Vilniaus universiteto Teisės fakulteto
Baudžiamosios justicijos katedra

Miglės Mackevičiūtės,
V kurso, baudžiamosios justicijos
šakos studentės

Magistro darbas

Sukčiavimo elektroninėje erdvėje ypatumai ir baudžiamojo persekiojimo praktika Lietuvoje

Features and practice of criminal prosecution of fraud in the cyber space in Lithuania

Vadovas: doc. dr. Gintautas Sakalauskas

Recenzentas: lekt. Darius Prapiestis

Vilnius
2023

ANOTACIJA IR PAGRINDINIAI ŽODŽIAI

Šiame magistro darbe nagrinėjami sukčiavimo elektroninėje erdvėje kriminologiniai ir baudžiamojo persekiojimo aspektai. Analizuojamas elektroninio sukčiavimo, kaip nusikalstamos veikos, uždraudimas Lietuvos Respublikos baudžiamajame įstatyme, nagrinėjami dažniausiai pasitaikantys elektroninio sukčiavimo padarymo būdai, jiems įtaką darantys objektyvūs ir subjektyvūs veiksniai. Analizuojama Lietuvos Respublikos teismų praktika bei statistiniai duomenys, pabrėžiant ir elektroninio sukčiavimo latentiškumą. Išskiriami jurisdikcijos, įrodinėjimo ypatumai. Aptariamos sukčiavimo elektroninėje erdvėje prevencijos užtikrinimo priemonės.

Pagrindiniai žodžiai: elektroninis sukčiavimas, elektroninė erdvė, apgaulė, kriminalizavimas, nusikalstamumas.

This master's thesis examines the legal and criminological aspects of cyber fraud, analyses the regulation of cyber fraud as a criminal offence in the criminal law of the Republic of Lithuania, and studies the most common methods of committing cyber fraud together with the objective and subjective factors influencing them. The paper also reviews the Republic of Lithuania case law and provides statistical data highlighting the latency of cyber fraud. The characteristics and features of jurisdiction and proof are identified while analysing fraud that occurs in cyberspace. Finally, the master's thesis presents information on measures to prevent cyber fraud.

Keywords: cyber fraud, cyberspace, deception, criminalisation, criminality.

TURINYS

ĮVADAS

Temos aktualumas. Informacinės technologijos ir skaitmenizacija šiuo metu yra neatsiejama mūsų gyvenimo dalis. Kasdienės paslaugos, pavyzdžiui, mokesčių mokėjimas, mokymosi procesas ar apsipirkimas šiomis dienomis yra patogiai ir nesunkiai atliekami kelių mygtukų paspaudimo pagalba. Materialius dokumentus vis dažniau keičia elektroninis formatas, o gyvus susitikimus – telekonferenciniai skambučiai. Lietuvoje ši skaitmenizacijos tendencija taip pat yra ryški. Pavyzdžiui, Europos Komisija pažymi, jog naudojimosi interneto paslaugomis lygis Lietuvoje panašus į Europos Sąjungos vidurkį. Lietuvos, kaip ir kitų Europos Sąjungos šalių, gyventojai noriai užsiima įvairia veikla internete. Interneto naudotojų skaičius auga ir šiuo metu jau siekia 81 proc. (Europos Komisija, 2020). Taigi dabartinė aplinka pasižymi ypatingai greita vystymosi raida, o naujų technologijų diegimas ar esamų modernizavimas, teisei kelia naujus iššūkius ir atveria naujas tyrinėjimų kryptis.

Vystantis technologijoms bei visuomenei žengiant modernizacijos keliu, keitėsi ir nusikalstamumas – atsirado naujos nusikalstamumo formos, apraiškos, keitėsi jau egzistuojantys nusikalstamų veikų padarymo būdai – nusikalstamos veikos vis dažniau padaromos ne klasikinėje – fizinėje erdvėje, o elektroninėje. Įvairūs autoriai pabrėžia, kad vis labiau nyksta perskyra tarp fizinės erdvės ir interneto, o informacijos ir komunikacijos technologijoms įsitvirtinus kasdieniame gyvenime, nusikalstamos veikos atliekamos ir virtualioje erdvėje (Kalpokas, 2009, p. 75–87; Kalpokas, 2010, p. 133–157; Šupa, 2021, p. 8–46). R. Marcinauskaitė taip pat pažymi, jog „atsižvelgiant į technologijų plėtros perspektyvas reikėtų pripažinti, kad fizinės ir elektroninės erdvės atskyrimas daugelyje sričių vis dėlto yra gana sąlyginis. Tikėtina, kad šių erdvių riba ims sparčiai nykti vis daugiau žmogaus gyvenimo sričių ir veiklos rūšių perkeliant į elektroninę erdvę“ (Marcinauskaitė, 2019, p. 4).

Viena tokių nusikalstamų veikų, analizuojamų šiame magistro darbe, yra sukčiavimas, kuris didėjant technologijų įtakai, daromas vis naujesniais būdais ir kryptimis. Europos kovos su sukčiavimu tarnyba 2021 m. ataskaitoje pažymėjo, kad besitęsianti pasaulinė pandemija ir COVID-19 iššūkiai paįvairino ir elektroninių sukčių galimybių spektrą, ypač susijusių su elektronine prekyba ar skaitmeninėmis paslaugomis (Europos Komisija, 2021, p. 14). Europolo duomenimis, pastaraisiais metais elektroniniai sukčiai labai greitai pritaikė gerai žinomas sukčiavimo schemas, kad pasinaudotų visuotiniu nerimu, kilusiu dėl COVID-19 pandemijos baimės ir iššūkių. Pastaraisiais metais plito įvairios telefoninio sukčiavimo schemų versijos, sukčiavimas susijęs su elektronine prekyba ir pan. (Europol, 2020).

Panaši tendencija pastebėta ir Lietuvoje. Lietuvos Respublikos valstybės kontrolės duomenimis, 2020 m. pandemija paskatino dar aktyvesnį visuomenės skaitmenizavimąsi: naudojimąsi elektroninėmis paslaugomis, darbą nuotoliniu būdu, internetinę prekybą, finansines operacijas, taigi padidino ir nusikalstamų veikų elektroninėje erdvėje pavojų. Nusikaltimų elektroninėje erdvėje grėsmės mastas yra didelis ir auga – kibernetinių incidentų per pastaruosius metus padidėjo beveik du kartus, tačiau nusikaltimų elektroninėje erdvėje specializuotų tyrimų padalinių veiklos rezultatyvumas išlieka nepakankamas. Nusikalstamų veikų žinybiniame registre 2019 m. buvo užregistruotos 1 288 nusikalstamos veikos, padarytos elektroninėje erdvėje. Didžiausią jų dalį sudarė elektroniniai sukčiavimai – 58 proc. (Valstybės kontrolė, 2020).

Pastaraisiais metais diskusijos dėl elektroninio sukčiavimo matomos ir žiniasklaidoje, taip pat institucijos, įstaigos ir bendrovės gyventojus vis dažniau ragina naiviai nepasikliauti elektroniniais sukčiais. Didėja ir iniciatyvų, susijusių su elektroninio sukčiavimo atpažinimu ir pranešimu apie jį[1].

Šiame magistro darbe tiriamas sukčiavimas elektroninėje erdvėje, jo apraiškos, Lietuvos teismų praktika bei nagrinėjami statistiniai duomenys, aptariant šią nusikalstamą veiką didėjančios visuomenės skaitmenizacijos ir elektroninių naujovių kontekste.

Darbo tikslas – išnagrinėti sukčiavimo elektroninėje erdvėje, kaip nusikalstamos veikos, požymius, pasireiškimo būdus, taip pat apžvelgti tokių nusikalstamų veikų tendencijas Lietuvoje, atskleidžiant labiausiai paplitusius pasireiškimo būdus, išanalizuoti tokių nusikalstamų veikų įrodinėjimo specifiką bei jurisdikcijos taisykles, nustatyti ir įvertinti elektroninio sukčiavimo latentiškumą bei galimas prevencijos priemones.

Siekiant įgyvendinti magistro darbo tikslą, buvo iškelti šie **uždaviniai**:

1) apžvelgti sukčiavimo elektroninėje erdvėje sampratą, jos turinį bei nusikalstamos veikos sudėties požymius ir kvalifikavimo problematiką.

2) aptarti sukčiavimo elektroninėje erdvėje padarymo būdus, jų specifiką, apraiškas Lietuvoje.

3) išnagrinėti bei įvertinti elektroninio sukčiavimo įrodinėjimo ypatumus, jurisdikcijos aspektus.

[1] Pavyzdžiui, SEB bankas išleido interaktyvų žaidimą, kuris padeda suprasti bei atpažinti sukčiavimo elektroninėje erdvėje modelius. Interaktyvi prieiga: https://www.seb.lt/pinkles; Lietuvos Respublikos Vyriausybės kanceliarija vykdo projektą su internetinių grėsmių atpažinimu. Interaktyvi prieiga: https://sustiprinkimuniteta.lt; Lietuvos policija dalijasi patarimais kaip išvengti elektroninių sukčių. Interaktyvi prieiga: https://policija.lrv.lt/lt/naujienos/kaip-isvengti-sukciavimu-internete.

4) išskirti ir išanalizuoti sukčiavimo elektroninėje erdvėje statistiką, latentiškumą bei galimus prevencijos metodus ir priemones.

Darbo objektas. Magistro darbo objektą sąlygoja iškeltas darbo tikslas bei jam pasiekti apibrėžti uždaviniai. Objektas – sukčiavimo elektroninėje erdvėje, kaip nusikalstamos veikos, teisinis ir praktinis vertinimas Lietuvoje.

Magistro darbe naudojami šie mokslinio tyrimo **metodai**:

1) Analizės – naudojant šį metodą analizuojama elektroninio sukčiavimo samprata, jos turinys, sudėties ypatumai, atliekama atitinkamų teisės aktų, doktrininių teiginių, teismų praktikos analizė. Taip pat analizuojami statistiniai duomenys, darant išvadas dėl šios veikos paplitimo ir apraiškų Lietuvoje.

2) Lingvistinis – šis metodas šiame magistro darbe taikomas analizuojant teisės aktų normų turinį, teisės mokslo doktrinoje bei teismų praktikoje įtvirtintus požymius.

3) Sisteminis – metodas naudojamas elektroninio sukčiavimo reglamentavimo ir jo taikymo Lietuvoje įvertinimui bei ištyrimui, remiantis tarptautiniais ir nacionaliniais teisės aktais, teismų praktika ir teisės mokslo doktrina.

4) Lyginamasis – analizuojama tarptautinių, Europos Sąjungos teisės aktų specifika lyginant su Lietuvos Respublikos baudžiamojo kodekso ir kitų nacionalinių teisės aktų nuostatomis.

5) Analitinis-kritinis – šio metodo pagalba atliekamos teisės norminių aktų įžvalgos, pateikiami reikšmingi apibendrinimai, paminint ir probleminius aspektus.

Pagrindiniai šaltiniai. Magistro darbe analizuojami tarptautiniai, Europos Sąjungos, Lietuvos Respublikos bei kitų užsienio valstybių teisės aktai, Lietuvos teismų praktika, viešai prieinami institucijų statistiniai duomenys, veiklos ataskaitos, remiamasi Lietuvos mokslininkų – Mindaugo Civilkos, Vaido Kalpoko, Mindaugo Kiškio, Renatos Marcinauskaitės, Dariaus Štitilio, Maryjos Šupos bei kitų autorių publikacijomis. Svarbią reikšmę magistro darbui turėjo ir užsienio autorių mokslinė literatūra – itin aktualūs buvo Xingan Li, Thomas. C. Folsom ir kitų autorių moksliniai darbai.

Darbo naujumas bei originalumas. Lietuvos autorių darbuose elektroninis sukčiavimas nėra plačiai nagrinėjama tema. Ši tema apžvelgiama epizodiškai, dažniausiai kitų elektroninių nusikaltimų kontekste. Užsienio teisinėje literatūroje yra mokslo darbų, susijusių su elektroninio sukčiavimo teisiniu, kriminologiniu vertinimu, tačiau juose nėra analizuojami Lietuvos teisiniam reguliavimui aktualūs niuansai ir aspektai, tokie kaip elektroninio sukčiavimo, kaip nusikalstamos veikos, sudėties analizė, kriminalizavimo ypatumai Lietuvos

Respublikos baudžiamajame kodekse, santykio su kitomis nusikalstamomis veikomis analizė. Autorės žiniomis, nėra vieno bendro šaltinio, kuris išsamiai nagrinėtų sukčiavimą elektroninėje erdvėje Lietuvos Respublikos teisiniame kontekste, todėl šiame darbe, atlikus tiek Lietuvos, tiek užsienio teisės mokslo darbų, teismų praktikos bei teisės aktų analizę, pateikiami elektroninio sukčiavimo, kaip nusikalstamos veikos aspektai, atsižvelgiant į Lietuvos Respublikos teisinio reglamentavimo ypatumus.

Autorių rašyti magistro darbai panašiomis temomis Vilniaus universitete ir Mykolo Romerio universitete:

1) Jonas Augulis „Sukčiavimai elektroninėje erdvėje: kriminologiniai aspektai“, 2021 m.
2) Tomas Versekėnas „Kibernetinių nusikaltimų sąvoka ir sistema“, 2017 m.

Šis magistro darbas nuo paminėtų darbų skiriasi tuo, kad jame išsamiai analizuojami tiek baudžiamieji teisiniai, tiek kriminologiniai sukčiavimo elektroninėje erdvėje aspektai. Magistro darbo Autorė ne tik nuosekliai ir sistemiškai pateikia sukčiavimo elektroninėje erdvėje sampratą, tačiau ir gilinasi bei analizuoja tokius probleminius aspektus kaip taikytinos jurisdikcijos klausimai, duomenų (įrodymų) rinkimo problematika, taip siekiant išsamiai atkleisti šios nusikalstamos veikos ypatumus.

1. SUKČIAVIMO ELEKTRONINĖJE ERDVĖJE SAMPRATA, JĮ LEMIANTYS VEIKSNIAI, PADARYMO BŪDAI IR TENDENCIJOS

1.1. Sukčiavimo elektroninėje erdvėje samprata ir ypatumai

Magistro darbo objektas suponuoja, kad analizuojamos temos išnagrinėjimui būtina tinkamai apibrėžti ir įvertinti, kas yra sukčiavimas elektroninėje erdvėje. Analizuojant sukčiavimo elektroninėje erdvėje sampratą bei šio nusikaltimo ypatumus, svarbu suprasti pačios elektroninės erdvės, kaip terpės, kurioje sukčiavimai gali būti padaromi, apibrėžimą ir jo turinį. Elektroninė erdvė suteikia naujų galimybių įvykdyti nusikaltimus, sudaro sąlygas naujiems nusikaltimų būdams atsirasti, be to, sudaro galimybes įvykdyti naujas veikas, iki tol nežinomas teisinėje praktikoje (Štitilis, 2011, p. 5).

Teisės mokslo doktrinoje elektroninė erdvė, kuri dar vadinama kibernetine erdve (angl. *cyber space*), apibūdinama kaip globaliai integruota, viešai ir visuotinai prieinama kompiuterių tinklų sistema, kuria naudojantis keičiamasi informacija (Kiškis *et al*., 2016, p. 19). Elektroninė erdvė sukurta sujungus milijonus kompiuterinės sistemos prietaisų į pasaulinį tinklą, pavyzdžiui, internetą arba telekomunikacijų ryšį, kuris įdiegtas kaip daugiasluoksnė konstrukcija, kurioje fiziniai elementai leidžia sukurti loginę tarpusavio ryšio sistemą, leidžiančią apdoroti, naudoti, papildyti informaciją (Choucri, 2013).

Autoriai sutinka, kad elektroninė erdvė neturi fizinių ribų, jos negalima apibrėžti ar apčiuopti. Svarbiausios elektroninės erdvės funkcijos yra keitimasis informacija ir prieiga prie tokios informacijos turinio (Kiškis *et al*., 2016, p. 19). Be interneto egzistuoja ir telekomunikacijų (telefonų bei kitų mobiliųjų įrenginių, kuriais perduodama informacija) sistema, kuri taip pat yra įkūnytas komutuojamasis tinklas (Folsom, 2006, p. 84). Toks informacijos srautas gali egzistuoti kompiuteriuose, išmaniuosiuose telefonuose, laikrodžiuose, programinėse įrangose ir kitose laikmenose. Šie materialūs objektai yra pagalbinis įrankis naudotis ir prisijungti prie elektroninės erdvės, o pati elektroninė erdvė suprantama kaip aplinka, terpė, kurią sudaro tarpusavyje susijęs informacinių technologijų infrastruktūrų tinklas, įskaitant internetą, telekomunikacijų tinklus, kompiuterių sistemas ir įterptinius procesorius bei valdiklius (Department of Defense Dictionary of Military and Associated Terms, 2010).

Elektroninėje terpėje, informacija gali būti kuriama, perduodama, gaunama, saugoma, apdorojama ir ištrinama. Taigi, elektroninės arba kibernetinės erdvės, kaip nusikalstamos veikos padarymo vietos ir aplinkos samprata yra plati ir apima fizinės formos neturinčią erdvę,

kurią sudaro medijos įrenginiuose, jų sistemoje, programinėje įrangoje esantys duomenys ir informacija, kuriuos vartotojai gali pasiekti ar keistis šių įrenginių pagalba.

Tokia plati elektroninės erdvės samprata suponuoja ir esminį požymį apibrėžiant veiką kaip priskirtiną elektroninei erdvei – objektyvioji veikos pusė turi pasireikšti/būti padaroma naudojant tam tikrą įrenginį, kuris leidžia pasiekti elektroninę erdvę, kurioje padaroma veika. Taigi, būtinoji sąlyga kvalifikuojant nusikalstamą veiką, kaip elektroninėje erdvėje padaromą veiką, yra ta, kad nusikalstama veika padaroma naudojant įrenginį, kuris leidžia prisijungti prie elektroninės erdvės. Elektroninė erdvė gali būti pasiekiama tiek internetu, tiek ir kitomis telekomunikacijos priemonėmis. Kartu pastebėtina, kad tai turėtų būti laikoma vieninteliu požymiu, leidžiančiu veiką kvalifikuoti kaip priskirtiną veikoms, kurios padaromos elektroninėje erdvėje. Nusikalstamos veikos objektas, subjektas ar subjektyvioji pusė šiuo atveju iš esmės nesikeičia, lyginant su nusikalstamomis veikomis, padaromomis fizinėje erdvėje. Objektas taip pat gali nesiskirti nuo fiziniame pasaulyje saugomų objektų – tai gali būti nuosavybė, turtinės teisės ir pan.

Toliau aptariant sukčiavimo elektroninėje erdvėje sampratą, akcentuotina, kad praktikoje galima sutikti keletą požiūrių, kas yra laikoma sukčiavimu elektroninėje erdvėje.

Siauruoju požiūriu, sukčiavimas elektroninė erdvėje yra siejamas su kylančiais padariniais kompiuterinių duomenų ar programų atžvilgiu. Pavyzdžiui, Europos Taryba dar 2001 m., matydama didėjančią kompiuterizacijos įtaką ir įžvelgdama, kad kompiuteriniai tinklai ir elektroninė erdvė gali būti naudojami nusikalstamoms veikoms daryti, pabrėžė poreikį kovoti tiek su naujomis, tiek su jau egzistuojančiomis ir besikeičiančiomis nusikalstamų veikų formomis, kurios padaromos elektroninėje erdvėje. Šio tikslo įgyvendinimui Europos Taryba 2001 m. lapkričio 23 d. priėmė Konvenciją dėl elektroninių nusikaltimų (toliau – Konvencija). Konvencijos 8 str. įtvirtina kompiuterinio sukčiavimo sąvoką. Pagal Konvencijos nuostatas, valstybės nacionalinėje teisėje turi nustatyti baudžiamąją atsakomybę už sąmoningus ir neteisėtus veiksmus, sąlygojusius kito asmens nuosavybės praradimą: a) įvedant, pakeičiant, sunaikinant kompiuterinius duomenis arba panaikinant galimybę naudotis tokiais duomenimis; b) paveikiant kompiuterinės sistemos darbą, nesąžiningai arba nedorai ketinant gauti neteisėtos ekonominės naudos sau arba kitam asmeniui. Taigi sukčiavimas elektroninėje erdvėje apibrėžtas daug siauriau nei suponuoja pačios elektroninės erdvės samprata. Konvencijos rengėjai nusprendė apriboti sukčiavimą susiejant jį ne tik su nuosavybės praradimu bet ir su elektroninėje erdvėje kylančiais padariniais (t. y. kompiuterinių duomenų ar programų

pakeitimu, sunaikinimu ar pan.). Vis dėlto, tai susiaurino sukčiavimo elektroninėje erdvėje sampratą.

2019 m. balandžio 17 d. Europos Parlamento ir Tarybos Direktyvoje (ES) 2019/713 Dėl kovos su sukčiavimu negrynosiomis mokėjimo priemonėmis ir jų klastojimu (toliau – Direktyva 2019/713**)** taip pat minimas poreikis kriminalizuoti „naujas“ nusikalstamas veikas, tarp jų ir kompiuterinį sukčiavimą. Įgyvendinant šią nuostatą, Direktyvos 2019/713 6 str. pateikiama su informacinėmis sistemomis susijusio sukčiavimo sudėtis. Toks sukčiavimas apibūdinamas dviem alternatyviais būdais: pirma, trukdant informacinės sistemos veikimui ar jį trikdant ir neturint teisės daryti tokius veiksmus, antra, neturint teisės įvedant, keičiant, ištrinant, perduodant ar pašalinant kompiuterinius duomenis. Direktyvoje 2019/713, kaip ir Konvencijoje sukčiavimas siejamas su neteisėtu kompiuterinės sistemos darbo sutrikdymu arba nutraukimu arba tam tikru poveikiu duomenims, neteisėtai įgyjant turtą ar turtinę teisę. Taigi Direktyvoje 2019/713 ir Konvencijoje sukčiavimas suprantamas siaurai ir apima informacinių sistemų darbo sutrikdymą ar tam tikrą poveikį duomenims, dėl kurio jie pasikeičia arba nustoja egzistuoti. Tokia siaura sukčiavimo elektroninėje erdvėje samprata susijusi su poveikiu, padaromu tam tikrų kompiuterinių duomenų ar programų atžvilgiu, Autorės nuomone, nėra tinkama. Tokia samprata nepagrįstai susiaurina sukčiavimo elektroninėje erdvėje apimtį bei veiką sieja išimtinai su kompiuterinių duomenų ar programų pakeitimu, ištrynimu ir pan., nors sukčiavimas elektroninėje erdvėje dėl elektroninės erdvės specifikos (galimybių anonimiškai susijungti su kitais įrenginiais, naudotis įrenginių tinklu) neturėtų būti apribojamas su elektroninėje erdvėje kylančiais padariniais.

Kitokio požiūrio laikomasi Lietuvoje, kur sukčiavimas elektroninėje erdvėje suprantamas plačiąja prasme. Perkeldamas Konvencijos ir Direktyvos 2019/713 nuostatas, įstatymų leidėjas neatliko Lietuvos Respublikos baudžiamojo kodekso (toliau – BK) pakeitimų, susijusių su sukčiavimu elektroninėje erdvėje, o Konvencijos ir Direktyvos 2019/713 nuostatos sukčiavimo atveju buvo ir yra įgyvendinamos per teismų praktiką. Tai reiškia, jog Lietuvoje, Konvencijoje ir Direktyvoje 2019/713 minimas kompiuterinis sukčiavimas patenką į bendrą BK 182 str. dispozicijos sudėtį, taip pat suprantamas plačiau ir apima ne tik atvejus, kai paveikiamas kompiuterinės sistemos darbas ar naudojimasis tam tikrais kompiuteriniais duomenimis, tačiau ir atvejus, kai paties įrenginio sistemos darbas gali būti nesutrikdomas, o kompiuteriniai duomenys nebūtinai yra tiesiogiai paveikiami, pvz., „telefoninių“ sukčių atveju nukentėję asmenys patys perveda tam tikras pinigų sumas, tai reiškia, kad asmenų įrenginiuose esantys duomenys nėra tiesiogiai veikiami ar paveikiami kito

asmens. Pasirinktas įstatymų leidėjo sprendimas leidžia plačiau ir tiksliau kategorizuoti sukčiavimą elektroninėje erdvėje, nesiejant jo su kylančiais padariniais kompiuteriniams duomenims ar programoms. Atitinkamai, atsižvelgiant į jau aptartą elektroninės erdvės sampratą, šiame darbe, elektroninis sukčiavimas aiškinamas ir nagrinėjamas plačiąja prasme, kaip apimantis ne tik neteisėtą poveikį informacinei sistemai ar kompiuteriniams duomenims juos modifikuojant ar kitaip neteisėtai juos veikiant, bet kaip sukčiavimas, kuris padaromas naudojantis elektronine erdve, kuri pasiekiama elektroninių įrenginių pagalba, taip neteisėtai įgyjant turtinės naudos.

Toliau siekiant atskleisti į BK 182 str. sudėtį patenkančio elektroninio sukčiavimo sampratą bei jos turinio ypatumus, visų pirma, reikėtų pradėti nuo įrenginio, kurio pagalba pasiekiama elektroninė erdvė santykio su elektroninio sukčiavimo norma. Nusikalstamų veikų elektroninėje erdvėje atveju, įrenginys gali būti panaudojamas kaip įrankis, arba gali tapti nusikalstamos veikos tikslu (Šupa, 2021, p. 14). Prie pirmojo atvejo, kai įrenginys naudojamas, kaip įrankis nusikalstamoms veikoms daryti, galima priskirti tokias nusikalstamas veikas kaip finansiniai nusikaltimai, kibernetinis persekiojimas, pornografija, nusikaltimai intelektinei nuosavybei ir pan. Prie antrojo atvejo, kai įrenginys ir jame esanti informacijos bei duomenų visuma gali tapti nusikalstamos veikos tikslu, priskiriamos tokios nusikalstamos veikos kaip duomenų vagystė, poveikis duomenims, neteisėta prieiga ir pan.

Kaip minėta, Lietuvoje sukčiavimas elektroninėje erdvėje neturi atskiros dispozicijos, kuri būtų laikoma bendrojo sukčiavimo, reglamentuojamo BK 182 str., specialiąją norma, palyginti su kitų šalių teisės įgyvendinimo kontekstu. Pavyzdžiui, Latvijos (BK 177^1 straipsnis), Lenkijos (BK 287 straipsnis), Estijos (BK 213 straipsnis) baudžiamuosiuose įstatymuose kompiuterinis sukčiavimas, t. y. sukčiavimas elektroninėje erdvėje siaurąja prasme, įtvirtintas kaip specialioji sukčiavimo norma, o Lietuvoje atskiroji sukčiavimo, padaromo elektroninėje erdvėje, sudėtis nėra išskirta, todėl BK 182 str. bendroji norma apima tiek sukčiavimą elektroninėje erdvėje siaurąja, tiek sukčiavimą plačiąja prasme.

Sukčiavimas BK 182 str. 1 d., kurioje įtvirtinta pagrindinė nusikalstamos veikos sudėtis, apibrėžiamas, kaip apgaulės panaudojimas savo ar kitų naudai svetimam turtui ar turtinei teisei įgyti arba turtinei prievolei išvengti ar ją panaikinti. Tai, jog elektroninis sukčiavimas BK nėra reguliuojamas kaip atskiroji norma, o yra laikomas sukčiavimo, įtvirtinto BK 182 str. pasireiškimo forma, būdu, lemia, jog šiuo atveju kėsinimosi objektas yra nuosavybė, turtinės teisės ir turtiniai interesai. Tai leidžia daryti išvadą, kad elektroninio sukčiavimo, nukreipto į fizinio ar juridinio asmens turtinių santykių visumą atveju, kompiuteris ar kitas įrenginys yra

naudojamas kaip įrankis, tačiau nėra šios nusikalstamos veikos tikslu. Tikslu yra materiali ar nemateriali turtinė nauda, kurią asmuo gali gauti tokio įrenginio pagalba darant elektroninį sukčiavimą.

BK 182 str. 1 dalyje įtvirtinta pagrindinė sukčiavimo sudėtis, 2 dalyje kvalifikuota, o 3 dalyje numatyta baudžiamoji atsakomybė už baudžiamąjį nusižengimą. Kadangi elektroninis sukčiavimas BK nėra atskirai reglamentuojamas specialiojoje normoje, jam inkriminuoti būtina nustatyti visus objektyviuosius ir subjektyviuosius bendrojo sukčiavimo požymius.

Esminis sukčiavimo požymis, pagal kurį sukčiavimas gali būti atribojamas ir nuo kitų nusikalstamų veikų – apgaulės panaudojimas nusikalstamai veikai daryti. Apgaulė sukčiavimo atveju yra naudojama kaip turto užvaldymo būdas (Lietuvos Aukščiausiojo Teismo 2012 m. rugsėjo 7 d. apžvalga). Apgaule siekiama suklaidinti turto savininką, valdytoją ar asmenį, kurio žinioje yra turtas, o pastarieji dėl suklydimo, suklaidinti naudojamos apgaulės, savanoriškai patys perleidžia turtą ar turtinę teisę kaltininkui, manydami, kad šis turi teisę jį gauti, arba panaikina jo turtinę prievolę (Lietuvos Aukščiausiojo Teismo 2019 m. gruodžio 19 d. nutartis baudžiamojoje byloje).

Elektroninio sukčiavimo atveju apgaulę taip pat būtina nustatyti. Apgaulė elektroninio sukčiavimo kontekste yra svarbi, nes leidžia elektroninį sukčiavimą atriboti nuo kitų nusikalstamų veikų padaromų elektroninėje erdvėje, pvz., nuo neteisėto elektroninės mokėjimo priemonės ar jos duomenų panaudojimo (BK 215 str.). Lietuvos Aukščiausiasis Teismas (toliau – LAT**)** yra išaiškinęs, jog elektroninės bankininkystės klientas su banku bendrauja ne tiesiogiai, o per elektroninę sistemą. Sistema sudaryta tokiu būdu, kad ji priima komandą ir atlieka operaciją, jei surinkti tinkami sąskaitų turėtojų identifikaciniai kodai. Būtent kodas pagal programos veikimo principus identifikuoja asmens, kaip sąskaitos turėtojo, tapatybę ir pažymi teisę atlikti operacijas su sąskaitoje esančiomis piniginėmis lėšomis. Jei kodą surenka ir komandą duoda asmuo, neturintis teisės atlikti operacijų su sąskaitoje esančiomis piniginėmis lėšomis, jis pateikia operacinei sistemai ir bankui save kaip kitą asmenį, turintį tokią teisę, ir taip suklaidina elektroninę sistemą ir kartu banką. Šie veiksmai, būtent dėl apgaulės naudojimo yra vertintini kaip sukčiavimas (Lietuvos Aukščiausiojo Teismo 2021 m. sausio 9 d. nutartis baudžiamojoje byloje).

Žvelgiant į sukčiavimo sudėties elementus, elektroninis sukčiavimas gali pasižymėti dalyko ypatumais. Sukčiavimo dalykas yra suprantamas kaip materialus turtas, turtinė teisė, kuri atitinka „bekūnio daikto“ sampratą bei turtinė prievolė (Abramavičius *et al*., 2009, p. 332). Neabejotina, kad sukčiavimu elektroninėje erdvėje siekiama gauti turtinės naudos, tačiau dėl

elektroninės erdvės, kurioje pasireiškia sukčiavimas, ypatumų, gali kisti ir pats dalyko pasirinkimas. Elektroninių sukčių taikiniu dažnu atveju tampa negrynieji pinigai, kurie vertinami kaip turtinė teisė. Jos įgijimui nebūtinas tiesioginis kontaktas su sukčiavimo auka, o pati turtinė teisė gali būti nesunkiai perduodama per kelias ar keliolika sekundžių. Turtinės teisės sąvoka yra dualistinė – pirma, turtinė teisė turi objektą, antra, ji pati yra objektas, kuris kažkam priklauso (Fedosiuk, 2008, p. 74). Turtinė teisė kaip turtinių nusikalstamų veikų dalykas apima tuos civilinių teisių objektus, kurie atitinka „bekūnio“ daikto sampratą, pvz., reikalavimo teisės prievolėje, prekės ženklas, firmos vardas, negrynieji pinigai, komercinės paslaptys, dizainas, išradimas, patentas, licencija ir kt. (Lietuvos Aukščiausiojo Teismo 2013 m. spalio 22 d. nutartis baudžiamojoje byloje). Pvz., Lietuvos bankas tyrė atvejį, kai asmuo prisijungdamas per Google paieškos sistemoje surastą trečiųjų asmenų suklastotą banko, pavadinimu „www.paeysera.com“ puslapį, atskleidė savo prisijungimo prie banko „www.paysera.lt“ paskyros duomenis bei SMS žinute gautą vienkartinį saugos kodą, kuriuo buvo patvirtintas trečiųjų asmenų prisijungimas prie pareiškėjo paskyros iš kito įrenginio. Taip asmuo neteko 500 Eur sumos (Lietuvos banko 2021 m. lapkričio 24 d. ginčo byla). Kitas elektroninio sukčiavimo pavyzdys, kurio metu pervedami negrynieji pinigai, galėtų būti APP (angl. *authorised push payment*), kuris suprantamas kaip piniginių lėšų pervedimas per greitųjų mokėjimų sistemą, kai asmuo ketino pervesti lėšas tam tikram asmeniui, tačiau buvo apgautas ir lėšos nukeliavo į kito asmens sąskaitą (Lending standards board, 2019). Taigi, elektroninis sukčiavimas yra palankus lengvai ir greitai užvaldyti asmens nematerialųjį turtą, dažnu atveju negrynuosius pinigus, esančius asmens elektroninėje banko sąskaitoje.

Elektroninio sukčiavimo sudėtis taip pat, kaip ir paprasto sukčiavimo, yra materiali, taigi elektroninis sukčiavimas laikomas baigtu, kai atsiranda turtinė žala. Tai lemia, jog būtinas ir priežastinio ryšio egzistavimas tarp veikos (apgaulės panaudojimo ir turto užvaldymo ar turinės teisės įgijimo) ir jos sukeltų padarinių (turtinės žalos). Toks priežastinio ryšio nustatymas elektroninėje erdvėje yra painus (Civilka *et al.*, 2004, p. 523), ypač vertinant turto ar turtinės teisės netekusio asmens veiksmų aspektu.

Taip pat, kaip ir minėta, elektroninis sukčiavimas išsiskiria ir įrankių naudojimu – įrankiu tampa bet koks įrenginys, kurio pagalba pasiekiama elektroninė erdvė – informacijos srautas, bei vieta, kuri peržengdama materialaus fizinio pasaulio ribas, persikelia į virtualią – kibernetinę erdvę.

Kitas sudėties ypatumas yra pats elektroninius sukčiavimus vykdantis subjektas. Nors jis laikomas bendruoju sukčiavimo subjektu, t. y. bet kuris pakaltinamas, sulaukęs 16 m. amžiaus

fizinis asmuo, tačiau toks asmuo, dažnu elektroninio sukčiavimo atveju, pasižymi ir tam tikromis ypatybėmis – informacinių žinių turėjimu, elektroninių programų ir sistemų veikimo supratimu ir pan. Praktika rodo, kad elektroninis sukčiavimas išsiskiria savo intelektualumu, taip pat yra sunkiai atskleidžiamas, kadangi kaltininkai dažniausiai jį suplanuoja nepriekaištingai (Civilka *et al.*, 2004, p. 523). Nors kai kuriuos elektroninio sukčiavimo veiksmus galima atlikti naudojant slaptažodžio atspėjimą ir kitus paprastus metodus, nereikalaujančius technologinio supratimo, daugumai elektroninio sukčiavimo atvejų reikia tam tikrų įgūdžių ir techninių žinių (Holt, 2017, p. 4). Techniniai įgūdžiai gali lemti ir paties sukčiavimo įgyvendinimo pasisekimą, pavyzdžiui, pastabūs vartotojai pamatę įtartiną elektroninį laišką gali jį ignoruoti, tačiau internetinių sukčių sukurtą fiktyvią banko interneto svetainę, kurios dizainas labai panašus į oficialios, nedideliu kompiuteriniu raštingumu pasižymintiems asmenims gali būti sunku atskirti. Įdomu ir tai, kad asmens fizinės savybės, tokios kaip lytis, amžius, ūgis, išvaizdos ypatybės, elektroninio sukčiavimo atveju yra nematomos, priešingai nei atliekant paprastą sukčiavimą, po kurio pagal kriminalistinės taktikos rekomendacijas atliekant nukentėjusiojo asmens apklausą, rekomenduojama išsiaiškinti subjekto fizines ypatybes (Kurapka *et al.,* 2013, p. 793). Elektroninėje erdvėje asmuo gali būti identifikuojamas ne pagal savo fizines savybes, o pagal kompiuterio, naršyklės ar kito įrenginio ar sistemos duomenis, pavyzdžiui, IP (angl. *internet protocol*) adresą – kompiuterio identifikatorių tinkle, kuris yra nesunkiai pakeičiamas naudojant VPN (angl. v*irtual private network*) programas, kas pasunkina ir pačio subjekto nustatymą. Taigi, sukčiavimo subjektas visuomet bus fizinis asmuo, kuris elektroninėje erdvėje dažnu atveju veikia neatskleisdamas savo tapatybės – anonimiškai. Tai lemia ir sunkumus išaiškinant elektroninį sukčiavimą padariusį asmenį.

Apibendrinant, sukčiavimas elektroninėje erdvėje gali būti suprantamas siaurąja ir plačiąja prasme. Siaurąja prasme, sukčiavimas siejamas su kompiuteriniu sukčiavimu, kuris tiek tarptautiniuose teisės aktuose, tiek Europos Sąjungos teisės aktuose yra suprantamas kaip neteisėtas poveikis kompiuteriniams duomenims ar kompiuterinei sistemai, įgyjant turtinės naudos. Plačiąja prasme sukčiavimas elektroninėje erdvėje, siejamas su elektroninės erdvės naudojimu, įgyjant turtinės naudos, nepriklausomai ar joje esantys duomenys ar programos buvo kaip nors paveikti. Lietuvoje elektroninis sukčiavimas patenka į bendrą BK 182 str. dispoziciją ir suprantamas plačiąja prasme (apimant sukčiavimą siaurąja prasme). Todėl, atsižvelgiant į aptartus sukčiavimo sudėties požymius ir elektroninės erdvės, kaip elektroninio sukčiavimo pasireiškimo terpės specifiką, elektroninį sukčiavimą reikėtų suprasti plačiąja

prasme ir jis turėtų būti apibūdinamas kaip nusikaltimas, padaromas naudojantis elektronine erdve, kurio metu panaudojant apgaulę, asmuo, paprastai turintis specialių žinių, pasinaudodamas išmaniaisiais įrenginiais, įgyja savo ar kitų asmenų naudai turtą, turtinę teisę, išvengia turtinės prievolės ar ją panaikina, taip padarydamas kitam subjektui turtinės žalos. Šis sukčiavimo elektroninėje erdvėje aiškinimas yra svarbus, siekiant suprasti jo padarymo būdus ir tendencijas Lietuvoje.

1.2. Sukčiavimą elektroninėje erdvėje lemiantys veiksniai

Aptarus elektroninio sukčiavimo sampratą, toliau darbe aptariami veiksniai, lemiantys sukčiavimo elektroninėje erdvėje padarymą bei elektroninio sukčiavimo pasireiškimo būdus. Sukčiavimo elektroninėje erdvėje veiksnių analizė leis geriau suprasti šios nusikalstamos veikos ypatumus bei kitas tik šiai nusikalstamai veikai aktualias ypatybes. Todėl toliau aptariami elektroninį sukčiavimą lemiantys veiksniai, siekiant geriau suprasti elektroninio sukčiavimo padarymo priežastis ir tolesnį veikos mechanizmą.

Elektroninį sukčiavimą, kaip ir bet kurią nusikalstamą veiką, gali lemti daugybė veiksnių: nuo individualių psichologinių, iki labiau ekonominių, socialinių ar techninių. Tam tikro nusikalstamo elgesio veiksnius išskiria pozityvistinės kriminologijos teorijos, kurių yra įvairių – nuo pabrėžiančių biologinę žmogaus prigimtį (Čezarė Lombrozo) iki žvelgiančių į socialinį išmokimą (Edwinas Sutherlandas) (Sakalauskas *et al.*, 2011, p. 280). Visgi, elektroninį sukčiavimą ir jo mastą gali sąlygoti ne tik bendrieji, tačiau ir specialieji veiksniai, būdingi dėl šios nusikalstamos veikos padarymo elektroninėje erdvėje specifikos. Informacinių sistemų mobilumas, naujumas, didėjanti jos įtaka ir pasaulinė situacija (pvz., COVID-19 pandemija ir dėl jos įvesti apribojimai) sudaro tinkamas sąlygas asmenims elektroninėje erdvėje nusikalsti vis dažniau. Psichologinis pasitenkinimas, finansinė nauda, naujų galimybių realizavimas – visa tai galima pasiekti naudojantis ir piktnaudžiaujant informacinėmis technologijomis (Li, 2017, p. 124).

Greta politinių, socialinių-ekonominių, teisinių, socialinių-psichologinių veiksnių, kurie turi įtakos nusikalstamumui, elektroninių nusikaltimų, kartu ir elektroninio sukčiavimo kontekste pabrėžiami techninio pobūdžio veiksniai, kuriems priskiriamas nusikaltimus darančių asmenų apsirūpinimas techninėmis priemonėmis, programomis, kitų asmenų ribotas technologijų supratimas, tyrėjų techninės žinios ir apsirūpinimas techninėmis priemonėmis ir kt. Kaip minėta, elektroniniai sukčiavimai pasižymi vietos ypatumais – jie padaromi elektroninėje (kibernetinėje) erdvėje/aplinkoje. Ši erdvė kartu su specialių – techninių

informacinių žinių panaudojimu ne tik subjektui suteikia anonimiškumą, tačiau gali ir palengvinti nusikaltimo padarymą, jo eigą – dažnu atveju, asmenys būna įgudę ir turimomis informacinėmis žiniomis pasunkina šio nusikaltimo atskleidimą arba jį padaro visiškai neįmanomu. Elektroninė erdvė asmenims suteikia plačias galimybes panaudoti apgaulę ir neteisėtai gauti turtinės naudos panaudojant informacines žinias arba pasinaudojant nukentėjusiojo technologiniu neišprusimu ar teisėsaugos institucijų reikiamos įrangos stoka (Kakati, Goswami, 2019, p. 89).

Taip pat akcentuojamas ir psichologinis veiksnys, galintis skatinti elektroninio sukčiavimo padarymą. Psichologinis aspektas glaudžiai susijęs su prieš tai aptartu techniniu veiksniu, lemiančiu elektroninį sukčiavimą, nes neretai asmens savybės ar būdo ypatybės sąveikauja ir determinuoja asmens specialių – technologinių žinių panaudojimą. Mokslinėje literatūroje išskiriami šie psichologiniai veiksniai, turintys įtakos nusikaltimams, padaromiems elektroninėje erdvėje, kartu ir elektroniniam sukčiavimui: asmens padėtis ar tam tikros vykdomos funkcijos (pvz., asmuo užima programuotojo pareigas, susijusias su kompiuterinių sistemų saugojimu), asmens sumanumas (pvz., asmuo dirbantis su kompiuterinių sistemų apsauga, žino apsaugos sistemų trūkumus ir tuo gali nesunkai manipuliuoti), manipuliacija telkiant bendrininkus nusikaltimui vykdyti, lankstumas, susidorojimas su stresu ir kt. (Kakati, Goswami, 2019, p. 88). Sukčiavimui elektroninėje erdvėje dažnu atveju būdingas tam tikras išankstinis pasiruošimas, gebėjimas komunikuoti, veikti anonimiškai, kurie susiję su noru panaudoti turimas žinias sukčiavimui įgyvendinti.

Pastaraisiais metais didelę reikšmę įgijo ir kitas nusikalstamų veikų elektroninėje erdvėje, kartu ir elektroninio sukčiavimo, veiksnys – socialinis-ekonominis – ir viena jo pasireiškimo formų – pasaulinė-ekonominė situacija susijusi su COVID-19 pandemijos iššūkiais. COVID-19 pandemija turėjo didelę įtaką ir virtualaus gyvenimo augimui (didėjančiam ir dažnėjančiam elektroniniam apsipirkimui, bendravimui, naršymui, naudojimuisi įvairiomis lengvai prieinamomis elektroninėmis paslaugomis – SODRA, VMI ir kt.). Lietuvos Respublikos Valstybės kontrolė 2020 m. veiklos ataskaitoje pažymi, jog 2020 m. pandemija paskatino dar aktyvesnį visuomenės skaitmenizavimąsi: naudojimąsi elektroninėmis paslaugomis, darbą nuotoliniu būdu, internetinę prekybą, finansines operacijas, taigi ir nusikalstamos veikos elektroninėje erdvėje pavojų (Lietuvos Respublikos Valstybės kontrolė, 2020). Pabrėžiama, kad pandemija turėjo įtakos nusikaltimų elektroninėje erdvėje, įskaitant, bet neapsiribojant, ir elektroninio sukčiavimo, masto didėjimui ir augimui – registruoto nusikalstamumo kontekste, kibernetinių incidentų per pastaruosius metus padidėjo

beveik du kartus, o elektroniniai sukčiai siekė pasinaudoti kiekviena pasitaikiusia galimybe (Europos Komisijos pranešimas spaudai, 2022, p. 3). Pavyzdžiui, 2020 m. pandemijos pradžioje Europos kovos su sukčiavimu tarnyba (toliau – OLAF) pradėjo tyrimą dėl neteisėtos elektroninės prekybos asmeninėmis apsaugos priemonėmis ir kitomis medžiagomis, susijusiomis su COVID-19 pandemija. 2021 m. OLAF tyrimų metu buvo nustatyti įtartini ūkio subjektai ir konfiskuota daugiau kaip 100 mln. su COVID-19 susijusių produktų. Tarp jų buvo rankų dezinfekavimo priemonių, kuriose buvo didelis kiekis metanolio, nestandartinių veido kaukių ir suklastotų testavimo rinkinių siuntų (Europos Komisijos pranešimas spaudai, 2022, p. 22).

Greta šių elektroninį sukčiavimą sąlygojančių veiksnių, išskiriama ir daugiau kitų papildomų veiksnių, būdingų elektroniniams nusikaltimams, įskaitant ir sukčiavimą elektroninėje erdvėje, pavyzdžiui:

1. Informacijos paplitimas, kuris ypač būdingas elektroniniam sukčiavimui, nukreiptam į juridinius asmenis, kai įmonės viešina daug informacijos apie save, savo turimą turtą, o įmonėms vadovaujantys asmenys apie savo laisvalaikio bei atostogų planus (Li, 2017, p. 112). Šis informacijos viešumas ir prieinamumas leidžia elektroniniams sukčiams geriau apgalvoti sukčiavimo strategijas ir inicijuoti sukčiavimą nusitaikant į konkretų įmonės materialųjį ar nematerialųjį turtą.

2. Taip pat išskiriamas ir elektroninis sukčiavimas iš neapykantos. Neapykanta gali kilti dėl įvairių priežasčių, pvz., nepatenkinti darbuotojai kenkia darbdavio turtui, disidentai yra motyvuoti sunaikinti valstybės infrastruktūrą, teroristai rengia išpuolius prieš taikinius nepriklausomai nuo jų pobūdžio ir kt. (Li, 2017, p. 115). Taigi, šiuo atveju greta savanaudiškų siekių, išryškėja ir kiti, kurie dažnu atveju tik pastipriną pasiryžimą daryti elektroninį sukčiavimą.

3. Konkurencija rinkoje taip pat yra vienas iš elektroninio sukčiavimo veiksnių, kai sukčiai gauna naudos iš konkurentų nuosmukio ir savo rinkos dalies padidėjimo (Li, 2017, p. 118).

Taigi, siekiant pabrėžti elektroninio sukčiavimo masto didėjimą svarbu akcentuoti ir galimas to priežastis. Nors sukčiavimą elektroninėje, kaip ir kitas nusikalstamas veikas elektroninėje erdvėje sąlygoja bendrieji veiksniai, tokie kaip ekonominiai, socialiniai, politiniai ir kt., teisės mokslo darbuose autoriai išskiria ir tam tikrus specifinius veiksnius – technologinę įtaką, psichologinius faktorius ar naujų galimybių nusikalsti elektroninėje erdvėje atsiradimą,

kuris ypač išryškėjo po pasaulį sukrėtusios COVID-19 pandemijos iššūkių. Todėl elektroninio sukčiavimo motyvai dažnai skiriasi priklausomai nuo siekiamų tikslų.

Vis dėlto, aptarti elektroninį sukčiavimą lemiantys veiksniai suponuoja ir keletą elektroninio sukčiavimo ypatumų, kuriais pasižymi visos sukčiavimo elektroninėje erdvėje nusikalstamos veikos: i) šią veiką ruošiamasi atlikti iš anksto, ji dažnai būna detaliai suplanuota; ii) elektroninė erdvė leidžia užtikrinti didesnį subjektų, padariusių nusikalstamą veiką, anonimiškumą, palengvina veikos atlikimą; iii) neretai subjektų turimos specialios žinios koreliuoja su subjektų psichologinėmis savybėmis ir noru šias žinias realizuoti.

1.3. Elektroninio sukčiavimo padarymo būdai

Aptarus elektroninio sukčiavimo veiksnius, svarbu paminėti ir elektroninio sukčiavimo pasireiškimo būdus, t. y., kaip dažniausiai realizuojamas sumanymas ir kaip kibernetinė erdvė padeda bei sudaro sąlygas nusikalsti. Kadangi, šiame magistro darbe elektroninis sukčiavimas analizuojamas per šio fenomeno ypatumus Lietuvos kontekste, tampa svarbu paminėti tuos elektroninio sukčiavimo pasireiškimo būdus, kurie mūsų šalyje yra labiausiai paplitę. Lietuvos policija 2020 m. balandžio 16 d. pateikė duomenis apie labiausiai paplitusius ir aktualiausius sukčiavimo būdus ikiteisminio tyrimo institucijų tyrimo praktikoje (Lietuvos policija, 2020).

1.3.1. Telefoninis sukčiavimas

Naudodami šį būdą sukčiai telefonu susisiekia su potencialia auka, dažnu atveju prisistato kaip asmenys, kurie atstovauja tam tikroms autoritetingoms institucijoms (pvz., bankų, policijos, VMI darbuotojai), ir pateikdami tariamą, neegzistuojančią situaciją, siekia išgauti iš asmenų tam tikrus duomenis (pvz., elektroninės bankininkystės duomenis), arba kitaip pasinaudodami asmens patiklumu siekia gauti tam tikros turtinės naudos (pvz., praneša apie neva įvykusį nelaimingą įvykį arba artimo asmens tariamą skolą, su tikslu gauti tam tikrą pinigų sumą). Šis būdas yra plačiai paplitęs ir kitose šalyse. Europos Komisija 2020 m. apklausoje dėl vartotojų patirties susiduriant su sukčiavimais ir apgavyste nurodė, jog telefono skambučiai tebėra svarbus sukčiavimo ir apgaulės kanalas, sudarantis net 28 proc. visų tirtų elektroninio sukčiavimo atvejų (Europos Komisija, 2020). Žvelgiant į kasacinio teismo praktikos pavyzdžius, buvo tirtas atvejis, kai asmuo paskambino nukentėjusiajam į telefoną ir apgaulingai prisistatęs ikiteisminio tyrimo pareigūnu pranešė neva nukentėjusiojo sūnus sužalojo mergaitę, o už gydymą reikia sumokėti tam tikrą pinigų sumą. Nukentėjusysis pervedė prašomą sumą dalimis, o kaltininkas taip apgaule įgijo svetimą turtą (grynuosius pinigus, kurie

buvo išgryninti ir perduoti asmeniui) (Lietuvos Aukščiausiojo Teismo 2012 m. gruodžio 18 d. nutartis baudžiamojoje byloje).

1.3.2. Avansinis sukčiavimas

Šis sukčiavimo būdas paprastai pasitelkiamas, kai lankomuose internetiniuose skelbimų portaluose paskelbiami melagingi skelbimai apie pigiau už įprastą rinkos kainą arba įprasta rinkos kaina parduodamą prekę, tačiau siekiant įsigyti tokią prekę prašoma pervesti išankstinį mokėjimą (avansą) tam, jog prekė pasiektų pirkėją. Vis dėlto, asmuo prekės negauna, skelbimas pašalinamas, o pirkėjas yra užblokuojamas. Šiuo atveju apgaulė pasireiškia tuo, jog viena sutarties šalis, sudariusi sutartį, iš kitos šalies priima pinigus (avansą) už sutartyje numatytų savo pareigų įvykdymą (dažnu atveju prekių perdavimą), tačiau tuo metu jau žino, kad nurodytų veiksmų neatliks, taigi tokiais veiksmais ši šalis apgauna kitą sutarties šalį (Pranka, 2012, p. 66). Pavyzdžiui, vienoje kasacinio teismo nagrinėtoje byloje asmuo buvo nuteistas už sukčiavimą, nes interneto puslapyje www.skelbiu.lt paskelbė netikrą skelbimą apie tariamai parduodamą žaidimų konsolę „SONY Playstation 4“ su dviem valdymo pulteliais ir keliais žaidimais. Nukentėjusiajam susitarus dėl žaidimų konsolės pirkimo ir pervedus pinigus į nurodytą banko sąskaitą, žaidimų konsolės su priedais nukentėjusiajam neišsiuntė (Lietuvos Aukščiausiojo Teismo 2019 m. liepos 3 d. nutartis baudžiamojoje byloje).

1.3.3. Neatsiskaitymas už prekę (pirkinių įgijimas sukčiavimo būdu)

Šis būdas panašus į prieš tai aptartą – avansinio sukčiavimo būdą. Skirtumas tas, kad šiuo atveju elektroniniai sukčiai veikia kaip klientas, t. y. pagal internete paskelbtus asmenų skelbimus apie kompiuterių, mobiliojo ryšio telefonų ir kitos technikos pardavimą, klientais prisistatantys sukčiai susitaria už prekę sumokėti negrynaisiais pinigais atlikdami banko pavedimą, po to suklastotą atlikto pavedimo patvirtinimą išsiunčia pardavėjui. Taip sukčiai įtikina pardavėją, kad banko pavedimas yra atliktas, o pinigai greitu metu pasieks pardavėjo sąskaitą. Apgautas pardavėjas išsiunčia arba perduoda prekę, o „pirkėjas“ prekę atsiima. Kasacinio teismo praktikoje buvo nagrinėtas toks atvejis, kai turėdamas tikslą apgaule savo naudai įgyti svetimą turtą, iš anksto žinodamas, kad už įgyjamas prekes neatsiskaitys, asmuo mobiliojo ryšio telefonu paskambino į bendrovę bei užsisakė prekių už 2 300 Eur vertės sumą. Kai prekės buvo pristatytos per kurjerių tarnybą į nurodytą adresą, asmuo už gautas prekes neatsiskaitė, prekių negrąžino ir taip apgaule įgijo bendrovei priklausantį turtą (Lietuvos Aukščiausiojo Teismo 2020 m. gegužės 20 d. nutartis baudžiamojoje byloje).

1.3.4. Lėšų išviliojimas prisidengiant įvairiomis investavimo platformomis

Šiam sukčiavimo modeliui būdinga tai, jog su asmenimis susisiekia (dažniausiai per mobiliojo ryšio telefonus) asmenys, siūlantys užsiimti investavimo veikla (investuoti į valiutas, akcijas, nekilnojamą turtą ir kt.) bei žadantys greitą pinigų grąžą per itin trumpą laikotarpį. Asmenims sudaroma iliuzija, kad po finansinių operacijų neva bus gaunamas tam tikras pelnas, taip sukčiai toliau siūlo plėtoti veiklą ir „investuoti“ dar daugiau. Galiausiai, asmenims, norintiems atgauti investuotas lėšas ir uždirbtą pelną, pranešama, kad pirma reikia sumokėti mokesčius ir tik tada pinigai bus pervesti per lengvatinio apmokestinimo (vadinamąją ofšorinę) bendrovę užsienyje, o vėliau pasieks ir nukentėjusiojo banko sąskaitą. Tačiau pinigai taip ir nėra pervedami. Taip pat šiomis dienomis toks modelis pasireiškia ir kitais moderniais būdais, pvz., naudojant sunkiai atsekamą kriptovaliutų sistemos tinklą, kai asmeniui sudaromas įspūdis, jog bus investuojama į kriptovaliutas, o bandant išsiimti investicijas, dingsta ir asmens lėšos ir tinklapis (Popper, 2018). Tokios veikos pavyzdžiai buvo nagrinėti ir LAT praktikoje. Vienoje byloje asmenys buvo nuteisti už tai, kad organizavo seminarus ir pateikdami klaidinančią informaciją siūlė asmenims investuoti 12 mėnesių į 10 metų pensijų programas, po nustatyto laiko žadėdami garantuotą investicinę grąžą, atsižvelgiant į mokėtos sumos dydį. Tam, kad siūlomos programos keltų pasitikėjimą, seminaro lankytojams buvo dalijama reklaminė medžiaga, kurioje lentelėmis bei diagramomis buvo pavaizduotas išmokamų palūkanų dydis ar papildoma kasmėnesinė suma, priklausanti nuo indėlio sumos. Taip buvo suklaidinti 167 seminaruose dalyvavę asmenys (Lietuvos Aukščiausiojo Teismo 2015 m. kovo 31 d. nutartis baudžiamojoje byloje).

1.3.5. Kiti elektroninio sukčiavimo būdai

Nors Lietuvos policijos 2020 m. balandžio 16 d. duomenų suvestinėje pateikiami tik tie elektroninio sukčiavimo būdai, kurie dažniausiai pasitaiko ikiteisminio tyrimo institucijų praktikoje, atsižvelgiant į šių dienų aktualijas, teisės mokslo doktrinoje ir praktikoje yra išskiriami ir kiti, vis dažniau Lietuvoje pasitaikantys elektroninio sukčiavimo būdai.

1.3.5.1. Sukčiavimas susijęs su asmens tapatybę patvirtinančių duomenų panaudojimu

Šio pobūdžio sukčiavimas yra susijęs su trimis būdais, kurių pagalba elektroniniai sukčiai pasinaudodami apgaule, gali neteisėtai užvaldyti asmens duomenis, siekiant gauti turtinės

naudos – fišingu (angl. *phishing),* smišingu (angl. *smishing*), višingu (angl. *vishing*) (Kalaharsha, Mehtre, 2021, p. 2).

Fišingas (angl. *phishing*) – tai elektroninio sukčiavimo būdas, kai aukas bandoma apgauti apgaulingomis el. laiškuose esančiomis nuorodomis. Nuoroda paprastai nukentėjusįjį nukreipia į iš pažiūros oficialų tinklapį, kuriame prašoma įvesti vartotojo vardą, slaptažodį, sąskaitos numerį ar kitą privačią informaciją. Po to ši informacija siunčiama sukčiams, o auka apie tai gali nieko nežinoti. Pavyzdžiui, elektroniniame laiške gali būti nurodyta, kad asmens banko sąskaita užblokuota, ir prašoma spustelėti nuorodą, kad asmuo atgautų prieigą. Iš tikrųjų ši nuoroda veda į apgaulingą tinklapio formą, kurioje paprasčiausiai renkama privati asmens informacija, pavyzdžiui, internetinės bankininkystės vartotojo vardas ir slaptažodis. Gavus šią informaciją, sukčiai gali prisijungti prie asmens paskyros ir pasisavinti pinigus (Chalil, 2020).

Smišingas (angl. *smishing*) – dar vadinamas SMS (angl. *short message service*) žinučių sukčiavimu. Smišingas taip pat vykdomas siekiant iš pradžių įgyti asmens duomenis, įskaitant asmeninę informaciją, finansinę informaciją, ir taip iš asmenų išvilioti pinigus ar kitą turtą ar turtinę teisę. Smišingo atveju sukčiai siunčia apgaulingus pranešimus SMS žinutėmis, kuriose yra kenkėjiška nuoroda arba nuoroda, kurią paspaudus į įrenginį įdiegiama kenkėjiška programa (Proofpoint, 2022). Šios apgaulingos SMS žinutės gali atrodyti kaip skubūs prašymai, siunčiami, pavyzdžiui, iš banko ar siuntų pristatymo tarnybos. Juose gali būti nurodoma, kad iš asmens banko sąskaitos yra išimta didelė suma arba kad reikia susekti dingusį siuntinį. Į šią apgavystę gali būti lengva įkliūti, jei asmuo įsitikinęs, jog turi imtis skubių veiksmų, kad išspręstų „skubią" problemą.

Višingas – šis elektroninio sukčiavimo būdas dar žinomas kaip fišingas balsu (angl. *voice phishing*). Šis elektroninio sukčiavimo būdas pasireiškia, kai naudojant balso žinutes iš aukų gaunami asmeniniai duomenys arba pinigai. Višingo atveju neretai naudojami automatiniai balso įrašai aukoms vilioti (Kalaharsha, Mehtre, 2021, p. 2). Galimos višingo pasekmės: asmens pokalbių pasiklausymas, neteisėta prieiga prie sąskaitų ar kredito kortelių informacijos, balso pašto perkrova (arba nepageidaujami balso pašto pranešimai) ir telefono numerių rinkimas (galiojančių telefono numerių rinkimo metodas) (Sjouwerman, 2021).

Už neteisėtą asmens duomenų įgijimą aptartais fišingo, smišingo ir višingo būdais, su tikslu šiuos duomenis panaudoti finansinėms operacijoms atlikti, baudžiamoji atsakomybė numatyta LR BK 214 str., o neteisėtas įgytų asmens duomenų panaudojimas finansinėms operacijoms atlikti būtų kvalifikuojamas kaip LR BK 214 str., BK 215 str. ir LR BK 182 str. sutaptis (Lietuvos Aukščiausiojo Teismo 2001 m. spalio 9 d. nutartis baudžiamojoje byloje).

1.3.5.2. „Romantinis sukčiavimas“.

Šis sukčiavimas dar yra žinomas kaip sukčiavimas pasitelkiant socialinius tinklus. Paprastai sukčiai galimos aukos ieško socialiniuose tinkluose ir internetinių pažinčių svetainėse bei programėlėse (pvz., Meta „Facebook“, Tinder, Discord ir pan.). Romantiniai sukčiai, skirtingai nei telefoniniai sukčiai, kurie veikia operatyviai ir greitai, pinigų vilioti neskuba, jiems svarbu įtikinti auką, užmegzti kontaktą. Bendravimas įprastai pradedamas rodant „nuoširdų“ susidomėjimą ir palaikant pokalbį. Visgi, tokio bendravimo eigoje, sukčiai pasitelkia įtaigias manipuliacijos technikas, taip įgyjant aukos pasitikėjimą. Scenarijų ir istorijų gali būti įvairių – nuo apsimetimo žinomu asmeniu, kurio mokėjimo kortelė neva buvo užblokuota, taip prašant pervesti tam tikrą sumą, iki netikrų socialinių tinklų anketų kūrimo ir pinigų viliojimo žadant ateityje juos grąžinti. SEB banko duomenimis, 2021 m. romantiniai sukčiai iš Lietuvos gyventojų išviliojo 0,6 mln. Eur (SEB, 2022). Žvelgiant per teismų praktikos išaiškinimus, pavyzdžiui, vienoje byloje buvo analizuojamas atvejis, kai moteris buvo nuteista už sukčiavimą, nes panaudodama apgaulę, įgijo didelės vertės turtą. Tiksliau, naudodamasi elektroninėmis ryšio priemonėmis užsiregistravo pažinčių svetainėje, pateikdama kito žmogaus išvaizdą, t. y. žinomos svetimos merginos kito socialinio bendravimo tinklalapio nuotraukas, susikūrė melagingą anketą ir taip susipažino su nukentėjusiuoju. Asmenys pradėjo bendrauti, kaltininkė teigė, kad nori su nukentėjusiuoju užmegzti ilgalaikius santykius, kurti bendrą gyvenimą. Taip įgijus nukentėjusiojo pasitikėjimą, aktyviai, sistemingai ir neketindama vykdyti savo įsipareigojimų teikė jam tikrovės neatitinkančią informaciją, t. y., kad serga jos motina, kurios operacijai reikalingi pinigai, taip pat pinigai reikalingi ir kelionei iš Lietuvos į Naująją Zelandiją. Nuteistoji nuolat prašė nukentėjusiojo paskolinti pinigų, galiausiai jį įtikino pinigus paskolinti, o pinigus išgryninusi, dingo. Tokie nuteistosios veiksmai buvo kvalifikuoti kaip sukčiavimas (Lietuvos Aukščiausiojo Teismo 2019 m. birželio 28 d. nutartis baudžiamojoje byloje).

Apibendrinant, galima daryti pagrįstą išvadą, jog kasdienėms funkcijoms persikėlus į virtualią erdvę, elektroniniai sukčiai surado naujų būdų veikti. Ikiteisminio tyrimo institucijų praktikoje daugiausiai pasitaiko telefoninio, avansinio, pirkinių įsigijimo panaudojant apgaulę, investicinio sukčiavimo atvejų. Šiuos sukčiavimo būdus svarbu išskirti ir dėl toliau analizuojamos elektroninio sukčiavimo statistikos, parodančios elektroninio sukčiavimo tendenciją.

1.4. Sukčiavimo elektroninėje erdvėje tendencijos

Išnagrinėjus elektroninį sukčiavimą lemiančius veiksnius bei padarymo būdus, toliau analizuojamos sukčiavimo elektroninėje erdvėje tendencijos Lietuvoje. Įvertinus registruoto sukčiavimo tendencijas, plačiau nagrinėjamas ir šios nusikalstamos veikos latentiškumas, analizuojami atvejai ir priežastys, dėl kurių elektroninis sukčiavimas lieka už registruotos statistikos ribų.

1.4.1. Registruoti sukčiavimai elektroninėje erdvėje ir jų tendencijos Lietuvoje

Į teisėsaugą ir elektroninio saugumo industriją nukreipti elektroninių nusikaltimų tyrimai dažnu atveju skirti skaitmeninei kriminalistikai ir elektroninių nusikaltimų prevencijai (Šupa, 2021, p. 20).

Sukčiavimas elektroninėje erdvėje patenka į bendrą sukčiavimo (BK 182 str.) dispoziciją, todėl elektroninio sukčiavimo atvejams Lietuvos Respublikos mastu atskleisti, pradžioje svarbu apžvelgti bendrą registruoto sukčiavimo statistiką. Nusikalstamų veikų žinybinio registro (toliau – NVŽR) duomenimis (*1 lentelė*) 2019 m. Lietuvoje buvo užregistruotas 2 981 sukčiavimo atvejis, iš jų 1 806 nusikalstamos veikos buvo ištirtos. 2020 m. Lietuvoje buvo registruoti 2 685 sukčiavimo atvejai, iš jų 1 656 atvejai buvo ištirti, o 2021 m. matomas sukčiavimo atvejų Lietuvoje didėjimas – fiksuoti 3 169 atvejai (didžiausias atvejų skaičius nuo 2015 m., kai buvo užfiksuoti 4 489 atvejai). 2021 m., sukčiavimų ištyrimo skaičius itin mažas – buvo ištirtas 1 441 sukčiavimo atvejis. 2022 m. matomas registruotų sukčiavimo atvejų didėjimas – registruotos 3 859 veikos. Ištirtų atvejų skaičius lieka panašus kaip ir 2021 m. – iš 3 859 veikų ištirti 1 418 atvejai. Iš pateikiamos statistikos, matyti, kad bendro registruoto sukčiavimo atvejų skaičius pastaraisiais metais išliko panašus, didėjimas matomas nuo 2020 m., o ištirtų atvejų dalis išlieka gana panaši, svyruoja tarp 40–60 proc. ištiriamų registruoto sukčiavimo atvejų. Bendro sukčiavimo statistika yra aktuali siekiant parodyti registruoto sukčiavimo (BK 182 str.), įskaitant ir elektroninį sukčiavimą, paplitimą Lietuvoje.

1 lentelė. **Registruotos sukčiavimo nusikalstamos veikos (LR BK 182 str.) Lietuvoje 2015–2022 m.**

Metai	Užregistruota nusikalstamų veikų	Ištirtos nusikalstamos veikos	Ištirtų nusikalstamų veikų proc.
2015 m.	4 486	2 968	66,2 proc.
2016 m.	3 112	2 681	86,2 proc.
2017 m.	2 999	1 928	64,3 proc.
2018 m.	2 783	1 552	55,8 proc.
2019 m.	2 981	1 806	60,6 proc.
2020 m.	2 685	1 856	69,1 proc.
2021 m.	3 169	1 441	45,5 proc.
2022 m.	3 859	1 418	36,7 proc.

Šaltinis: Nusikalstamų veikų žinybinio registro duomenys.

NVŽR neišskiria atskiros sukčiavimų, padaromų elektroninėje erdvėje statistikos rodiklių. Visgi, elektroninio sukčiavimo mastą ir paplitimą, galima įvertinti iš kitų institucijų ar įstaigų pateikiamų duomenų.

Pavyzdžiui, Lietuvos Banko duomenimis (*2 lentelė*) Lietuvos Respublikos gyventojai, patikėję sukčiais, kurie veikia investicinio sukčiavimo srityje, 2017 m. prarado 700 000 Eur, 2018 m. fiksuota rekordiška suma – 1 100 000 Eur. 2018 m., Lietuvos bankui pradėjus blokuoti neteisėtus investavimo pasiūlymus siūlančias svetaines, gerokai sumažėjo gyventojų finansiniai nuostoliai – 2019 m. gyventojai prarado 300 000 Eur, 2020 m. – 538 000 Eur, o 2021 m. – 559 000 Eur sumą. Taigi, nors 2018 m., Lietuvos bankui pradėjus imtis prevencinių priemonių prieš elektroninius sukčius, veikiančius investavimo srityje, buvo užfiksuotas sumų, kurias prarado Lietuvos Respublikos gyventojai, sumažėjimas, visgi, nuo 2019 m. šis skaičius vėl augo. To priežastys gali būti įvairios – didesnis gyventojų patiklumas, vis tobulėjantys elektroninių sukčių veikimo metodai, didesnis naudojimasis išmaniaisiais įrenginiais ir pan.

2 lentelė. **Registruoto investicinio sukčiavimo duomenys**

	Gyventojai, patikėję sukčiais, iš viso prarado	Didžiausia suma, kurią prarado vienas gyventojas	Skundai, pateikti Lietuvos bankui dėl sukčių
2017 m.	700 000 Eur	500 000 Eur	62 skundai
2018 m.	1 100 000 Eur	210 950 Eur	70 skundų
2019 m.	300 000 Eur	97 000 Eur	99 skundai
2020 m.	538 000 Eur	137 269 Eur	60 skundų
2021 m.	559 000 Eur	125 000 Eur	46 skundai

Šaltinis: Lietuvos banko duomenys.

Lietuvos bankų asociacijos (toliau – LBA) duomenimis finansiniai sukčiai iš Lietuvos gyventojų ir įmonių 2022-aisiais išviliojo beveik 12 mln. eurų (Lietuvos banku asociacija, 2023). 2021 m. finansiniai sukčiai išviliojo 10,2 mln. Eur – dukart daugiau nei 2020 m., kai nuostoliai sudarė 4,8 mln. Eur.

Vertinant elektroninio sukčiavimo atvejų tendencijas, pastebėtina, kad LBA duomenys rodo elektroninio sukčiavimo atvejų augimą. Pavyzdžiui, vadovaujantis LBA duomenimis, 2021 m. pustrečio karto išaugo elektroninio sukčiavimo atvejų skaičius: 2021 m. LBA priklausantys finansų bei kredito rinkos dalyviai fiksavo 3 511 sukčiavimo atvejus elektroninėje erdvėje, palyginti su 2020 m., kai buvo fiksuoti 1 336 atvejai. Tokią pačią išvadą patvirtina ir 2022 m. pirmo pusmečio duomenys. Nuo 2022 m. sausio iki balandžio pradžios LBA priklausančiuose bankuose užfiksuoti 1 056 sukčiavimo atvejai – dvigubai daugiau nei analogišku laikotarpiu 2021 m. (Lietuvos bankų asociacija, 2022).

Toliau analizuojant LBA duomenis, pastebėtina, kad labiausiai paplitę elektroninio sukčiavimo būdai – fišingas ir smišingas. LBA teigimu, 2022 metais bene labiausiai paplitęs sukčiavimo būdas buvo fišingas, kai gyventojams siunčiami elektroniniai laiškai, primenantys banko ar kitų institucijų pranešimus, turint tikslą išvilioti interneto banko prisijungimo duomenis, patvirtinti apgaule atliekamus pavedimus ir pan. Per metus LBA nariai fiksavo 3 500 fišingo atvejų, tai yra beveik tris kartus daugiau nei 2021 metais. Investicinio sukčiavimo, kai asmenims žadama didelė grąža už investuotus pinigus, užfiksuotų incidentų skaičius taip pat augo (2021 m. fiksuoti 576 atvejai, 2022-aisiais – 852 atvejai), tačiau per metus šia schema išviliotų lėšų suma mažėjo nuo 3 mln. eurų iki 2 mln. eurų.

Akcentuotina, kad taip pat matomas ir smišingo augimas. LBA duomenys rodo, kad 2022 m. pirmąjį ketvirtį augo smišingo atvejų skaičius: 2022 m. pirmąjį ketvirtį iš gyventojų ir įmonių buvo išviliota 342 tūkst. Eur, t. y. penkiskart daugiau lėšų nei pirmąjį ketvirtį 2021 m.

Matoma, kad 2022 m. kaip elektroninio sukčiavimo tendencija vis dar išlieka fišingas, telefoninis sukčiavimas, daugėja ir smišingo atvejų. LBA prezidentės Eivilės Čepkutės teigimu „Tendencija aiški – sukčiai neketina trauktis iš Lietuvos elektroninės erdvės bei nuolat didina resursus, nukreiptus į atakų organizavimą“.

Be to, didėja ir kitų – mažiau modernių – elektroninio sukčiavimo atvejų. Pavyzdžiui, 2022 m. daugiau kaip šimtu padaugėjo registruotų romantinio sukčiavimo atvejų – nuo 195 iki 322, tačiau dėl šio scenarijaus patirtų nuostolių suma per metus pakito nedaug.

Taigi, elektroninio sukčiavimo atvejų skaičius išlieka didelis. Daugiausiai elektroninių sukčiavimų, LBA duomenimis, padaroma naudojant fišingo, smišingo būdus, taip pat aktyviai nusikalstamas veikas daro ir telefoniniai sukčiai. Taip pat stebimas ir naujų elektroninio sukčiavimo formų, pavyzdžiui, romantinio sukčiavimo, atvejų augimas. Populiarus ir investicinis sukčiavimas žadant greitą finansinę naudą. Pateikta statistika rodo, kad elektroninis sukčiavimas Lietuvoje retai apima sudėtingas sukčiavimo schemas bei dažniausiai yra susijęs su asmens duomenų išviliojimu pakankamai nesudėtingais būdais (sukuriant į oficialią panašią svetainę ar pan.). Tokie LBA duomenys Autorei leidžia daryti išvadą, kad šių elektroninio sukčiavimo būdų skaičiaus didėjimą gali lemti didelis gyventojų patiklumas, informacinių žinių stoka, naivumas.

Analogišką išvadą pagrindžia ir kiti šaltiniai, kuriuose yra analizuojami elektroninio sukčiavimo atvejai. Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos (toliau – NKSC) duomenimis 2021 m. išlieka tendencija, kad nusikalstamumą elektroninėje erdvėje labiausiai lemia sukčiavimo atvejai, jie 2021 m. sudarė dominuojančią 71 proc. dalį, palyginti su kitomis elektroninėje erdvėje padarytomis nusikalstamomis veikomis. Dominuojantys sukčiavimo elektroninėje erdvėje būdai 2021 m. buvo fišingas ir telefoninis sukčiavimas (apgaulingi skambučiai ir smišingas), kurie sudarė 70 proc. visų sukčiavimo atvejų, investicinis sukčiavimas – 17 proc., sukčiavimas panaudojant bendravimo programėles – 8 proc. (Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos, 2022, p. 9). Taigi, matyti, kad NKSC duomenys iš esmės sutampa ir su LBA pateiktais duomenimis bei rodo panašias tendencijas.

Apibendrinant bei įvertinant minėtuose šaltiniuose pateiktus duomenis, galime įžvelgti šias sukčiavimo elektroninėje erdvėje tendencijas: i) bendroje nusikalstamų veikų, padarytų

elektroninėje erdvėje, statistikoje elektroniniai sukčiavimai sudaro didžiąją dalį. Tai yra elektroninėje erdvėje labiausiai paplitusios nusikalstamos veikos; ii) sukčiavimų elektroninėje erdvėje atvejų skaičius pastaraisiais metais auga arba išlieka didelis. Gyventojai vis dažniau nukenčia nuo elektroninių sukčiavimų bei didėja elektroninių sukčiavimų metu padaroma žala; iii) didžioji dalis elektroninio sukčiavimo atvejų, tikėtina, nėra ištiriami; iv) Lietuvoje dominuoja keletas elektroninio sukčiavimo būdų – fišingas, smišingas, telefoninis sukčiavimas. Šių elektroninių sukčiavimo atvejų skaičius auga. Ši aplinkybė kartu su kitais paplitusiais elektroninio sukčiavimo atvejais rodo, kad gyventojai yra gana patiklūs, detaliai neperžiūri ir kritiškai neįvertina ar nežino, kaip tinkamai įvertinti, gautą informaciją.

1.4.2. Sukčiavimo elektroninėje erdvėje latentiškumas

Įvertinus viešai prieinamus sukčiavimo elektroninėje erdvėje duomenis ir tendencijas, toliau analizuojamas elektroninio sukčiavimo latentiškumas, siekiant suprasti ir jo priežastis.

Elektroninis sukčiavimas, kaip ir kitos nusikalstamos veikos, kurios padaromos elektroninėje erdvėje pasižymi latentiškumu (Sakalauskas *et al.,* 2011, p. 174). Lotynų kalbos žodyne „*lateo*“ reiškia „būti pasislėpusiam, slypėti, slėptis“. Latentiniu nusikalstamumu įvardijami faktiškai padarytų, tačiau nepatekusių į apskaitą, ar neužregistruotų arba neatskleistų nusikaltimų (nusikalstamų veikų) visumos raiškos procesai. Šių nusikaltimų skaičius niekada nėra tiksliai žinomas, lieka užslėptas, neaiškus (Babachinaitė *et al.*, 2009, p. 9). Tai reiškia, jog statistikose pateikiami tik registruoto nusikalstamumo duomenys, neįtraukiant latentinių nusikaltimų, taigi dažnu atveju statistika atspindi tik nedidelę dalį viso nusikalstamumo. Latentiškumui paaiškinti, dažnai vaizduojama ledkalnio viršūnės arba piltuvėlio metafora.

Elektroninių nusikaltimų, įskaitant ir sukčiavimą elektroninėje erdvėje, latentiškumo priežastys gali būti įvairios.

Pirma, pelno siekiančioms bendrovėms labiau rūpi ne pats nusikaltimas ir kaip jį atskleisti, o kaip užtikrinti jų kompiuterinių sistemų saugumą, nustatyti elektroninio sukčiavimo metu padarytą finansinę žalą, nuostolius, taip pat prevencijos būdai ir priemonės, kad ateityje tokių įvykių būtų išvengta. Dėl šių priežasčių privačios įmonės labiau linkusios atlikti savo vidinius tyrimus tokiems atvejams tirti (savo jėgomis arba pasamdydamos privačius informacinės saugos ekspertus) ir neviešinti kylančių problemų (Sakalauskas *et al.*, 2011, p. 176).

Antra, latentiškumo priežastimi gali būti ir technologinės kliūtys. Prie technologinių kliūčių priskiriama teisėsaugos institucijų kvalifikacijos bei technologinių priemonių, būtinų

tirti tokio pobūdžio nusikaltimus, trūkumas. Sukčiavimas elektroninėje erdvėje, kaip ir kiti elektroninio pobūdžio nusikaltimai, gali pasižymėti sudėtingomis schemomis, kurias yra dar sunkiau išaiškinti, neturint visos reikiamos įrangos ar kvalifikuotų specialistų. 2020 m. liepos 16 d. Valstybinio audito ataskaitoje teigiama, kad net ir egzistuojant specializuotiems nusikaltimų elektroninėje erdvėje tyrimo padaliniams, jų veikimo rezultatyvumas nėra pakankamas. Valstybės kontrolė pažymi, kad mažėja ikiteisminių tyrimų perduodamų į teismą, o daugiau nei trečdalis ikiteisminių tyrimų trunka ilgiau nei 9 mėnesius, taip pat nustatomi trūkumai priimant procesinius sprendimus. Valstybės kontrolė pažymi, jog aukštesnieji prokurorai, atlikdami tikrinimus nustato, kad ne visais atvejais buvo kreiptasi į užsienio valstybes, siekiant gauti tyrimui svarbios informacijos, neišsamiai atliekami ikiteisminiai tyrimai, nutarimuose daromos išvados prieštarauja tyrimo metu nustatytoms faktinėms aplinkybėms, laiku neatliekami ikiteisminio tyrimo veiksmai ir t. t. (Valstybės kontrolė, 2020, p. 36–37). Visgi, šis ikiteisminių tyrimų, susijusių su nusikaltimais elektroninėje erdvėje, įskaitant ir elektroninį sukčiavimą, nerezultatyvumas siejamas su tuo, jog ikiteisminiai tyrimai, kuriems būdingas sistemiškumas, yra sudėtingi ir komplikuoti, nes vykdant šio pobūdžio nusikaltimus naudojama daug įvairių technologinių išteklių. Be to, tokius nusikaltimus darantys asmenys gali veikti gerai organizuotose grupėse kartu su įvairiose pasaulio šalyse esančiais bendrininkais.

Trečia, elektroninio sukčiavimo nepatekimą į statistiką gali lemti ir tai, jog pačios aukos nėra suinteresuotos pranešti apie sukčiavimą. Doktrinoje toks aukos elgesys, kai nepranešama apie elektroninius nusikaltimus, įskaitant ir elektroninį sukčiavimą, yra siejamas su tuo, jog naudingumas iš tokio pranešimo yra mažas (UNODC, 2019). Naudingumo vertinimo, kurį mato auka, priežastys gali būti įvairios, įskaitant gėdą, susijusią su tapimu elektroninio sukčiavimo auka (pvz., romantinio sukčiavimo atveju), riziką reputacijai, susijusią su elektroninio sukčiavimo viešinimu (pvz., jei elektroninio sukčiavimo auka yra privati įmonė, atskleidus, jog prieš ją buvo nukreiptas elektroninis sukčiavimas, tokia įmonė gali prarasti vartotojų pasitikėjimą). Pavyzdžiui, Eurobarometro duomenimis, 2022 m. Lietuvoje iš apklaustų ir kibernetinius incidentus patyrusių smulkių ir vidutinių įmonių, didžioji dalis jų apie įvykusius kibernetinius incidentus nepranešė ir nesikreipė į teisėsaugos institucijas (56 įmonės), o į teisėsaugos institucijas kreipėsi vos 13 įmonių (Europos Komisija, 2022). Visgi, pagal 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos Reglamentą (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas)

įmonėms, kaip asmens duomenų tvarkytojoms nustatyta pareiga pranešti kompetentingoms institucijoms apie bet kokius pažeidimus, susijusius su asmens duomenimis, įskaitant elektroninį sukčiavimą, tačiau praktika rodo, kad įmonės dažnu atveju delsia atlikti tokius veiksmus (pvz., CityBee atvejis). Taip pat prie priežasčių priskiriamas ir menkas pasitikėjimas teisėsauga ar mažas lūkestis, kad teisėsaugos institucijos gali asmeniui padėti. Be to, pranešimas apie elektroninį sukčiavimą, asmenų nuomone, gali reikalauti daug laiko ir pastangų, asmenys nežino kur kreiptis, kam pranešti.

Ketvirta, elektroniniai sukčiai deda daug pastangų, kad paslėptų savo tapatybę ir buvimo vietą. Šie asmenys gali naudoti VPN (angl. *virtual private network*) ir tarpinius serverius (angl. *proxy*), kad paslėptų savo tikrąjį IP (angl. *internet protocol*) adresą, todėl labai sunku išsiaiškinti, kur jie iš tikrųjų yra. Tarpinius serverius arba VPN paslaugas teikianti bendrovė paprastai turi savo įrašuose tikrąjį IP adresą, tačiau jei ji nenori savanoriškai dalytis šia informacija, ikiteisminio tyrimo institucijos turi gauti teismo nutartį, kad priverstų ją tai padaryti. Taip pat tokio pobūdžio nusikaltimai dažnai pasižymi tuo, jog nusikaltėlis ir auka yra skirtingose valstybėse, taigi kyla ir jurisdikcijos problematika. Todėl tyrimas gali būti apsunkintas ir užimti daug laiko, jei sukčiai veikia iš užsienio valstybės arba pati auka yra užsienyje.

Elektroninį sukčiavimo latentiškumą lemiančių priežasčių kiekis ir įvairovė suponuoja ir tai, kad yra labai tikėtina, jog Lietuvoje į oficialią statistiką nėra įtraukiama didelė dalis elektroninio sukčiavimo atvejų. Kaip ir minėta, tiek juridiniai asmenys, tiek ir fiziniai asmenys nėra suinteresuoti pranešti apie elektroninio sukčiavimo atvejus dėl netinkamo jų nagrinėjimo, galimos reputacinės ar/ir turtinės rizikos ir t. t. Tikėtina, kad tai lemia ganėtinai aukštą elektroninio sukčiavimo latentiškumo laipsnį bei apsunkina galimybes tinkamai įvertinti Lietuvoje vyraujančias tendencijas.

Taigi, didelė dalis elektroninio sukčiavimo, kaip ir kitų elektroninių nusikaltimų, neiškyla į viešumą, kartu nepatenka į oficialią statistiką, todėl vertinant statistinius duomenis, svarbu suvokti, jog statistika gali netinkamai atspindėti realią padėtį. Didelį elektroninio sukčiavimo latentiškumą gali sąlygoti šie faktoriai – aukos vengimas informuoti apie elektroninį sukčiavimą, kuris gali būti susijęs tiek su baime prarasti klientus, susigadinti reputaciją, tiek gėdos jausmu. Taip pat elektroninio sukčiavimo latentiškumui daro įtaką ir ikiteisminio tyrimo institucijų techninių priemonių arba kvalifikacijos stoka (trūksta itin kvalifikuotų specialistų). Galiausiai, elektroniniai sukčiai taip pat įdeda daug pastangų, kad paslėptų savo tapatybę ir buvimo vietą ar sukčiavimo schemas.

2. SUKČIAVIMO ELEKTRONINĖJE ERDVĖJE BAUDŽIAMOJO PERSEKIOJIMO YPATUMAI IR PROBLEMOS

2.1. Sukčiavimo elektroninėje erdvėje kvalifikavimo problemos

Aptarus sukčiavimo elektroninėje erdvėje sudėties požymius bei padarymo būdus, kyla elektroninio sukčiavimo atskyrimo nuo kitų nusikalstamų veikų, padaromų elektroninėje erdvėje, klausimas. Iš analizuotos elektroninio sukčiavimo sudėties bei jo pasireiškimo būdų, galima įžvelgti, kad elektroninis sukčiavimas parodo egzistuojantį ryšį tarp apgaulės panaudojimo, neteisėto naudos gavimo ir naudojimosi elektroninių įrenginių pagalba. Tokie elektroninio sukčiavimo požymiai kelia klausimų ir dėl kitų nusikalstamų veikų, ypač padaromų elektroninėje erdvėje, kvalifikavimo bei atskyrimo. Pavyzdžiui, ar neteisėtas konfidencialių nukentėjusiojo duomenų įgijimas, neteisėtas prisijungimas prie sistemos ir kiti veiksmai turėtų būti priskirti sukčiavimui ar vis dėlto, tai yra atskiros nusikalstamos veikos? Atitinkamai toliau aptariamas elektroninio sukčiavimo santykis su kitomis elektroninėje erdvėje padaromomis nusikalstamomis veikomis.

Visų pirma, elektroninis sukčiavimas neretai susijęs su duomenų ir informacinių sistemų konfidencialumo pažeidimais. Neteisėtas duomenų, kurie leidžia identifikuoti asmenį elektroninėje erdvėje, įgijimas dažnai yra tarpinis etapas siekiant šiuos duomenis panaudoti sukčiaujant ar atliekant kitas nusikalstamas veikas (Kalpokas, Marcinauskaitė, 2012, p. 32). Kaip buvo atskleista poskyryje apie elektroninio sukčiavimo padarymo būdus, konfidencialūs duomenys gali būti neteisėtai įgyjami, pavyzdžiui, fišingo (angl. *phishing)*, smišingo (angl. *smishing*), višingo (angl. *vishing*) ar kitais fiziniais ar elektroniniais būdais.

Vis dėlto, sukčiavimo sudėtis neapima neteisėto duomenų gavimo, o baudžiamoji atsakomybė už įvairius elektroninių duomenų ir informacinių sistemų saugumo pažeidimus yra daugiausiai nustatyta BK XXX skyriuje (Nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui). Todėl praktikoje nustačius, kad nusikalstama veika yra susijusi su disponavimu įrenginiais, programine įranga, slaptažodžiais, kodais ar kitais duomenimis, siekiant daryti nusikalstamas veikas (šiuo atveju elektroninį sukčiavimą), tokioms veikoms kvalifikuoti taikytinas BK 198^2 straipsnis (o ne BK 182 str.). Pavyzdžiui, Vilniaus miesto 1-asis apylinkės teismas asmeniui inkriminavo BK 198^2 straipsnį dėl to, jog asmuo neteisėtai disponavo netikru internetinės bankininkystės paslaugos puslapiu, sukurtu banko klientų prisijungimų prie elektroninės bankininkystės paslaugos tarnybinės stoties kodams ir slaptažodžiams fiksuoti (Vilniaus miesto 1-ojo apylinkės teismo 2009 m. rugsėjo 14 d. baudžiamasis įsakymas).

BK 198 straipsnis taip pat numato atsakomybę už neviešų elektroninių duomenų perėmimą ir panaudojimą. Kaip nurodoma teismų praktikoje, BK 198 straipsnis saugo neviešų elektroninių duomenų konfidencialumą. Nevieši elektroniniai duomenys – tai bet kokia informacija, kurios tvarkymui naudojamos informacinių technologijų priemonės bei su kuria susipažinti turi teisę ribotas asmenų ratas (Kauno apygardos teismo 2017 m. rugsėjo 27 d. nuosprendis baudžiamojoje byloje).

BK 198^1 straipsnyje įtvirtinta atsakomybė už neteisėtą prisijungimą prie sistemos. Šiuo atveju svarbu, kad neteisėtai prisijungdamas prie sistemos, asmuo gali lengvai pasiekti ir šioje sistemoje esančius konfidencialius duomenis (Abramavičius *et al.*, 2009, p. 436).

Antra, baudžiamoji atsakomybė už kai kuriuos elektroninių duomenų konfidencialumo pažeidimo aspektus įtvirtinta ir BK 214, 215 straipsniuose, numatančiuose baudžiamąją atsakomybę už neteisėtą disponavimą elektronine mokėjimo priemone bei neteisėtą jos panaudojimą finansinei operacijai atlikti. Analizuojant BK 214 bei 215 straipsnių santykį su elektroninio sukčiavimo norma, teismų praktikoje išaiškinta, jog svetimo mokėjimo instrumento panaudojimu inicijuojant finansinę operaciją ir siekiant užvaldyti svetimą turtą tiesiogiai kėsinamasi į norminiais aktais apibrėžtą mokėjimo kortelių naudojimo tvarką bei svetimą turtą. Svetimu mokėjimo instrumentu inicijuodamas ir atlikdamas finansinę operaciją su sąskaitoje esančiais pinigais, kaltininkas operacinei banko sistemai save pateikia kaip asmenį, turintį teisę atlikti tokias operacijas ir teisę į sąskaitoje esančius pinigus, t. y. užvaldo turtą suklaidindamas elektroninę sistemą, taip pat ir banką (Lietuvos Aukščiausiojo Teismo 2005 m. lapkričio 15 d. nutartis baudžiamojoje byloje). Nuo tokios nusikalstamos veikos nukenčia du nusikalstamo kėsinimosi objektai, todėl svetimo mokėjimo instrumento įgijimas bei panaudojimas didesnei nei 1 MGL dydžio finansinei operacijai inicijuoti kvalifikuotinas kaip BK 214, 215 ir 182 straipsniuose numatytų nusikalstamų veikų sutaptis.

Taigi BK 198 straipsnyje atsakomybė numatyta už neviešų elektroninių duomenų perėmimą ir panaudojimą, BK 198^2 straipsnis iš esmės apibrėžia neteisėtą slaptažodžių, prisijungimo kodų ar kitokių panašių duomenų įgijimą, laikymą ir kitas veikas, o BK 198^1 straipsnyje atsakomybė nustatyta už neteisėtą prisijungimą prie sistemos. BK 214 straipsnyje kriminalizuotas neteisėtas elektroninių mokėjimo priemonių teisėto naudotojo tapatybės patvirtinimo priemonių duomenų, pakankamų finansinei operacijai inicijuoti, įgijimas ar laikymas, o BK 215 str. kriminalizuotas šių duomenų panaudojimas finansinei operacijai atlikti. Tokia situacija iš esmės leidžia kalbėti apie baudžiamosios teisės normų konkurenciją,

kai padarytos nusikalstamos veikos sudėties požymiai atitinka ne vieną, o kelias baudžiamojo įstatymo normas.

Žvelgiant į šių normų santykį ir atribojimo kontekstą, galima paminėti šiuos esminius aspektus: BK 198 straipsnyje esantys nusikalstamos veikos požymiai yra bendresnio pobūdžio – įtvirtinamas „neviešų duomenų“ požymis, o BK 198^2 straipsnyje „nevieši duomenys“ yra detalizuojami – BK 198^2 straipsnio dalykas – slaptažodžiai, prisijungimo kodai ar kitokie panašūs duomenys. BK 214, 215 straipsnių dalykas dar siauresnis – elektroninių mokėjimo priemonių naudotojo tapatybės patvirtinimo priemonių duomenys, pakankami finansinei operacijai inicijuoti. Taigi, atribojant šias nusikalstamas veikas, svarbu paminėti teisinėje literatūroje suformuotą baudžiamosios teisės normų konkurencijos įveikimo taisyklę, kad esant bendrosios ir specialiosios normos konkurencijai, taikoma specialioji norma (Pavilonis, 1996, p. 40):

1) BK 198^2 straipsnyje nurodyti slaptažodžiai, prisijungimo kodai ar kitokie panašūs duomenys gali būti ir BK 214 straipsnyje numatytu dalyku, jei jie yra elektroninės mokėjimo priemonės naudotojo tapatybės patvirtinimo priemonių duomenys, pakankami finansinei operacijai inicijuoti. Šiuo atveju, nustačius, kad kaltininkas neteisėtai įgijo tuos elektroninius duomenis, kurie yra pakankami finansinei operacijai inicijuoti, jo veika turėtų būti kvalifikuojama taikant BK 214, o ne BK 198^2 straipsnį (Kalpokas, Marcinauskaitė, 2012, p. 44).

2) Nustačius, kad asmuo neteisėtai įgijo BK 214 straipsnyje nurodytus požymius turinčius duomenis, jo veika kvalifikuotina ne pagal bendrąją BK 198 straipsnyje numatytą normą, o pagal specialiąją – esančią BK 214 straipsnyje. Jei asmuo šiuos duomenis panaudojo didesnei nei 1 MGL dydžio finansinei operacijai inicijuoti, veikos kvalifikuojamos kaip BK 214, 215 ir 182 str. sutaptis. Taip pat svarbu pažymėti, jog BK 214, 215 str. pasikėsinimo dalykas – mokėjimo instrumentas – tai toks elektroninis instrumentas, kuris skirtas atsiskaityti ne grynaisiais pinigais (pavyzdžiui, banko mokėjimo kortelės, kredito kortelės ir kt.). Mokėjimo instrumento sąvoka neapima identifikavimo kodų generatoriaus, nes jo pagalba yra tik generuojami (sukuriami) kodai, bet nevykdomi atsiskaitymai ne grynaisiais pinigais (Vilniaus apygardos teismo 2011 m. gruodžio 23 d. nuosprendis baudžiamojoje byloje). Todėl, tais atvejais, kai neteisėtai įgyjami ir panaudojami identifikavimo kodų generatoriaus duomenys, siekiant neteisėtai įgyti turtinės naudos, veika kvalifikuojama kaip 198 ir 182 str. idealioji sutaptis. Šiuo atveju, BK 214, 215 str. neinkriminuojami.

3) Informacinės sistemos, atliekančios duomenų perdavimo, apdorojimo procesus, prieinamos tik prieigos teisę prie šių sistemų turintiems asmenims. Nusikalstama veika, pasireiškianti neteisėtu prisijungimu prie informacinės sistemos pažeidžiant informacinės sistemos apsaugos priemones, yra numatyta BK 198^1 straipsnyje (Kalpokas, Marcinauskaitė, 2012, p. 45). Nors šis etapas sukčiavimo elektroninėje erdvėje padarymo schemose yra tarpinis, tačiau jis yra neišvengiamas ir būtinas, kaltininkui siekiant atlikti neteisėtą lėšų pervedimą mokėjimo sistemoje. Todėl tais atvejais, kai sukčiavimas padaromas prieš tai neteisėtai prisijungiant prie informacinės sistemos, veika kvalifikuojama pagal BK 198^1 bei 182 str. (Lietuvos Aukščiausiojo Teismo 2012 m. birželio 26 d. nutartis baudžiamojoje byloje). Visgi, autorė R. Marcinauskaitė bei autorius V. Kalpokas pastebi, jog kylant konkurencijai tarp BK 198^1 str. ir BK 215 str., pirmenybė suteikiama BK 215 str. (Kalpokas, Marcinauskaitė, 2012, p. 48). Kasacinio teismo praktikoje taip pat pažymėta, kad BK 215 straipsnis taikytinas tais atvejais, kai neteisėtos mokėjimo operacijos yra inicijuojamos ar atliekamos naudojantis elektroninės bankininkystės paslaugomis elektroninėje sistemoje suvedus naudotojo tapatybės patvirtinimo priemonių duomenis (autorizavus mokėjimo operaciją) (2012-05-02 Teismų praktikos sukčiavimo baudžiamosiose bylose apžvalga).

Taigi, minėtos veikos ir jų atribojimas tik parodo, jog sukčiavimas elektroninėje erdvėje yra sudėtingas procesas, kurio padarymui neretai būtini tam tikri veiksmai, kurie vertinami ne tik kaip atskiri etapai, siekiant vieningo nusikalstamo tikslo – sukčiauti elektroninėje erdvėje, tačiau kurių neapima bendroji sukčiavimo norma (BK 182 str.), ir kurie kvalifikuojami atskirai. Autorės nuomone, veikų atskyrimo atvejai, kai greta sukčiavimo (BK 182 str.), kaltininkui inkriminuojami ir kiti straipsniai, susiję su neteisėtu disponavimu duomenimis, sistema ir pan., yra vertintini teigiamai, kadangi asmuo darydamas šias nusikalstamas veikas kėsinasi į visiškai skirtingas teisės saugomas vertybes – elektroninio sukčiavimo (BK 182 str.) atveju kėsinamasi į nuosavybę bei jos įgijimo pagrindus, o papildomos BK XXX skyriuje numatytos nusikalstamos veikos saugo elektroninių duomenų ir informacinių sistemų saugumą.

2.2. Baudžiamojo persekiojimo už sukčiavimą elektroninėje erdvėje jurisdikcija

Valstybės baudžiamoji jurisdikcija įgyvendinama principų, kurie apibrėžia tos valstybės baudžiamųjų įstatymų galiojimą erdvėje, pagrindu. Baudžiamoji jurisdikcija gali remtis teritoriniu principu, taip pat baudžiamųjų įstatymų galiojimo teisinė erdvė gali būti išplėsta pasitelkus eksteritorinės baudžiamosios jurisdikcijos principus (Nevera, 2006, p. 12). Mūsų BK greta teritorinio principo (BK 4 str.) pripažįsta ir įtvirtina aktyvųjį personalinį principą (BK

5 str.), realinį arba dar kitaip vadinamą – valstybės interesų apsaugos principą (BK 6 str.) bei universalųjį principą (BK 7 str.). Valstybės interesų apsaugos principas yra aktualus, kai kalbama apie nusikalstamas veikas, padarytas užsienyje, kuriomis kėsinamasi į Lietuvos Respublikos interesus, o universalusis principas yra pagrįstas *numerus clausus* principu, t. y. jame yra įtvirtintas baigtinis nusikalstamų veikų sąrašas, kurių atžvilgiu, šis principas yra taikomas (Nevera, 2006, p. 139). Universalusis principas neapima sukčiavimo elektroninėje erdvėje, todėl universalusis principas, kaip ir valstybės interesų apsaugos principai elektroninio sukčiavimo atveju nėra taikomi ir toliau šiame darbe nebus apžvelgiami.

Taip pat svarbu paminėti ir tai, jog BK neįtvirtina individualių interesų apsaugos (pasyvaus personalinio) principo, todėl sukčiavimo elektroninėje erdvėje, kaip ir kitų elektroninėje erdvėje padaromų veikų atveju, nėra galimybės nustatyti Lietuvos baudžiamąją jurisdikciją pagal nukentėjusiojo teisinį statusą, pavyzdžiui, Lietuvos pilietybę ar nuolatinę gyvenamąją vietą Lietuvoje. Taigi, aktualūs išlieka teritorinis principas, siejamas su nusikalstamos veikos padarymo vieta, bei aktyvios pilietybės principas, siejamas su tuo, jog Lietuva tam tikrais atvejais gali perimti Lietuvos piliečių baudžiamąjį persekiojimą dėl užsienyje padarytų nusikaltimų. Dėl ribotos darbo apimties plačiau nebus analizuojami *non bis in idem* (negalima bausti du kartus už tą patį) principas, ekstradicijos ar asmens perdavimo pagal arešto orderį klausimai. Toliau analizuojami teritorinio ir aktyvaus personalinio principo taikymo nusikalstamoms veikoms elektroninėje erdvėje, įskaitant ir elektroninį sukčiavimą, aspektai bei problematika.

2001 m. Europos Tarybos Konvencija dėl elektroninių nusikaltimų (kurioje be kita ko, įtvirtintas ir kompiuterinio sukčiavimo (elektroninio sukčiavimo siaurąja prasme) kriminalizavimas) nusikalstamoms veikoms, padaromoms elektroninėje erdvėje, nustato teritorinį (įskaitant valstybės vėliavos principą) bei aktyvųjį personalinį principą (Konvencijos 3 skirsnio 22 str. 1 d.). Konvencijos aiškinamojoje ataskaitoje (angl. *Convention on Cybercrime explanatory report*) atskleidžiant teritorinį principą, atkreipiamas dėmesys į tai, kad valstybė turi bausti už Konvencijoje minimą nusikalstamą veiką, jei ji padaryta tos valstybės teritorijoje. Pavyzdžiui, teritorinė jurisdikcija Konvencijos atveju būtų įgyvendinama tiek tada, kai abu – kaltininkas ir neteisėtai veikiamas prietaisas, kuriame yra asmens duomenys, kurie bus panaudojami sukčiaujant – yra valstybės teritorijoje, tiek ir tada, kai jos teritorijoje yra tik informacinės sistemos prietaisas, nors kaltininko joje ir nėra (Convention on Cybercrime explanatory report, 2001), pvz., fiktyvių elektroninių tinklalapių naudojimo atvejai.

2013 m. rugpjūčio 12 d. Europos Parlamento ir Tarybos Direktyva 2013/40/ES dėl atakų prieš informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR (toliau – Direktyva 2013/40/ES), nustato panašias jurisdikcijos taisykles, t. y. pabrėžia teritorinį bei aktyvųjį personalinį principą, tačiau svarbu paminėti, jog Direktyva 2013/40/ES, skirtingai nei Konvencija, nustato tik išimtinai dėl informacinių technologijų raidos atsiradusias nusikalstamas veikas, o tradicinių nusikalstamų veikų, padarytų elektroninėje erdvėje (tuo pačiu ir elektroninio sukčiavimo), ji nereguliuoja.

Jurisdikcijos klausimai Europos Sąjungos mastu išimtinai kompiuterinio sukčiavimo (elektroninio sukčiavimo siaurąja prasme) atvejais, sprendžiami pagal jau minėtą 2019 m. balandžio 17 d. Europos Parlamento ir Tarybos Direktyvą (ES) 2019/713 dėl kovos su sukčiavimu negrynosiomis mokėjimo priemonėmis ir jų klastojimu. Šioje Direktyvoje taip pat nustatomi du aktualūs jurisdikcijos principai – teritorinis bei aktyvusis personalinis.

Atkreiptinas dėmesys, jog tiek Europos Sąjungos, tiek tarptautinės teisės aktai nusikalstamų veikų elektroninėje erdvėje, taip pat ir elektroninio sukčiavimo atveju pirmumą teikia teritorinei jurisdikcijai, palyginti su kitais baudžiamosios jurisdikcijos principais (Klip, 2016, p. 209). Tokio požiūrio laikomasi ir teisės mokslo doktrinoje, kurioje nurodoma, jog „nepaisant nematerialios interneto prigimties teritorialumas vis dar laikomas pagrindiniu veiksniu“ (Valatkevičius, 2007, p. 136). BK 4 str. 2 d. įtvirtinanti, kad „nusikalstamos veikos padarymo vieta yra vieta, kurioje asmuo veikė arba turėjo ir galėjo veikti, arba vieta, kurioje atsirado baudžiamojo įstatymo numatyti padariniai“, yra skirta ne tik fizinei, bet ir elektroninei erdvei (Marcinauskaitė, 2021, p. 202). Šiuo aspektu svarbu ir tai, kad toks nusikalstamos veikos padarymo vietos aiškinimas turėtų būti taikomas visoms elektroninėms veikoms, suvokiant jas plačiąja prasme, todėl yra aktualus ir elektroninio sukčiavimo atveju (Marcinauskaitė, 2021, p. 207). Taigi, teritorinis principas akcentuoja veikų padarymą valstybės teritorijoje, tačiau ar gali būti apribojama, apibrėžiama ir prilyginama valstybės teritorijai pati elektroninė erdvė? Šį probleminį aspektą išryškina ir nusikalstamų veikų elektroninėje erdvėje, įskaitant ir elektroninį sukčiavimą, išplitimo mastas ir pobūdis bei tarpvalstybinis elementas (Xiaobing, Yongfeng, 2019, p. 724). Kita vertus, nors elektroninis sukčiavimas yra daromas elektroninėje erdvėje, tačiau panaudojant materialias priemones (elektroninius prietaisus), kurios egzistuoja tam tikroje valstybėje, taip pat pavojingų padarinių gali atsirasti fizinėje erdvėje.

Autorė R. Marcinauskaitė pažymi, jog nors elektroninė erdvė nėra analogiška fizinei erdvei (ji tiesiogiai neatkartoja tradicinių fizinės erdvės geografinių ribų), tačiau asmuo, atliekantis veiksmus elektroninėje erdvėje, niekada nebus tik elektroninėje erdvėje, o visada

bus pagal savo prigimtį abiejose erdvėse – fizinėje ir elektroninėje – tuo pačiu metu (Marcinauskaitė, 2021, p. 204). Tačiau, kadangi nematerialios elektroninės erdvės neįmanoma suskirstyti į atitinkamas teritorijas kaip fizinės erdvės, sprendžiant dėl teritorinės baudžiamosios jurisdikcijos iki galo lieka neaiškus veikos elektroninėje erdvėje padarymo vietos ir fizinės teritorijos ryšys (ypač atsižvelgiant į elektroninės erdvės globalumą ir decentralizaciją) (Marcinauskaitė, 2021, p. 203).

Kita vertus, kaip matyti, iš Konvencijos nuostatų, nusikalstamos veikos padarymo vietos apibrėžimas išplečiamas – nusikalstamos veikos padarymo vieta yra siejama ne tik su kaltininko, bet ir su informacinės sistemos buvimo vieta ar prietaisu, kuris naudojamas darant elektroninį sukčiavimą. Teisės mokslo autoriai taip pat pabrėžia, kad kompiuterinių nusikaltimų padarymo vieta yra „kompiuterinės įrangos ar elektroninių ryšių buvimo vieta“ (Valatkevičius, 2007, p. 136). Taigi, informacinės sistemos buvimo vieta leidžia susieti nusikalstamas veikas elektroninėje erdvėje, įskaitant elektroninį sukčiavimą su fizine erdve, su tam tikra teritorija ir sudaro galimybių atrasti fizinei erdvei – nors veika ir padaroma elektroninėje erdvėje, tačiau elektroninę erdvę sukuria informacinės sistemos ir prietaisai, esantys fizinėje erdvėje. Taigi, teisės mokslo darbuose akcentuojant, kad teritorinis baudžiamosios jurisdikcijos principas yra dominuojantis (įskaitant ir nusikalstamas veikas, kurios yra padaromos elektroninėje erdvėje), taip pat teigiama, jog yra būtina „rasti būdą kibernetinei veiklai „įžeminti“, ją susiejant ir su fizine erdve“ (Bernat, Godlove, 2012, p. 12).

„Lietuvos Respublikos tarptautinių sutarčių ir ES teisės aktų įgyvendinimas nacionalinėje materialiojoje baudžiamojoje teisėje galimas tik suderinus nacionalinio baudžiamojo įstatymo nuostatas su tarptautinės sutarties ar ES teisės aktų reikalavimais“ (Švedas *et al.,* 2017, p. 39). Lietuvai 2004 m. ratifikavus Konvenciją, taip pat perkėlus Direktyvos 2019/713 nuostatas į nacionalinę teisę, baudžiamojo įstatymo galiojimo asmenims, padariusiems nusikalstamas veikas Lietuvos valstybės teritorijoje (BK 4 str.), nuostatos keičiamos nebuvo. Atitinkamai, galima teigti, kad, įstatymo leidėjo nuomone, Lietuvos BK, įtvirtinantis teritorinį principą ir su juo susijusius nusikalstamos veikos padarymo vietos nustatymo klausimus, atitinka tiek Konvencijos, tiek Direktyvos 2019/713 nuostatas. Atsižvelgiant į tai, Lietuva turėtų užtikrinti savo teritorinės jurisdikcijos taikymą, jeigu kaltininkas padarė elektroninį sukčiavimą fiziškai būdamas jos teritorijoje. Taigi, kaip jau minėta, sukčiavimo elektroninėje erdvėje padarymo vieta galėtų būti laikoma ir ta vieta, kurioje kaltininkas panaudojo sukčiavimo padarymo priemones (įrankius) (pvz., kompiuterių tinklą) ar vieta, kurioje atsirado nusikalstamų padarinių. Šių priemonių (įrankių), panaudotų

nusikalstamai veikai daryti, buvimo vieta dėl informacinių sistemų veikimo ypatumų ir elektroninės erdvės globalumo gali nesutapti su kaltininko ar nukentėjusiojo turimo įrenginio buvimo vieta.

Nuostata, kad veikos padarymo vieta gali būti tiek kaltininko, tiek informacinės sistemos prietaiso buvimo vieta, išryškinama ir kasacinio teismo praktikoje. Pavyzdžiui, vienoje byloje kasacinis teismas padarė išvadą, kad Lietuva tinkamai taikė savo baudžiamąją jurisdikciją, nes minėtos kaltininko organizuotos atakos įvykdytos iš Lietuvos, nors ir buvo nukreiptos prieš informacinę sistemą Švedijoje. Teismas pažymėjo, jog „sprendžiant dėl <...> nusikalstamų veikų padarymo vietos, yra aktuali BK 4 straipsnio 2 dalis, kurioje nurodoma, kad nusikalstamos veikos padarymo vieta yra vieta, kurioje asmuo veikė arba turėjo ir galėjo veikti, arba vieta, kurioje atsirado baudžiamojo įstatymo numatyti padariniai. Taigi, nusikalstamo neteisėto poveikio informacinei sistemai padarymo vieta yra tiek ta, iš kurios buvo trikdomas tinklalapių darbas, tiek ir ta, kurioje kilo BK 197 straipsnyje nurodyti padariniai“ (Lietuvos Aukščiausiojo Teismo 2015 m. gegužės 12 d. nutartis baudžiamojoje byloje). Pavyzdžiui, sukčiavimo elektroninėje erdvėje atveju, kai nukentėjusį asmenį klaidinanti informacija siunčiama elektroniniu paštu, šio asmens suklaidinimas (apgaulės realizavimas) gali būti konstatuojamas ten, kur elektroniniai laiškai buvo gauti (Marcinauskaitė, 2021, p. 209).

Skirtingai nei nusikaltimo padarymo vietos atveju, kaltininko pilietybė yra daug lengviau nustatoma ir nepriklauso nuo ateritorinio interneto pobūdžio ir kompiuterinių duomenų. Valstybė tiek pagal Konvenciją, tiek pagal Direktyvą 2019/713, BK pripažįsta jurisdikciją, kai jos pilietis užsienyje padaro nusikaltimą, jeigu padaryta veika pripažįstama nusikaltimu ir už jos padarymą taip pat yra baudžiama ir pagal padarymo vietos valstybės baudžiamuosius įstatymus. Doktrinoje išsakoma pozicija, jog nusikaltėlio pilietybė yra lengviau nustatoma negu nusikaltėlio veikimo vieta, todėl būtent šiuo pagrindu elektroninio sukčiavimo, kaip ir kitų nusikalstamų veikų, padaromų elektroninėje erdvėje, yra lengviau nustatyti jurisdikciją nei prieš tai aptarto teritorinio principo taikymo atveju (Valatkevičius, 2007, p. 136).

Visgi, teisės mokslo doktrinoje pasisakoma, kad elektroninių nusikalstamų veikų, įskaitant ir elektroninį sukčiavimą, jurisdikcijų kolizijų atveju, sprendžiant klausimą, kuri valstybė turi artimiausią ryšį su padaryta nusikalstama veika elektroninėje erdvėje, suinteresuotos valstybės turėtų vadovaujantis „protingumo standartais, numatančiais daug veiksnių, kurie kiekvieną kartą turi būti įvertinti, sprendžiant, kuri valstybė turi artimiausią ryšį su padaryta nusikalstama veika“ (Valatkevičius, 2007, p. 131). Tokiu atveju vertinama, kiek esminis (svarbus) ryšys su konkrečios valstybės teritorija turi būti nustatytas, kad valstybė

galėtų konstatuoti savo baudžiamąją jurisdikciją dėl atitinkamos elektroninėje erdvėje padarytos veikos. Pavyzdžiui, elektroninio sukčiavimo atveju, kai fiktyvus tinklapis, kuris panaudojamas kaip apgaulės priemonė yra užsienyje esančiuose serveriuose, vertinant esminio ryšio kriterijų, atsižvelgiama į šios veikos sąsają su valstybės geografinėmis ribomis: ar interneto puslapis yra žinomas, lengvai prieinamas valstybės teritorijoje, ar jame pateikiama informacija valstybės kalba, ar tinklapyje pateikiamos nuorodos, turinčios sąsajų su valstybe, ar naudojamos tai valstybei žinomų asmenų nuotraukos, įvairūs faktai ar įvykiai, ar yra numatyta galimybė žadamas prekės siųsti (gabenti), paslaugas suteikti valstybės teritorijoje, jei sukčiavimas siejamas su prekių ar paslaugų užsakymu, ar iš valstybės teritorijos priimami mokėjimai ir pan. Būtent šių aplinkybių visuma rodo, kad veika ir panaudota apgaulė yra nukreipta į konkrečios valstybės teritoriją net ir tuo atveju, jei kaltininko ir informacinės sistemos buvimo vieta yra už šios valstybės teritorijos ribų (Marcinauskaitė, 2021, p. 212). Tačiau toks problemos sprendimas turi ir savų trūkumų: „protingumo standartai“ yra ganėtinai lankstūs, todėl nacionaliniai teismai gali juos interpretuoti sau palankiai siekdami pagrįsti jurisdikciją, nepaisant silpno veikos ryšio su valstybe.

Konvencija dėl elektroninių nusikaltimų baudžiamajam persekiojimui tinkamos jurisdikcijos nustatymo klausimą palieka spręsti pačioms valstybėms, kurios pareiškia teisę į jurisdikciją dėl konkretaus elektroninio nusikaltimo (Konvencijos 3 skirsnio 22 str. 5 d.). ES mastu yra priimtas 2009 m. lapkričio 30 d. Tarybos pamatinis sprendimas 2009/948/TVR dėl jurisdikcijos įgyvendinimo kolizijų baudžiamuosiuose procesuose prevencijos ir sprendimo, kuriame įtvirtintas bendradarbiavimas tarp valstybių narių ir tai, kad valstybių narių kompetentingos institucijos turėtų tiesiogiai konsultuotis, siekdamos konsensuso dėl veiksmingo sprendimo, kurio tikslas – išvengti paralelių procesų neigiamų padarinių ir atitinkamų kompetentingų institucijų laiko ir išteklių eikvojimo. ES kaip ir tarptautinėje teisėje, jurisdikcijos taikymo ir kolizijų sprendimo atvejus paliekama nusistatyti pačioms valstybėms narėms.

Taigi, nors elektroninei erdvei nėra būdingas materialumas, sprendžiant baudžiamosios jurisdikcijos nustatymo atvejus, nepaisant aktyvaus personalinio principo taikymo paprastumo, pirmumas suteikiamas teritoriniam baudžiamosios jurisdikcijos principui. Tačiau kiekvienu konkrečiu atveju būtina identifikuoti kriterijus, kurie leistų nusikalstamą veiką elektroninėje erdvėje (įskaitant ir elektroninio sukčiavimo atvejus) susieti su tam tikros valstybės teritorija. Kaltininko, įrankių (priemonių), kuriais kaltininkas padarė nusikalstamą veiką, ir informacinės sistemos, į kurią kėsinamasi (t. y. nusikalstamų padarinių), buvimo vieta gali ir nesutapti, tačiau

valstybės įgyvendina teritorinę baudžiamąją jurisdikciją, jei bent viena iš šių aplinkybių buvo/kilo tos valstybės teritorijoje. Toliau įvertinus objektyvius ir subjektyvius požymius ir nustačius veikos glaudų ryšį su valstybės teritorija, galima daryti išvadą, kad ši valstybė gali taikyti savo teritorinę jurisdikciją dėl šios veikos padarymo.

2.3. Sukčiavimo elektroninėje erdvėje duomenų (įrodymų) rinkimas ir panaudojimas

Padarius išvadą, jog sukčiavimui persikėlus iš fizinės – materialios erdvės į elektroninę, tampa sunkiau jį atskleisti, o elektroniniam sukčiavimui, kaip ir kitoms nusikalstamoms veikoms, pasižymint dideliu latentiškumo laipsniu, neišvengiamai susiduriama ir su įrodymų fiksavimo, rinkimo ir jų panaudojimo problematika tiriant ir atskleidžiant šį nusikaltimą. Elektroninio sukčiavimo atvejais mažai tikėtina rasti fizinius įrodymus, nes kaip ir minėta, pati veika yra padaroma elektroninėje erdvėje, todėl dažnu atveju kaip įrodymas gali būti naudojami duomenys, išlikę materialiose elektroninėse laikmenose, pavyzdžiui, mobiliajame telefone, kompiuteryje, el. pašto dėžutėje ir pan. Todėl yra aktualu įvertinti ir duomenų (įrodymų) rinkimo ir panaudojimo problematiką.

2.3.1. Sukčiavimo elektroninėje erdvėje duomenų rinkimas

Tiriant nusikalstamas veikas elektroninėje erdvėje, įskaitant ir elektroninį sukčiavimą, siekiant surinkti reikšmingų tyrimui duomenų, dažniausiai atliekami šie proceso veiksmai (Kurapka *et al*., 2013, p. 668):

1. **Krata ir poėmis**. Krata ir poėmis tiriant elektroninius sukčiavimus gali būti atliekami turint tikslą surasti ir paimti sukčiavimo įrankius/priemones (elektroninį įrenginį ar elektroninę laikmeną), dalyką, rezultatą ar kitus tyrimui reikšmingus duomenis ar informaciją. Rengiantis kratai ir poėmiui būtina išsiaiškinti, kokia programinė įranga ir technika yra tikrinamame objekte. Tokiais atvejais turi būti kviečiamas informacinių technologijų specialistas, ypač, kai naudojamos sudėtingos sukčiavimo schemos, įtraukiami fiktyvūs tinklalapiai ar programos, ruošiamos priemonės, kurias pasitelkus galima skaityti ir įrašyti paimtą informaciją, nustatoma, kokios informacijos reikia ieškoti (Kurapka *et al*., 2013, p. 663).

2. **Kompiuterinių ir kitokių elektroninių prietaisų apžiūra**. Kratos, poėmio ir apžiūros metu, tais atvejais, kai kompiuteris ar kitas prietaisas, kuris buvo panaudotas darant elektroninį sukčiavimą, yra įjungtas, tyrėjas turi kiek leidžia galimybės, nuodugniai aprašyti elektroniniame įrenginyje esantį vaizdą, jį užfiksuoti kriminalistinės fotografijos būdu, nustatyti, ar prie įtaiso yra prijungti išoriniai atminties įrenginiai (išorinis standusis diskas ir

kt.), nustatyti, ar yra naudojamos elektroninio ryšio priemonės, po šių veiksmų išjungti elektroninį prietaisą. Kai elektroninis įrenginys išjungtas, tyrėjui svarbu tinkamai užfiksuoti įrenginių ir pagalbinių prietaisų buvimo vietą, laidus kabelius bei tinkamai supakuoti tolesniems tyrimams (Kurapka *et al*., 2013, p. 665).

3. **Apklausa**. Tiriant elektroninio sukčiavimo atvejus yra svarbios nukentėjusiųjų, liudytojų ir įtariamųjų apklausos. Apklausos tikslas yra nustatyti sukčiavimo sudėties požymių egzistavimą, sukčiavimo padarymo laiką, būdą ir kitas aplinkybes, nukentėjusiojo veiksmus, jų seką, padarytos žalos dydį ir kt. (Kurapka *et al*., 2013, p. 665). Nukentėjusįjį tikslinga apklausti apie sukčiavimo aplinkybes, nukentėjusiojo veiksmus, padarytos žalos dydį. Liudytojais elektroninio sukčiavimo atveju gali būti asmenys, kurie anksčiau nukentėjo nuo kaltininko daromų sukčiavimų, tam tikrų svetainių ar serverių valdytojai arba asmenys, galintys duoti reikšmingos informacijos apie melagingo skelbimo ar anketos patalpinimo aplinkybes, ir pan. Apklausiant kaltininką, svarbu išsiaiškinti sukčiavimo objektyviuosius ir subjektyviuosius požymius.

4. **Ekspertizės skyrimas**. Tarp ekspertizių tyrimų rūšių, vertėtų paminėti informacinių technologijų tyrimą (ekspertizę) (Bilevičiūtė, Novikienė, 2010, p. 317–329). Šios ekspertizės metu gali būti tiriami šie objektai: a) aparatinė kompiuterių įranga; b) kompiuterių duomenų laikmenos; c) kompiuterio sistema – aparatinė įranga, sisteminė programinė įranga, taikomoji programinė įranga, duomenys; d) neapsaugoti slaptažodžiu kišeniniai kompiuteriai (delninukai), mobiliojo ryšio telefono aparatai, skaitmeniniai fotoaparatai; e) mokėjimo kortelės. Tiriant elektroninio sukčiavimo atvejus ir siekiant nustatyti nusikalstamos veikos aplinkybes, ekspertui gali būti užduodami šie klausimai: kokia informacija yra mobiliajame telefone? (Lietuvos teismo ekspertizės centre galima sužinoti visą informaciją, esančią mobiliajame telefone – skambučių registrą, kalendorių, darbotvarkės įrašus, SMS, EMS, MMS pranešimus, vaizdo, garso įrašus ir kt.). Ar kompiuteryje (duomenų laikmenoje), yra virusas? Kokio operatoriaus yra tyrimui pateikta SIM, eSIM kortelė? Ar el. laiške esanti nuoroda iš karto nuskaito visas asmens lėšas? Ir kt.

5. **Reikalavimas pateikti informaciją**. Telekomunikacijų, informacinių technologijų bendrovėms turint informaciją, reikšmingą tyrimui, prokuroras, priėmęs nutarimą ir gavęs ikiteisminio tyrimo teisėjo sutikimą, gali reikalauti šių bendrovių pateikti reikšmingus tyrimui duomenis (pavyzdžiui, siekiant identifikuoti asmenį, kuris naudojasi IP adresu ar pan.).

Vis dėlto, tokie standartiniai duomenų rinkimo veiksmai ne visais atvejais leidžia tinkamai ištirti nusikalstamas veikas, kurios padaromos naudojantis elektronine erdve. Kadangi

elektroninė erdvė suteikia galimybę padaryti nusikalstamas veikas naudojantis programomis, kurių valdytojai yra užsienyje, dažnai tyrimui aktuali informacija gali būti saugoma užsienio valstybėse (pavyzdžiui, jeigu veika atlikta naudojantis pažinčių programėle, programėlės valdytojas gali turėti informaciją apie naudotojo IP adresą ir pan., elektroniniai laiškai ar jų meta duomenys gali būti saugomi „debesų“ platformoje, kurios serveriai yra užsienio valstybėje, ir pan.). Todėl minėtos duomenų rinkimo priemonės gali būti neveiksmingos stengiantis išsiaiškinti padariusį elektroninį sukčiavimą asmenį. Tokia nusikalstamų veikų, kurioms padaryti naudojama elektroninė erdvė, specifika apsunkina įrodymų rinkimo procesą bei ilgina tyrimų trukmę (ypač, jeigu prie informacijos negalima prieiti iš pačio elektroninio įrenginio).

Pavyzdžiui, Europos Komisija yra pažymėjusi, kad skaitmeninių įrodymų rinkimą apsunkina trys priežastys: i) pagal galiojančias teisminio bendradarbiavimo procedūras per ilgai užtrunka gauti elektroninius įrodymus kitose šalyse, todėl tyrimai ir baudžiamasis persekiojimas tampa mažiau veiksmingi (European Commission, 2018). Pavyzdžiui, pagal šiuo metu taikomą 2014 m. balandžio 3 d. Europos Parlamento ir Tarybos direktyvą Nr. 2014/41/ES dėl Europos tyrimo orderio baudžiamosiose bylose, sprendimas dėl veiksmų vykdymo priimamas per 120 dienų (30 dienų skirta vykdančiajai institucijai priimti sprendimą dėl Europos tyrimo orderio pripažinimo arba vykdymo ir 90 dienų tyrimo priemonei atlikti). Tokie terminai labai apsunkina elektroninio sukčiavimo tyrimo galimybes, kai veika susijusi su tarpvalstybiniu elementu; ii) viešojo ir privataus sektorių bendradarbiavimo tarp paslaugų teikėjų ir valdžios institucijų neveiksmingumas trukdo veiksmingiems tyrimams ir baudžiamajam persekiojimui (pavyzdžiui, kreipimasis į užsienyje veikiančias įmones tiesiogiai nėra veiksminga priemonė, nes įmonės, esančios užsienio valstybėje, neturi pareigos pateikti duomenis pagal kitoje valstybėje esančios teisminės įstaigos reikalavimą ar prašymą, jei nėra naudojamos teisminio bendradarbiavimo procedūros); iii) valstybių narių teisėsaugos institucijoms bandant teigti, kad jos turi teisę gauti prieigą prie užsienio valstybėje esančių duomenų vadovaujantis nacionaliniais teisiniais instrumentais, netinkamai apibrėžta jurisdikcija gali trukdyti veiksmingiems tarpvalstybiniams tyrimams ir baudžiamajam persekiojimui.

Be to, tyrimui reikšminga informacija dar iki reikalavimo pateikti informaciją išsiuntimo gali būti ištrinama, kadangi paslaugos teikėjai neturi pareigos neribotą laiką saugoti tokios informacijos, taip pat paslaugų teikėjai gali atsisakyti pateikti aktualius duomenis, jeigu į juos kreipiamasi tiesiogiai. Šios problemos mastą iliustruoja ir Europos Komisijos 2018 m.

analizėje pateikta statistika, pagal kurią apie 55–75 proc. tyrimų, kuriuose yra tyrimui reikšmingi skaitmeniniai įrodymai, yra neigiamai paveikiamos dabartinių procedūrų, o skaitmeniniai įrodymai suteikiami per vėlai arba prieiga prie jų nesuteikiama iš viso (European Commission, 2018).

Siekiant išspręsti šią problemą, dar 2018 m. buvo pateikti Europos Komisijos pasiūlymai dėl Reglamento dėl Europos elektroninių įrodymų baudžiamosiose bylose pateikimo ir saugojimo orderių ir Direktyvos, kuria nustatomos teisinių atstovų skyrimo įrodymams baudžiamosiose bylose rinkti suderintos taisyklės. Šios taisyklės turėjo leisti teisėsaugos institucijoms, gavus teismo sankciją, tiesiogiai kreiptis į bendroves su specialiu orderiu bei reikalauti užsienyje esančių paslaugų teikėjų pateikti tyrimui reikalingus skaitmeninius įrodymus arba juos išsaugoti. Vis dėlto, pasiūlymai ilgą laiką nebuvo priimti ir tik 2023 m. pradžioje buvo pasiektas susitarimas tarp Europos Parlamento ir Europos Sąjungos Tarybos dėl reglamento ir direktyvos dėl tarpvalstybinės prieigos prie skaitmeninių įrodymų projektų (European Commission, 2022). Todėl artimiausiu metu skaitmeninių įrodymų rinkimas turėtų tapti veiksmingesnis bei turėtų padėti lengviau surinkti įrodymus tiriant elektroninį sukčiavimą.

2.3.2. Sukčiavimo elektroninėje erdvėje duomenų (įrodymų) panaudojimas

Įrodymais gali būti pripažįstami bet kokie faktiniai duomenys, patvirtinantys arba paneigiantys bylai reikšmingas aplinkybes, įskaitant ir elektroninius duomenis, gautus nepažeidžiant teisės aktų reikalavimų. Tokie duomenys gali būti išreikšti rašytine forma arba egzistuoti elektroninėse laikmenose, o draudimo byloje remtis elektroniniais įrodymais nėra. Be to, nė viena įrodymų rūšis neturi pranašumo prieš kitas rūšis – visi įrodymai, įskaitant ir elektroninius, turi būti vertinami bendra tvarka. Teismai, vertindami šalių pateiktus įrodymus, remiasi įrodymų pakankamumo taisykle, vertina įrodymų liečiamumą (sąsajumą) bei įrodymų leistinumą, o išvada dėl konkrečios faktinės aplinkybės egzistavimo daroma pagal vidinį teismo įsitikinimą, grindžiamą objektyviu ir visapusišku visų reikšmingų bylos aplinkybių išnagrinėjimu.

Tyrimo metu pripažįstami tik tokie įrodymai, kurių nei turinys, nei forma neturi esminių trūkumų – įrodymai turi būti gauti įstatymo nustatyta tvarka, taikant teisėtus būdus, kurių patikimumą galima patikrinti BPK numatytais veiksmais. Taip pat įrodymai turi patvirtinti arba paneigti bent vieną reikšmingą bylai aplinkybę (Goda *et al,* 2011, p. 166–169).

Be kita ko, greta leistinumo ir liestinumo (sąsajumo) požymių, teisės doktrinoje kalbant apie elektroninius įrodymus yra minimas ir elektroninių įrodymų autentiškumo požymis, pagal kurį duomenų turinys, kuriuo remiasi proceso šalis, turi būti nepakitęs nuo duomenų sukūrimo

momento, o informacija turi būti gauta iš pirmojo šaltinio. Jei bylos šalis negalės pagrįsti elektroninių duomenų autentiškumo, teismas tokio įrodymo gali apskritai nevertinti (Čėsna, 2007, p. 96).

Tiriant elektroninį sukčiavimą, surinkti duomenys teismui gali būti pateikiami dviem būdais: 1) duomenys išreiškiami materialioje formoje (atspausdinami, nukopijuojami), pavyzdžiui, elektroninis susirašinėjimas tarp šalių. Kauno apygardos teismas pažymėjo, kad elektroniniai duomenys, kitaip nei, pavyzdžiui, popieriuje užfiksuoti duomenys, gali turėti savybę keistis net be žmogaus įsikišimo. Svarbu ir tai, kad elektroninių duomenų forma – tik skaitmeninė. Tačiau ji gali būti specialiomis programomis konvertuojama į tekstą, vaizdą, garsą (Kauno apygardos teismo Baudžiamųjų bylų skyriaus 2022 m. vasario 11 d. nutartis baudžiamojoje byloje); 2) duomenys, kurie negali būti pateikiami materialioje formoje, gali būti pateikiami elektroninėje laikmenoje. Autorės nuomone, šis duomenų pateikimo būdas galėtų būti naudojamas tais atvejais, kai duomenų objektyviai negalima išreikšti materialioje formoje, pavyzdžiui, siekiant nustatyti skirtumus tarp fiktyvios ir tikros internetinės svetainės dizaino, prie kurios prisijungus, iš nukentėjusiojo buvo nuskaitytos piniginės lėšos. Vis dėlto, teismų praktikoje dominuoja pirmasis būdas, t. y. elektroninių duomenų išreiškimas materialioje formoje.

Teismai, grįsdami asmens kaltumą dėl BK 182 str., bylose remiasi ir elektroniniais duomenimis, pavyzdžiui, pokalbiais, susirašinėjimais programėlėje „Viber“ (Panevėžio apygardos teismo 2022 m. gruodžio 22 d. nutartis baudžiamojoje byloje), susirašinėjimais el. paštu (Kauno apygardos teismo 2022 m. gruodžio 13 d. nuosprendis baudžiamojoje byloje) ir kt. Teismai taip pat vertina ir pateiktus vaizdo įrašus (Šiaulių apygardos teismo 2022 m. birželio 16 d. nuosprendis baudžiamojoje byloje).

Taigi, tiriant ir atskleidžiant elektroninio sukčiavimo atvejus, ikiteisminio tyrimo metu, siekiant surasti bylai reikšmingus duomenis, paprastai atliekami šie proceso veiksmai: krata ir poėmis, apžiūra, apklausa, skiriama informacinių technologijų ekspertizė. Nėra nustatyto draudimo byloje remtis elektroniniais duomenimis. Elektroniniuose įrenginiuose ir laikmenose esantys duomenys teismui gali būti pateikiami juos išreiškus materialioje formoje, o jei tai pakenktų duomenų autentiškumui – duomenys pateikiami kartu su laikmena. Siekiant, kad duomenys būtų pripažįstami įrodymais, kaip ir bendru atveju, turi būti laikomasi įrodymų liečiamumo (sąsajumo), leistinumo kriterijų.

3. SUKČIAVIMO ELEKTRONINĖJE ERDVĖJE PREVENCIJOS GALIMYBĖS

Apžvelgus sukčiavimo elektroninėje erdvėje veiką bei jos padarymo ypatumus Lietuvos kontekste, matyti, kad ši veika ir jos padarymo būdai sparčiai tobulėja, atrandama naujų būdų veikti, išnaudojant elektroninės erdvės galimybes. Nusikalstamumo ir jo padarymo apraiškų negalime sustabdyti, tačiau galime bandyti jas kontroliuoti, imantis tam tikrų prevencinio poveikio priemonių, todėl toliau aptariamos sukčiavimo elektroninėje erdvėje prevencijos galimybės.

Elektroninio sukčiavimo prevenciją galima apibrėžti kaip priemonių, nukreiptų siekiant užkirsti kelią elektroninio sukčiavimo nusikalstamoms veikoms įvykdyti, nustatyti ar pašalinti jų atsiradimo veiksnius, individualiai paveikti asmenis, linkusius daryti sukčiavimo nusikalstamas veikas ar ateityje galinčius tapti nusikaltėliais arba nusikalstamų veikų aukomis, visumą (Babachinaitė, Kiškis, 2010, p. 460). Taigi, iš esmės kalbėdami apie tam tikros nusikalstamos veikos prevenciją, šiuo atveju elektroninio sukčiavimo, mintyje turime visa tai, ko imamės ir ką galime padaryti, siekiant kontroliuoti elektroninio sukčiavimo mastą ir paplitimą.

Lietuvos Respublikos Seimo nutarime dėl Viešojo saugumo plėtros 2015–2025 metų programos patvirtinimo pažymima, kad siekiant mažinti nusikalstamų veikų darymo elektroninėje erdvėje galimybes, iškelti šie uždaviniai:

1) plėtoti teisėsaugos, kitų valstybės institucijų ir įstaigų ir privataus sektoriaus partnerystę;

2) didinti gyventojų informuotumą apie nusikalstamų veikų elektroninėje erdvėje grėsmes ir priemones bei būdus joms išvengti;

3) sustiprinti nusikalstamų veikų elektroninėje erdvėje tyrimus atliekančių įstaigų darbuotojų pajėgumą ir gebėjimus;

4) aktyviai bendradarbiauti su Europos kovos su elektroniniu nusikalstamumu centru ir užtikrinti tarptautinių įsipareigojimų teisėsaugos srityje vykdymą.

Taigi, sukčiavimui pasireiškiant elektroninėje erdvėje, šie uždaviniai tampa reikšmingi apibrėžiant konkrečių prevencijos priemonių taikymo kryptį. Toliau darbe aptariamas kiekvienos krypties įgyvendinimas ir prevencinių priemonių taikymas.

Pirma, pagal Europolo Europos kovos su elektroniniu nusikalstamumu centro duomenis, kovojant su nusikalstamomis veikomis elektroninėje erdvėje (įskaitant ir elektroninį sukčiavimą) ir siekiant apsaugoti visuomenę nuo galimų nusikaltimų, būtina investuoti į jų prevenciją (Nacionalinė sunkaus ir organizuoto nusikalstamumo grėsmių vertinimo ataskaita, 2015, p. 63). Europolo Europos kovos su elektroniniu nusikalstamumu centras teikia

operatyvinę, strateginę, analitinę ir kriminalistinę pagalbą valstybių narių tyrimams dėl nusikalstamų veikų elektroninėje erdvėje, todėl tais atvejais, kai susiduriama su vidutinio arba didelio masto elektroniniais sukčiavimais, kurie daromi neapsiribojant Lietuvos Respublikos sienomis, siekiant atskleisti nusikaltimą ir jį užkardyti, valstybė turėtų bendradarbiauti su Europos kovos su elektroniniu nusikalstamumu centru.

Antra, 2020 m. Valstybinėje audito ataskaitoje pabrėžiama, jog teisėsaugos bei kitų valstybių institucijų bendradarbiavimo su privataus sektoriaus įstaigomis uždavinys turi būti įgyvendintas organizuojant šviečiamojo pobūdžio renginius ar vedant seminarus. Pateiktoje statistikoje matyti, jog toks organizuojamų renginių ar seminarų skaičius nuo 2015 m. didėjo – 2015 m. Lietuvos policija organizavo ir įgyvendino 84 renginius, 2017 m. – 209 renginius, o 2019 m. renginių skaičius pasiekė 457. Policijos įstaigose 2015–2019 m. didžioji dalis įgyvendinamų prevencinių priemonių buvo skirtos bendroms temoms (43 proc.), sukčiavimui (24 proc.) ir patyčioms elektroninėje erdvėje (17 proc.). Taip pat elektroninio sukčiavimo klausimais mokymus, susitikimus organizavo ir informaciją viešumoje teikė Valstybinė vartotojų teisių apsaugos tarnyba, Nacionalinis kibernetinio saugumo centras, Ryšių reguliavimo tarnyba, „Sustiprink imunit@ą!“ projekto vykdytojai. Kaip vieną iš teigiamų pavyzdžių, galima nurodyti Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos ir Kauno technologijos universiteto, 2019 m. spalio 22-24 dienomis surengtas ir kasmet organizuojamas nacionalines kibernetinio saugumo pratybas „Kibernetinis skydas“ (Pratybų „Kibernetinis skydas 2019“ ataskaita, 2019), kuriose gali dalyvauti ir privataus sektoriaus įstaigų atstovai. Pratybų tikslas – formuoti praktinius pratybų dalyvių kibernetinio saugumo įgūdžius, patikrinti kibernetinių incidentų valdymo procedūras, gerinti bendradarbiavimą tarp kibernetinius incidentus valdančių, tiriančių institucijų ir kibernetinio saugumo subjektų. Antras teigiamas pavyzdys yra 2013 m. įsteigtas VšĮ „Lietuvos kibernetinių nusikaltimų kompetencijų ir tyrimų centras“ (L3CE)[2], kurio pagrindinis tikslas yra mokslinių bei akademinių programų, skirtų visuomenės kibernetinio saugumo stiprinimui, rengimas. Siekiant šio tikslo, centras sėkmingai bendradarbiaudamas su nacionalinėmis ir Europos Sąjungos institucijomis, įskaitant ir Europolą, Jungtinių Tyrimų Centrą ir kt., organizuoja mokymus, pvz., dėl išorinių laikmenų apžiūros, įvykio vietos tyrimo elektroninėje erdvėje, tapatybės vagystės ir elektroninio sukčiavimo, prisideda prie projektų, susijusių su kibernetinio saugumo stiprinimu.

[2] VšĮ „Lietuvos kibernetinių nusikaltimų kompetencijų ir tyrimų centras“ puslapis. Interaktyvi nuoroda: https://www.l3ce.eu/apie-l3ce/

Trečia, gyventojų ir įmonių darbuotojų švietimas ir informacijos sklaida taip pat yra svarbi prevencijos priemonė, kadangi taip asmenys yra supažindinami su sukčiavimo būdais bei mokomi juos atpažinti. Ši prevencinė kryptis svarbi ir tuo, jog pats elektroninis sukčiavimas kaip nusikalstama veika yra padaromas nukentėjusiajam patikint kaltininko apgaule, taigi elektroninio sukčiavimo kontrolė taip pat priklauso nuo paties nukentėjusiojo bei jo veiksmų atpažįstant elektroninio sukčiavimo atvejus. Ši prevencijos kryptis Lietuvoje dažnu atveju įgyvendinama per gyventojų informavimą. Pavyzdžiui, Europolas kartu su Lietuvos policija parengtoje informacinėje skrajutėje[3] pateikia elektroninio sukčiavimo būdus, kartu su informacija kaip šiuos būdus atpažinti ir ką reikėtų daryti siekiant nuo tokių būdų apsisaugoti. Pavyzdžiui, apsipirkinėjant internetu svarbu atsiskaityti tik saugiais mokėjimo būdais, neapsigauti pasiūlymu, jei jis skamba „per daug gerai“. Susidūrus su apgaulingais el. laiškais, svarbu atidžiai peržiūrėti el. laiško turinį, jei tai tariama žinutė iš banko, palyginti siuntėjo el. pašto adresą su oficialiu banko el. pašto adresu, niekada nespausti ant įtartinų el. nuorodų ir pan. Tiesa, pasak SEB banko Prevencijos departamento vadovo Audriaus Šapolos, greita klientų reakcija ir operatyvūs banko sprendimai ir koordinuoti veiksmai taip pat padeda užkirsti kelią sukčių finansinėms operacijoms ir sugrąžinti prarastas lėšas[4]. SEB bankas primena, jog finansinio sukčiavimo, fišingo bei smišingo mechanizme svarbiausia, kad asmuo niekada nevestų tik jam vienam žinomų „Smart-ID“ PIN1 ir PIN2, jei pats neinicijavo mokėjimo – tada pinigai sąskaitoje liks saugūs. 2022 m. Eurobarometro duomenimis, didžioji dalis apklausoje dalyvavusių vidutinių ir smulkių Lietuvos įmonių, atsakė, jog mano, kad jų įmonėse dirbantys darbuotojai yra gerai arba pakankamai informuoti apie kibernetinį saugumą (45 įmonės), dalis įmonių įsitikinusios, kad darbuotojams trūksta mokymų kibernetinio saugumo temomis (27 įmonės), o apie darbuotojų puikias žinias kibernetinio saugumo klausimais atsakė vos 13 apklausoje dalyvavusių įmonių. Mokymus kibernetinio saugumo temomis savo darbuotojams organizavo vos 14 įmonių ir net 85 įmonės atsakė, kad tokio pobūdžio mokymų nėra organizavusios (Europos Komisija, 2022). Taigi, gyventojų ir įmonių darbuotojų švietimas ir informacijos sklaida yra ir turi būti matoma kaip prioritetinė prevencinė kryptis.

Galiausiai, Valstybės kontrolės ataskaitoje pažymima, kad siekiant kontroliuoti nusikalstamas veikas elektroninėje erdvėje, įskaitant ir elektroninį sukčiavimą, turi būti

[3] Europolo ir Lietuvos policijos teikiama informacija: https://www.europol.europa.eu/sites/default/files/documents/lt_0.pdf

[4] SEB banko straipsnis „Apgaulingas SMS žinutes siunčiantiems sukčiams SEB bankas užkirto kelią pavogti daugiau negu 116 tūkst. eurų“: https://www.seb.lt/naujienos/2019-09-26/apgaulingas-sms-zinutes-siunciantiems-sukciams-seb-bankas-uzkirto-kelia-pavogti-

sudaromos sąlygos gerinti tyrimų, susijusių su veikomis, kurios padaromos elektroninėje erdvėje, rezultatyvumą (Valstybės kontrolė, 2020). Valstybės kontrolė pažymi, jog turi būti tobulinamas sisteminių nusikaltimų identifikavimo procesas, siekiant, kad visi ikiteisminiai tyrimai dėl nusikalstamų veikų elektroninėje erdvėje, kurie yra sisteminiai ir reikalauja specializuotų žinių, būtų tiriami specializuotose padaliniuose, taigi būtina tobulinti šių ikiteisminių tyrimų paskirstymo mechanizmą. Kaip matyti iš pateiktų statistinių duomenų, 2016–2019 m. nespecializuoti pareigūnai vidutiniškai atliko 62 proc. visų nusikalstamų veikų elektroninėje erdvėje ikiteisminių tyrimų, iš jų, 72 proc. buvo elektroninio sukčiavimo atvejai. Taip pat, Autorės nuomone, reiktų tobulinti esamą prokurorų specializacijos tvarką, kad nusikalstamų veikų elektroninėje erdvėje specializuotų pareigūnų ikiteisminiams tyrimams vadovautų šios srities specializuoti prokurorai. Siekiant gerinti specializuotų pareigūnų ir prokurorų bendrą ugdymo procesą, reikia parengti bendrą specializuotų pareigūnų ir prokurorų mokymų programą ir ją įgyvendinti. Generalinei Prokuratūrai siūloma įvertinti metodinių rekomendacijų nusikalstamoms veikoms elektroninėje erdvėje tirti poreikį ir jas parengti. Visgi, kaip teigiamą teisėsaugos institucijų sprendimą Autorė norėtų paminėti Lietuvos policijos patobulintą pranešimo apie įvykį sistemą. Šiuo metu, egzistuoja elektroninė pranešimo apie įvykį forma – ePolicija.lt[5], kuri skatina asmenis apie įvykį pranešti elektroniniu būdu. Tokia forma ypač praverčia elektroninio sukčiavimo atvejais, kai asmenys gali pridėti elektroninius „įrodymus“, taip pat ji nereikalauja fizinio atvykimo į policijos įstaigą, yra daug paprastesnė. Dar viena Lietuvos policijos iniciatyva – 2021 m. pradžioje paleistas Virtualus policijos patrulis bei tam specialiai sukurta socialinio tinklo Meta „Facebook“ paskyra[6]. Šios paskyros tikslas – reaguoti į akivaizdžius elektroninėje erdvėje daromus ar rengiamus daryti teisės pažeidimus, įskaitant elektroninį sukčiavimą.

Taigi, siekiant kovoti su elektroninio sukčiavimo atvejais, būtina imtis tam tikrų prevencinių priemonių. Lietuvos Respublikos kontekste, teigiamos prevencinių priemonių kryptys yra visuomenės informuotumas ir informacijos sklaida, seminarų organizavimas valstybės ir privatiems sektoriams, bendradarbiavimas su kitų šalių ar Europos Sąjungos kompetentingomis institucijomis bei teisėsaugos institucijų pajėgumų stiprinimas ir rezultatyvumo gerinimas.

[5] ePolicija internetinis tinklapis. Interaktyvi nuoroda: https://www.epolicija.lt

[6] Policijos virtualaus patrulio paskyra. Interaktyvi nuoroda: https://www.facebook.com/policijosvirtualuspatrulis/

IŠVADOS

Atlikus sukčiavimo elektroninėje erdvėje analizę, galima daryti tokias išvadas:

1. Sukčiavimas elektroninėje erdvėje siaurąja prasme, siejamas su kompiuteriniu sukčiavimu, kuris tiek tarptautiniuose teisės aktuose, tiek Europos Sąjungos teisės aktuose yra suprantamas kaip neteisėtas poveikis kompiuteriniams duomenims ar kompiuterinei sistemai, įgyjant turtinės naudos. Plačiąja prasme sukčiavimas elektroninėje erdvėje, siejamas su elektroninės erdvės naudojimu, apgaule įgyjant turtinės naudos, nepriklausomai ar joje esantys duomenys, ar programos buvo kaip nors paveikti. Lietuvoje elektroninis sukčiavimas patenka į bendrą BK 182 str. dispoziciją ir suprantamas plačiąja prasme.

2. Sukčiavimas elektroninėje erdvėje gali būti padaromas skirtingais būdais. Praktikoje dažniausiai pasitaikantys elektroninio sukčiavimo padarymo būdai yra telefoninis sukčiavimas, avansinis sukčiavimas, sukčiavimas susijęs su lėšų išviliojimu ar pirkinių įsigijimu, sukčiavimas padaromas neteisėtai pasinaudojant asmens tapatybę patvirtinančiais duomenimis bei romantinis sukčiavimas.

3. Lietuvos kontekste elektroninių sukčiavimų atvejų skaičius pastaraisiais metais auga arba išlieka didelis. Dominuojantys elektroninio sukčiavimo būdai, kurių tendenciją galima matyti pastarųjų kelių metų statistikoje – fišingas, smišingas, telefoninis sukčiavimas, investicinis sukčiavimas.

4. Sukčiavimas elektroninėje erdvėje yra sudėtingas, kompleksinis procesas, kurio padarymui neretai būtini tam tikri paruošiamieji veiksmai, kurie vertinami ne tik kaip atskiri etapai, siekiant nusikalstamo tikslo – sukčiauti elektroninėje erdvėje, tačiau kurių neapima bendroji sukčiavimo norma ir kurie kvalifikuojami atskirai – BK 198 str., BK 198^{2}, BK 198^{1}, BK 214, BK 215 str.

5. Sprendžiant baudžiamosios jurisdikcijos nustatymo atvejus elektroniniam sukčiavimui svarbūs du principai – teritorinis bei aktyvusis personalinis. Tarptautinėje ir Europos Sąjungos teisėje nepaisant aktyvaus personalinio principo taikymo paprastumo, pirmumas suteikiamas teritoriniam baudžiamosios jurisdikcijos principui. Visgi, kiekvienu konkrečiu atveju būtina identifikuoti kriterijus, kurie leistų nusikalstamą veiką elektroninėje erdvėje (įskaitant ir elektroninio sukčiavimo atvejus) susieti su tam tikros valstybės teritorija.

6. Tiriant ir atskleidžiant elektroninio sukčiavimo atvejus, ikiteisminio tyrimo metu, siekiant surasti bylai reikšmingus duomenis, įprastai atliekami šie proceso veiksmai: krata ir poėmis, apžiūra, apklausa, skiriama informacinių technologijų ekspertizė. Nėra nustatyto draudimo byloje remtis elektroniniais duomenimis. Elektroniniuose įrenginiuose ir laikmenose

esantys duomenys teismui gali būti pateikiami juos išreiškus materialioje formoje, o jei tai pakenktų duomenų autentiškumui – elektroniniai duomenys teikiami kartu su materialia laikmena.

7. Siekiant kovoti su elektroninio sukčiavimo atvejais, būtina imtis tam tikrų prevencinio pobūdžio priemonių. Lietuvoje prevencinių priemonių taikymo kryptys yra orientuotos į teisėsaugos, kitų valstybės institucijų ir privataus sektoriaus komunikavimą, visuomenės informuotumą, nusikalstamų veikų elektroninėje erdvėje tyrimus atliekančių įstaigų darbuotojų pajėgumų ir gebėjimų stiprinimą.

PASIŪLYMAI

Remiantis atlikta tarptautinių ir nacionalinių teisės aktų, Lietuvos ir užsienio mokslininkų formuojama doktrina, sukčiavimo sudėties požymių analize, pateiktais statistiniais duomenimis, teismų praktika bei atsižvelgiant į suformuluotas išvadas, teikiami šie pasiūlymai:

1. Laikantis nustatytų prevencinio pobūdžio krypčių, siūlytina didinti jų matomumą ir visuomenės informuotumą. Šis tikslas gali būti pasiekiamas užtikrinant didesnę informacijos sklaidą internete ir ypatingai socialinėse medijose, pavyzdžiui, reguliariai išleidžiant informacines skrajutes, organizuojant nuotolines ar gyvas konferencijas, dalijantis įvykusiais elektroninio sukčiavimo atvejais ir kt.

2. Teisėsaugos ar kitos valstybės institucijos turėtų reguliariai vykdyti mokymus ar seminarus tiek juridinių asmenų darbuotojams, tiek nevyriausybinėms organizacijoms ar savivaldybės mastu.

3. Finansinėms įstaigoms, visų pirma, bankams didesnių mokėjimų pavedimų atvejais siūlytina vykdyti dviejų lygių autentifikavimo sistemą, tai padėtų apsisaugoti nuo fišingo atvejų. Ši apsaugos priemonė vartotojui jungiantis prie banko tinklalapio prašytų papildomos autentifikacijos vartotojo pasirinktu būdu, pvz., trumpąja SMS žinute.

ŠALTINIŲ SĄRAŠAS

Teisės norminiai aktai

Tarptautiniai teisės aktai

1. Konvencija dėl elektroninių nusikaltimų (2001). *Valstybės žinios*, 2004, 36-1188.
2. Council of Europe (2021). Convention on Cybercrime explanatory report. [interaktyvus]. Prieiga per internetą: https://rm.coe.int/16800cce5b [žiūrėta 2023 m. sausio 17 d.]

Europos Sąjungos teisės aktai

3. Europos Parlamento ir Tarybos 2014 m. balandžio 3 d. Direktyva (ES) 2014/41 dėl Europos tyrimo orderio baudžiamosiose bylose.
4. Europos Parlamento ir Tarybos 2019 m. balandžio 17 d. Direktyva (ES) 2019/713 dėl kovos su sukčiavimu negrynosiomis mokėjimo priemonėmis ir jų klastojimu.
5. Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. Reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB.
6. Europos Parlamento ir Tarybos 2013 m. rugpjūčio 12 d. Europos Parlamento ir Tarybos Direktyva (ES) 2013/40 dėl atakų prieš informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR.
7. Tarybos 2009 m. lapkričio 30 d. Pamatinis sprendimas 2009/948/TVR dėl jurisdikcijos įgyvendinimo kolizijų baudžiamuosiuose procesuose prevencijos ir sprendimo.

Lietuvos Respublikos teisės aktai

8. Lietuvos Respublikos baudžiamasis kodeksas (2000). *Valstybės žinios*, 89-2741 (su vėlesniais pakeitimais ir papildymais).
9. Lietuvos Respublikos Seimo 2015 m. birželio 7 d. nutarimas dėl Viešojo saugumo plėtros 2015–2025 metų programos patvirtinimo. *Teisės aktų registras*, 7293.

Užsienio valstybių teisės aktai

10. Estijos baudžiamasis kodeksas (2001). [interaktyvus]. Prieiga per internetą: https://www.riigiteataja.ee/en/eli/522012015002/consolide [žiūrėta 2022 m. gruodžio 15 d.]

11. Latvijos baudžiamasis kodeksas (1998). [interaktyvus]. Prieiga per internetą: https://likumi.lv/ta/en/en/id/88966-criminal-law [žiūrėta 2022 m. gruodžio 15 d.]
12. Lenkijos baudžiamasis kodeksas (1997). [interaktyvus] Prieiga per internetą: https://www.imolin.org/doc/amlid/Poland_Penal_Code1.pdf [žiūrėta 2022 m. gruodžio 15 d.]

Specialioji literatūra

Monografijos, vadovėliai ir kiti leidiniai

13. Abramavičius, A. ir kt. (2009). *Lietuvos Respublikos baudžiamojo kodekso komentaras (Specialioji dalis: 99-212 straipsniai)*. Vadovėlis. Vilnius: Registrų centras.
14. Babachinaitė, G. ir kt. (2010). *Kriminologija*. Vilnius: Mykolo Romerio universiteto leidybos centras.
15. Babachinaitė, G. (2009). *Latentinio nusikalstamumo kriminologinio tyrimo metodikos*. Metodinis leidinys. Vilnius: Mykolo Romerio universitetas. [interaktyvus]. Prieiga per internetą: https://www3.mruni.eu/~akiskis/alfredo-str-latent_nus_tyrimo_metodikos2009.pdf [žiūrėta 2022 m. gruodžio 27 d.]
16. Bernat, F., Godlove, N. (2012). *Understanding 21st century cybercrime for the 'common' Victim. Criminal Justice Matters* No. 89, p. 12–13. [interaktyvus]. Prieiga per internetą: https://www.tandfonline.com/doi/abs/10.1080/09627251.2012.721962 [žiūrėta 2023 m. vasario 15 d.]
17. Bilevičiūtė, E., Novikovienė, L. (2010). *Application of it examination in investigation of Crimes on safety of electronic Data and information systems. Jurisprudencija* Nr. 1(119), p. 317–329.
18. Civilka, M. ir kt. (2004). *Informacinių technologijų teisė*. Vadovėlis. Vilnius: NVO Teisės institutas.
19. Čėsna, R. (2007). *Kai kurie elektroninių įrodymų panaudojimo civiliniame procese aspektai. Jurisprudencija* Nr. 10(100), p. 92–98.
20. Fedosiuk, O. (2008). *Patikėtos svetimos turtinės teisės pasisavinimo ir iššvaistymo samprata. Jurisprudencija* Nr. 11(113), p. 72–83.
21. Folsom, T. (2006). *Defining Cyberspace (Finding Real Virtue in the Place of Virtual Reality)*. Regent University School of Law, p. 75–121 [interaktyvus]. Prieiga per internetą: https://journals.tulane.edu/TIP/article/view/2525 [žiūrėta 2022 m. gruodžio 3 d.]

22. Goda, G. ir kt. (2011). *Baudžiamojo proceso teisė*. Vadovėlis. Vilnius: Registrų centras.
23. Holt. T. J. (2017). *Cybercrime Through an Interdisciplinary Lens*. Book. London: Routledge.
24. Jankauskas, V., Kligys, V. (2005) *Informacinių technologijų ekspertizė Lietuvos teismo ekspertizės centre: dabartis ir perspektyvos*. Vilnius: Mykolo Romerio universiteto leidybos centras.
25. Kakati, S., Goswami, C. (2019). *Factors and Motivation of Fraud in the Corporate Sector. A Literature Review. Journal of Commerce & Accounting Research*, No. 3, p. 86–96. [interaktyvus]. Prieiga per internetą: https://www.researchgate.net/publication/337388684_FACTORS_AND_MOTIVATION_OF_FRAUD_IN_THE_CORPORATE_SECTOR_A_LITERATURE_REVIEW [žiūrėta 2023 m. sausio 12 d.]
26. Kalaharshaa, P., Mehtrea, B. M. (2021). *Detecting Phishing Sites – An Overview*. Center of excellence in cyber security, Institute for Development and Research in Banking Technology (IDRBT), Hyderabad, India and School of Computer Science and Information Sciences (SCIS), University of Hyderabad, Hyderabad, India [interaktyvus]. Prieiga per internetą: https://arxiv.org/pdf/2103.12739.pdf [žiūrėta 2023 m. sausio 3 d.]
27. Kalpokas, V. (2009). *Nusikaltimai elektroninėje erdvėje: kriminologinės sampratos dilemos. Teisės problemos*. Nr. 1 (63), p. 75–87.
28. Kalpokas, V. (2010). *Skaitmeninės erdvės reguliavimas ir kontrolė: saugumo aspektai. Teisės problemos*. Nr. 4 (70), p. 133–157.
29. Kalpokas, V., Marcinauskaitė, R. (2012). *Tapatybės vagystė elektroninėje erdvėje: technologiniai aspektai ir baudžiamasis teisinis vertinimas. Teisės problemos.* Nr. 3 (77), p. 30–52.
30. Kiškis, M. ir kt. (2016). *Interneto ir technologijų teisė*. Vadovėlis. Vilnius: Registrų centras.
31. Klip, A. (2016). *European Criminal Law. An Integrative Approach, Third edition*. Cambridge: Intersentia.
32. Kshetri, N. (2010). *The Global Cybercrime Industry: Economic, Institutional and Strategic Perpective*. Springer-Verlag. [interaktyvus]. Prieiga per internetą: https://link.springer.com/content/pdf/bfm:978-3-642-11522-6/1.pdf [žiūrėta 2023 m. vasario 16 d.]
33. Kurapka, V. E. ir kt. (2013). *Kriminalistika: taktika ir metodika*. Vadovėlis. Vilnius: Mykolo Romerio universiteto Leidybos centras.

34. Li, X., Yongfeng, O. (2019). *Research on criminal jurisdiction of computer cybercrime. Procedia Computer Science* No. 131, p. 793–799 [interaktyvus]. Prieiga per internetą: https://www.sciencedirect.com/science/article/pii/S1877050918306434 [žiūrėta 2023 m. sausio 23 d.]
35. Li, X. (2017). *A Review of Motivations of Illegal Cyber Activities*. School of Governance, Law and Society, Tallinn University, Estonia. [interaktyvus]. Prieiga per internetą: https://hrcak.srce.hr/file/266976 [žiūrėta 2022 m. gruodžio 17 d.]
36. Marcinauskaitė, R. (2021). *Nusikalstamos veikos elektroninėje erdvėje ir teritorinė baudžiamoji jurisdikcija. Jurisprudencija* Nr. 28(1), p. 200–216.
37. Nevera, A. (2006). *Valstybės baudžiamosios jurisdikcijos principai*. Monografija. Vilnius: Mykolo Romerio universiteto Leidybos centras. [interaktyvus]. Prieiga per internetą: https://repository.mruni.eu/bitstream/handle/007/15489/NEVERA.pdf?sequence=1&isAllowed=y [žiūrėta 2023 m. vasario 18 d.]
38. Pranka, D. (2012). *Nusikalstamos veikos ir civilinės teisės pažeidimo atribojimo koncepcija Lietuvos baudžiamojoje teisėje*. Daktaro disertacija. [interaktyvus]. Prieiga per internetą: https://repository.mruni.eu/handle/007/15968 [žiūrėta 2022 m. gruodžio 19 d.]
39. Sakalauskas, G. ir kt. (2011) *Registruotas ir latentinis nusikalstamumas Lietuvoje: tendencijos, lyginamieji aspektai ir aplinkos veiksniai*. [interaktyvus]. Prieiga per internetą: https://teise.org/wp-content/uploads/2011/12/Registruotas-ir-latentinis-nusikalstamumas.pdf [žiūrėta 2023 m. sausio 5 d.]
40. Štitilis, D. (2011). *Elektroniniai nusikaltimai*. Metodinė priemonė. Vilnius: Mykolo Romerio universitetas.
41. Šupa, M. (2021). Socialiniai tyrimai apie elektroninius nusikaltimus. *Kriminologijos studijos*. t. 9, p. 8–46.
42. Švedas, G. ir kt. (2017). *Lietuvos Respublikos baudžiamojo kodekso bendrosios dalies vientisumo ir naujovių (su)derinimo iššūkiai*. Vilnius: Vilniaus universiteto leidykla. [interaktyvus]. Prieiga per internetą: https://www.tf.vu.lt/publications/baudziamojo-kodekso-bendrosios-dalies-vientisumo-ir-naujoviu-suderinimo-issukiai-2017/ [žiūrėta 2023 m. vasario 20 d.]
43. Valatkevičius, D. (2007). *Jurisdikcijos problematika tiriant kompiuterinius nusikaltimus. Teisė* Nr. 62, p. 127-139.

Teismų praktika

Lietuvos teismų sprendimai

44. Lietuvos Aukščiausiojo Teismo 2001 m. spalio 9 d. nutartis baudžiamojoje byloje Nr. 2K-682/2001. Teismų praktika Nr. 16.
45. Lietuvos Aukščiausiojo Teismo 2005 m. lapkričio 15 d. nutartis baudžiamojoje byloje Nr. 2K-587/2005.
46. Lietuvos Aukščiausiojo Teismo 2012 m. gegužės 2 d. Teismų praktikos sukčiavimo (Baudžiamojo kodekso 182 straipsnis) baudžiamosiose bylose apžvalga.
47. Lietuvos Aukščiausiojo Teismo 2012 m. birželio 26 d. nutartis baudžiamojoje byloje Nr. 2K-375/2012.
48. Lietuvos Aukščiausiojo Teismo 2012 m. rugsėjo 7 d. Teismų praktikos sukčiavimo baudžiamosiose bylose (BK 182 straipsnis) apžvalga Nr. AB-36-1.
49. Lietuvos Aukščiausiojo Teismo 2012 m. gruodžio 18 d. nutartis baudžiamojoje byloje Nr. 2K-699/2012.
50. Lietuvos Aukščiausiojo Teismo 2013 m. spalio 22 d. nutartis baudžiamojoje byloje Nr. 2K-7-262/2013.
51. Lietuvos Aukščiausiojo Teismo 2015 m. kovo 31 d. nutartis baudžiamojoje byloje Nr. 2K-112-788/2015.
52. Lietuvos aukščiausiojo Teismo 2015 m. gegužės 12 d. nutartis baudžiamojoje byloje Nr. 2K-188-489/2015.
53. Lietuvos Aukščiausiojo Teismo 2018 m liepos 3 d. nutartis baudžiamojoje byloje Nr. 2K-228-895/2018.
54. Lietuvos Aukščiausiojo Teismo 2019 m. birželio 28 d. nutartis baudžiamojoje byloje Nr. 2K-192-489/2019.
55. Lietuvos Aukščiausiojo Teismo 2019 m. gruodžio 19 d. nutartis baudžiamojoje byloje Nr. 2K-303-693/2019.
56. Lietuvos Aukščiausiojo Teismo 2020 m. gegužės 20 d. nutartis baudžiamojoje byloje Nr. 2K-120-895/2020.
57. Kauno apygardos teismo 2017 m. rugsėjo 27 d. nuosprendis baudžiamojoje byloje Nr. N1-173-319/2017.
58. Kauno apygardos teismo 2022 m. vasario 11 d. nutartis baudžiamojoje byloje Nr. 1A-107-493/2022.

59. Kauno apygardos teismo 2022 m. gruodžio 13 d. nuosprendis baudžiamojoje byloje Nr. 1-173-954/2022.
60. Panevėžio apygardos teismo 2022 m. gruodžio 22 d. nutartis baudžiamojoje byloje Nr. 1A-207-491/2022.
61. Šiaulių apygardos teismo 2022 m. birželio 16 d. nuosprendis baudžiamojoje byloje Nr. 1-65-316/2022.
62. Vilniaus apygardos teismo 2011 m. gruodžio 23 d. nuosprendis baudžiamojoje byloje Nr. 1A-977-92-2011.
63. Vilniaus miesto 1-ojo apylinkės teismo 2009 m. rugsėjo 14 d. teismo baudžiamasis įsakymas baudžiamojoje byloje Nr. N1- 1470-88/2009.

Kiti šaltiniai

64. Cahill, E. (2022). *What's the Difference Between Phishing, Smishing and Vishing?* [interaktyvus]. Prieiga per internetą: https://www.experian.com/blogs/ask-experian/phishing-smishing-vishing/ [žiūrėta 2022 m. gruodžio 17 d.]
65. Choucri, N. (2013). *Co-Evolution of Cyberspace and International Relations: New Challenges for the Social Sciences*. World Social Science Forum (WSSF). [interaktyvus]. Prieiga per internetą: https://ecir.mit.edu/sites/default/files/documents/%5BChoucri%5D%202013%20Co-Evolution%20of%20Cyberspace%20and%20International%20Relations.pdf [žiūrėta 2022 m. gruodžio 3 d.]
66. Department of Defense Dictionary of Military and Associated Terms (2011). Elektroninės erdvės sąvoka. [interaktyvus]. Prieiga per internetą: https://csrc.nist.gov/glossary/term/cyberspace [žiūrėta 2022 m. gruodžio 3 d.]
67. European Commission (2022). SMEs and Cybercrime. [interaktyvus]. Prieiga per internetą: https://europa.eu/eurobarometer/surveys/detail/2280 [žiūrėta 2023 m. vasario 20 d.]
68. European Commission (2022). e-*Evidence: Commission welcomes political agreement to strengthen cross-border access for criminal investigations*. [interaktyvus]. Prieiga per internetą: https://ec.europa.eu/commission/presscorner/detail/es/ip_22_7246 [žiūrėta 2023 m. vasario 25 d.]
69. European Commission (2020). *Survey on "Scams and fraud experienced by consumers"*. Final Report. [interaktyvus]. Prieiga per internetą: https://ec.europa.eu/info/sites/default/files/aid_development_cooperation_fundamental_righ

ts/ensuring_aid_effectiveness/documents/survey_on_scams_and_fraud_experienced_by_consumers_-_final_report.pdf [žiūrėta 2022 m. gruodžio 14 d.]

70. European Commission (2018). Impact Assessment. [interaktyvus]. Prieiga per internetą: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018SC0118&from=EN [žiūrėta 2023 m. vasario 25 d.]
71. Europol. (2015). Nacionalinė sunkaus ir organizuoto nusikalstamumo grėsmių vertinimo 2015 m. ataskaita. [interaktyvus]. Prieiga per internetą: https://www.europol.europa.eu/sites/default/files/documents/europol_iocta_web_2015.pdf [žiūrėta 2023 m. sausio 10 d.]
72. Europool (2020). *How criminals profit from the COVID-19 pandemic*. [interaktyvus]. Prieiga per internetą: https://www.europol.europa.eu/media-press/newsroom/news/how-criminals-profit-covid-19-pandemic [žiūrėta 2023 m. sausio 10 d.]
73. Europos Komisija (2020). *2020 m. Skaitmeninės ekonomikos ir visuomenės indeksas (DESI)*. Lietuvos ataskaita. [interaktyvus]. Prieiga per internetą: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=66948 [žiūrėta 2022 m. vasario 13 d.]
74. Europos Komisija (2022). Pranešimas spaudai Nr. 7/2022. [interaktyvus]. Prieiga per internetą: https://anti-fraud.ec.europa.eu/system/files/2022-09/olaf-report-2021_en.pdf [žiūrėta 2022 m. gruodžio 20 d.]
75. Harnnet, D., Jones, S. (2022). *Smishing vs. Phishing: Understanding the Differences.* [interaktyvus]. Prieiga per internetą: https://www.proofpoint.com/us/blog/email-and-cloud-threats/smishing-vs-phishing-understanding-differences [žiūrėta 2023 m. sausio 9 d.]
76. Lietuvos bankas (2021). *Investavimas: kaip atpažinti sukčius*. [interaktyvus]. Prieiga per internetą: https://www.lb.lt/lt/investavimas-kaip-atpazinti-sukcius#ex-1-4 [žiūrėta 2023 m. sausio 19 d.]
77. Lietuvos banko Teisės ir licencijavimo departamento direktorius 2021 m. lapkričio 24 d. sprendimas Nr. 429-435. [interaktyvus]. Prieiga per internetą: https://www.lb.lt/lt/frd/view_dispute?id=5872 [žiūrėta 2023 m. sausio 11 d.]
78. Lietuvos bankų asociacija (2023). *Finansiniai sukčiai pernai išviliojo 12 mln. eurų, savininkams grąžinti 5 mln. eurų*. [interaktyvus]. Prieiga per internetą: https://www.lba.lt/lt/apie-mus/asociacijos-naujienos/finansiniai-sukciai-pernai-isviliojo-12-mln-euru-savininkams-grazinti-5-mln-euru [žiūrėta 2023 m. sausio 19 d.]

79. Lietuvos bankų asociacija (2022). *Finansiniai sukčiai iš gyventojų ir verslo pernai išviliojo 10,2 mln. Eurų*. [interaktyvus]. Prieiga per internetą: https://www.lba.lt/lt/apie-mus/asociacijos-naujienos/finansiniai-sukciai-is-gyventoju-ir-verslo-pernai-isviliojo-10-2-mln-euru [žiūrėta 2023 m. sausio 19 d.]
80. Lietuvos bankų asociacija (2022). *Į finansinių sukčių rankas šiemet nepakliuvo per 800 tūkst. eurų, tačiau apgaulių SMS ir telefonu daugėja*. [interaktyvus]. Prieiga per internetą: https://www.lba.lt/lt/apie-mus/asociacijos-naujienos/i-finansiniu-sukciu-rankas-siemet-nepakliuvo-per-800-tukst-euru-taciau-apgauliu-sms-ir-telefonu-daugeja [žiūrėta 2023 m. vasario 18 d.]
81. Lietuvos policija. DUK. [interaktyvus] Prieiga per internetą: https://policija.lrv.lt/lt/duk/sukciavimo-budai [žiūrėta 2022 m. gruodžio 18 d.]
82. Lietuvos Respublikos Informatikos ir ryšių departamentas prie LR VRM. Atviri duomenys. [interaktyvus]. Prieiga per internetą: https://ird.lt/lt/atviri-duomenys/sukciavimai [žiūrėta 2023 m. sausio 16 d.]
83. Lietuvos Respublikos Informatikos ir ryšių departamentas prie LR VRM. Nusikalstamumo duomenų rinkiniai. [interaktyvus]. Prieiga per internetą: https://ird.lt/lt/paslaugos/tvarkomu-valdomu-registru-ir-informaciniu-sistemu-paslaugos/nusikalstamu-veiku-zinybinio-registro-nvzr-atviri-duomenys-paslaugos/nusikalstamumo-duomenu-rinkiniai/dimension.BK?BK%5B%5D=BK182&BK%5B%5D=BK182-2D&BK%5B%5D=BK182-3D&DT%5B%5D=2022-09&DT%5B%5D=2021-09&cols=DT [žiūrėta 2023 m. sausio 15 d.]
84. Lietuvos Respublikos Valstybės kontrolė (2020). 2020 m. veiklos ataskaita. [interaktyvus]. Prieiga per internetą: https://www.valstybeskontrole.lt/TVS/Content/Administracine_informacija/Veiklos_ataskaitos/2020_metu_VK_veiklos_ataskaita.pdf [žiūrėta 2023 m. vasario 20 d.]
85. Lietuvos Respublikos Valstybės kontrolė (2020). *Ar veiksmingai kovojama su elektroniniais nusikaltimais*. Valstybinio audito ataskaita. [interaktyvus]. Prieiga per internetą: https://www.lrs.lt/sip/getfile?guid=160d2f45-f62a-4282-bbc6-4fe1b715aa89 [žiūrėta 2023 m. vasario 21 d.]
86. Nacionalinis kibernetinio saugumo centras (2022). *Svarbiausia Lietuvos kibernetinio saugumo būklės statistika ir tendencijos*. [interaktyvus]. Prieiga per internetą: https://www.nksc.lt/doc/Svarbiausia-Lietuvos-kibernetinio-saugumo-bukles-statistika-ir-tendencijos-2021-2022-I-ketv.pdf [žiūrėta 2023 m. vasario 19 d.]

87. Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos. (2019). Pratybų „Kibernetinis skydas 2019“ ataskaita visuomenei. [interaktyvus]. Prieiga per internetą: https://www.nksc.lt/doc/KS2019_pratybu_ataskaita.pdf [žiūrėta 2023 m. vasario 25 d.]
88. Popper, N. (2018). *When Good Crypto Investment Goes Bad*. [interaktyvus] Prieiga per internetą: https://www.nytimes.com/2018/05/31/technology/envion-initial-coin-offering.html [žiūrėta 2022 m. gruodžio 15 d.]
89. SEB bankas (2022). *Romantinis sukčiavimas – pakilime. Kaip nepatekti į internetinių „mylimųjų“ pinkles*. [interaktyvus]. Prieiga per internetą: https://www.seb.lt/infobankas/kasdieniai-finansai/romantinis-sukciavimas-pakilime-kaip-nepatekti-i-internetiniu [žiūrėta 2023 m. sausio 15 d.]
90. Sjouwerman, S. (2021). *Smishing and vishing: Explained and explored*. [interaktyvus]. Prieiga per internetą: https://www.securitymagazine.com/articles/94634-smishing-and-vishing-explained-and-explored [žiūrėta 2023 m. sausio 15 d.]
91. The Lending Standards Board (2019). *Contingent Reimbursement Model Code for Authorised Push Payment Scams*. [interaktyvus]. Prieiga per internetą: https://www.lendingstandardsboard.org.uk/wp-content/uploads/2019/05/CRM-code.pdf [žiūrėta 2023 m. sausio 17 d.]
92. United Nations Office on Drugs and Crime (2019). *Reporting cybercrime*. [interaktyvus]. Prieiga per internetą: https://www.unodc.org/e4j/en/cybercrime/module-5/key-issues/reporting-cybercrime.html [žiūrėta 2023 m. sausio 11 d.]

SANTRAUKA

Sukčiavimo elektroninėje erdvėje ypatumai ir baudžiamojo persekiojimo praktika Lietuvoje

Miglė Mackevičiūtė

Šiame magistro darbe analizuojama sukčiavimo, kuris pasireiškia elektroninėje erdvėje, nusikalstama veika. Pirmame magistro darbo skyriuje aptariama sukčiavimo elektroninėje erdvėje samprata siaurąja bei plačiąja prasme, išskiriami šios nusikalstamos veikos sudėties požymiai ir jų ypatumai. Antrame poskyryje išskiriami elektroninį sukčiavimą lemiantys veiksniai, paminint ir COVID-19 pandemijos kontekstą bei didėjančią visuomenės skaitmenizaciją, taip pat išskiriami elektroninio sukčiavimo padarymo būdai, paminint visuotinai paplitusius būdus, tokius kaip telefoninis sukčiavimas, investicinis sukčiavimas ar sukčiavimas, neteisėtai pasinaudojant asmens duomenimis. Analizuojant pateiktus statistinius duomenis, apžvelgiami labiausiai Lietuvoje paplitę elektroninio sukčiavimo būdai. Antrajame magistro darbo skyriuje analizuojamas elektroninio sukčiavimo ir kitų nusikalstamų veikų, pasireiškiančių elektroninėje erdvėje, pavyzdžiui, neteisėto elektroninių duomenų panaudojimo, disponavimo tokiais duomenimis ar neteisėto prisijungimo prie elektroninės sistemos santykis bei atribojimas. Išskiriami teritorinis bei aktyvus personalinis jurisdikcijos principai, jų taikymas nusikalstamoms veikoms, padaromoms elektroninėje erdvėje, bei įtvirtinimas Lietuvoje palyginant su reguliavimu tarptautinės teisės ar Europos Sąjungos teisės aktuose. Taip pat antrajame magistro darbo skyriuje aptariami elektroninio sukčiavimo tyrimo ir įrodinėjimo aspektai. Galiausiai, trečiajame magistro darbo skyriuje, atsižvelgiant į elektroninio sukčiavimo padarymo būdus, jų paplitimą, pateikiamos prevencinių priemonių taikymo kryptys bei teigiami Lietuvos praktikos pavyzdžiai.

SUMMARY

Features and practice of criminal prosecution of fraud in the cyber space in Lithuania

Miglė Mackevičiūtė

This Master's thesis analyses the criminal offence of fraud, which occurs in cyberspace. The first chapter of the Master's thesis discusses the concept of cyber fraud in the narrow and broad sense and identifies the elements of the offence and its specific features. The second section identifies the factors that lead to cyber fraud, including the influence of the COVID-19 pandemic and the increasing digitalisation of society, as well as the ways in which cyber fraud is perpetrated, mentioning the most common methods, such as telephone fraud, investment fraud, or fraud through the unauthorised use of personal data. The analysis of the statistical data provides an overview of the most common types of e-fraud in Lithuania. The second chapter of the Master thesis analyses the relationship and distinction between electronic fraud and other criminal offences occurring in cyberspace, such as the unlawful downloading and use of electronic data, the disposition of such data, or the unauthorized access to an electronic system. The territorial and active personal jurisdiction principles are distinguished, an overview is made of their application to offences committed in cyberspace and how they are established in Lithuania in comparison with the regulation under international or European Union law. The second chapter of the Master's thesis also discusses the investigation and evidentiary aspects of e-fraud. Finally, the third chapter of the Master's thesis, taking into account the methods of committing e-fraud and the prevalence of cyber fraud, presents the directions of preventive measures and positive examples of Lithuanian practice.