

Socialiniai tyrimai apie elektroninius nusikaltimus: globali paradigų takoskyra bei jos raiška Lietuvoje

Maryja Šupa

Vilnius universitetas
Vilnius University
El. paštas maryja.supa@fsf.vu.lt
ORCID iD: <https://orcid.org/0000-0003-2984-5384>

Santrauka. Straipsnio tikslas – nustatyti, kokiomis pagrindinėmis teorinėmis ir metodologinėmis pozicijomis remiasi tyrėjai, atlikdami socialinius tyrimus apie elektroninius nusikaltimus. Temos aktualumą lemia tai, kad dauguma šios srities apžvalgų apsiriboja vienos arba kelių siauresnių teorinių prieigų pristatymu, todėl trūksta sisteminės viso tyrimų lauko analizės. Nustatyta, kad dvi pagrindinės paradigmos elektroninių nusikaltimų tyrimuose – *neopozityvistinė*, kuri telkia dėmesį į individualius veiksnius ir remiasi kiekybine metodologija, bei *kritinė-kultūrinė*, kuri telkia dėmesį į platesnius socialinius veiksnius ir teikia pirmenybę kokybinės metodologijos taikymui tyrimuose. Lietuvoje tyrimai apie elektroninius nusikaltimus kaip socialines praktikas atliekami retai ir fragmentiška, jie kol kas nepateikia išsamesnių teorinių debatų ir metodologinės įvairovės.

Pagrindiniai žodžiai: elektroniniai nusikaltimai, kriminologija, socialinių tyrimų metodologija, technologijų diskursai, interneto tyrimai.

Social Research about Online Crime: Key Global Paradigms and the State of Research in Lithuania

Summary. This paper analyses key differences between two paradigms dominant in social research on online crime: the more prevalent neopositivist paradigm and the more recent critical–cultural paradigm. Based on an extensive analysis of up-to-date literature, the key paradigmatic oppositions in online crime research encompass: 1) in neopositivism, the conceptual separation of technological and social practices, the reliance on rational choice approaches in theory, especially routine activity theory, and the tendency towards quantitative research methods; 2) in the critical–cultural paradigm, a complex and context-dependent approach to the technosocial as a continuum, theoretical roots in critical theory, cultural criminology, actor-network theory, and feminist theory, and the emphasis on qualitative methods. The field of online crime research in Lithuania is dominated by legal studies, while social research is rare and fragmented. The existing social research of online crime in Lithuania lacks a solid theoretical basis in either paradigm. Methodologically, there are examples of both quantitative (surveys, analysis of registered crime statistics) and qualitative studies (interviews, discussion groups, content analysis). However, most of the studies are small-scale and their scarcity makes it nearly impossible to evaluate the strengths, weaknesses, and complimentary potential of each approach in the specific national and regional context.

Keywords: cybercrime, online crime, criminological theory, social research methodology, technology discourses, online research.

Received: 20/01/2020. Accepted: 28/07/2020

Copyright © 2021 Maryja Šupa. Published by Vilnius University Press. This is an Open Access article distributed under the terms of the [Creative Commons Attribution Licence](https://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Įvadas

Straipsnio aktualumas. Elektroninio saugumo ir informacinių technologijų taikymo srityje pagrindinė mokslinė perspektyva, formuojanti problematiką, žodyną, sąvokų konceptualizavimą ir tyrimų metodus, yra techninė-inžinerinė, apimanti telekomunikacijų ir informatikos inžineriją, ją veja teisinė perspektyva (Yar, 2018, p. 119–120). O socialinių tyrimų apie elektroninius nusikaltimus trūksta (Diamond, Bachmann, 2015; Maimon, Louderback, 2019, p. 192) kriminologijoje ir kitose socialinių mokslų disciplinose – deviacijų sociologijoje, komunikacijos moksluose, medijų studijose, socialinėse technologijų studijose. Tai yra **reikšminga žinių spraga**, atsižvelgiant į elektroninių nusikaltimų kaip socialinio reiškinių paplitimą, globalumą, įsitvirtinimą šiuolaikinėse visuomenėse, ekonominių ir politinių poveikį.

Socialinių mokslų disciplinoms būtina **įveikti atsilikimą** nuo inžinerinio ir teisinio diskurso – jį iliustruoja dažnai pasikartojanti situacija, kai socialinių mokslų atstovai savo tyrimuose naujomis vadina technologijas, kurios 20 ir daugiau metų yra masinio naudojimo rinkoje (Lee, 2018, p. 238) ir nebegali būti laikomos naujove nei technologiniu, nei socialiniu požiūriu. Skirtingose disciplinose ir veiklos sferose – akademinuose tyrimuose, politikos formavimo procese, verslo įmonėse, teisėsaugoje – technologinių arba socialinių žinių spragos egzistuoja skirtingose nišose (Broadhead, 2018, p. 1180), kurios lemia **poreikį konsoliduoti** skirtingų sričių žinias, jas plėsti bei gilinti, stiprinti tarpdalykinį ir tarpsektorinį bendradarbiavimą, tiriant elektroninių nusikaltimų reiškinių.

Nagrinėjama problematika. Socialinių tyrimų apie elektroninius nusikaltimus laukas socialinių mokslų disciplinose yra **fragmentuotas**. Pirma, tebevyksta ginčai dėl tinkamo internetinės veiklos – tiek kasdienės, tiek deviantinės bei nusikalstamos – konceptualizavimo. Antra, lauko susiskaldymą atspindi naujausi apžvalginiai kriminologų straipsniai, kurių autoriai iškelia tikslą susisteminti visas lauko žinias, tačiau publikacijose paliečia tik dalį pagrindinių taikomų teorinių ir metodinių priėgų, o empiriniuose tyrimuose kiekybinės ir kokybinės prieigos refleksija, jų derinimas pasitaiko retai. Kriminologijoje (kuri šios temos kontekste svarbi kaip *a priori* į nusikaltimus nukreipta mokslinė disciplina) pagrindinė takoskyra brėžiama tarp neopozityvistinių ir kritinių-kultūrinių šios srities tyrimų. Jie remiasi skirtingais, dažnai vienas kitam priešpriešinamais teoriniais ir metodologiniais sprendimais. Panaši skirtis būdinga ir kitoms šią temą nagrinėjančioms disciplinoms.

Kviesdami įveikti minėtas spragas, tyrėjai pabrėžia **paradigmų derinimo ir tarpdalykinių tyrimų svarbą**, įtraukiant sociologijos, informatikos, politikos mokslų, žurnalistikos, medijų ir kultūros studijų tyrėjus (Stratton, Powell, Cameron, 2017, p. 27). Bendradarbiavimas tarp skirtingų teorinių ir metodologinių krypčių tyrėjų, teorinių perspektyvų ir metodų derinimas prisidėtų prie geresnio supratimo, kokia nelegali veikla įmanoma, pasitelkiant informacijos ir komunikacijos technologijas, kaip ji vyksta, kaip ji kinta, įsitvirtinant technologinėms inovacijoms, kaip turimą patirtį pritaikyti naujoms, ateityje įsitvirtinsiančioms technologijoms, kaip besikeičiant technologijoms veikia normų kūrimas ir socialinė kontrolė.

Straipsnio tikslas. Atsižvelgiant į minėtas problemas, šio straipsnio tikslas – apibrėžti, kokios egzistuoja teorinės ir metodologinės takoskyros elektroninių nusikaltimų

socialiniuose tyrimuose, ir apibrėžti lauką kaip visumą. Šiam tikslui įgyvendinti keliami uždaviniai:

- 1) **Išskirti ir kritiškai įvertinti pagrindinius prieštaravimus** šiuolaikinių elektroninių nusikaltimų mokslinių tyrimų lauke, apibendrinti ir palyginti pagrindines **teorines ir metodines priegas**, atstovaujančias neopozityvistinei bei kritinei-kultūrinei paradigoms. Šis tikslas svarbus norint suvokti tyrimo lauką kaip visumą, nustatyti skirtingų paradigų privalumus ir trūkumus, santykį tarp jų, apibrėžti būsimų empirinių tyrimų aktualumą, paradigų derinimo potencialą ir galimybes įveikti lauko fragmentiškumą.
- 2) **Įvertinti Lietuvoje atliekamų socialinių tyrimų apie elektroninius nusikaltimus būklę** – kokią teorinę ir metodinę įvairovę atspindi atliekamos studijos, lyginant su globaliu kontekstu? Kur ir kaip turėtų judėti socialiniai tyrimai apie elektroninius nusikaltimus Lietuvoje?

Straipsnyje susitelkiama į specifinį elektroninių nusikaltimų socialinių tyrimų lauką, atspindintį, visų pirma, kriminologijos, kaip su nusikaltimais tiesiogiai susijusios disciplinos, perspektyvą, kurios įžvalgos tinka ir kitoms disciplinoms – deviacijų sociologijai, komunikacijos ir informacijos mokslams, medijų studijoms, socialinėms technologijų studijoms. Į iškeltus klausimus atsakoma analizuojant naujausią pasaulinę literatūrą apie įvairius elektroninių nusikaltimų aspektus, taip pat pagrindinius socialinės srities elektroninių nusikaltimų tyrimus, atliktus Lietuvoje. Siekiant įgyvendinti straipsnio tikslus, pagrindinis dėmesys buvo sutelktas į **teorinių prielaidų, argumentų, metodologinių nuostatų įvertinimą ir palyginimą**, teorinės įvairovės apimtį ir aprėptį, o ne kiekybines charakteristikas. Tai nėra į empirinės metodologijos taikymą orientuotas darbas taip pat ir dėl tos priežasties, kad dauguma aptariamų šaltinių – naujausios tarptautinės šio lauko publikacijos, kurių įprasta sisteminė analizė paprasčiausia neužčiuoptų, nes jos apima per daug skirtingų disciplinų ir sričių, naudojančių labai skirtingas reiškinių operacionalizavimo nomenklatūras bei vartojančių skirtingus pagrindinius terminus.

Elektroninių nusikaltimų kaip tyrimo objekto konceptualizavimo prielaidos

Apibrėždami, konceptualizuodami, o empiriniuose tyrimuose – operacionalizuodami elektroninius nusikaltimus kaip socialinio tyrimo objektą, tyrėjai remiasi skirtingomis pamatinėmis prielaidomis apie šį reiškinį, kurių prieštaravimai kelia visam laukui bendras problemas, nepriklausomai nuo tyrėjų pasirenkamos teorinės ir metodologinės priegios konkrečiame tyrime. Jie kyla iš pamatinės technologijų filosofijos bei technologijų sociologijos diskusijos apie tai, kokius interpretacinius rėmus suteikti informacijos ir komunikacijos įrankiams bei šiuolaikinėms masinėms medijoms: kas būdinga internetinei (elektroninei, kibernetinei, virtualiai) ir fizinei (gyvai, realiai, trimatei) tikrovei? Koks jų tarpusavio santykis ir kokia tarp jų skirtis? Nuo pasirinktos pozicijos priklauso nuostatos kitais klausimais – kaip konceptualizuoti technologinę veiklą, kaip vertinti tikrą arba tariamą technologijomis paremtų socialinių praktikų naujumą, kaip pagrįsti vienos ar kitos mokslinės teorijos pasitelkimą joms paaiškinti?

Internetinės ir fizinės tikrovės perskyra problemiška. Vieni tyrėjai užima supaprastintą poziciją – vienareikšmiškai teigia arba paneigia šios perskyros egzistavimą. Pirmieji palaiko požiūrį, kad tai kardinaliai atskiri vienas nuo kito reiškiniai, antri tokių skirtumų nenagrinėja iš viso. Trečia pozicija vertina internetinę ir fizinę tikrovę kaip kontinuumą. Ji leidžia svarstyti, kokiais būdais socialinės praktikos skirtingu mastu įtraukia virtualią ir realią dimensiją, kaip priklausomai nuo situacijos kinta socialinių veikėjų suvokimas apie elektroninės ir trimatės tikrovės santykį, jų įsitraukimas į vieną arba abi bendrabūvio formas, pasiekiamumas, vienos ar kitos tikrovės reikšmė skirtingose socialinėse praktikose.

Griežtas elektroninės ir fizinės tikrovės atskyrimas dažnai išreiškiamas pasitelkiant erdvės metaforą: egzistuoja trimatė fizinė erdvė ir nuo jos atskira, kitokia, kitoniška internetinė erdvė. Remiantis tokiu požiūriu, šios erdvės yra aiškiai atskirtos, joms būdingos skirtingos savybės, veikimo taisyklės, poveikis individams. Individai vienu metu priklauso tik vienai iš šių erdvių, veikdami tarsi peržengia iš vienos į kitą. Iš esmės mokslinėje fantastikoje įtvirtinta kibernetinės erdvės (angl. *cyberspace*) samprata migravo į viešąją vaizduotę ir paskatino atsirasti daugybę susijusių sąvokų (žr. Strate, 1999) – anglų kalboje su dėmeniu *cyber*, lietuvių kalboje – su būdvardžiu *kibernetinis*. Tarp tokių naujadarų yra ir sąvoka *kibernetiniai nusikaltimai* – nusikaltimai, vykstantys, tęsiant erdvinę metaforą, kitokioje, kitokioms taisyklėms paklūstančioje erdvėje.

Šio požiūrio kritikai įvardija dvi jame slypinčias konceptualines klaidas.

Pirma, jeigu internetinė tikrovė interpretuojama kaip visiškai atskira nuo fizinės tikrovės, kyla rizika neatsižvelgti į tai, kaip joje skleidžiasi jau egzistuojančios, įsitvirtinusios socialinės praktikos, kaip masinio vartojimo rinkoje informacijos ir komunikacijos technologijos tampa ne atskira veikla, o nuolatiniu kasdienio gyvenimo pratęsimu, netekusiu to unikalumo ir išskirtinumo, kuriuo pasižymėjo prieš 20 ir daugiau metų. Lyginant su informacijos ir komunikacijos technologijų įsitvirtinimo pradžia, stipriai transformavimosi globalios technologijų naudojimo socialinės praktikos. Globaliai vykdomi elektroniniai nusikaltimai susiduria su neišvengiamai lokalizuotomis aukų bei teisėsaugos institucijų praktikomis (Wall, 2017, p. 4). O socialinė tikrovė gaubia abi sferas – tiek fizinę erdvę, tiek internetą.

Antra, būdvardis „kibernetinis“ (lietuvių kalboje taip pat vartojami sinonimai „elektroninis“, „skaitmeninis“, žr. Stunžinas, 2017, p. 153) tarsi subendrina visas veiklas, susijusias su informacijos ir komunikacijos technologijomis. Jis akcentuoja technologinį lygmenį, o ne socialines praktikas, taigi, neatskleidžia internetinės veiklos praktikų ir įrankių įvairovės, jų susisaistymo su šiuolaikinių visuomenių kasdieniu gyvenimu (Stratton, Powell, Cameron, 2017, p. 22), dabartyje patiriamų transformacijų, istorinės kaitos ir globalios įvairovės.

Būtent ši problema būdinga *elektroninio* (kibernetinio, skaitmeninio) nusikaltimo terminui, kuris iki šiol dažnai tebevartojamas socialiniuose tyrimuose. Jeigu tyrėjai nesilaiko deramos kritinės distancijos, šios sąvokos vartojimas gali užkirsti kelią tyrėjams užduoti ir atsakyti į esminius su šia tyrimų sritimi susijusius klausimus ir analizuoti, kaip informacijos ir komunikacijos technologijų naudojimas nusikaltimams susijęs su platesniais šiuolaikiniais politiniais, ekonominiais ir socialiniais kontekstais.

Naujesnės konceptualizacijos remiasi požiūriu, kad internetinė ir fizinė tikrovė sudaro

vieną bendrą *technosocialinę* sistemą arba kontinuumą. Joje vykstančios praktikos suprantamos kaip *technosocialinės* – įgalintos technologijų, bet paremtos socialinėmis sąveikomis tarp individų ir jų grupių. Anot šio požiūrio šalininkų (kriminologijos teoriniame kontekste pirmoji autorė, pateikusi išsamų šios pozicijos pagrindimą, buvo Brown, 2006), būtina atsisakyti griežtos skirties tarp internetinės ir fizinės tikrovės – t. y. „nusikaltimus, deviacijas ir teisingumą konceptualizuoti kaip vis labiau *technosocialines praktikas*, vykstančias *skaitmeninėje visuomenėje*“ (Stratton, Powell, Cameron, 2017, p. 24). Skaitmeninės visuomenės samprata padeda įveikti internetinės ir fizinės tikrovės perskyrą, nes įvietina technologijas socialiniuose santykiuose (o ne vienoje ar kitoje šių santykių skleidimosi erdvėje) ir suteikia galimybę tirti „reprodukuojamus, reinstitucionalizuojamus, reliacinius, kultūrinius, afektinius, politinius, socialinius-struktūrinius nusikaltimų ir teisingumo aspektus, kuriems potencialiai gali būti priešinamasi pažįstamais ir nepažįstamais veikimo būdais“ (Stratton, Powell, Cameron, 2017, p. 24).

Oponuodami tiems, kas įvardija technologijas esant naujų, iki šiol nežinomų nusikaltimų šaltinių, technosocialinių praktikų koncepcijos šalininkai ragina atsisakyti viena-reikšmės perskyros tarp virtualių ir realių, senų ir naujų nusikaltimų: „visi nusikaltimai įvyksta tinkluose, kurie palaiko skirtingą pusiausvyrą tarp elektroninės ir fizinės tikrovės“ (Stratton, Powell, Cameron, 2017, p. 22). O šiame lauke dirbantys tyrėjai turi nagrinėti sankirtas tarp „biologijos ir technologijų, gamtos ir visuomenės, objektų ir agentų, dirbtinių ir žmogiškų veikėjų“ (Brown, cit. iš: Stratton, Powell, Cameron, 2017, p. 22). Taip apibrėžiamas tyrimų laukas apima gerokai daugiau už tradicinius elektroninių nusikaltimų socialinius tyrimus – technologinius nusikaltimus plačiaja prasme.

Technosocialinis konceptualizavimas padeda įveikti ir kitą susijusią problemą: ar elektroniniai nusikaltimai yra kokybiškai naujos praktikos, ar naują formą įgavę seni nusikaltimai? Ar elektroniniams nusikaltimams aiškinti tinka egzistuojančios kriminologijos, deviacijų sociologijos, komunikacijos mokslų teorijos, ar būtina kurti visiškai naujas teorijas? Remiantis technosocialiniu požiūriu, vienareikšmiško atsakymo į šiuos klausimus negali būti ir kiekvienoje tyrimo situacijoje reikia iš naujo atsakyti į specifinius, prie temos pritaikytus klausimus: kas yra nauja, o kas tęsia egzistuojančias praktikas konkretaus elektroninio nusikaltimo atveju? Kokios technosocialinės praktikos būdingos pažeidėjams, aukoms, teisės saugos institucijoms ir kiek konkrečiu atveju jas lemia technologijų naudojimas, o kiek – gyvos sąveikos tarp proceso dalyvių? Kokius klasikinių teorijų aspektus tinka pritaikyti interpretuojant konkrečius elektroninių nusikaltimų atvejus?

Įvertinus konceptualiuosius rėmus, kuriuose atliekami tyrimai, būtina kritiškai apibrėžti elektroninio nusikaltimo sąvoką. Šiuolaikiniai tyrėjai elektroninius nusikaltimus paprastai skirsto į dvi pagrindines kategorijas, priklausomai nuo to, koks yra technologijų vaidmuo, vykdant nusikaltimą. Šią tipologiją pasiūlė Wallas (žr. Wall, 2001), vėliau ją papildė (Wall, 2017, p. 8). Ją dažnai pasitelkia kiti autoriai, apibrėždami savo tyrimo objektą ir jo ribas (žr. Maimon, Louderback, 2019, p. 192; Stratton, Powell, Cameron, 2017, p. 20):

1. Nusikaltimai, kuriuose informacijos ir komunikacijos *technologijos yra nusikaltimo taikiny*s (angl. *cyber-dependent crime, computer-dependent crime*). Tai nusikaltimai, kurie gali įvykti tik naudojant informacijos ir komunikacijos technologijas (Wall, 2017, p. 8). Wallas šiai kategorijai priskiria elektroninius įsilaužimus (angl.

cyber-tresspass), kuriuos kiti autoriai tiksliau įvardija kaip „neautorizuota prieiga prie kompiuterinių sistemų, tinklų arba duomenų šaltinių“ (Stratton, Powell, Cameron, 2017, p. 20). Nors teisiškai vien neautorizuota prieiga prie kompiuterinės sistemos gali būti traktuojama kaip nusikaltimas, praktiškai pažeidėjai paprastai šią veiklą įvykdo turėdami papildomų tikslų – keisti sistemą, kopijuoti arba naikinti duomenis, atlikti kitus, jau su technologijomis nesusijusius nusikaltimus. Be neautorizuotos prieigos, kiti galimi šios kategorijos pažeidimai – išorinis sistemų veiklos trikdyimas, fizinės infrastruktūros pažeidimai.

2. Nusikaltimai, kuriuose informacijos ir komunikacijos *technologijos yra nusikaltimo įrankis* (angl. *cyber-assisted crime, computer-assisted crime*). Tai nusikaltimai, kurie vyko ir vyksta nepriklausomai nuo technologijų (Wall, 2017, p. 8), o technologijos gali tik keisti jų formą. Wallas šioje kategorijoje įvardijo tris nusikaltimų tipus – sukčiavimai ir vagystės, pornografija, internetinis smurtas. Nors neatnaujintą, pradinę šio skirstymo versiją mokslininkai vis dar pasitelkia aptardami bendrą elektroninių nusikaltimų apibrėžimą (pavyzdžiui, Holt, Bossler, 2014), ji atspindi specifinį ir jau pasikeitusį 2000 metais vyravusį technologinį kontekstą. Tikslinant šią kategoriją, viena iš galimų prieigų – technologijas kaip nusikaltimų įrankį skirstyti pagal tai, kas yra pagrindinis pažeidimo taikinytis, kokie pažeidėjų tikslai:

- a) Finansiniai ir investiciniai ištekliai – vagystės iš atsiskaitymo kortelių ir banko sąskaitų, vagystės iš bankų ir kitų finansinių institucijų, skaitmeninių vertybių (pavyzdžiui, internetinio žaidimo artefaktų) vagystės, sukčiavimas, nelegali prekyba ir mokesčių vengimas globaliose rinkose, prekyba juodosiose rinkose internete, vagystės ir machinacijos kriptovaliutų rinkoje.
- b) Skaitmeninis turinys – intelektinės nuosavybės teisių pažeidimas (neteisėtas kūrinių vartojimas, neteisėtas kūrinių platinimas su arba be pasipelnymo), viešosios informacijos sklaidos pažeidimai (probleminis pavyzdys – ne visada akivaizdi perskyra tarp satyros ir melagingų naujienų), pornografinis turinys arba tam tikros jo formos (jų naudojimas, saugojimas, platinimas, vaidybos ir kvazirealizmo problema), nepilnamečių seksualinį išnaudojimą vaizduojantis turinys.
- c) Žmogus arba socialinė grupė – nepageidaujami elektroniniai laišakai (siunčiami ne vien turint tikslą sukčiauti arba platinti kenkėjišką programinę įrangą), sekimas ir persekiojimas (angl. *cyberstalking*), tapatybės pasisavinimas, internetinės patyčios ir neapykantos nusikaltimai, asmeninių duomenų nutekinimas ir viešinimas.

Kartais išskiriama trečia elektroninių nusikaltimų kategorija – nusikaltimai, kuriuose technologijos įgalina nusikaltimą (angl. *cyber-enabled crime, computer-enabled crime*). Tai nusikaltimai, kuriems įvykti technologijos nėra būtinos, bet technologijų panaudojimas kiekybiškai ir kokybiškai paveikia šių nusikaltimų poveikį ir mastą (Wall, 2017, p. 8). Tačiau toks atskyrimas yra abejotinas, nes suponuoja, kad kai pažeidėjai ima pasitelkti naujas technologijas nusikaltimams vykdyti, nusikaltimų mastas ir poveikis išauga tik kai kuriais atvejais. Prasmingiau analizuoti *technologijų, kaip nusikaltimo įrankio, raidos*

stadijas: iš pradžių jų poveikis konkretaus nusikaltimo atveju yra retas, nišinis kaip ir pati technologija, o vėliau, technologijoms iš ankstyvųjų vartotojų tarpo plintant į masinio naudojimo rinką, jie įgauna galimybę, Wallo terminais, įgalinti pažeidėją veikti globaliu mastu, paveikti ne tik auką, kuriai sukelta žala, bet ir kitus socialinius, ekonominius bei politinius procesus.

Apibendrinant galima teigti, kad esminė elektroninių nusikaltimų konceptualizavimo problema – tinkamų rėmų suteikimas. Kol vieni autoriai laikosi vienpusio požiūrio, kad internetinė ir fizinė tikrovė – dvi skirtingos erdvių formos, arba visiškai nesigilina į šią perskyrą, kiti autoriai siūlo konceptualizuoti individų veiklą internete ir fizinėje erdvėje kaip *technosocialines praktikas*. Pastarasis požiūris akcentuoja, kad technologijų naudojimas – tai, visų pirma, socialinės praktikos, kurios turi būti nagrinėjamos kaip sudėtingi reiškiniai, o internetinės ir fizinės tikrovės santykis yra daugiareikšmis, kintantis ir kompleksinis.

Taip pat problemiška ir elektroninių nusikaltimų samprata, kuri pernelyg supaprastina jai priskiriamas veiklas ir į pirmą vietą iškelia technologinį, o ne socialinį šių nusikaltimų lygmenį. Galima tiksliau apibrėžti, kad yra bendras reiškinys, nepriklausantis nuo konkrečios technologijų srities – technologiniai nusikaltimai, kuriuos galima skirstyti į dvi kategorijas – technologijos kaip nusikaltimų taikynys ir technologijos kaip nusikaltimų įrankis. Tokio skirstymo pagrindu galima konkretizuoti veiklas, atliekamas su konkrečios srities technologijomis. Pavyzdžiui, informacijos ir komunikacijos technologijų atveju atskirti veiklas, kurių metu kompiuteriai ir kompiuteriniai tinklai yra *nusikaltimų taikynys*, nuo veiklų, kurių metu technologijos naudojamos kaip *nusikaltimų įrankis*. Technologinių nusikaltimų samprata, savo ruožtu, leidžia į tyrimų matymo lauką įtraukti ne tik šiuo metu išsivysčiusią technologijų sritį – informacijos ir komunikacijos technologijas, bet ir naujusias technologijas (angl. *emerging technologies*) – šiuo metu plėtojamas, o masinį vartojimą pasiekiančias per artimiausius 5 ar 10 metų, pavyzdžiui, biotechnologijas ar išmaniąsias transporto sistemas.

Teorinės ir metodinės paradigmos socialiniuose tyrimuose apie elektroninius nusikaltimus

Pagrindiniai teoriniai ir metodologiniai uždaviniai, kylantys tiriant elektroninius nusikaltimus – pagrįstas ir tikslus sąvokų konceptualizavimas ir operacionalizavimas (Holtfreter, Meyers, 2015, p. 56), nuolatinis pokyčių ir transformacijų įtraukimas į egzistuojančias teorijas, metodų pritaikymas tiriant kintančias socialines praktikas. Dalis elektroninių nusikaltimų socialinių tyrimų problemų yra tos pačios kaip tiriant baltųjų apykaklių nusikaltimus, su kuriais jie dažnai lyginami: trūksta aiškaus elektroninių nusikaltimų ribų apibrėžimo, riboti duomenų apie pažeidėjus ir aukas šaltiniai, teisinio reguliavimo skirtumai tarp valstybių, įstatymų ir vykstančių veiklų neatitikimai, ribotas atraminių tyrimų skaičius, konkurencija dėl dėmesio su emociškai paveikesniais smurtiniais nusikaltimais, taip pat – transnacionalinis elektroninių nusikaltimų pobūdis ir neerdvinė raiška (Holtfreter, Meyers, 2015, p. 57).

Elektroninių nusikaltimų socialiniuose tyrimuose stebima teorinių ir metodologinių priegų įvairovė (Holt, Bossler, 2014, p. 21). Kriminologinėje literatūroje jas jungia dvi

pagrindinės paradigmos, apimančios skirtingas teorines ir metodologines nuostatas. Dominuojančia laikoma neopozityvistinė teorinė ir kiekybinė tiriamoji paradigma, o alternatyvioji, ją išplečianti – kritinę arba kultūrinę teorinę prieigą ir kokybinę metodologiją palaikanti paradigma.

Neopozityvistinė teorinė paradigma aptinkama psichologiniuose ir kriminologiniuose elektroninių nusikaltimų tyrimuose, kurių tyrėjai dažniau remiasi metodologiniu individualizmu (Yar, 2018, p. 120–121). Metodologinis individualizmas lemia, kad pažeidėjai ir aukos laikomi racionaliai pasirenkančiais, nepriklausomais veikėjais, kurių apsisprendimas įvykdyti nusikaltimą arba tikimybė tapti nusikaltimo auka priklauso nuo jų pačių asmeninių apsisprendimų ir atliktų veiksmų, už kuriuos individai laikomi visapusiškai atsakingais. Socialinio, politinio, kultūrinio konteksto įtaka tokiuose tyrimuose dažnai lieka kokybiškai neatskleista, o kiekybiškai – menkai operacionalizuota.

Teorijos, kurias vienija racionalaus pasirinkimo prielaidos – bendroji nusikaltimų teorija, socialinio išmokymo, kontrolės, atgrasymo teorijos (Maimon, Louderback, 2019, p. 196), dažniausiai taikoma – rutininių veiksmų teorija (Maimon, Louderback, 2019, p. 201; Yar, 2018, p. 121). Pastaroji redukuoja elektroninį nusikaltimą į jo racionalų arba ekonominį motyvą (Yar, 2018, p. 121–122), o internetą traktuoja kaip atskirą erdvę, kuri padidina galimybes motyvuotiems pažeidėjams sutikti tinkamas aukas (Lee, 2018, p. 231). Neopozityvistinės paradigmos atstovai teigia, kad XX a. antrosios pusės racionalaus pasirinkimo kriminologijos teorijos *gali* būti pritaikomos elektroniniams nusikaltimams, jos sukuria pagrindą toliau pagrįstai kurti situacinės prevencijos priemones, siekiant užkirsti kelią nusikaltimams (Holtfreter, Meyers, 2015, p. 56–57). Tačiau šios teorijos pritaikymui būdingi apribojimai, susiję su interneto konceptualizavimu kaip atskirai veikiančios erdvės arba kaip tik atsisakymas deramai atsižvelgti į skirtumus tarp interneto ir fizinės tikrovės. Oponentai teigia, kad šios teorijos silpnai paaiškina elektroninius nusikaltimus, nes originalios jų versijos pabrėžia būtent aplinkos ir fizinių veiksnių įtaką galimybėms daryti nusikaltimus, o kaip tik erdvės aspektą elektroniniuose tyrimuose apibrėžti sudėtinga (Yar, 2005; Diamond, Bachmann, 2015, p. 28). Kol kas nėra ir vienareikšmiško empirinio jų patvirtinimo arba paneigimo (Leukfeldt, Yar, 2016).

Neopozityvistinės paradigmos atstovai dažniausiai remiasi *kiekybine metodologine prieiga* – visų pirma, visuomenės ir atskirų socialinių grupių apklausomis (Maimon, Louderback, 2019, p. 200; Holtfreter, Meyers, 2015, p. 58), teisėsaugos institucijų duomenimis apie registruotus nusikaltimus. Šie duomenys siekia reprezentatyvumo ir galimybės apibendrinti duomenis valstybės mastu, tačiau jiems būdingos patikimumo ir validumo problemos. Atlikdami apklausas, tyrėjai dažnai pasirenka nereprezentatyvias, patogiausias studentų arba organizacijų darbuotojų imtis (Maimon, Louderback, 2019, p. 208). Nestandartizuoti tyrimo instrumentai (Maimon, Louderback, 2019, p. 208–209) lemia menkas galimybes lyginti skirtingų tyrimų rezultatus arba skirtingų valstybių duomenis. Apklausoms ir teisėsaugos institucijų duomenims būdingas tiek sumažintas, tiek padidintas realių nusikaltimų skaičius (angl. *underreporting*, *overreporting*), duomenų pertrūkiai (Broadhead, 2018, p. 1184). Globaliai vykdomus elektroninius nusikaltimus problemiška nagrinėti apsiribojus nacionalinių valstybių ir atskirų visuomenių lygmeniu (Broadhead, 2018, p. 1184).

Be apklausų, kiti kiekybiniai metodai, įvardijami elektroninių nusikaltimų tyrimų apžvalgose – ekonominiai žalos vertinimai, kvaziekperimentai. Ekonominių žalos vertinimų tikslas – nustatyti bendrą ekonominį poveikį, kurį padaro elektroniniai nusikaltimai valstybei arba tam tikrai ekonominės veiklos sričiai, ir pagrįsti priimamus politinius sprendimus, tačiau jie yra metodologiškai problemiški, nes siekia daryti visuminius apibendrinimus pagal palyginti mažas duomenų imtis: pavyzdžiui, organizacijų apklausa apie elektroninius nusikaltimus, patirtus per pastarąjį mėnesį, tampa pagrindu apskaičiuoti metinę elektroninių nusikaltimų žalą visame ekonominės veiklos sektoriuje (Broadhead, 2018, p. 1185).

Kvaziekperimentai nagrinėja, kaip pažeidėjai, neteisėtai sąveikaujantys su informacinėmis sistemomis, specialiai sukurtomis tyrimo tikslais, reaguoja į skirtingas perspėjimo ir atgrasymo priemones (Maimon, Louderback, 2019, p. 204–206), nors gaunami rezultatai menkai reikšmingi, lyginant su informacijos saugumo paslaugas teikiančių profesionalų galimybėmis taikyti ir testuoti atgrasymo priemones, realiu laiku stebėti įrenginių ir tinklų duomenis (kurių informaciją kaip svarbią išskiria Maimon, Louderback, 2019, p. 208).

Kritinė-kultūrinė teorinė paradigma elektroninių nusikaltimų socialiniuose tyrimuose aptinkama rečiau. Klasikinės kritinės kriminologijos teorijos, taikomos elektroniniams nusikaltimams – socialinio išmokimo teorija, diferencinės asociacijos teorija, neutralizacijos technikų teorija (Diamond, Bachmann, 2015, p. 29–30). Jos atskleidžia pažeidimų kaip socialinių praktikų specifiką pažeidėjų socialinio rato ir visuomenės kontekste. Tačiau šios paradigmos atstovai atsargiai vertina senesnių teorijų taikymą elektroniniams nusikaltimams, teigdami, kad empirinė medžiaga yra būtina sąlyga apsispręsti dėl teorijų pritaikymo, o ne atvirksčiai. Pirma būtina įsigilinti į internete kuriamas ir palaikomas socialines praktikas, o tada ieškoti arba pritaikyti joms geriausią egzistuojantį teorinį paaiškinimą, nes nebūtinai vienareikšmiškai tiks tos teorijos, kurios pagrįstai paaiškina fiziniame erdvėje vykstančias praktikas (Lee, 2018, p. 232–237).

Kritinės-kultūrinės paradigmos atstovai nurodo į potencialą taikyti kultūrinės kriminologijos teorinę bazę elektroninių nusikaltimų tyrimams, pabrėždami, kad kol kas šis derinys nepelnytai retas (Yar, 2018, p. 116). Kultūrinė kriminologija suteikia galimybę nuodugniau interpretuoti interneto ir elektroninių nusikaltimų socialinį poveikį, nes iš principo nagrinėja, kaip internetas, medijos, technologijos keičia kultūras bei individualias tapatybes (Yar, 2018, p. 116), kaip nuolat kinta santykis tarp normos ir deviacijos, kaip kuriamos normos naujai diegiamose, anksčiau nereguliuojamose srityse, ką reiškia technologinių subkultūrų veikla. Tokiu būdu ji atliepia technosocialinę nuostatą, kad technologijos ir visos su jomis susijusios deviacijos (ne tik nusikaltimai) glaudžiai siejasi su kasdieniu gyvenimu. Savo siūlymą daugiau dėmesio sutelkti į kultūrinius elektroninių nusikaltimų tyrimus Yaras grindžia teiginiu, kad „individualių ir kolektyvinių reikšmių kūrimas (ir vartojimas) svarbus formuojant internetinius nusikaltimus, deviacijas ir socialinę kontrolę“ (Yar, 2018, p. 116).

Technosocialinis požiūris artimas kitai teorinei kryptčiai, kildinamai iš mokslo ir technologijų studijų (angl. *science and technology studies*) disciplinos, kuri taikoma ir elektroninių nusikaltimų studijose (Balzacq, Cavelti, 2016; Wagen, Pieters, 2015). Tai veikėjo–tinklo arba veiksniatinklio teorija (angl. *actor–network theory*). Ji įvardijama kaip ontologiškai priešinga rutininių veiksmų teorijai (Stratton, Powell, Cameron, 2017,

p. 23), nes nutrina ribas tarp socialinių ir technologinių veikėjų, traktuodama juos kaip visuminio tinklo dalyvius, taigi ir unikalus individo racionalumas praranda prasmę kaip pagrindinis nusikaltimo motyvas. Ši teorinė prieiga sutelkia dėmesį į sąveikas, vykstančias kompleksiniame žmonių ir technologijų tinkle. Ji gali būti taikoma analizuojant skirtingus elektroninius nusikaltimus – nuo internetinių patyčių iki terorizmo (Luppicini, 2014), konceptualizuojant ir interpretuojant visų tinklo dalyvių socialinius vaidmenis bei patirtis (Wagen, Pieters, 2018).

Kritinei perspektyvai taip pat atstovauja feministinė ir *queer* teorija, kuri išryškina elektroninių nusikaltimų niansus, susijusius su lytimi, menkai atskleidžiamus kitų teorinių prieigų atstovų (Lazarus, 2019, p. 15; Hutchings, Ting Chua, 2016). Feministinė elektroninių nusikaltimų analizė, kaip besiformuojanti tyrimų kryptis, gali remtis feministinės kriminologijos, feministinių medijų studijų, feminizmo ir *queer* krypčių socialinėje teorijoje perspektyvomis ir derinti jų iškeliamą problematiką. Moterų įsitraukimas į veiklą internete, dalyvavimas globalioje politikoje ir aktyvizmas vykdomas pasitelkus socialines medijas bei kitus techninius įrankius, technologijų įgalinamos lyčių ideologijos – reiškiniai, kuriuos vieni tyrėjai vadina *ketvirtąja feminizmo banga* (Jackson, 2018, p. 35), kiti – postfeminizmu (Gill, 2016). Šios teorinės diskusijos ir jų empiriniai atitikmenys turi potencialo užpildyti ankstesniame dešimtmetyje įvardytą „globalios feministinės politinės ekonominės analizės“ trūkumą feministiniuose medijų tyrimuose (Lee, 2006, p. 201–202).

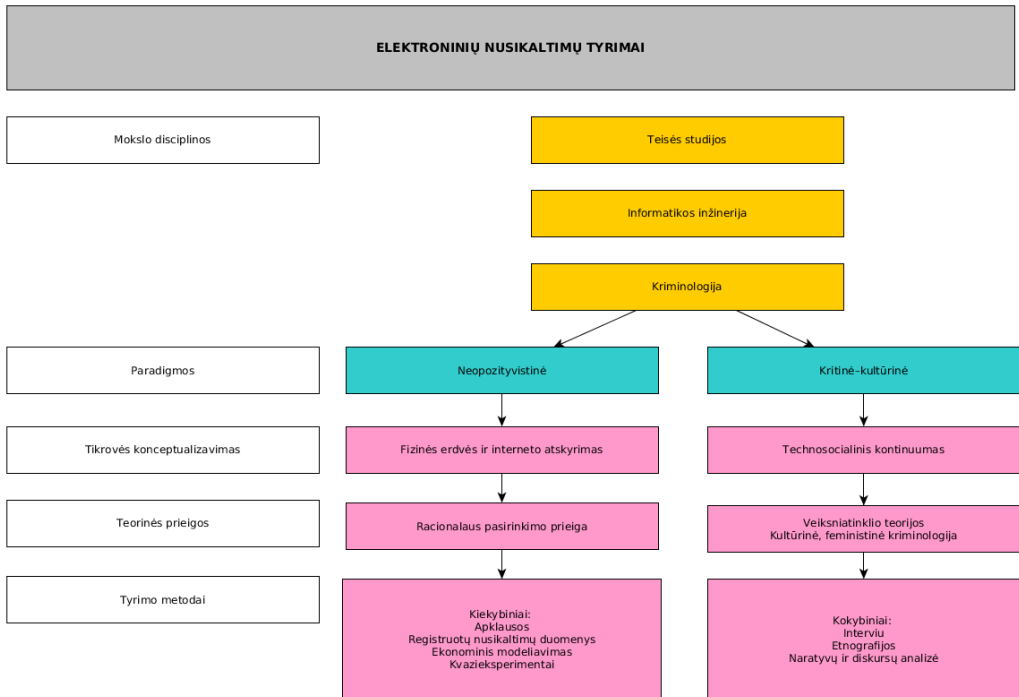
Naudodami minėtas prieigas tyrėjai pateikia, visų pirma, kritinį požiūrį į lyties dimensiją turinčius nusikaltimus, pavyzdžiui, persekiojimą internete, neapykantos nusikaltimus, seksualinį priekabiavimą arba, pavyzdžiui, klausimus, kaip lytis susijusi su elektroninius nusikaltimus atliekančių pažeidėjų bei jų aukų motyvacija bei patirtimis? Kartu jie apima ir gerokai platesnę lytimi irėmintų technosocialinių patirčių paletę. Pavyzdžiai – vyriškų, moteriškų, *queer* technologijų naudojimo patirčių kritinė analizė, lyties homogeniškumo ir heterogeniškumo poveikis interneto bendruomenėms, socialinio konflikto raiška interneto medijose per lyties prizmę. Kompleksinę technosocialinę perspektyvą atliepia ir naujai konceptualizuojami kūnai bei kūniškumo patirtys, kurias keičia technologijos, įtinklintų seksualinių praktikų tyrinėjimas.

Taigi, lyties perspektyva iš esmės išryškina nevienareikšmį normų ir deviacijų, socialinės kontrolės, socialinio teisingumo santykį. Pridėjus prie jos interseksionalumo perspektyvą – nuostatą, kad individo socialinę poziciją išreiškia ne pavienės sociodemografinės charakteristikos, o kompleksinės lyties, rasės, klasės, amžiaus sankirtos (Burgess-Proctor, 2006), kurios turi būti įtraukiamos į tyrėjų akiratį, feministinė perspektyva dar stipriau praplečia kritinės-kultūrinės analizės ribas. Vadovaudamiesi šiomis prieigomis, tyrėjai telkia dėmesį ne tik į individualius veikėjus, kurie yra pagrindinis racionalaus pasirinkimo prieigos šalininkų objektas, bet į socialines grupes ir tapatybes, jų tarpusavio santykius, reprezentacijas internete, technosocialines praktikas bei patirtis, *mikro-* ir *makrolygmens* galios santykių raišką.

Kritinės-kultūrinės paradigmos atstovai, taip pat jiems nepriklausantys autoriai, kurie savo darbuose, iš esmės, pritaiko panašius principus, remiasi *kokybine metodologine prieiga*. Taip jie atliepia poreikį kreipti tiriamąjį žvilgsnį „iš apačios“ – remtis grindžiamąja teorija (angl. *grounded theory*), dalyvavimu bei įsitraukimu, siekiu suprasti niansus,

neužčiuopiamus kiekybiniais matavimais (Lee, 2018, p. 238). Giluminiai interviu, etnografijos, naratyvų ir diskursų analizės įvairiose medijose atskleidžia ir nusikalstamos veiklos, ir su technologijomis susijusių socialinių normų kūrimo ir socialinės kontrolės palaikymo bruožus.

Kokybiniai metodai suteikia galimybę aprėpti transnacionalinę arba globalią perspektyvą, kurios dažnai neatspindi nacionaliniu mastu renkami ir analizuojami kiekybiniai duomenys, atskleisti tarpkultūrinius (deviantinių) socialinių praktikų skirtumus (žr. Nguyen, 2016), santykį tarp deviacinės veiklos, technologinių subkultūrų ir dominuojančios kultūros (Steinmetz, 2014). Taip paneigiami neopozityvistinės paradigmos atstovų teiginiai, neva pasiekti elektroninius nusikaltimus darančius pažeidėjus, kurių nepasiekia teisėsauga, „socialiniams tyrėjams yra mažai vilties“ (Holtfreter, Meyers, 2015, p. 59). Praktiniu požiūriu, kokybinių tyrimų rezultatai suteikia galimybę ieškoti alternatyvių, patirtimi paremtų, technologijų ribas peržengiančių sprendimų elektroninių nusikaltimų keliamoms problemoms ir jų prevencijai (Steinmetz, 2018, p. 132; Wagen, Pieters, 2018, p. 14).



1 pav. Mokslinių tyrimų apie elektroninius nusikaltimus paradigmos (sudaryta autorės)

Taigi, neopozityvistinė paradigma apima racionalaus pasirinkimo prieigą taikančias teorijas, iš kurių taikymo dažnumu pasižymi rutininių veiksmų teorija, o kritinei-kultūrinei paradigmai galima priskirti kultūrinės kriminologijos teorines nuostatas, taip pat artimas principines nuostatas turinčią veiksniatinklio teoriją ir feministines teorijas. Neopozityvistinės paradigmos atstovams būdingas dėmesys individualiems nusikaltėlių motyvams

ir viktimizacijos – tapimo auka – veiksniams, kuriuos jie tiria pasitelkdami kiekybinę metodologiją. Jie dažniau traktuoja internetą ir fizinę erdvę kaip atskiras erdves arba nekreipia dėmesio į skirtumus tarp jų. Kritinės-kultūrinės paradigmos atstovai interpretuoja elektroninius nusikaltimus kaip globalią ir lokalią dimensiją turinčias socialines praktikas, įtinklinančias socialines grupes. Jiems artimesnis kompleksinis technosocialinis požiūris į informacijos ir komunikacijos technologijų naudojimą. Nustatytos takoskyros tarp paradigmų grafiškai apibendrintos 1 paveiksle.

Teorinės ir metodinės paradigmos socialiniuose tyrimuose apie elektroninius nusikaltimus Lietuvoje

Tyrimų, kurie elektroninius nusikaltimus nagrinėja iš socialinių mokslų perspektyvos, Lietuvoje atliekama nedaug. Apie elektroninius nusikaltimus palyginti gausiai rašomi magistro darbai – bent 100 jų yra prieinama viešai per Lietuvos disertacijų ir baigiamųjų darbų duomenų bazę Lietuvos akademinėje elektroninėje bibliotekoje (eLABa ETD, <https://lvb.lt>), o šiuo metu neprieinamų, tikėtina, yra dar daugiau. Recenzuojamų mokslinių publikacijų yra gerokai mažiau. Atliekant šaltinių paiešką mokslinėse duomenų bazėse buvo naudojami įvairūs paieškos metodai (terminai „elektroniniai nusikaltimai“ ir jų sinonimai – „kibernetiniai“, „skaitmeniniai“, „kompiuteriniai“ nusikaltimai, atskiros elektroninių nusikaltimų rūšys, išvardytos pirmame šio straipsnio skyriuje, taip pat konkrečių šiomis temomis rašančių autorių publikacijų sąrašai, šios temos publikacijų bibliografinės nuorodos į kitas susijusias publikacijas), padedantys aprėpti kuo didesnę perspektyvą ir tyrimų įvairovę.

Didžiąją dalį lietuvių kalba išleidžiamų publikacijų apie elektroninius nusikaltimus sudaro teisinės analizės. Tarp naujausių – moksliniai straipsniai (Marcinauskaitė, Pukanasytė, Šukytė, 2019; Šttilis et al., 2017a; Šttilis, Laurinaitis, 2017; Meškauskaitė, Lankauskas, 2016; Marcinauskaitė, 2016; Šttilis et al., 2016; Bučiūnas, 2016) ir kitos publikacijos, taip pat disertacijos (Šidlauskienė, 2019; Malinauskaitė-van de Castel, 2017; Akulavičius, 2015; Laurinaitis, 2015). Šios tematikos publikacijų gausa išsiskiria Šttilis, Marcinauskaitė. Kai kurie Lietuvos mokslininkai, tiesiogiai nenagrinėdami elektroninių nusikaltimų, pateikia pavienius darbus apie kriminalistinius šių nusikaltimų aspektus (tarp naujausių – Grigaliūnas, Toldinas, Venčkauskas, 2017; Barkauskas, Spiečiūtė, Juodkaitė-Granskienė, 2016; Venčkauskas et al., 2015), nacionalinį saugumą ir kritinę infrastruktūrą (Šttilis et al., 2017b; Limba, Stankevičius, Andrulevičius, 2019; Limba et al., 2017b; Martišius, 2014; ir kiti), elektroninius rinkimus (Limba et al., 2017a; Limba, Agafonov, 2012). Šių sričių mokslininkų įdirbį detalai analizuoti reikėtų atskirai dėl kitokių nei socialiniuose tyrimuose teorinių ir metodinių pagrindų, specifinių praktinio taikymo galimybių. Kartu su teisiniais darbais jie toliau šiame straipsnyje nenagrinėjami.

Toliau, vertinant teorinių ir metodologinių prieigų įvairovę ir jų taikymo specifika, aptariamoms tos studijos ir tyrimai, kurių dėmesio centre – socialiniai elektroninių nusikaltimų aspektai, socialinių praktikų analizė, poveikis visuomenei ir sąsajos su kitais socialiniais reiškiniais.

Elektroninių nusikaltimų teoretizavimo ir konceptualizavimo problemos yra nagrinėtos šiais aspektais: informacijos kūrimas ir platinimas informacinėje visuomenėje žmogaus teisių ir reguliavimo kontekste (Prokopčik, 2004), elektroninės erdvės apibrėžimas ir elektroninių nusikaltimų traktavimas kaip kokybiškai naujų veiklų ar tokių pačių veiklų, atliekamų naujomis priemonėmis (Kalpokas, 2009), informacinės visuomenės kaip bendrabūvio formos pokyčiai ir dirbtinio intelekto taikymas teisinėje sistemoje (Čaplinskas, 1999; taip pat žr. Amilevičius, 2017), tarpsektorinio, tarpinstitucinio, tarptautinio bendradarbiavimo modeliai, reguliuojant skaitmeninį elgesį informacinėje visuomenėje (Kalpokas, 2010). Tarp kitų konceptualizavimui skirtų darbų taip pat galima išskirti ankstyvą bandymą apibrėžti elektroninių nusikaltimų kategorijas ir konceptualiai susieti jas su platesniu technologijų poveikiu tapatybės ir tarpasmeninių santykių kūrimui (Starkus, 2001) bei naujesnę Wallo elektroninių nusikaltimų tipologijos apžvalgą, kuri pabrėžia tarpdalykinių tyrimų svarbą, siekiant geriau suprasti elektroninius nusikaltimus (Kuklytė, Ūsas, 2017).

Visos išvardytos publikacijos viena ar kita forma remiasi informacinės visuomenės sąvoka, apibrėždamos kontekstą, kuriame vykdomi elektroniniai nusikaltimai. Nors tai, iš esmės, sudaro pagrindą konceptualizuoti elektroninius nusikaltimus technosocialinių praktikų paradigmoje, dažniau tokia išvada lieka veikiau numanoma nei tiesiogiai išsakyta. Be to, darbai, nusikaltimus informacinėje visuomenėje nagrinėjantys kaip pagrindinę temą (Starkus, 2001; Kalpokas, 2009), buvo parašyti prieš daugiau nei 10 metų, o aktualią situaciją atspindinčių interpretacijų trūksta. Taip pat trūksta sąsajų tarp įvardytų teorinių apžvalgų ir nacionalinės arba regioninės elektroninių nusikaltimų specifikos, kuri galėtų suteikti konkretesnę teorinį pagrindą šioje srityje Lietuvoje atliekamiems empiriniams tyrimams. Aiškaus interpretacinio rėmo trūkumas lemia ir tai, kad neatsiranda skirtingų pozicijų, kurioms atstovaujantys mokslininkai tarpusavyje diskutuotų, dėl pernelyg mažo tyrimų skaičiaus nėra ir ginčų dėl elektroninio nusikaltimo sampratos iš socialinių mokslų perspektyvos.

Elektroninius nusikaltimus nagrinėjantys empiriniai tyrimai savo teorinėse dalyse dažniausiai remiasi siauresniais, konkrečios dalykinės srities tyrimais, taikomaisiais jų aspektais (pavyzdžiui, Jokubaitė, 2014; Skališienė, Žukauskienė, 2018; Balsevičienė, Ruibytė, 2015; Paluckaitė, Žardeckaitė-Matulaitienė, 2015; Gasparėnienė et al., 2018; ir kiti) arba iš esmės išlieka ateoretiniai. Tai reiškia, kad kol kas neužpildyta spraga – platesnio masto teorinių modelių analizė ir taikymas, skirtingų tyrimo nuostatų pagrindimas, paaiškinimo ir interpretacijos lygmuo. Nei neopozityvistinė, nei kritinė-kultūrinė paradigma (ar bent kokios su jomis susijusios prielaidos) kol kas nėra išreikštai aptinkama.

Elektroninių nusikaltimų empiriniuose tyrimuose Lietuvoje nominaliai atstovaujama ir kiekybinė, ir kokybinė metodologinė prieiga. Kiekybinės prieigos taikymo atvejai – registruotų elektroninių nusikaltimų statistikos analizė (Bilevičienė, Bilevičiūtė, 2011), statistiniai duomenys apie interneto paplitimą ir vartojimo praktikas (Kalpokas, 2010), kiekybinės apklausos, atliktos su moksleiviais (Pilkauskaitė-Valickienė, Raižienė, Žukauskienė, 2009; Gedutienė et al., 2012; Valeckienė, 2011; Žibėnienė, Brasienė, 2013), studentais (Butrimė, Zuzevičiūtė, 2017), bankų klientais (Čepinskis, Rakevičienė, Rudytė, 2004). Kokybinei prieigai atstovauja interviu (Skališienė, Žukauskienė, 2018), ekspertų

interviu (Gasparėnienė et al., 2016), fokusuotos diskusijų grupės su moksleiviais (Ruškus, Žvirdauskas, Kačėnuskaitė, 2010), kokybinė masinių medijų turinio analizė (Auškalnienė, 2006), tarptautinių politikos formavimo dokumentų analizė (Kalpokas, 2010). Paminėtini metodologiniai darbai – intelektinės nuosavybės pažeidimų tyrimų metodologijų palyginamoji analizė (Kiškis, Krikščionaitis, 2008), ekonominio modelio, skirto skaitmeninei šešėlinei ekonomikai apskaičiuoti, kūrimas (Gasparėnienė et al., 2018).

Kaip matyti iš negausaus empirinių tyrimų, atliktų per pastaruosius 15 metų, sąrašo, jie yra pavieniai, atliekami nesistemiškai, todėl yra sudėtinga vertinti stipriąsias ir silpnąsias skirtingų metodų taikymo lietuviškame kontekste puses arba galimybes tyrimams vienas kitą papildyti. Kiti trūkumai – menkas tęstinumas arba atnaujinimas, pavyzdžiui, registruotos elektroninių nusikaltimų statistikos analizė nebuvo atlikta nuo 2011 m. (žr. Bilevičienė, Bilevičiūtė, 2011), kiekybiniuose tyrimuose – nereprezentatyvių imčių naudojimas, apribojantis galimybes apibendrinti rezultatus. Moksleivių dominavimas kaip tyrimų tikslinės grupės taip pat lemia tai, kad elektroniniai nusikaltimai priskiriami edukologijos, o ne kriminologijos ar informacijos ir komunikacijos mokslams. Taigi esminių žinių apie kitų visuomenės grupių nuostatas ir patirtis su įvairiausių formų elektroniniais nusikaltimais trūksta.

Išvados

Pagrindinės paradigmos, apimančios teorines ir metodines nuostatas socialiniuose tyrimuose apie elektroninius nusikaltimus – *neopozityvistinė* ir *kritinė-kultūrinė*. Jos atliepia bendresnę paradigmą skirtą kriminologijos disciplinoje, tačiau esmingai prisideda prie tyrimų lauko konceptualaus formavimo. Dėl šios priežasties jo aktualios kitų disciplinų atstovams, tiriantiems elektroninius nusikaltimus.

Straipsnyje pateikta teorinė lauko analizė išskyrė, kad yra trys pagrindiniai, vienas kitam priešingi šių paradigmų principai:

- 1) Skirtingai konceptualizuojamas supratimas apie santykį tarp internetinės ir fizinės tikrovės: neopozityvistai dažniau griežtai atskiria interneto tikrovę nuo fizinės, atskiria technologines ir socialines praktikas, o kritinės-kultūrinės paradigmos atstovai dažniau įvardija jas kaip vientisą, sudėtingą technosocialinių ryšių sistemą.
- 2) Neopozityvistai atstovauja individualistinėms teorinėms perspektyvoms (dažniausiai – priklausančioms racionalaus pasirinkimo prieigai), kurios koncentruojasi į pažeidėjų motyvus, viktimizaciją. Kritinės-kultūrinės paradigmos atstovai vadovaujasi holistinėmis perspektyvomis (veiksniatinklio teorija, kultūrinė ir feministinė teorija), kurios padeda užčiuopti lokalius ir globalius elektroninių nusikaltimų aspektus, jų poveikį skirtingoms socialinėms grupėms, lyties ir tarpkultūrinius skirtumus elektroninių nusikaltimų socialinėse praktikose, normų nustatymą ir socialinę kontrolę internete.
- 3) Metodologiškai šios paradigmos atliepia klasikinę kiekybinių (neopozityvizmas) ir kokybinių (kritinė-kultūrinė paradigma) metodų skirtą socialiniuose moksluose.

Šių įtampų suvokimas, taip pat supratimas, kad pats laukas apima abu požiūrius, gali tapti gerokai įvairesnių ir subtilesnių žinių šaltiniu negu pavienių teorinių pozicijų aktua-

lizavimas. Tai, savo ruožtu, padeda vertinti konkrečių tyrimų užimamas nišas, formuluoti išsamiau pagrįstus politinius sprendimus, telkti individualistinę ir holistinę žinojimą, ieškoti naujų galimybių derinti tyrimų metodologijas.

Lietuvoje atliekami negausūs socialiniai tyrimai apie elektroninius nusikaltimus. Teorinės publikacijos remiasi informacinės visuomenės koncepcija arba fragmentiškai apžvelgia vieną ar kitą elektroninių nusikaltimų apibrėžimo modelį, tačiau nepateikia išsamesnių diskusijų apie tyrimams reikšmingas prielaidas, nesusieja jų su nacionaline ir regionine elektroninių nusikaltimų specifika. Pavieniai empiriniai tyrimai linkę savo teorinį pagrindą apibrėžti lakoniškai, susiaurindami jį iki dalykinės srities apžvalgos, arba išlieka ateoretiniai. Jie atliekami pasitelkiant tiek kiekybinę, tiek kokybinę metodologiją, tačiau pačių tyrimų yra per mažai, kad juos būtų galima vertinti kaip savarankišką teminį lauką, lyginti skirtingų metodų atskleidžiamus rezultatus apie lietuvišką elektroninių nusikaltimų kontekstą. Šią sritį reiktų gerokai plėsti, užtikrinti tyrimų įvairovę ir tęstinumą, rezultatų įvairovę ir skirtingų paradigminių nišų užpildymą.

Literatūra

AKULAVIČIUS, Marius (2015). *Digital Piracy Management in Creative Content Industry*. Kaunas: Vilnius University.

AMILEVIČIUS, Darius (2017). Dirbtinis intelektas ir besiformuojančių technologijų etika. *Naujasis židinys-Aidai*, vol. 4, p. 19–24.

AUŠKALNIENĖ, Lina (2006). Etninis nepakantumas Lietuvos internetinėje žiniasklaidoje: komentarai internete. *Etniškumo studijos*, vol. 1, p. 45–58.

BALSEVIČIENĖ, Birutė; RUIBYTĖ, Laima (2015). Kriminalinio profiliavimo pritaikymo galimybės nusikaltimų, įvykdytų elektroninėje erdvėje, tyrimui. *Visuomenės saugumas ir viešoji tvarka*, vol. 15, p. 13–26.

BALZACQ, Thierry; CAVELTY, Myriam Dunn (2016). A Theory of Actor-network for Cyber-security. *European Journal of International Security*, vol. 1 (2), p. 176–198. <https://doi.org/10.1017/eis.2016.8>

BARKAUSKAS, Marius; SPIEČIŪTĖ, Audronė; JUODKAITĖ-GRANSKIENĖ, Gabrielė (2016). Ekonominių ekspertinių tyrimų galimybės tiriant ūkines ir finansines nusikalstamas veikas. *Teisės apžvalga*, vol. 2 (14), p. 281–305.

BILEVIČIENĖ, Tatjana; BILEVIČIŪTĖ, Eglė (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*, vol. 18 (2), p. 689–702.

BROADHEAD, Stearns (2018). The Contemporary Cybercrime Ecosystem: A Multi-disciplinary Overview of the State of Affairs and Developments. *Computer Law and Security Review*, vol. 34, p. 1180–1196. <https://doi.org/10.1016/J.CLSR.2018.08.005>

BROWN, Sheila (2006). The Criminology of Hybrids: Rethinking Crime and Law in Technosocial Networks. *Theoretical Criminology*, vol. 10 (2), p. 223–224.

BUČIŪNAS, Gediminas (2016). Laikino nuosavybės teisės apribojimo taikymo ypatumai krypto-valiutai [sic]. *Visuomenės saugumas ir viešoji tvarka*, vol. 17, p. 21–30.

BURGESS-PROCTOR, Amanda (2006). Intersections of Race, Class, Gender, and Crime. *Feminist Criminology*, vol. 1 (1), p. 27–47. <https://doi.org/10.1177%2F1557085105282899>

BUTRIMĖ, Edita; ZUZEVIČIŪTĖ, Vaiva (2017). Rizika socialiniuose tinkluose: Būsimumų teisėsaugos pareigūnų informuotumas. *Informacijos mokslai*, t. 79, p. 7–16. <https://doi.org/10.15388/Im.2017.79.11373>

ČAPLINSKAS, Albertas (1999). Informacinė visuomenė, dirbtinis intelektas ir teisė. *Jurisprudencija*, vol. 14 (6), p. 73–85.

ČEPINSKIS, Jonas; RAKEVIČIENĖ, Jolita; RUDYTĖ, Dalia (2004). Saugumo rizikos valdymas internetinėje bankininkystėje. *Organizacijų vadyba: sisteminiai tyrimai*, vol. 31, p. 31–41.

- DIAMOND, Brie; BACHMANN, Michael (2015). Out of the Beta Phase: Obstacles, Challenges, and Promising Paths in the Study of Cyber Criminology. *International Journal of Cyber Criminology*, vol. 9 (1), p. 24–34. <http://doi.org/10.5281/zenodo.22196>
- GASPARĖNIENĖ, Ligita; REMEIKIENĖ, Rita; GINEVIČIUS, Romualdas; SCHIEG, Martin (2018). Adoption of Mimic Model for Estimation of Digital Shadow Economy. *Technological and Economic Development of Economy*, vol. 24 (4), p. 1453–1465. <https://doi.org/10.3846/20294913.2017.1342287>
- GASPARĖNIENĖ, Ligita; REMEIKIENĖ, Rita; SADECKAS, Alius; GINEVIČIUS, Romualdas (2016). Level and Sectors of Digital Shadow Economy: The Case of Lithuania. *Entrepreneurship and Sustainability Issues*, vol. 4 (2), p. 183–197.
- GEDUTIENĖ, Reda; ŠIMULIONIENĖ, Roma; ČEPIENĖ, Ramutė; RUGEVIČIUS, Mindaugas (2012). Patyčios elektroninėje erdvėje: jaunesniojo amžiaus paauglių patirtis. *Tiltai*, vol. 1, p. 133–148.
- GILL, Rosalind (2016). Post-postfeminism? New Feminist Visibilities in Postfeminist Times. *Feminist Media Studies*, vol. 16 (4), p. 610–630. <https://doi.org/10.1080/14680777.2016.1193293>
- GRIGALIŪNAS, Šarūnas; TOLDINAS, Jevgenijus; VENČKAUSKAS, Algimantas (2017). An Ontology-based Transformation Model for the Digital Forensics Domain. *Elektronika ir elektrotechnika*, vol. 23 (3), p. 78–82. <https://doi.org/10.5755/j01.eie.23.3.18337>
- HOLT, Thomas J.; BOSSLER, Adam M. (2014). An Assessment of the Current State of Cybercrime Scholarship. *Deviant Behavior*, vol. 35 p. 20–40. <https://doi.org/10.1080/01639625.2013.822209>
- HOLTFRETER, Kristy; MEYERS, Travis J. (2015). Challenges for Cybercrime Theory, Research and Policy. *The Norwich Review of International and Transnational Crime*, vol. 1, p. 54–66.
- HUTCHINGS, Alice; TING CHUA, Yi (2016). Gendering Cybercrime. In Thomas J. Holt (ed.). *Cybercrime through an Interdisciplinary Lens*. London: Routledge.
- JACKSON, Sue (2018). Young Feminists, Feminism and Digital Media. *Feminism & Psychology*, vol. 28 (1), p. 32–49. <https://doi.org/10.1177%2F0959353517716952>
- JOKUBAITĖ, Rasa (2014). Paauglių rizikingo elgesio internete veiksniai. *Tiltai*, vol. 1, p. 1–12.
- KALPOKAS, Vaidas (2009). Nusikaltimai elektroninėje erdvėje: kriminologinės sampratos dilemos. *Teisės problemos*, vol. 1 (63), p. 75–87.
- KALPOKAS, Vaidas (2010). Skaitmeninės erdvės reguliavimas ir kontrolė: saugumo aspektai. *Teisės problemos*, vol. 4 (70), p. 133–157.
- KIŠKIS, Mindaugas; KRIKŠČIONAITIS, Mindaugas (2008). Intelektinės nuosavybės teisių pažeidimų tyrimai: metodologiniai aspektai. *Teisė*, vol. 68, p. 37–50.
- KUKLYTĖ, Jūratė; ŪSAS, Antanas (2017). Informacinės visuomenės iššūkiai: kokios yra kibernetinių nusikaltimų formos? *Visuomenės saugumas ir viešoji tvarka*, vol. 18, p. 184–194.
- LAURINAITIS, Marius (2015). *Elektroninių pinigų teisinis reguliavimas*. Vilnius: Mykolo Romerio universitetas.
- LAZARUS, Suleman (2019). Just Married: The Synergy between Feminist Criminology and the Tripartite Cybercrime Framework. *International Social Science Journal*, vol. 69 (231), p. 15–33. <https://doi.org/10.1111/issj.12201>
- LEE, Micky (2006). What's Missing in Feminist Research in New Information and Communication Technologies. *Feminist Media Studies*, vol. 6 (2), p. 191–210. <https://doi.org/10.1080/14680770600645168>
- LEE, Murray (2018). Crime and the Cyber Periphery: Criminological Theory beyond Time and Space. In Kerry Carrington, Russel Hogg, John Scott, Maximo Sozzo (eds.). *The Palgrave Handbook of Criminology and the Global South*. Basingstoke: Palgrave, p. 223–244.
- LEUKFELDT, Eric Rutger; YAR, Majid (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior*, vol. 37 (3), p. 263–280. <https://doi.org/10.1080/01639625.2015.1012409>
- LIMBA, Tadas; AGAFONOV, Konstantin (2012). Elektroninių rinkimų sistemų konstravimo principai, modeliai ir jų apsaugos užtikrinimas. *Socialinės technologijos*, vol. 2 (2), p. 376–389.
- LIMBA, Tadas; AGAFONOV, Konstantin; PAUKŠTĖ, Linas; DAMKUS, Martynas; PLĖTA, Tomas (2017a). Peculiarities of Cyber Security Management in the Process of Internet Voting Implementation. *Entrepreneurship and Sustainability Issues*, vol. 5 (2), p. 368–402. [https://doi.org/10.9770/jesi.2017.5.2\(15\)](https://doi.org/10.9770/jesi.2017.5.2(15))

LIMBA, Tadas; PLĖTA, Tomas; AGAFONOV, Konstantin; DAMKUS, Martynas (2017b). Cyber Security Management Model for Critical Infrastructure. *Entrepreneurship and Sustainability Issues*, vol. 4 (4), p. 559–573.

LIMBA, Tadas; STANKEVIČIUS, Andrius; ANDRULEVIČIUS, Antanas (2019). Industry 4.0 and National Security: The Phenomenon of Disruptive Technology. *Entrepreneurship and Sustainability Issues*, vol. 6 (3), p. 1528–1535. DOI: 10.9770/jesi.2019.6.3(33)

LUPPICINI, Rocci (2014). Illuminating the Dark Side of the Internet with Actor-Network Theory: An Integrative Review of Current Cybercrime Research. *Global Media Journal*, vol. 7 (1), p. 35–49.

MAIMON, David; LOUDERBACK, Eric R. (2019). Cyber-dependent Crimes: An Interdisciplinary Review. *Annual Review of Criminology*, vol. 2, p. 191–216. <https://doi.org/10.1146/annurev-criminol-032317-092057>

MALINAUSKAITĖ-VAN DE CASTEL, Inga (2017). *Duomenų subjekto teisės virtualiuose socialiniuose tinkluose*. Vilnius: Mykolo Romerio universitetas.

MARCINAUSKAITĖ, Renata (2016). Neteisėto prisijungimo prie informacinės sistemos kriminalizavimo ypatumai ir kvalifikavimo problemos. *Teisės apžvalga*, vol. 2 (14), p. 250–266.

MARCINAUSKAITĖ, Renata; PUKANASYTĖ, Indrė; ŠUKYTĖ, Jolita (2019). Cyber Security Issues: Problematic Aspects of Hacking. *Journal of Security and Sustainability Issues*, vol. 8 (3), p. 331–343.

MARTIŠIUS, Mantas (2014). Rusiško informacinio karo bruožai. *Informacijos mokslai*, t. 69, p. 7–25. <https://doi.org/10.15388/Im.2014.69.5095>

MEŠKAUSKAITĖ, Liudvika; LANKAUSKAS, Mindaugas (2016). Baudžiamoji atsakomybė už asmens privataus gyvenimo neliečiamumo pažeidimus Europos Žmogaus Teisių Teismo bei Lietuvos teismų praktikos kontekste. *Teisės problemos*, vol. 1 (91), p. 52–80.

NGUYEN, Lilly U (2016). Infrastructural Action in Vietnam: Inverting the Techno-politics of Hacking in the Global South. *New Media & Society*, vol. 18 (4), p. 637–652. <https://doi.org/10.1177%2F1461444816629475>

PALUCKAITĖ, Ugnė; ŽARDECKAITĖ-MATULAITIENĖ, Kristina (2015). Rizikingas elgesys internete: jo formos ir pasekmės tarpasmeniniams santykiams bei asmens privatumui. *Visuomenės sveikata*, vol. 3 (70), p. 29–38.

PILKAUSKAITĖ-VALICKIENĖ, Rasa; RAIŽIENĖ, Saulė; ŽUKAUSKIENĖ, Rita (2009). Elektroninių patyčių paplitimas tarp Klaipėdos apskrities vyresniųjų klasių moksleivių. *Socialinis darbas*, vol. 8 (2), p. 114–121.

PROKOPČIK, Marija (2004). Informacinės technologijos ir žmogaus teisės: galimybės ir grėsmės. *Informacijos mokslai*, t. 30, p. 14–28.

RUŠKUS, Jonas; ŽVIRDAUSKAS, Dainius; KAČENAUSKAITĖ, Viktorija (2010). Interneto vartojimo grėsmių suvokimas ir patirtis: moksleivių viktimizacijos prielaidos. *Socialinis darbas*, vol. 9 (2), p. 70–78.

SKALIŠIENĖ, Rasa; ŽUKAUSKIENĖ, Lilia (2018). Paauglių mergaičių atsakingumo dalyvaujant interneto socialiniuose tinkluose ugdymo galimybės vaikų dienos centruose. *Pedagogika*, vol. 129 (1), p. 250–267. <https://doi.org/10.15823/p.2018.17>

STARKUS, Saulius (2001). Kriminologiniai kompiuterizacijos aspektai. *Jurisprudencija*, vol. 20 (12), p. 85–92.

STEINMETZ, Kevin F. (2014). Craft(y)ness: An Ethnographic Study of Hacking. *British Journal of Criminology*, vol. 55, p. 125–145. <https://doi.org/10.1093/bjc/azu061>

STEINMETZ, Kevin F. (2018). Technocrime at the Margins: Introduction to the Special Issue on Critical or Marginal Perspectives and Issues in the Study of Technocrime. *Journal of Qualitative Criminal Justice and Criminology*, vol. 6 (2), p. 131–136. <https://doi.org/10.21428/88de04a1.1d0b3f17>

STRATE, Lance (1999). The Varieties of Cyberspace: Problems in Definition and Delimitation. *Western Journal of Communication*, vol. 63 (3), p. 382–412.

STRATTON, Greg; POWELL, Anastasia; CAMERON, Robin (2017). Crime and Justice in Digital Society: Towards a Digital Criminology? *International Journal for Crime, Justice and Social Democracy*, vol. 6 (2), p. 17–33. <https://doi.org/10.5204/ijcjsd.v6i2.355>

STUNŽINAS, Robertas (2017). Europos Sąjungos kibernetinio saugumo terminai su dėmeniu kibernetinis, (-ė): reikšmės, kilmė, sinonimija. *Terminologija*, vol. 24, p. 145–163.

ŠIDLAUSKIENĖ, Jūratė (2019). *Teisės į privatų gyvenimą pažeidimas anoniminiais komentarais: inter-*

neto tinklalapių valdytojų civilinės atsakomybės taikymą pateisinantys kriterijai. Vilnius: Mykolo Romerio universitetas.

ŠTITILIS, Darius; LAURINAITIS, Marius (2017). Treatment of Biometrically Processed Personal Data: Problem of Uniform Practice under EU Personal Data Protection Law. *Computer Law & Security Review*, vol. 33, p. 618–628.

ŠTITILIS, Darius; PAKUTINSKAS, Paulius; KINIS, Uldis; MALINAUSKAITĖ, Inga (2016). Concepts and Principles of Cyber Security Strategies. *Journal of Security and Sustainability Issues*, vol. 6 (2), p. 197–210.

ŠTITILIS, Darius; PAKUTINSKAS, Paulius; LAURINAITIS, Marius; MALINAUSKAITĖ-VAN DE CASTEL, Inga (2017a). *Rekomendacijos Lietuvos Respublikos kibernetinio saugumo įstatymui*. Vilnius: Mykolo Romerio universitetas.

ŠTITILIS, Darius; PAKUTINSKAS, Paulius; LAURINAITIS, Marius; MALINAUSKAITĖ-VAN DE CASTEL, Inga (2017b). Model for the National Cyber Security Strategy: The Lithuanian Case. *Journal of Security and Sustainability Issues*, vol. 6 (3), p. 357–372. [http://dx.doi.org/10.9770/jssi.2017.6.3\(3\)](http://dx.doi.org/10.9770/jssi.2017.6.3(3))

VALECKIENĖ, Džiuginta (2011). Elektroninių patyčių tarp 5–12 klasių mokinių prevencijos gairės mokykloje: mokinių ir pedagogų požiūris. *Tiltai*, vol. 3, p. 345–356.

VENČKAUSKAS, Algimantas; DAMAŠEVIČIUS, Robertas; JUSAS, Vacius; TOLDINAS, Jevgenijus; RUDZIKA, Darius; DRĖGVAITĖ, Giedrė (2015). A Review of Cyber-crime in Internet of Things: Technologies, Investigation Methods and Digital Forensics. *International Journal of Engineering Sciences & Research Technology*, vol. 4 (10), p. 460–477.

WAGEN, Wytke van der; PIETERS, Wolter (2015). From Cybercrime to Cyborg Crime: Botnets as Hybrid Criminal Actor-networks. *The British Journal of Criminology*, vol. 55 (3), p. 578–595. <https://doi.org/10.1093/bjc/azv009>

WAGEN, Wytke van der; PIETERS, Wolter (2018). The Hybrid Victim: Reconceptualizing High-tech Cyber Victimization through Actor-network Theory. *European Journal of Criminology*, Online first, p. 1–18. <https://doi.org/10.1177%2F1477370818812016>

WALL, David S. (2001). Cybercrimes and the Internet. In David S. Wall (ed.). *Crime and the Internet*. London: Routledge.

WALL, David S. (2017). Crime, Security and Information Communication Technologies: The Changing Cybersecurity Threat Landscape and Implications for Regulation and policing. In Roger Bronsword, Eloise Scotford, Karen Yeung (eds.). *The Oxford Handbook on the Law and Regulation of Technology*. Oxford: Oxford University Press.

YAR, Majid (2005). The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory. *European Journal of Criminology*, vol. 2 (4), p. 407–427. <https://doi.org/10.1177%2F147737080556056>

YAR, Majid (2018). Toward a Cultural Criminology of the Internet. In Kevin Steinmetz, Matt R. Nobles (eds.). *Technocrime and Criminological Theory*. New York, London: Routledge, p. 116–132.

ŽIBĖNIENĖ, Gintautė; BRASIENĖ, Dovilė (2013). Naudojimasis internetu, internetiniais socialiniais tinklais ir galimai patiriamos grėsmės: mokinių nuomonė. *Socialinės technologijos*, vol. 3 (1), p. 53–67.