuo 2004 iki 2020 metų. Taigi, nors elektroninių nusikaltimų socialiniai tyrimai Lietuvoje atliekami anksčiausiai nuo to laikotarpio, kai interneto naudojimas sparčiai augo, tačiau jų iki dabar buvo atlikta per mažai, kad būtų galima išskirti konkrečius šio tyrimų lauko vystymosi etapus (kaip tai darė Stratton, Powell, Cameron 2017) pagal tematikos raidą.

Analizuojamose publikacijose dominavo dviejų sričių atstovai: teisininkai, aprėpiantys kelių skirtingų tipų elektroninių nusikaltimų socialinius aspektus (9 iš 26 publikacijų), ir daugiausia edukologines bei psichologines prieigas taikantys mokslininkai, nagrinėjantys elektronines patyčias tarp moksleivių ir moksleivių požiūrį į elektroninius nusikaltimus bei riziką su jais susidurti (10 iš 26 publikacijų). Taip pat dėmesio šiai temai buvo skyrę ekonomikos ir vadybos tyrėjai (4 iš 26 publikacijų).

Iš 41 išskirtos temos 29, arba du trečdaliai, analizuojamose publikacijose buvo nenagrinėtos, dar keturios buvo nagrinėtos be empirinių tyrimų, o aštuoniomis temomis buvo atlikta bent po vieną empirinį tyrimą, kurio metu buvo renkami duomenys Lietuvoje, vienu atveju – Lietuvoje ir Ispanijoje. Taigi kiek daugiau nei pusė visų publikacijų buvo su tyrimais, o likusios – teorinio pobūdžio.

Publikacijose neatskleistos temos. Tyrimų, kurie aiškintųsi elektroninių nusikaltimų ypatybes, kai technologijos yra nusikaltimo taikinys (neautorizuota prieiga, neteisėti veiksmai su duomenimis, sistemų veiklos trikdymai, ryšių infrastruktūros pažeidimai), nebuvo rasta[4]. Kai technologijos yra nusi-

[4] Šios temos ne vienus metus kartojasi ir yra plėtojamos viešai prieinamuose įvairiausių socialinių mokslų disciplinų bakalauro ir magistro darbuose, tačiau tolimesnių mokslininkų vykdomų tyrimų objektu netampa.

kaltimų įrankis, neatskleistos temos – vagystės, draudžiamos pornografijos formos, nepageidaujama reklama, persekiojimas internete, asmens duomenų apsaugos pažeidimai, grėsmė fiziniam saugumui.

Nematomos išliko ir dauguma temų, susijusių su proceso dalyviais – tiek pažeidėjais, tiek nukentėjusiaisiais, tiek teisėsaugos institucijomis. Nebuvo rasta straipsnių apie elektroninius nusikaltimus padariusių pažeidėjų priklausymą nusikalstamoms grupėms, nusikalstamos veiklos organizavimo modelius, nežmogiškųjų veikėjų indėlį, nukentėjusiųjų kolektyvines viktimologines patirtis, veiksnius, lemiančius tapimą auka, aukų prisitaikymo ir išgyvenimo strategijas, antrinę viktimizaciją, santykį su teisėsaugos institucijomis, savipagalbą, aktyvizmą, savisaugą, teisėsaugos institucijų asmenines ir organizacines kompetencijas, elektroniniams nusikaltimams skiriamus resursus ir jų optimizavimą, tarptautinio bendradarbiavimo praktikas ir iššūkius.

Neatskleista didžioji dalis temų apie elektroninių nusikaltimų diskursus, jų pateikimą masinėse medijose ir populiariojoje kultūroje, įtaką politinių sprendimų priėmimui, medijų efektų sąsajas su viktimizacija, algoritminės amplifikacijos problemas. Nerasta ir tyrimų, kuriuose Lietuvos situacija būtų lyginama su kitomis valstybėmis.

Temos su pavienėmis publikacijomis. Kelios publikacijos buvo skirtos sukčiavimui internete (Šidlauskas, Ungurytė-Ragauskienė 2020), socialiniams aspektams, susijusiems su intelektinės nuosavybės teisių pažeidimais (Kiškis, Petrauskas 2006; Kiškis, Krikščionaitis 2008), galimybėmis naudoti technologijas informacijos sklaidos pažeidimų kontrolei (Amilevičius 2011), tapatybės pasisavinimui (Štitilis, Laurinaitis 2009; Kalpokas, Marcinauskaitė 2012), seksualiniams nusikaltimams (Kuklytė 2018), tačiau visi jie neturi empirinių tyrimų, o didesnė jų dalis yra 10 ir daugiau metų senumo. Pavieniai tyrimai atlikti apie skaitmeninę šešėlinę ekonomiką (Gasparėnienė ir kiti 2016; Gasparėnienė ir kiti 2018), nelegalaus kūrinių platinimo bendruomenes (Rekis, Rekienė 2016), neapykantos sklaidą (Auškalnienė 2006), tapatybės pasisavinimą (Štitilis ir kiti 2011).

Taip pat buvo publikacijų, kurių autoriai aptarė pavienius proceso dalyvių aspektus: pažeidėjų profiliavimo būdus aprašančią literatūrą (Balsevičienė, Ruibytė 2015), teisėsaugos studentų nuostatas apie saugumą internete, remiantis empiriniu tyrimu (Butrimė, Zuzevičiūtė 2017). Elektroninių nusikaltimų struktūrą ir kiekybines sąsajas su kitais veiksniais, remdamosi 2003–

2010 m. registruotų nusikaltimų statistiniais duomenimis, analizavo Bilevičienė ir Bilevičiūtė (2011).

Intensyviau tiriamos temos. Atlikta analizė atskleidė, kad yra viena nuosekliau tiriama temų grupė, kurioje dominuoja edukologijos ir psichologijos atstovai, tai – tarp moksleivių vykstančios patyčios internete. Ši tema buvo atskleidžiama per kelias skirtingas potemes – bendri duomenys apie internetines patyčias, jų paplitimą, prevencijos priemones, pasekmes (Pilkauskaitė-Valickienė, Raižienė, Žukauskienė 2009; Valeckienė 2011; Grigutytė, Raižienė, Pakalniškienė 2019), moksleivius kaip socialinę grupę, galinčią tapti tiek pažeidėjais (Jokubaitė 2014; Paluckaitė, Žardeckaitė-Matulaitienė 2015), tiek nukentėjusiaisiais (Ruškus, Žvirdauskas, Kačenauskaitė 2010; Gedutienė ir kiti 2012); moksleivių (Žibėnienė, Brasienė 2013) ir vaikų dienos centrų darbuotojų (Skališienė, Žukauskienė 2018) požiūrį į tai, kas įvardijama kaip grėsmės internete.

Lentelėje pateikta medžiaga taip pat parodo, kad kita tema, kuria buvo atlikti daugiau nei pavieniai tyrimai – elektroninių nusikaltimų recepcija atskirose, gana siaurose tikslinėse grupėse: tarp internetinės bankininkystės klientų (Čepinskis, Rakevičienė, Rudytė 2004), jau minėtų moksleivių bei vaikų dienos centrų darbuotojų ir imties, kurioje dominuoja studentai (Gasparėnienė, Remeikienė, Ginevičius 2018). Visais atvejais tyrimų dėmesys buvo sutelktas ne į elektroninius nusikaltimus kaip objektą, o į siauresnius jų atvejus – duomenų nutekėjimą interneto bankininkystėje, šešėlinę ekonomiką internete, arba platesnes elgesio formas, kurios gali apimti ir tam tikrus elektroninius nusikaltimus, rizikingu laikomą elgesį internete. Tuo tarpu nacionaliniu mastu reprezentatyvių visuomenės apklausų, kurios būtų sutelktos būtent į elektroninių nusikaltimų recepciją ir vertinimą, aptikti nepavyko.

Išvados ir rekomendacijos

Nuo XX a. devintojo dešimtmečio atliekami socialiniai tyrimai apie elektroninius nusikaltimus sudaro daugiadalykį, kartais teoriškai ir metodologiškai fragmentuotą lauką, apimantį platų temų diapazoną. Dominuojančios temos priklauso keturioms skirtingoms kategorijoms:

1) tyrimai, skirti charakterizuoti atskirus nusikaltimų tipus – nuo technologijų kaip nusikaltimų taikinių iki technologijų kaip nusikaltimų įrankių;

2) tyrimai, sutelkti į proceso dalyvius – pažeidėjus, nukentėjusiuosius ir teisėsaugą;
3) tyrimai apie elektroninių nusikaltimų diskursus ir recepciją visuomenėje;
4) tyrimai apie lokalius ir globalius elektroninių nusikaltimų ypatumus.

Šios kategorijos parodo, kad elektroninių nusikaltimų temos ir galimybės jas tirti socialiniuose moksluose yra labai plačios, o tam tikri klausimai, kuriuos vieni autoriai nurodo kaip (beveik) netiriamus, iš tikrųjų turi plačius literatūros klodus, tik ši informacija, pavyzdžiui, apie geografinius ir kultūrinius elektroninių nusikaltimų atlikimo arba recepcijos skirtumus, kol kas dar silpnai konsoliduota. Paskutinė kategorija – apie lokalius ir globalius elektroninių nusikaltimų ypatumus parodo, kad būtina atsargiai vertinti mėginimus kurti universalias teorijas ir įdėmiau vertinti *mikro-* ir *makro-*, lokalaus ir globalaus lygmens veiksnius.

Sisteminė literatūros analizė parodė, kad Lietuvoje 2004–2020 metais buvo rastos 26 publikacijos, atitikusios paieškos kriterijus, priklausančios minėtoms temoms ir jas nagrinėjančios iš socialinių mokslų, išskyrus teisę, perspektyvos. Nepaisant tiek mokslinio, tiek praktinio aktualumo, tema išlieka menkai tiriama, o prieš 10 ir daugiau metų atlikti pavieniai tyrimai sensta ir nėra iš naujo aktualizuojami. Dėl nedidelio tyrimų skaičiaus nėra galimybių išskirti ir įvertinti skirtingų šio tematinio lauko raidos etapų, mokyklų formavimosi Lietuvoje. Dalį šių temų iš socialinės pusės aprašo teisininkai, daugiau įdirbio turi psichologijos ir edukologijos sričių tyrėjai, dirbantys su internetinių patyčių problematika, kelis tyrimus yra atlikę ekonomikos ir vadybos disciplinų atstovai. Trūksta įdirbio iš kriminologijos, sociologijos, komunikacijos ir informacijos, politikos mokslų atstovų.

Kiek mažiau nei pusė publikacijų yra teorinės, o likusiose pristatomi tyrimai dažnai yra žvalgomojo pobūdžio, nereprezentatyvūs arba nukreipti į siauras pavienes socialines grupes. 29 iš 41 temos, aktualizuojamos globalioje mokslinėje diskusijoje apie elektroninius nusikaltimus Lietuvoje, 2021 m. buvo nenagrinėtos. Trūksta tyrimų, apibendrinančių elektroninių nusikaltimų padėtį ir struktūrą Lietuvoje – susiejančių mikro- ir makrolygmens veiksnius.

Atlikti daugiau empirinių tyrimų būtina visomis išskirtomis temomis, užtikrinant duomenų validumą, tikslumą ir galimybes tinkamai generalizuoti išvadas. Elektroninių nusikaltimų tyrimai svarbūs ne tik dėl reikalingų žinių

apie nusikaltimų raidą ir poveikį visuomenėje, tačiau dėl to, kad jie atneša ir galimybę tinkamam krizinių situacijų vertinimui ir bendresnėms kritinėms diskusijoms apie informacijos ir komunikacijos įtaką visuomenei, pamatiniams socialinių normų ir socialinės kontrolės veikimo klausimams, susijusiems su kompiuterių ir interneto technologijų paplitimu.

Literatūra

Aas K. F. 2012, „'The Earth is one but the world is not': Criminological theory and its geopolitical divisions", *Theoretical criminology*, 16 (1), p. 5–20.

Abhishta A. 2019, *The blind man and the elephant: Measuring economic impacts of DDOS attacks*. University of Twente.

Abhishta A., van Heeswijk W., Junger M., Nieuwenhuis L. J. M., Joosten R. 2020, „Why would we get attacked? An analysis of attacker's aims behind DDoS attacks", *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 11 (2), p. 3–22.

Alladi T., Chamola V., Zeadally S. 2020, „Industrial control systems: Cyberattack trends and countermeasures", *Computer Communications*, 155, p. 1–8.

Allcott H., Gentzkow M. 2017, „Social media and fake news in the 2016 election", *Journal of Economic Perspectives*, 31 (2), p. 211–36.

Alotaibi F., Furnell S., Stengel I., Papadaki M. 2016, „A survey of cyber-security awareness in Saudi Arabia", *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*, p. 154–158.

Amilevičius D. 2011, „Smurto kontrolės lietuviškame saityne sąryšis su semantinių ir kalbos technologijų plėtra", *Visuomenės saugumas ir viešoji tvarka*, 6, p. 5–21.

Argaw S. T., Bempong N.-E., Eshaya-Chauvin B., Flahault A. 2019, „The state of research on cyberattacks against hospitals and available best practice recommendations: a scoping review", *BMC Medical Informatics And Decision Making*, 19 (1), p. 1–11.

Arntfield M. 2015, „Toward a cybervictimology: Cyberbullying, routine activities theory, and the anti-sociality of social media", *Canadian Journal of Communication*, 40 (3), p. 371–388.

Arora A., Mendhekar A. 2017, „Threats to Security and privacy of Information due to growing use of social media in India", *Asian Journal of Managerial Science*, 6 (2), p. 42–49.

Auškalnienė L. 2006, „Etninis nepakantumas Lietuvos internetinėje žiniasklaidoje: komentarai internete", *Etniškumo studijos*, 1, p. 45–58.

Bakhsh M., Mahmood A., Awan I. I. 2016, „A comparative analysis of cybercrime and cyberlaws in Islamic Republic of Pakistan, Kingdom of Saudi Arabia, and the United Arab Emirates", *Imam Journal of Applied Sciences*, 1 (1), p. 9–15.

Bakir V., McStay A. 2018, „Fake news and the economy of emotions: Problems, causes, solutions", *Digital journalism*, 6 (2), p. 154–175.

Balsevičienė B., Ruibytė L. 2015, „Kriminalinio profiliavimo pritaikymo galimybės nusikaltimų, įvykdytų elektroninėje erdvėje, tyrimui“, *Visuomenės saugumas ir viešoji tvarka*, 15, p. 13–26.

Barkauskas M., Spiečiūtė A., Juodkaitė-Granskienė G. 2016, „Ekonominių ekspertinių tyrimų galimybės tiriant ūkines ir finansines nusikalstamas veikas“, *Teisės apžvalga*, 2 (14), p. 281–305.

Bilevičienė T., Bilevičiūtė E. 2011, „Dynamics of crimes against the security of electronic data and information systems, and its influence on the development of electronic business in Lithuania“, *Jurisprudencija*, 18 (2), p. 689–702.

Black A., Lumsden K., Hadlington L. 2019, „Why Don't You Block Them? Police Officers' Constructions of the Ideal Victim When Responding to Reports of Interpersonal Cybercrime“, in K. Lumsden, E. Harmer (eds.). *Online Othering: Exploring Violence And Discrimination On The Web*. Basingstoke: Palgrave Macmillan, p. 355–378.

Bliuc A.-M., Faulkner N., Jakubowicz A., McGarty C. 2018, „Online networks of racial hate: A systematic review of 10 years of research on cyber-racism“, *Computers in Human Behavior*, 87, p. 75–86.

Blythe J. M., Johnson S. D. 2019, „A systematic review of crime facilitated by the consumer Internet of Things“, *Security Journal*, 34 (1), p. 97–125.

Brands J., van Wilsem J. 2021, „Connected and fearful? Exploring fear of online financial crime, Internet behaviour and their relationship“, *European Journal of Criminology*, 18 (2), p. 213–234.

Brey P. 2016, „Constructive philosophy of technology and responsible innovation“, in M. Fransen, P. E. Vermaas, P. Kroes, A. W. M. Meijers (eds.). *Philosophy Of Technology After The Empirical Turn*. Springer, p. 127–143.

Broadhead S. 2018, „The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments“, *Computer Law, Security Review*, 34 (6), p. 1180–1196.

Broadhurst R., Chang L. Y. C. 2013, „Cybercrime in Asia: Trends and challenges“, in J. Liu, S. Jou, B. Hebenton (eds.). *Handbook Of Asian Criminology*. New York: Springer, p. 49–64.

Broadhurst R., Lord D., Maxim D., Woodford-Smith H., Johnston C., Chung H. W., Carroll S., Trivedi H., Sabol B. 2018, *Malware trends on 'darknet'crypto-markets: Research review*. Canberra: Australian National University, Cybercrime Observatory.

Broome L. J., Izura C., Lorenzo-Dus N. 2018, „A systematic review of fantasy driven vs. contact driven internet-initiated sexual offences: Discrete or overlapping typologies?“, C*hild Abuse & Neglect*, 79, p. 434–444.

Bučiūnas G. 2016, „Laikino nuosavybės teisės apribojimo taikymo ypatumai krypto-valiutai [sic]“, *Visuomenės saugumas ir viešoji tvarka*, 17, p. 21–30.

Butrimė E., Zuzevičiūtė V. 2017, „Rizika socialiniuose tinkluose: būsimųjų teisėsaugos pareigūnų informuotumas“, *Informacijos mokslai*, 79, p. 7–16.

Čepinskis J., Rakevičienė J., Rudytė D. 2004, „Saugumo rizikos valdymas internetinėje bankininkystėje“, *Organizacijų vadyba: sisteminiai tyrimai*, 31, p. 31–41.

Chang L. Y. C. 2017, „Cybercrime and cyber security in ASEAN“, in J. Liu, M. Travers, L. Y. C. Chang (eds.). *Comparative Criminology In Asia*. Cham: Springer, p. 135–148.

Chang L. Y. C., Zhong L. Y., Grabosky P. N. 2018, „Citizen co-production of cyber security: Self-help, vigilantes, and cybercrime', *Regulation, Governance*, 12 (1), p. 101–114.

Chavarria J. A., Andoh-Baidoo F. K., Midha V., Hughes J. 2016, „Software piracy research: A cross-disciplinary systematic review“, *Communications of the Association for Information Systems*, 38 (1), p. 624–669.

Choi K.-S., Lee C. S., Cadigan R. 2018, „Spreading propaganda in cyberspace: Comparing cyber-resource usage of al Qaeda and ISIS“, *International Journal of Cybersecurity Intelligence, Cybercrime*, 1 (1), p. 21–39.

Chun J., Lee J., Kim J., Lee S. 2020, „An international systematic review of cyberbullying measurements“, *Computers in human behavior*, 113, p. 1–12.

Clevenger S. L., Navarro J. N., Gilliam M. 2018, „Technology and the endless "cat and mouse" game: A review of the interpersonal cybervictimization literature“, *Sociology Compass*, 12 (12), p. 1–13.

Conway G., Hadlington L. 2021, „How do undergraduate students construct their view of cybercrime? Exploring definitions of cybercrime, perceptions of online risk and victimization“, *Policing: A Journal of Policy and Practice*, 15 (1), p. 119–129.

Cross C. 2018a, „(Mis) understanding the impact of online fraud: Implications for victim assistance schemes“, *Victims and Offenders*, 13 (6), p. 757–776.

Cross C. 2018b, „Victims' motivations for reporting to the 'fraud justice network'“, *Police Practice and Research*, 19 (6), p. 550–564.

Cross C. 2020, „'Oh we can't actually do anything about that': The problematic nature of jurisdiction for online fraud victims“, *Criminology and Criminal Justice*, 20 (3), p. 358–375.

Cross C., Layt R. 2021, „"I Suspect That the Pictures Are Stolen": Romance Fraud, Identity Crime, and Responding to Suspicions of Inauthentic Identities“, *Social Science Computer Review*, p. 1–19.

Cross C., Parker M., Sansom D. 2019, „Media discourses surrounding 'non-ideal' victims: The case of the Ashley Madison data breach“, *International Review of Victimology*, 25 (1), p. 53–69.

Cross C., Richards K., Smith R. G. 2016, „The reporting experiences and support needs of victims of online fraud“, *Trends And Issues In Crime And Criminal Justice*, 518, p. 1–14.

Diamond B., Bachmann M. 2015, „Out of the Beta Phase: Obstacles, Challenges, and Promising Paths in the Study of Cyber Criminology“, *International Journal of Cyber Criminology*, 9 (1), p. 24–34.

Dimc M., Dobovšek B. 2010, „Perception of cyber crime in Slovenia', *Journal of Criminal Justice and Security*, 12 (4), p. 378–396.

Ennin D., Mensah R. O. 2019, „Cybercrime in Ghana and the reaction of the law“, *Journal of Law, Policy and Globalization*, 84, p. 36–45.

Ferrara E. 2018, „Measuring social spam and the effect of bots on information diffusion in social media“, in S. Lehmann, Y–Y. Ahn (eds.). *Complex Spreading Phenomena in Social Systems: Influence and Contagion in Real-World Social Networks.* Cham: Springer International Publishing, p. 229–255.

Fleming P., Watson S. J., Patouris E., Bartholomew K. J., Zizzo D. J. 2017, „Why do people file share unlawfully? A systematic review, meta-analysis and panel study“, *Computers in Human Behavior*, 72, p. 535–548.

Franko Aas K. 2007, „Analysing a world in motion: Global flows meet 'criminology of the other'“, *Theoretical criminology*, 11 (2), p. 283–303.

Gasparėnienė L., Remeikienė R., Ginevičius R. 2018, „Attitudes of European consumers towards digital shadow economy: Lithuanian and Spanish cases“, *Acta Polytechnica Hungarica*, 15 (4), p. 121–142.

Gasparėnienė L., Remeikienė R., Ginevičius R., Schieg M. 2018, „Adoption of mimic model for estimation of digital shadow economy“, *Technological And Economic Development Of Economy*, 24 (4), p. 1453–1465.

Gasparėnienė L., Remeikienė R., Sadeckas A., Ginevičius R. 2016, „Level and sectors of digital shadow economy: the case of Lithuania“, *Entrepreneurship and Sustainability Issues*, 4 (2), p. 183–197.

Gedutienė R., Šimulionienė R., Čepienė R., Rugevičius M. 2012, „Patyčios elektroninėje erdvėje: jaunesniojo amžiaus paauglių patirtis“, *Tiltai*, 1, p. 133–148.

Ghazali S., Ghani N. M. 2018, „Perception of female students towards social media-related crimes“, *Pertanika Journal Of Social Sciences And Humanities*, 26 (2), p. 769–786.

Ghazi-Tehrani A. K., Pontell H. N. 2021, „Phishing Evolves: Analyzing the Enduring Cybercrime“, *Victims and Offenders*, 16 (3), p. 316–342.

Gies S. V., Piquero N. L., Piquero A. R., Green B., Bobnis A. 2021, „Wild, wild theft: Identity crimes in the digital frontier“, *Criminal Justice Policy Review*, 32 (6), p. 592–617.

Grigaliūnas Š. 2020, *Nusikaltimų elektroninėje erdvėje ekspertinio tyrimo metodas*. Kaunas: Kauno technologijos universitetas.

Grigaliūnas Š., Toldinas J. 2020, „Habits Attribution and Digital Evidence Object Models Based Tool for Cybercrime Investigation“, *Baltic Journal of Modern Computing*, 8 (2), p. 275–292.

Grigaliūnas Š., Toldinas J., Venčkauskas A. 2017, „An ontology-based transformation model for the digital forensics domain“, *Elektronika ir elektrotechnika*, 23 (3), p. 78–82.

Grigaliūnas Š., Toldinas J., Venčkauskas A., Morkevičius N., Damasevičius R. 2020, „Digital Evidence Object Model for Situation Awareness and Decision Making in Digital Forensics Investigation“, *IEEE Intelligent Systems* (early access).

Grigutytė N., Raižienė S., Pakalniškienė V. 2019, „Vaikų (ne)dalyvavimas elektroninėse patyčiose ir emociniai bei elgesio sunkumai“, *Psichologija*, 60, p. 72–85.

Gupta D., Agrawal N. 2018, „Empirical Study of Cyber Crimes in India using Data Analytics“, *Global Journal of Enterprise Information System*, 10 (1), p. 99–103.

Hadlington L., Lumsden K., Black A., Ferra F. 2021, „A qualitative exploration of police officers' experiences, challenges, and perceptions of cybercrime“, *Policing: A Journal of Policy and Practice*, 15 (1), p. 34–43.

Hall A. A., Wright C. S. 2018, „Data security: A review of major security breaches between 2014 and 2018“, *Federation of Business Disciplines Journal*, 6, p. 50–63.

Hall T., Sanders B., Bah M., King O., Wigley E. 2020, „Economic geographies of the illegal: the multiscalar production of cybercrime“, *Trends in Organized Crime*, p. 1–26.

Hill J. B., Marion N. E. 2016, „Presidential rhetoric on cybercrime: links to terrorism?“, *Criminal justice studies*, 29 (2), p. 163–177.

Holt T. J. 2018, „Regulating cybercrime through law enforcement and industry mechanisms“, *The Annals of the American Academy of Political and Social Science*, 679 (1), p. 140–157.

Holt T. J., Bossler A. M. 2014, „An assessment of the current state of cybercrime scholarship“, *Deviant Behavior*, 35 (1), p. 20–40.

Holt T. J., Burruss G. W., Bossler A. M. 2019, „An examination of English and Welsh constables' perceptions of the seriousness and frequency of online incidents“, *Policing and Society*, 29 (8), p. 906–921.

Holt T. J., Fitzgerald S., Bossler A. M., Chee G., Ng E. 2016, „Assessing the risk factors of cyber and mobile phone bullying victimization in a nationally representative sample of Singapore youth“, *International Journal Of Offender Therapy And Comparative Criminology*, 60 (5), p. 598–615.

Holt T. J., Lee J. R., Freilich J. D., Chermak S. M., Bauer J. M., Shillair R., Ross A. 2020, „An exploratory analysis of the characteristics of ideologically motivated cyberattacks“, *Terrorism and Political Violence*, p. 1–16.

Holt T. J., Leukfeldt R., van de Weijer S. 2020, „An examination of motivation and routine activity theory to account for cyberattacks against Dutch web sites“, *Criminal Justice and Behavior*, 47 (4), p. 487–505.

Holtfreter K., Meyers T. J. 2015, „Challenges for cybercrime theory, research, and policy“, in *The Norwich Review of International and Transnational Crime*. Norwich: Norwich University, p. 54–66.

Hou T., Wang V. 2020, „Industrial espionage–A systematic literature review (SLR)“, *Computers and Security*, 98, p. 1–12.

Hutchings A. 2014, „Crime from the keyboard: organised cybercrime, co-offending, initiation and knowledge transmission“, *Crime, Law and Social Change*, 62 (1), p. 1–20.

Hutchings A., Holt T. J. 2017, „The online stolen data market: disruption and intervention approaches“, *Global Crime*, 18 (1), p. 11–30.

International Telecommunications Union, I. T. U. 2019, *Global Cybersecurity Index (GCI) 2018*, Technical report, ITU Publications, ISBN 978-92-61-28201-1. Prieiga per internetą: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

Jansen J., Leukfeldt R. 2018, „Coping with cybercrime victimization: An exploratory study into impact and change", *Journal of Qualitative Criminal Justice and Criminology*, 6 (2), p. 205–228.

Jenaro C., Flores N., Frias C. P. 2018, „Systematic review of empirical studies on cyberbullying in adults: What we know and what we should investigate", *Aggression and Violent Behavior*, 38, p. 113–122.

Jokubaitė R. 2014, „Paauglių rizikingo elgesio internete veiksniai", *Tiltai*, 1, p. 1–12.

Jones L. M., Mitchell K. J., Finkelhor D. 2012, „Trends in youth internet victimization: Findings from three youth internet safety surveys 2000–2010", *Journal of adolescent Health*, 50 (2), p. 179–186.

Junger M., Montoya L., Hartel P., Heydari M. 2017, „Towards the normalization of cybercrime victimization: a routine activities analysis of cybercrime in Europe", *2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, p. 1–8.

Kalpokas V. 2009, „Nusikaltimai elektroninėje erdvėje: kriminologinės sampratos dilemos", *Teisės problemos*, 63 (1), p. 75–87.

Kalpokas V., Marcinauskaitė R. 2012, „Tapatybės vagystė elektroninėje erdvėje: technologiniai aspektai ir baudžiamasis teisinis vertinimas", *Teisės problemos*, 77 (2), p. 30–52.

Kamruzzaman M., Islam M. A., Islam M. S., Hossain M. S., Hakim M. A. 2016, „Plight of youth perception on cyber crime in South Asia", *American Journal of Information Science and Computer Engineering*, 2 (4), p. 22–28.

Kaur R., Singh S., Kumar H. 2018, „Rise of spam and compromised accounts in online social networks: A state-of-the-art review of different combating approaches", *Journal of Network and Computer Applications*, 112, p. 53–88.

Kerschner C., Ehlers M.-H. 2016, „A framework of attitudes towards technology in theory and practice", *Ecological Economics*, 126, p. 139–151.

Khan S. K., Shiwakoti N., Stasinopoulos P., Chen Y. 2020, „Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions", *Accident Analysis and Prevention*, 148, p. 1–16.

Kiškis M., Krikščionaitis M. 2008, „Intelektinės nuosavybės teisių pažeidimų tyrimai: metodologiniai aspektai", *Teisė*, 68, p. 37–50.

Kiškis M., Petrauskas R. 2006, „Intelektinės nuosavybės elektroninėje erdvėje pažeidimų ypatumai", *Jurisprudencija*, 83 (5), p. 29–36.

Koops T., Dekker A., Briken P. 2018, „Online sexual activity involving webcams: An overview of existing literature and implications for sexual boundary violations of children and adolescents", *Behavioral Sciences and the Law*, 36 (2), p. 182–197.

Kranenbarg M. W. 2020, „Global Voices in Hacking (Multinational Views)“, in T. J. Holt, A. M. Bossler (eds.). *The Palgrave Handbook of International Cybercrime and Cyberdeviance.* Cham: Springer International Publishing, p. 771–792.

Kshetri N. 2015, „Cybercrime and cybersecurity issues in the BRICS economies“, *Journal of Global Information Technology Management*, 18 (4), p. 245–249.

Kshetri N. 2019, „Cybercrime and cybersecurity in Africa“, *Journal of Global Information Technology Management*, 22 (2), p. 77–81.

Kshetri N. 2017, „Cybersecurity in India: Regulations, governance, institutional capacity and market mechanisms“, *Asian Research Policy*, 8 (1), p. 64–76.

Kuklytė J. 2018, „Cybersexual harassment as icts development consequences: a review“, *European Journal Of Business Science And Technology*, 4 (2), p. 187–195.

Kuklytė J., Ūsas A. 2017, „Informacinės visuomenės iššūkiai: kokios yra kibernetinių nusikaltimų formos?“, *Visuomenės saugumas ir viešoji tvarka*, 18, p. 184–194.

Kumar P. V. 2016, „Growing cyber crimes in India: A survey“, *2016 International Conference on Data Mining and Advanced Computing (SAPIENCE)*, p. 246–251.

Kusz J., Bouchard M. 2020, „Nymphet or lolita? A gender analysis of online child pornography websites“, *Deviant Behavior*, 41 (6), p. 805–813.

Lallie H. S., Shepherd L. A., Nurse J. R. C., Erola A., Epiphaniou G., Maple C., Bellekens X. 2021, „Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic“, *Computers and Security*, 105.

Lavorgna A. 2015, „Organised crime goes online: realities and challenges“, *Journal of Money Laundering Control*, 18 (2), p. 153–168.

Lavorgna A. 2019, „Cyber-organised crime. A case of moral panic?“, *Trends in Organized Crime*, 22 (4), p. 357–374.

Lazarus S., Okolorie G. U. 2019, „The bifurcation of the Nigerian cybercriminals: Narratives of the Economic and Financial Crimes Commission (EFCC) agents“, *Telematics and Informatics*, 40, p. 14–26.

Lee C. S. 2020, „A crime script analysis of transnational identity fraud: Migrant offenders' use of technology in South Korea“, *Crime, Law and Social Change*, 74 (2), p. 201–218.

Lee H., Choi K.-S. 2021, „Interrelationship between bitcoin, ransomware, and terrorist activities: Criminal opportunity assessment via cyber-routine activities theoretical framework“, *Victims and Offenders*, 16 (3), p. 363–384.

Lee M. 2018, „Crime and the cyber periphery: Criminological theory beyond time and space“, in *The Palgrave Handbook of Criminology and the Global South*, Springer, p. 223–244.

Leukfeldt R., Kleemans E., Stol W. 2017, „The use of online crime markets by cybercriminal networks: A view from within“, *American Behavioral Scientist*, 61 (11), p. 1387–1402.

Leverett E., Kaplan A. 2017, „Towards estimating the untapped potential: A global malicious DDoS mean capacity estimate“, *Journal of Cyber Policy*, 2 (2), p. 195–208.

Levi M. 2008, „White-collar, organised and cyber crimes in the media: Some contrasts and similarities“, *Crime, Law and Social Change*, 49 (5), p. 365–377.

Levi M. 2017, „Assessing the trends, scale and nature of economic cybercrimes: Overview and issues“, *Crime, Law and Social Change*, 67 (1), p. 3–20.

Lusthaus J., Varese F. 2021, „Offline and local: The hidden face of cybercrime“, *Policing: A Journal of Policy and Practice*, 15 (1), p. 4–14.

Maas M. K., Cary K. M., Clancy E. M., Klettke B., McCauley H. L., Temple J. R. 2021, „Slutpage use among US college students: the secret and social platforms of image-based sexual abuse“, *Archives of sexual behavior*, p. 1–12.

Madigan S., Villani V., Azzopardi C., Laut D., Smith T., Temple J. R., Browne D., Dimitropoulos G. 2018, „The prevalence of unwanted online sexual exposure and solicitation among youth: a meta-analysis“, *Journal of Adolescent Health*, 63 (2), p. 133–141.

Maimon D., Louderback E. R. 2019, „Cyber-dependent crimes: An interdisciplinary review“, *Annual Review of Criminology*, 2, p. 191–216.

Malinauskaitė-Van De Castel I. 2017, *Duomenų subjekto teisės virtualiuose socialiniuose tinkluose*. Vilnius: Mykolo Romerio universitetas.

Marcinauskaitė R. 2016, „Neteisėto prisijungimo prie informacinės sistemos kriminalizavimo ypatumai ir kvalifikavimo problemos“, *Teisės apžvalga*, 2 (14), p. 250–266.

Marcinauskaitė R. 2021, „Nusikalstamos veikos elektroninėje erdvėje ir teritorinė baudžiamoji jurisdikcija“, *Jurisprudencija*, 28 (1), p. 200–216.

Marcinauskaitė R., Girdenis T., Laurinaitis M. 2020, „The concept of a technology neutral payment instrument in criminal law“, *Entrepreneurship and Sustainability Issues*, 8 (1), p. 917–928.

Marcinauskaitė R., Pukanasytė I., Šukytė J. 2019, „Cyber security issues: Problematic aspects of hacking“, *Journal of Security and Sustainability Issues*, 8 (3), p. 331–343.

Meškauskaitė L., Lankauskas M. 2016, „Baudžiamoji atsakomybė už asmens privataus gyvenimo neliečiamumo pažeidimus Europos Žmogaus Teisių Teismo bei Lietuvos teismų praktikos kontekste“, *Teisės problemos*, 1 (91), p. 52–80.

Meško G., Bernik I. 2011, „Cybercrime: Awareness and fear: Slovenian perspectives“, *2011 European Intelligence and Security Informatics Conference*, p. 28–33.

Messing J., Bagwell-Gray M., Brown M. L., Kappas A., Durfee A. 2020, „Intersections of stalking and technology-based abuse: Emerging definitions, conceptualization, and measurement“, *Journal of Family Violence*, 35 (7), p. 693–704.

Moosavi L. 2019, „A friendly critique of 'Asian Criminology' and 'Southern Criminology'“, *The British Journal of Criminology*, 59 (2), p. 257–275.

Mshana J. A. 2015, „Cybercrime: An empirical study of its impact in the society-a case study of Tanzania“, *Huria: Journal of the Open University of Tanzania*, 19 (1), p. 72–87.

Näsi M., Oksanen A., Keipi T., Räsänen P. 2015, „Cybercrime victimization among young people: a multi-nation study', *Journal of Scandinavian Studies in Criminology and Crime Prevention*, 16 (2), p. 203–210.

Nguyen H. V. 2019, *Cybercrime in Vietnam: A critical analysis of its regulatory framework*, PhD thesis. Portsmouth: University of Portsmouth.

Nguyen T., Luong H. T. 2020, „The structure of cybercrime networks: transnational computer fraud in Vietnam“, *Journal of Crime and Justice*, p. 1–22.

Nouh M., Nurse J. R. C., Webb H., Goldsmith M. 2019, „Cybercrime investigators are users too! Understanding the socio-technical challenges faced by law enforcement“, *Proceedings of the 2019 Workshop on Usable Security (USEC) at the Network and Distributed System Security Symposium (NDSS)*, p. 1–11.

Odinot G., Verhoeven M. A., Pool R. L. D., de Poot C. J. 2017, *Organised cybercrime in the Netherlands*. S. l.: Ministerie von Veiligheid en Justitie.

Olatunbosun S. B., Edwards N. J., Martineau C. D. 2018, „Capturing the existential cyber security threats from the Sub-Saharan Africa zone through literature database“, *KSU Proceedings on Cybersecurity Education, Research and Practice*, 3, p. 1–13.

Olayemi O. J. 2014, „A socio-technological analysis of cybercrime and cyber security in Nigeria“, *International Journal of Sociology and Anthropology*, 6 (3), p. 116–125.

Paluckaitė U., Žardeckaitė-Matulaitienė K. 2015, „Rizikingas elgesys internete: jo formos ir pasekmės tarpasmeniniams santykiams bei asmens privatumui“, *Visuomenės sveikata*, 3 (70), p. 29–38.

Perkins R. C., Howell C. J., Dodge C. E., Burruss G. W., Maimon D. 2020, „Malicious spam distribution: A routine activities approach“, *Deviant Behavior*, p. 1–17.

Popović S. 2018, „Child sexual abuse news: A systematic review of content analysis studies“, *Journal of Child Sexual Abuse*, 27 (7), p. 752–777.

Powell A., Henry N. 2018, „Policing technology-facilitated sexual violence against adult victims: Police and service sector perspectives“, *Policing and Society*, 28 (3), p. 291–307.

Reep-van den Bergh C. M. M., Junger M. 2018, „Victims of cybercrime in Europe: a review of victim surveys“, *Crime Science*, 7 (1), p. 1–15.

Rekis D., Rekienė S. 2016, „Lietuvos interneto piratų subkultūra socialinio dalyvavimo aspektu: *Torrent* tipo svetainės atvejis“, *Tiltai*, 3, p. 99–113.

Reyns B. W. 2015, „A routine activity perspective on online victimisation: Results from the Canadian General Social Survey“, *Journal of Financial Crime*, 22 (4), p. 396–411.

Ron M., Fuertes W., Bonilla M., Toulkeridis T., Diaz J. 2018, „Cybercrime in Ecuador, an exploration, which allows to define national cybersecurity policies“, *2018 13th Iberian Conference on Information Systems and Technologies (CISTI)*, p. 1–7.

Ruškus J., Žvirdauskas D., Kačenauskaitė V. 2014, „Interneto vartojimo grėsmių suvokimas ir patirtis: moksleivių viktimizacijos prielaidos“, *Socialinis darbas*, 9 (2), p. 70–78.

Shanmugam B., Azam S., Yeo K. C., Jose J., Kannoorpatti K. 2017, „A critical review of Bitcoins usage by cybercriminals“, *2017 International Conference on Computer Communication and Informatics (ICCCI)*, p. 1–7.

Šidlauskienė J. 2019, *Teisės į privatų gyvenimą pažeidimas anoniminiais komentarais: interneto tinklalapių valdytojų civilinės atsakomybės taikymą pateisinantys kriterijai*. Vilnius: Mykolo Romerio universitetas.

Skališienė R., Žukauskienė L. 2018, „Paauglių mergaičių atsakingumo dalyvaujant interneto socialiniuose tinkluose ugdymo galimybės vaikų dienos centruose“, *Pedagogika: mokslo darbai*, 129 (1), p. 250–267.

Stankevičiūtė S. 2020, *Asmens duomenų rinkimo elektroninėje erdvėje teisėsaugos ir žvalgybos tikslais reglamentavimas*. Vilnius: Mykolo Romerio universitetas.

Steel C. M. S., Newman E., O'Rourke S., Quayle E. 2020, „An integrative review of historical technology and countermeasure usage trends in online child sexual exploitation material offenders“, *Forensic Science International: Digital Investigation*, 33, p. 1–17.

Stratton G., Powell A., Cameron R. 2017, „Crime and justice in digital society: Towards a 'digital criminology'?“, *International Journal for Crime, Justice and Social Democracy*, 6 (2), p. 17–33.

Šidlauskas A., Ungurytė-Ragauskienė S. 2020, „Iššūkiai kibernetiniam saugumui: socialinė inžinerija institucinio izomorfizmo kontekste“, *Visuomenės saugumas ir viešoji tvarka*, 25, p. 389–405.

Štitilis D., Laurinaitis M. 2009, „Tapatybės vagystė elektroninėje erdvėje“, *Informacijos mokslai*, 50, p. 240–247.

Štitilis D., Laurinaitis M. 2017, „Treatment of biometrically processed personal data: Problem of uniform practice under EU personal data protection law“, *Computer Law & Security Review*, 33, p. 618–628.

Štitilis D., Pakutinskas P., Laurinaitis M., Dauparaitė I. 2011, *Tapatybės vagystė elektroninėje erdvėje: socialiniai, elektroninio verslo ir teisinio reguliavimo aspektai.* Vilnius: Mykolo Romerio universitetas.

Štitilis D., Pakutinskas P., Laurinaitis M., Malinauskaitė-Van De Castel I. 2017a, *Rekomendacijos Lietuvos Respublikos kibernetinio saugumo įstatymui*. Vilnius: Mykolo Romerio universitetas.

Tauri J. M. 2018, „The master's tools will never dismantle the master's house: An Indigenous critique of criminology“, *Journal of Global Indigeneity*, 3 (1), p. 1–18.

Tcherni M., Davies A., Lopes G., Lizotte A. 2016, „The dark figure of online property crime: Is cyberspace hiding a crime wave?“, *Justice Quarterly*, 33 (5), p. 890–911.

Tyrowicz J., Krawczyk M., Hardy W. 2020, „Friends or foes? A meta-analysis of the relationship between "online piracy" and the sales of cultural goods“, *Information Economics and Policy*, 53, 100879.

Valeckienė D. 2011, „Elektroninių patyčių tarp 5–12 klasių mokinių prevencijos gairės mokykloje: mokinių ir pedagogų požiūris“, *Tiltai*, 3, p. 345–356.

Valickienė R. P., Raižienė S., Žukauskienė R. 2009, „Elektroninių patyčių paplitimas tarp Klaipėdos apskrities vyresniųjų klasių moksleivių“, *Socialinis darbas*, 8 (2), p. 114–121.

Van de Weijer S. G. A., Leukfeldt R., Bernasco W. 2019, „Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking“, *European Journal of Criminology*, 16 (4), p. 486–508.

Van der Wagen W., Pieters W. 2020, „The hybrid victim: Re-conceptualizing high-tech cyber victimization through actor-network theory“, *European Journal of Criminology*, 17 (4), p. 480–497.

Venčkauskas A., Damaševičius R., Jusas V., Toldinas J., Rudzika D., Drėgvaitė G. 2015, „A review of cyber-crime in Internet of Things: Technologies, investigation methods and digital forensics“, *International Journal of Engineering Sciences & Research Technology*, 4 (10), p. 460–477.

Virtanen S. M. 2017, „Fear of cybercrime in Europe: Examining the effects of victimization and vulnerabilities“, *Psychiatry, Psychology and Law*, 24 (3), p. 323–338.

Walker K., Sleath E. 2017, „A systematic review of the current knowledge regarding revenge pornography and non-consensual sharing of sexually explicit media“, *Aggression and Violent Behavior*, 36, p. 9–24.

Wall D. S. 2001, „Cybercrimes and the Internet“, in D. S. Wall (ed.), *Crime and the Internet*. London: Routledge.

Wall D. S. 2008a. „Cybercrime and the culture of fear: Social science fiction (s) and the production of knowledge about cybercrime“, *Information, Communication, and Society*, 11 (6), p. 861–884.

Wall D. S. 2008b. „Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime“, *International Review of Law, Computers, and Technology*, 22(1–2), p. 45–63.

Wall D. S. 2015, „Dis-organised crime: Towards a distributed model of the organization of cybercrime“, *The European Review of Organised Crime*, 2 (2), p. 71–90.

Wall D. S. 2017, „Crime, security and information communication technologies: The changing cybersecurity threat landscape and its implications for regulation and policing“, in R. Brownsword, E. Scotford, K. Yeung (eds.), *The Oxford Handbook on the Law and Regulation of Technology*. Oxford: Oxford University Press.

Wang J., Shan Z., Gupta M., Rao H. R. 2019, „A longitudinal study of unauthorized access attempts on information systems: The role of opportunity contexts“, *MIS Quarterly*, 43 (2), p. 601–622.

Wei R., Liu X. S., Liu X. 2019, „Examining the perceptual and behavioral effects of mobile internet fraud: A social network approach“, *Telematics and Informatics*, 41, p. 103–113.

Westerlund M. 2019, „The emergence of deepfake technology: A review“, *Technology Innovation Management Review*, 9 (11), p. 39–52.

Whitty M. T. 2018, „Do you love me? Psychological characteristics of romance scam victims“, *Cyberpsychology, Behavior, and Social Networking*, 21 (2), p. 105–109.

Whitty M. T., Ng M. 2017, *Literature review for UNDERWARE: UNDERstanding West African culture to pRevent cybercrimEs,* Report for the National Cyber Security Centre as part of a group of studies funded in the Research Institute in Science of Cyber Security. Melbourne: University of Melbourne.

Wood M. A. 2017, „Antisocial media and algorithmic deviancy amplification: Analysing the id of Facebook's technological unconscious", *Theoretical Criminology*, 21 (2), p. 168–185.

Wu Y., Ngai E. W. T., Wu P., Wu C. 2020, „Fake online reviews: Literature review, synthesis, and directions for future research", *Decision Support Systems*, 132, p. 1–15.

Žibėnienė G., Brasienė D. 2013, „Naudojimasis internetu, internetiniais socialiniais tinklais ir galimai patiriamos grėsmės: mokinių nuomonė", *Socialinės technologijos*, 3 (1), p. 53–67.