

**Vilniaus universiteto Teisės fakulteto
Baudžiamosios justicijos katedra**

Andros Mažrimaitės,
V kurso, baudžiamosios
justicijos šakos studentės

Magistro darbas

**Asmens duomenų vagystės, kaip nusikalstamos veikos, teorinės ir
praktinės problemos**

Vadovas: prof. dr. Aurelijus Gutauskas

Recenzentas: lekt. Darius Prapiestis

Vilnius

2022

ANOTACIJA IR PAGRINDINIAI ŽODŽIAI

Šis magistro darbas nagrinėja fizinio asmens tapatybės vagystės, kaip socialinio – teisinio reiškimo, teisinius aspektus. Darbe analizuojamas asmens tapatybės vagystės, kaip nusikalstamos veikos, reglamentavimas užsienio šalyse, nagrinėjami dažniausi tokios veikos atlikimo būdai bei padaroma žala. Galiausiai, pateikiama informacija apie šiuo metu Lietuvoje esantį tokios veikos teisinį reglamentavimą, nusikalstamas veikas, kurių sudėtyse yra šios veikos požymių bei išanalizuojamas tokios veikos kriminalizavimo reikalingumas bei pateikiamas galimas tokios nusikalstamos veikos įtraukimo į Lietuvos Respublikos baudžiamąjį kodeksą modelis.

Pagrindiniai žodžiai: tapatybė, vagystė, asmens duomenys, privatumas, elektroninė erdvė, asmens tapatybės vagystė, kriminalizavimas.

This master's thesis examines the legal aspects of the theft of a natural person's identity as a social-legal phenomenon. The work analyzes the regulation of identity theft as a criminal offense in foreign countries, examines the most common ways of committing such an offense and causes damage. Finally, information is provided on the current legal regulation of such an offense in Lithuania, criminal offenses containing signs of such an offense and the need to criminalize such a criminal offense is analyzed, as well as a possible model for including such an offense in the Criminal Code of the Republic of Lithuania.

Keywords: identity, theft, personal data, privacy, cyberspace, identity theft, criminalization.

TURINYS

ĮVADAS	2
1. ASMENS DUOMENŲ VAGYSTĖS ELEKTRONINĖJE ERDVĖJE SAMPRATA.....	6
1.1. Asmens duomenų vagystės samprata ir tapatybės nustatymo kriterijai.....	6
1.2. Asmens duomenų vagystės istorinis vystymasis ir aktualumas.....	11
2. TAPATYBĖS VAGYSTĖS ELEKTRONINĖJE ERDVĖJE FORMOS IR BŪDAI ...	15
2.2. Tapatybės vagystės formos	15
2.2. Tapatybės vagystės elektroninėje erdvėje įvykdymo būdai.....	17
3. ASMENS DUOMENŲ VAGYSTĖS ELEKTRONINĖJE ERDVĖJE KRIMINALIZAVIMAS	20
3.1. Tapatybės vagystės kriminalizavimas užsienio valstybėse.....	20
3.2. Asmens duomenų vagystė kaip nusikaltimas asmens privataus gyvenimo pažeidžiamumui	24
3.3. Atskirų asmens duomenų vagystės elementų kriminalizavimas Lietuvoje	27
4. GALIMAS ASMENS TAPATYBĖS VAGYSTĖS, KAIP NUSIKALSTAMOS VEIKOS, SUDĖTIES MODELIS	30
4.1. Tapatybės vagystės elektroninėje erdvėje sudėties objektyvieji požymiai.....	30
4.2. Tapatybės vagystės elektroninėje erdvėje sudėties subjektyvieji požymiai	31
4.3. Lietuvos Respublikos baudžiamojo kodekso specialiosios dalies pakeitimo projektas.....	33
IŠVADOS	37
PASIŪLYMAI.....	38
ŠALTINIAI IR LITERATŪRA.....	39
SANTRAUKA	45
SUMMARY	46

IVADAS

Temos aktualumas. Kiekvienas iš mūsų esame skirtingas bei unikalus, kiekvienas iš mūsų turime tik sau priklausančius asmens duomenis, kiekvienas iš mūsų turime savo tapatybę, kuri ir išskiria mus iš visų kitų žmonių, esančių pasaulyje. Vos ne kiekvieną dieną susiduriame su savo asmens duomenų tikrinimu, turime pateikti savo tapatybę patvirtinančius dokumentus, identifikuotis elektroninėje bankininkystėje, pateikdami asmens kodą bei atliekame dar begales veiksmų, kurių dėka identifikuojame save. Šiuolaikiniame gyvenime mes taip pat vis dažniau susiduriame su technologijomis. Nepaisant kasdieninių interneto suteikiamų funkcijų, priklausomybės nuo socialinės žiniasklaidos tyrimai atskleidžia, kad apie 333 milijonai žmonių visame pasaulyje kenčia net nuo tam tikros formos priklausomybės nuo interneto ir socialinės žiniasklaidos. Be to, tyrimai rodo, kad padėtis tik blogės (Geysler, 2021). Atsižvelgiant į tai, modernėja ir vagysčių padarymo būdai, o tuo labiau, ne išimtis yra ir vis tobulėjančios asmens duomenų bei tapatybės vagystės. Vis nauji padarymo būdai atneša į mūsų gyvenimus vis naujų iššūkių – asmens tapatybės vagystė elektroninėje erdvėje tampa vis didesne grėsme.

Nors pirmiausia neteisėtą veiklą skaitmeninėje erdvėje galėjome laikyti papokštavimais, vandalizmu ar chuliganiškų veiksmų atlikimu, pavyzdžiui, kompiuteriniai virusai, skirti kompiuterių operacinės sistemos veiklai sutrikdyti, arba internetinių puslapių išvaizdos pakeitimas (angl. *defacement*), laikui bėgant tokie veiksmai tapo orientuoti konkrečiai į finansinės naudos siekimą (Kalpokas, Marcinauskaitė, 2012, p. 30). Pirmiausia internetas ir skaitmeninė erdvė buvo pradėti naudoti kaip priemonė atlikti jau anksčiau žinomas nusikalstamas veikas, tokias kaip pinigų plovimas, sukčiavimas, taip pat tapo puikia platforma realizuoti vagystės metu įgytus daiktus, vykdyti tokius nusikaltimus kaip prekyba žmonėmis. Tačiau kuo toliau, tuo praktikoje vis dažniau išvystame ir tokių nusikalstamų veikų, kurios būdingos tik elektroninei erdvei, pavyzdžiui, neteisėtas prisijungimas prie informacinės sistemos, kompiuterinių sistemų atakos ir kt.

Tačiau tam, kad būtų galima vykdyti nusikalstamas veikas, asmuo dažnu atveju siekia sužinoti duomenis, kurie jam padėtų tai padaryti. Dažnu atveju, asmuo tiesiog nori apsimesti kitu žmogumi, identifikuoti save ir taip atlikti veiksmus, kuriems jis neturi jokio teisėto pagrindo. Tuomet susiduriame su nauju socialiniu – teisiniu reiškiniu – tapatybės vagyste. Tapatybės vagystė didelę žalą gali padaryti ne tik paprastiems vartotojams – fiziniams asmenims, finansinėms institucijoms, tačiau ir visai šaliai ar net pasaulio ekonomikai. Tai naujas reiškinys, susijęs ne tik su asmenų privataus gyvenimo neliečiamumo, saugumo pažeidimais, tačiau ir apskritai su neteisėtu informacijos apie

asmenį gavimu. Ji gali būti atliekama įvairiai – nuo neteisėto prisijungimo prie asmens elektroninės bankininkystės, banko kortelės duomenų panaudojimo apsiperkant internetu iki visiško kito asmens tapatybės pasisavinimo bei apsimetimo šiuo asmeniu visose gyvenimo situacijose.

Kaip bebūtų, pati sąvoka „tapatybės vagystė“ ar „asmens duomenų vagystė“ šiais technologijų laikais labiau siejama su elektronine erdve, kadangi šis būdas dažniau pasirenkamas dėl platesnių identifikacijos galimybių ir vis naujesnių technologinių išradimų. Be to, tapatybės vagystė elektroninėje erdvėje gali būti atliekama bet kuriuo metu, būnant bet kurioje vietoje, kas tik dar didina šios veikos pavojingumą ir padaro ją globalia problema. Atsižvelgiant į tai, matome, jog pasaulyje vyksta diskusijos ar tokia veika, kaip asmens tapatybės vagystė, turėtų būti kriminalizuota, ar tokia veika turėtų būti įtraukta į valstybių baudžiamuosius įstatymus bei koks bendradarbiavimas tarp valstybių turėtų būti plėtojamas, norint siekti mažinti tokius reiškinius bei kovoti su šia veika, kurios mastas, atrodo, neišvengiamai didėja. Vienose valstybėse toks reiškinys *per se* apskritai nėra įtvirtintas kaip teisės pažeidimas, tuo tarpu kitose valstybėse tapatybės vagystė laikoma nusikaltimu už kurį yra taikoma baudžiamoji atsakomybė. Pažymėtina, jog daugumoje valstybių (taip pat ir Lietuvos Respublikoje) tapatybės vagystė bendrąja prasme ir (ar) tapatybės vagystė elektroninėje erdvėje nėra laikoma kaip atskirą sudėtį turinti nusikalstama veika, taip pat ši sąvoka nėra minima jokiuose kituose Lietuvos Respublikos įstatymuose ar teisės aktuose. Atsižvelgiant į darbo apimties reikalavimus, šiame darbe bus nagrinėjama fizinio asmens tapatybės vagystė, bei koncentruojamasi būtent į asmens tapatybės vagystės elektroninėje erdvėje aspektus.

Darbo tikslas. Išnagrinėti tapatybės vagystės elektroninėje erdvėje kaip socialinio – teisinio reiškinio teisinius aspektus, įvertinti ar tikslinga būtų Lietuvos Respublikos baudžiamajame kodekse kriminalizuoti tapatybės vagystę kaip atskirą veiką bei pateikti tokio teisinio vertinimo siūlymus.

Darbo uždaviniai. Siekiant įgyvendinti magistro darbo tikslą, buvo iškelti šie uždaviniai:

- 1) Apžvelgti tapatybės vagystės elektroninėje erdvėje reikšmę, istorinį vystymąsi bei sampratų įvairovę, išanalizavus šiuos aspektus pateikti vieną galimą tokios sąvokos formuluotę;
- 2) Aptarti tapatybės vagystės elektroninėje erdvėje, kaip vienos iš tapatybės vagystės rūšių, atlikimo būdus, jų specifiką;
- 3) Išnagrinėti bei įvertinti atskirų asmens duomenų vagystės elementų kriminalizavimą užsienio šalyse bei Lietuvoje;

- 4) Išskirti ir išanalizuoti tapatybės vagystės elektroninėje erdvėje požymius bei pateikti Lietuvos teisiniam reguliavimui tinkamiausią šios veikos sudėties modelį.

Darbo objektas. Magistro darbo objektą sąlygoja darbo tikslas bei jam pasiekti išskelti uždaviniai. Objektas – fizinio asmens duomenų vagystė elektroninėje erdvėje bei jos, kaip nusikalstamos veikos, teorinės ir praktinės problemos.

Tyrimo metodai. Magistro darbe naudojami šie mokslinio tyrimo metodai:

- 1) Analizės – naudojant šį metodą tapatybės vagystės elektroninėje erdvėje reiškiny išskaidomas į atskiras sudėtines dalis, požymius, kurie kiekvienas nagrinėjami atskirai, kad būtų atskleisti ir aptarti tiriamojo objekto ypatumai, atliekama atitinkamų teisės aktų, doktrininių teiginių analizė;
- 2) Lingvistinis – šis metodas magistro darbe taikomas analizuojant atitinkamų teisės aktų normų turinį;
- 3) Sisteminis – metodas naudojamas tam, kad, remiantis tarptautiniais ir nacionaliniais teisės aktais, teismų praktika ir doktrina, įvertinti bei iširti asmens tapatybės vagystės, kaip nusikalstamos veikos, galimą reglamentavimą ir jo taikymą;
- 4) Loginis – remiantis šiuo metu atskleidžiamos problemos, pateikiami galimi jų sprendimo būdai, formuojama atitinkama pozicija magistro darbe keliamais probleminiais klausimais;
- 5) Lyginamasis – analizuojama tarptautinių, Europos Sąjungos, užsienio valstybių teisės aktų specifika lyginant su Lietuvos Respublikos baudžiamojo kodekso ir kitų nacionalinių teisės aktų nuostatomis;
- 6) Analitinis – kritinis – šio metodo pagalba akcentuojami esamo tapatybės vagystės elektroninėje erdvėje teisinio reguliavimo trūkumai, atliekamos teisės norminių aktų trūkumų įžvalgos;
- 7) Teleologinis – šis metodas padeda magistro darbe atskleisti galiojančio teisinio reglamentavimo bei teisėkūros subjektų tikrusius ketinimus ir tikslus, susijusius su tarptautiniais bei nacionaliniais teisės aktais, asmens tapatybės vagystės kvalifikavimo bei pritaikymo praktikoje klausimais.

Pagrindiniai šaltiniai. Atsižvelgiant į magistro darbo tikslus, uždavinius, magistro darbo objektą bei tai, jog Lietuvoje ši tema nėra plačiai analizuojama, vienu iš pagrindinių šaltinių yra laikomas Lietuvos Respublikos baudžiamasis kodeksas (2000), kurio normos yra analizuojamos šiame darbe. Taip pat, magistro darbe remiamasi kitais tarptautiniais, Europos Sąjungos, Lietuvos Respublikos bei kitų užsienio valstybių teisės aktais, Lietuvos

bei užsienio valstybių teismų praktika. Darbe daugiausia remiamasi Lietuvių autorių – Dariaus Štītilio, Ingos Dauparaitės, Mariaus Laurinaičio, Pauliaus Pakutinsko, Vaido Kalpoko bei Renatos Marcinauskaitės mokslinė literatūra. Svarbią reikšmę magistro darbui turi ir užsienio autorių mokslinė literatūra – itin aktualūs buvo Sandra K. Hoffman, Tracy G. McGinley, Marco Gercke moksliniai darbai.

Darbo naujumas bei originalumas. Lietuvių autorių darbuose asmens tapatybės vagystė nėra plačiai nagrinėjama tema, ypač paskutiniųjų metų perspektyvoje. Atsižvelgiant į tai, jog asmens tapatybės vagystė yra vertinama kaip socialinis – teisinis reiškinys, daugiausia ši tema nagrinėjama tarpdiscipliniškai – darbuose pasitelkiami socialinių mokslų autoriai. 2011 m. išleista kolektyvinė mokslų monografija (Štītilis *et al.*, 2011), nagrinėjanti tapatybės vagystę elektroninėje erdvėje bei apjungianti informacinių technologijų, ekonomikos ir teisės sritis. Po šios monografijos daugiau Lietuvos autorių darbų išleista nėra. Užsienio teisinėje literatūroje randama mokslo darbų, susijusių su asmens tapatybės vagystės teisiniu vertinimu, tačiau juose nėra nagrinėjami Lietuvos teisiniam reguliavimui aktualūs aspektai, tokie kaip asmens tapatybės vagystės, kaip nusikalstamos veikos sudėties analizė, kriminalizavimo galimybės Lietuvos Respublikos baudžiamajame kodekse, kitų nusikalstamų veikų lyginamoji analizė. Taigi, autorės žiniomis, asmens tapatybės vagystės elektroninėje erdvėje teisiniai aspektai bei tokios nusikalstamos veikos kriminalizavimo galimybės bei reikiamybė Lietuvoje atskiruose mokslo darbuose nagrinėta nėra.

1. ASMENS DUOMENŲ VAGYSTĖS ELEKTRONINĖJE ERDVĖJE SAMPRATA

Šis magistro darbo skyrius analizuos asmens tapatybės vagystės elektroninėje erdvėje sampratą – įvardinama, kokia ji yra pateikiama skirtinguose šaltiniuose, ir kaip vystėsi skirtinguose laiko tarpsniuose. Apibrėžiama, kas yra laikoma asmens duomenimis bei kaip ši sąvoka yra susijusi su asmens tapatybės sąvoka ir koks turėtų būti (jei turėtų būti) tokių sąvokų tapatumas. Galiausiai, apibrėžiami asmens tapatybės nustatymo kriterijai, kurie itin reikšmingi tolimesniam tokios veikos tyrimui bei analizavimui.

1.1. Asmens duomenų vagystės samprata ir tapatybės nustatymo kriterijai

Visų pirma, pradėdami kalbėti apie tapatybės ar asmens duomenų vagystę mes susiduriame su klausimais, kas tai yra? Kas yra duomenys, kas yra asmens tapatybė? Ar šias sąvokas mes galime vadinti sinonimais, ar priešingai, šios sąvokos apima vieną kitą ir be vienos, nebūtų kitos? Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas (1996) mus nukreipia į 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, kurio 4 straipsnio 1 dalyje yra apibrėžiama, jog: „asmens duomenys – bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti (duomenų subjektas); fizinis asmuo, kurio tapatybę galima nustatyti, yra asmuo, kurio tapatybę tiesiogiai arba netiesiogiai galima nustatyti, visų pirma pagal identifikatorių, kaip antai vardą ir pavardę, asmens identifikavimo numerį, buvimo vietos duomenis ir interneto identifikatorių arba pagal vieną ar kelis to fizinio asmens fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar socialinės tapatybės požymius“. Tuo tarpu apibrėžiant tapatybės sąvoką, dėmesys turi būti kreipiamas į tapatybę, susijusią su asmens duomenimis – tai, pagal ką mus atpažįsta įvairios kompanijos, asociacijos ar valdžios institucijos. Tapatybę sudaro bet koks vardas, numeris ar kitas požymis, kuris suteikia informaciją apie mus arba kuriuo pasinaudojus galima prieiga prie kitų asmens duomenų (Sileo, 2005). Atsižvelgiant į tai, galime daryti išvadą, jog asmens duomenys yra platesnė sąvoka, apibūdinanti daug daugiau negu asmens tapatybę. Tačiau be konkrečių asmens duomenų, mes negalėtume apibūdinti ir to konkretaus asmens tapatybės, taigi, asmens tapatybė yra sudaroma iš asmens duomenų, todėl šių sąvokų mes negalime laikyti sinonimais – tai labiau kaip viena kitą papildančios sąvokos.

Akcentuotina tai, kad nors tapatybės vagystė yra tarptautinio pobūdžio problema, nei tarptautiniu, nei regioniniu lygiu privalomo pobūdžio teisės aktuose nėra įtvirtintos tapatybės vagystės ar tapatybės vagystės elektroninėje erdvėje sąvokos. Nacionaliniu lygiu tapatybės vagystės sąvoka suprantama gana skirtingai, o tapatybės vagystės elektroninėje

erdvėje sąvoka iš viso nepateikiama (Štītīlis, *et al.*, 2011, p. 70). Atsižvelgiant į tai, šioje darbo dalyje bus apibūdinamos mokslinėje literatūroje randamos tapatybės vagystės sąvokos.

Tapatybės vagystė yra kompleksinis reiškinys, susijęs su vartotojų teisių, saugumo, privatumo, taisyklių, reglamentuojančių nepageidaujamos informacijos gavimą, pažeidimais. Ji gali būti atliekama įvairiai – nuo neteisėto mokėjimo kortelės panaudojimo iki visiško kito asmens tapatybės perėmimo ir užvaldymo. Akademine prasme Jaishankar (2008) tvirtina, kad tapatybės nusikaltimas yra sąvoka, kurią galima suskirstyti į tris kategorijas: asmeninę, socialinę ir teisinę tapatybę.

Akademiniuose ištekliuose yra randama įvairių nuomonių, kaip reikėtų apibūdinti tapatybės vagystę, nes apibrėžimas yra ne tik labai svarbus akademiniam tyrimams, bet ir suteikia didžiulę naudą teisinei praktikai bei teisėkūros procesui, kuris yra pagrindas kovojant su elektroniniais nusikaltimais. Tapatybės vagystė įvyksta, kai kas nors panaudoja kito asmens tapatybę identifikuojančią informaciją, pvz., vardą, pavardę, gimimo datą, motinos mergautinę pavardę, asmens tapatybės numerį ir pan., kad sukčiautų arba užsiimtų kita neteisėta veikla (Collins, 2005, p. 7) .

Tapatybės vagystės procesas pripažįstamas, kai: „nusikaltėliai įgyja esminę asmens tapatybę identifikuojančią informaciją, pvz., vardą, pavardę, adresą, gimimo datą, motinos mergautinę pavardę, informaciją apie darbą, kredito informaciją ir kitus itin svarbius faktus, kad galėtų apsimesti ir apgauti auką. Ši pasisavinta informacija suteikia galimybę įvykdyti daugybę sukčiavimo formų, įskaitant aukos finansinių sąskaitų perėmimą – kreiptis dėl paskolos, kredito kortelių ir socialinio draudimo išmokų, įsigyti būstą ar automobilį bei teikti paslaugas, pavyzdžiui, komunalinių paslaugų ir telefono ryšio bendrovėse (Digital Agenda of Europe, 2010, p. 1-4).

Kiti šaltiniai ne kartą nurodo beveik tą pačią situaciją: „Tapatybės vagystė įvyksta, kai nusikaltėlis įgyja pagrindines asmens tapatybę identifikuojančios informacijos dalis, kad galėtų pasiekti asmens finansines sąskaitas“ (Copes, Vieraitis, 2012). Palyginus su tuo, Jungtinių Valstijų slaptoji tarnyba tapatybės nusikaltimus apibrėžia kaip „piktnaudžiavimą asmeniniais ar finansiniais identifikatoriais, siekiant įgyti ką nors vertingo ir (arba) palengvinti kitą nusikalstamą veiklą“ (United States Secret Service, 2011). Asmens tapatybės vagystė – tai asmens duomenų naudojimas be jo žinios ir siekiant padėti arba paskatinti bet kokią neteisėtą veiklą, pvz., apgaulingą paslaugų, prekių, pinigų ir (arba) kredito gavimą (Hoffman, McGinley, 2010, p. 1).

Visi šie apibrėžimai pirmiausia nurodo, kad informaciją galima gauti legaliai ar nelegaliai, metodas nėra toks svarbus, nes tokių kibernetinių nusikaltimų tikslas iš savo

esmės yra neteisėtas – gauti naudos iš asmens, kuriam priklauso asmeninė informacija, susijusi su jo finansine/turtine veikla. Apsimetinėjimas asmeniu yra nusikaltimo dalis, nes jis suteikia sukčiui galimybę apsimesti konkrečiu asmeniu ir atlikti savo neteisėtus intelektinius ir (ar) fizinius veiksmus. Paprastai paskutinis žingsnis įvyksta jau perėmus finansines sąskaitas, tuomet tapatybės vagystės nusikaltimas laikomas visiškai baigtu, pavyzdžiui, gauta informacija panaudota kreipiantis dėl paskolos, pirktas automobilis ir pan. (Allstate, 2018).

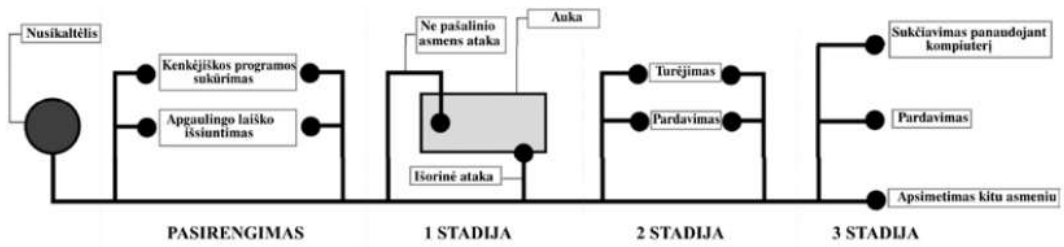
Sunkiausia tapatybės vagystės forma yra „visiškas tapatybės perėmimas“. Tai įvyksta, kai pavagiama pagrindinė asmens tapatybę identifikuojančios informacijos dalis, kurią vagis naudoja siekdamas kontroliuoti kiekvieną aukos gyvenimo aspektą, taigi, paprastai perimama visa tapatybė. Dažniausiai pasisavinamas asmens kodas arba motinos mergautinė pavardė, bet kuri asmeninė informacija, kuri gali būti naudojama norint gauti papildomus dokumentus, prieigą ar prisijungimus, turint esminius asmens duomenis (Hoffman, McGinley, 2010, p. 3).

Kai sąvoka tapatybė ir nusikaltimas yra sujungiami į bendrinę sąvoką, jie vadinami „tapatybės nusikaltimais“, o terminas reiškia visų formų neteisėtus veiksmus, atliekamus prisidengiant kito asmens tapatybe, taip pat parengiamuosius veiksmus, susijusius su tapatybės rinkimu, manipuliavimu ir prekyba šia informacija (Lawson, 2011, p. 111). Be to, vienas iš išsamiausių tapatybės nusikaltimo apibrėžimų galėtų būti tas, kuris jį traktuoja kaip ciklą su penkiomis skirtingomis fazėmis (The Cross-Border Crime Forum, 2019, p. 2):

- 1) neteisėtas identifikuojančių duomenų ar daiktų (pvz., kortelių ar dokumentų) gavimas;
- 2) iš pradžių gautų identifikacinių duomenų ar dokumentų perdavimas;
- 3) manipuliavimas duomenimis arba elementais (pvz., keičiant, sujungiant arba klastojant);
- 4) manipuluojamų duomenų arba elementų perdavimas; ir
- 5) duomenų ar elementų naudojimas sukčiavimui arba nusikalstamai tapatybei nuslėpti.

Tačiau šiame darbe bus remiamasi kiek siauresne asmens tapatybės vagystės sąvoka, kurioje yra išskiriamos trys tapatybės vagystės stadijos: pirma stadija – su tapatybe susijusios informacijos gavimas, antra stadija – sąveika su tapatybe susijusia informacija, trečia stadija – su tapatybe susijusios informacijos panaudojimas siekiant padaryti nusikaltimą (Gercke, 2011, p. 17-20).

1 paveikslas. Tapatybės vagystės sąvoka



Šaltinis: Štītīlis et al., Tapatybės vagystės elektroninėje erdvėje kriminalizavimas: lyginamieji aspektai, 2011, p. 2011.

Vartojamas tapatybės nusikaltimo terminas ir naudojamas kaip bendras terminas, apimantis įvairius nusikaltimus tapatybei skirtingose atskirose stadijose. Tokia veikla galėtų būti klastojimas, keitimas, vogimas, naikinimas, naudojimas ir panašiai. Žvelgiant į tapatybės nusikaltimą atskirais etapais, galima spręsti apie nusikalstamą veiklą skirtingose stadijose. Pavyzdžiui, kai kurie nusikaltėliai gali rinkti informaciją, o kiti gali eiti toliau ir manipuluoti ar naudoti tokią informaciją tolesniems nusikaltimams daryti. Taigi, visų šių etapų aptarimas apie nusikaltimą tapatybei ir galiojančių nuostatų žinojimas, jei tokių yra, galėtų padėti pažaboti tuos sunkius nusikaltimus ir sušvelninti neigiamą jų poveikį.

Taigi, tapatybės vagystė yra kenkėjiška grėsmė. Šiais laikais asmeninei ar identifikuojančiai informacijai bet kuriuo momentu kyla didelė vagystės rizika, nes vėliau ji gali būti panaudota „apgaulingam paslaugų, prekių, pinigų ir (arba) kredito gavimui“ (ibid, p. 2). Šios galimų tapatybės vagysčių aukų apžvalgos rodo didelę galimų grėsmių, kurias gali kelti nusikaltėliai, riziką. Didesnio teisinio dėmesio šiai nusikalstamumo sričiai tikimasi ir dėl teisės į privatumą pažeidžiamumo bei išvados, kad gintis nuo tokio pobūdžio nusikaltimų yra itin sunku, lyginant su kitų rūšių ir formų vagystės nusikaltimais. Šiems aspektams reikalingas konkrečiai orientuotas teisinis dėmesys, taip pat efektyvios technologinės ir teisinės priemonės, kurios turi būti įdiegtos į nacionalinę teisę.

Kalbant apie tapatybės nustatymo kriterijus ir duomenis, reikalingus asmens tapatybei identifikuoti, turėtume paminėti, jog fizinėje erdvėje identifikavimo procesas nėra toks sudėtingas, kaip elektroninėje erdvėje. Asmens tapatybė gali būti identifikuojama naudojant tokią teisinę priemonę kaip pasas, kurį išduoda nacionalinė valstybė. Pase pavaizduotas asmuo bus identifikuojamas realiu laiku ir erdvėje, tačiau būtina nurodyti, kad oficialius dokumentus gali sufabrikuoti ir nusikaltėliai.

Be to, toks tapatybės nustatymo procesas, kai konkretaus asmens tapatybei nustatyti naudojamas teisėtai išduotas individualus dokumentas, paprastai vadinamas oficialiu identifikavimu (Chiffelle et al., 2009, p. 20). Palyginus su daugeliu Europos identifikavimo sistemų, pavyzdžiui, Jungtinės Valstijos susiduria su daugybe tapatybės vagysčių dėl priežasties, kad yra labai lanksti identifikavimo sistema, leidžianti naudoti įvairius asmens tapatybę identifikuojančius dokumentus, galime teigti, jog Lietuvoje yra nedidelis kiekis dokumentų, kuriais remiantis gali būti nustatoma asmens tapatybė – Lietuvos Respublikos asmens tapatybės kortelės ir paso įstatymu (2014), turime dvi oficialias valstybės išduodamas priemones tapatybei nustatyti – pasą bei asmens tapatybės kortelę.

Elektroninėje erdvėje identifikavimo procesas tapo esminis reikalavimas. Taip yra iš dalies dėl intensyvaus elektroninės erdvės naudojimo, įskaitant išaugusius komercinius sandorius, balsavimą ir socialinių tinklų naudojimą. Akademinėje literatūroje pastebima, kad identifikavimas virtualioje erdvėje yra kelis kartus didesnis rizikos lygiu, palyginti su realiu pasauliu. Dėl to logiška pastebėti, kad daugiau tapatybės vagysčių įvyksta virtualioje erdvėje, palyginti su realiu laiku ir erdve (Higgins, 2010, p. 74).

Internetinis pasaulis taip pat yra specifiskesnis, palyginti su realiu pasauliu dėl to, kad atpažinimo procesas nereikalauja asmens buvimo, nes internetinis pasaulis suteikia galimybę atlikti įvairius veiksmus per didelį atstumą ir laiką. Šie veiksmai gali apimti duomenų operaciją, duomenų išsaugojimą ir (ar) duomenų naudojimą, naudojant technines priemones, dažniausiai pasitelkiant kompiuterius ar mobiliuosius telefonus (Štītīlis *et al.*, 2010, p. 22-23). Be to, identifikavimo procesas elektroninėje aplinkoje laikomas sudėtingesniu, palyginti su realia erdve, nes elektroninė aplinka dažniausiai turi daug tarpininkų, kurie identifikavimą dar labiau apsunkina, ir susiduriama su konkretaus asmens tapatybės nustatymo mechanizmu, taip pat su vartotojų teisėmis ir duomenų apsauga, privatumo apsaugos politika (*ibid.*, p. 22). Žinoma, skiriasi aplinkos sfera, kurioje reikia identifikuoti asmenį: elektroninės komercinės paslaugos, administracinės paslaugos ir kt., be to, skiriasi ir identifikavimo būdai, nes asmuo gali būti atpažįstamas ir identifikuojamas naudojant elektroninį parašą, kompiuterio adresą IP, belaidės stoties adresą, domeno pavadinimą ir kt. (Bullot, 2014, p. 567). Tapatybės sąvokos apibrėžimas ir klasifikacija, taip pat struktūra išlieka labai svarbios norint suprasti aktualius tapatybės vagystės internetiniame pasaulyje aspektus, nes požiūriai į šį apibrėžimą vis dar skiriasi. Norint turėti tobulą teisinį pagrindą nacionaliniam, regioniniam, tarptautiniam kibernetinių nusikaltimų srities ir jos specifinių nusikalstamų tapatybės vagysčių teisiniui reguliavimui, būtina sukurti vieną pagrindinį teorinį tapatybės požiūrį, kuris atspindėtų

visus būtinus teisinius aspektus ir punktus, yra svarbūs ir būtini siekiant veiksmingų teisėkūros tikslų ir teisinės harmonijos šioje srityje.

Atsižvelgiant į tai, galime daryti išvadą, jog tapatybės vagystė turi būti suprantama kaip „neteisėti veiksmai pasitelkiant kito asmens duomenimis ir (ar) informaciją, kurie suteikia galimybę identifikuoti kitą asmenį, turint tikslą apsimesti tuo asmeniu“. Tuo tarpu tapatybės vagystės elektroninėje erdvėje sąvoka turėtų skambėti kaip: „tapatybės vagystės rūšis, kai tapatybės vagystė atliekama nuotoliu, pasinaudojant informacinėmis ir ryšio technologijomis“.

1.2. Asmens duomenų vagystės istorinis vystymasis ir aktualumas

Tapatybes vagystė, tai santykinai nesena frazė, kurios kilmę lėmė populiari mintis, o ne teisėkūros išraiška, teisminė išmonė ar akademinė abstrakcija. Pabrėžtina, jog tai yra itin senas reiškinys, tačiau mūsų šalyje atsirado gana nesena ir apie tai visi pradėjo kalbėti lyg tai būtų tik kažkokia nauja mada. Žinoma, esminis pokytis yra internetas ir jo atsiradimas, kuris itin palengvino tokio pobūdžio nusikaltimų įvykdymą ir suteikia nusikaltėliams naujų bei modernesnių būdų juos vykdyti.

Tapatybės vagystės raidą galima pamatyti žemiau esančioje 1 lentelėje nuo 1800-ųjų iki 2018 m. bei numatomos būklės vėliau (Irshad, Soomro, 2018, p. 43).

1 lentelė. Tapatybės vagystės eros raida

Era	Tapatybes vagystės tipai
1800– 1918	Šios eros uždrausti žmonės žudė žmones, kad prisiimtų savo aukų tapatybes.
1919– 1921	Tapatybės buvo vagiamos dėl įvairių rinkimų.
1922– 1930	Kontrabandininkai sukūrė savo liudininkų apsaugos programų versiją ir žudė žmones, kad gautų teisinius dokumentus ir to pagrindu kurtų naujas tapatybes žmonėms.
1931– 1959	Jaunuoliai kurdavo netikrus asmens tapatybės dokumentus ar naudodavo/klastodavo esamus, norėdami nusipirkti alkoholio.
1960– 1969	Kreditinių kortelių įvedimas nusikaltėliams suteikė naujų tapatybės vagysčių būdų.
1970– 1989	Garsusis sukčius Frankas Abagnale'as vogė grynųjų pinigų čekių tapatybes.

1990– 1998	Technologijų pažanga itin padidino tapatybės nusikaltimų atvejus.
1999– 2000	Internetas ir paieškos sistemos, tokios kaip Google, paskatino žmones perduoti savo asmeninę informaciją.
2001– 2003	Kredito ataskaitų agentūroms buvo nurodyta teikti kredito ataskaitas klientams, kad būtų išvengta apgaulingų sąskaitų atidarymo.
2004– 2015	Įtraukiamos naujos tapatybės vagystės formos vis atsirandančios kartu su interneto egzistavimu ir itin plačiu paplitimu pasaulyje.
2016	Tapatybės vagystė buvo populiariausias vartotojų skundas JAV 15 metų iš eilės.
2017	Bankai itin padidino savo saugumą, ko pasekoje nusikaltėliai tapatybei vogti naudojami kitomis ir vis naujomis platformomis.
2018– ****	Technologijos tobulėja ir pristatomos vis naujos aplikacijos/internetinės svetainės/socialiniai tinklai, ko pasekoje, vagys gauna vis daugiau galimybių bei prieigos prie asmeninės žmonių informacijos.

Šaltinis: Shareen ir Tariq, Identity Theft and Social Media, 2018.

Plačiau aptariant tapatybės nusikaltimų istoriją ir raidą yra randami įvairūs istoriniai pavyzdžiai:

Pirmiausia, remiantis anksčiausiai žinomais pavyzdžiais, asmuo, vardu Jokūbas, buvo laikomas pirmuoju asmeniu, pavogusiu kito asmens tapatybę. Toks atvejis yra aprašomas Biblijoje, kuomet jis mėgdžiojo savo brolio tapatybę, kad galėtų paveldėti šeimos turtą, kadangi jis jam nepriklausė ir Jokūbas galėjo gauti šeimos turtą tik naudodamasis apsimitinėjimo būdu (Hoffman, McGinley, 2010, p. 21). Apsimitinėjimas, kaip tapatybės vagystės būdas, reiškia teisėto asmens mėgdžiojimą, norint apgauti asmenį, siekiant gauti asmeninės naudos.

Sekantis tapatybės vagystės atvejis įvyko Jungtinėje Karalystėje dar 1450 m., kai asmuo, dirbęs gydytoju Anglijoje iki 1440 m., kuomet buvo apkaltintas žmogžudyste ir 1449 m. pabėgo į Prancūziją. Po vienerių metų jis grįžo į Angliją prisiimtu kito asmens vardu (ibid, p. 22) ir po kurio laiko net ne kartą pagautas bei nubaustas jis vis keisdavo įvairias tapatybes ir toliau sėkmingai apsimitinėdavo kitais žmonėmis.

Retkarčiais kaltininkas vagia kito asmens informaciją, kad pasinaudotų ja asmeninei naudai gauti arba pabėgti nuo siaubingų gyvenimo sąlygų ar įsipareigojimų. Pavyzdžiui, vienas iš neretai pasikartojančių atvejų įvyko dar 1771 m. Šeimininkas, su jo dvare dirbusia tarnaitė elgėsi itin žiauriai – ją mušė bei kitaip kankino. Dėl tokio griežto elgesio ji

nusprendė palikti buvusį gyvenimą ir pradėti naują etapą – jau nebe tarnaitės, o itin pasiturinčios ir privilegijuotos. Siekdama tokio gyvenimo, ji panaudojo britų karalienės sesers vardą ir adresą, kurį ji pavogė dirbdama tarnaitė karalienės dvare (ibid, p. 23).

Žinoma, įdomu ir tai, jog mirusieji taip pat nebuvo ir vis dar nėra apsaugoti nuo tapatybės vagystės atvejų. Pavyzdžiui, 1917 m. Rusijos caras Nikolajus II buvo nuverstas per perversmą ir visame pasaulyje pasklido gandai apie tai, jog po jo mirties liko gyvi jo įpėdiniai – jo vaikai. Daugelį metų begalės asmenų bandė apsimesti jo vaikais. Dauguma apsimitėlių bandė apsimesti jo jauniausia dukra Anastasija. Garsusis Anastasijos apsimitimas įvyko 1920 m., kai moteris bandė nusižudyti, tačiau ją išgelbėjo patrulis, o vėliau ji buvo išvežta į psichiatrinę ligoninę. Psichikos įstaigoje ji pasakė gydytojui, kad jos vardas yra Anastasija, Nikolajaus II dukra, tačiau, deja, ji negalėjo įrodyti savo tapatybės (Lyzhina, Zaghrud, 2004).

Dvidešimtojo amžiaus pradžioje nusikaltėliai pradėjo keisti vykdomus tapatybės vagystės metodus. Jie naudojo jau kur kas sudėtingesnius metodus: kūrė netikrus dokumentus, klastodavo arba vogdavo dokumentus su asmenų informacija, kad pavogtų ir pasisavintų kito asmens tapatybę. Pavyzdžiui, asmuo, kuris metė studijas negavęs mokslo baigimo pažymėjimo iš jokios mokyklos, užėmė daug svarbių pareigų, tokių kaip kolegijos dėstytojas, ligoninės prižiūrėtojas ir mokyklos mokytojas. Galiausiai, jis pavogė vieno gydytojo medicininį pažymėjimą ir naudojosi jo vardu bei pareigomis, kuomet tada, prisidengdamas tokia informacija, prisijungė prie Kanados karinio jūrų laivyno jau kaip chirurgas. Nepaisant oficialios medicinos praktikos nebuvimo, Korėjos konflikte jis atliko daug operacijų kariams. Galiausiai jį atrado asmens, kuriuo apsimitė, mama. Po to jis buvo paleistas iš karinio jūrų laivyno ir deportuotas iš šalies. Nors kaltininkas buvo daug kartų suimtas, jis ir toliau sėkmingai vykdė tapatybės vagystes (Hoffman, McGinley, 2010, p. 25).

Vienas iš svarbiausių įvykių tapatybės vagystės plėtroje įvyko tuomet, kai Jungtinėse Amerikos Valstijose socialinio draudimo numeris buvo priimtas ir naudojamas kaip priemonė atlikti asmenų sandorius. Šio numerio tikslas buvo padėti susigrąžinti ekonominę saugumą, kuri tuo metu palietė krizė, ir užtikrinti jo stabilumą ateityje. Todėl 1935 m. Jungtinių Amerikos Valstijų prezidentas priėmė įstatymą, reglamentuojantį socialinio draudimo numerio naudojimą. Pirmoji socialinio draudimo kortelė buvo išduota 1936 m., o jų naudojimas buvo sukurtas bėgant laikui. Tačiau, kaip minėta pirmiau, nusikaltėliai patobulino savo technologijas, kad galėtų išnaudoti pažeidžiamumą, susijusį su socialinio draudimo numeriu. Todėl bėgant metams itin išaugo piktnaudžiavimo socialinio draudimo numeriu rizika. Socialinio draudimo numeris ir išduota kredito kortelė suteikė dar vieną

galimybę nusikaltėliams įvykdyti tapatybės vagystę. Po kelerių metų kreditinė kortelė tapo pagrindine priemone, kuri gali būti naudojama atliekant asmenų pinigines operacijas. 1966 m. ir prieš šventinį apsipirkimo sezoną pirmosios tapatybės vagystės įvyko, kai daugybė laiškų, imituojančių kelių bankų laiškų, buvo išsiųsti įvairiausiais adresais Čikagoje. Daugelis asmenų, gavusių šiuos laiškus, neturėjo kredito kortelių. Be to, daugelis iš jų buvo vaikai ir (ar) jų augintiniai (ibid, p. 27).

Taigi, apibendrinant galima būtų teigti, jog šiais laikais tapatybės vagystės tapo epidemija ir nekontroliuojamu nusikaltimu, nes informacija apie asmenis yra prieinama visur. Be to, internetas palengvina tapatybės vagystės vykdymą. Dauguma asmenų turi informacijos internete ir naudojami internetu kaip įrankiu daugumai savo operacijų atlikti. Internetas tapo nepakeičiamu įrankiu žmogaus gyvenime. Be to, naudojant šią technologinę plėtrą, nusikaltėliai gali sukurti ir naudoti sudėtingus tapatybės vagystės metodus. Jie gali išsiugdyti gebėjimą itin gerai nuslėpti savo nusikaltimą. Kaip ir bet kuri nauja technologija, internetas turi stipriųjų ir silpnųjų vietų, todėl nusikaltėliai gali pasinaudoti šiomis silpnybėmis, kad pasisavintų žmonių tapatybes. Pirmoji oficiali tapatybės vagystė internete įvyko 1971 m., kai rusų tautybės pilietis internete įvykdė internetinę ataką prieš „Citibank“ ir pervedė pinigus iš jo klientų sąskaitų į savo asmeninę sąskaitą Suomijoje. Skelbiama, kad šiai operacijai atlikti jis buvo įdarbinęs itin daug asmenų. Kiek vėliau – 1994 m. tuomet veikusio nusikalstamo susivienijimo nariai naudojo pavogtus vartotojo vardus ir slaptažodžius, kad prisijungtų prie to paties „Citibank“ kompiuterių tinklo ir greitai pervedavo milijonus dolerių finansų įstaigoms, esančioms visame pasaulyje. Jų nusikaltimas buvo išaiškintas, kai banko pareigūnai pastebėjo du abejotinus pavedimus ir pranešė apie incidentą Federaliniam tyrimų biurui (ibid, p. 27). Taigi, taip nusikaltėliai galėjo ir vis dar gali panaudoti žmonių tapatybes darydami kitus nusikaltimus arba siekdami neteisėtų tikslų sau ar kitam asmeniui, o dažnu atveju, yra itin sunku tokius nusikaltimus išsiaiškinti ir už juos pritaikyti reikalingą atsakomybę, taip stabdant šio reiškinio plėtrą.

2. TAPATYBĖS VAGYSTĖS ELEKTRONINĖJE ERDVĖJE FORMOS IR BŪDAI

Šiame magistro darbo skyriuje bus įvardijamos ir apibrėžiamos pagrindinės tapatybės vagystės formos, kadangi būtent šių veikų gilesnė analizė atspindi tokių veikų mastą ir padaromą žalą. Atsižvelgiant į šiuolaikinių technologijų svarbą bei sparčią plėtrą šiomis dienomis, plačiau bus analizuojama asmens tapatybės vagystė, atliekama elektroninėje erdvėje. Plačiau apibūdinami skirtingi tokių veiksmų padarymo būdai, įrankiai, disponavimo būdai bei galima žala.

2.1. Tapatybės vagystės formos

Tapatybės vagystė yra didelė problema ir kylanti grėsmė. Ji gali pasireikšti įvairiomis formomis – nuo paprasto neteisėto kredito kortelės naudojimo iki visiško asmens tapatybės perėmimo. Dažnai pasirenkamas tapatybės vagystės traktavimas plačiąja prasme, kai sąvoka „tapatybės vagystė“ apima abi šio reiškinio rūšis, išskiriamas pagal įvykdymo vietą ir atlikimo būdą – tapatybės vagystę fizinėje erdvėje ir tapatybės vagystę elektroninėje erdvėje (Štitilis, et al., 2011, p. 76).

Nors yra daugybė šio nusikaltimo variantų, bei nusikaltėliai naudoja aukos asmeninę informaciją įvairiais būdais, tarp dažniausiai pasitaikančių naudojimo pavyzdžių (United States Secret Service, 2011):

- Jie gali paskambinti kredito kortelės išdavėjui, kad pakeistų atsiskaitymo adresą aukos kredito kortelės sąskaitoje;
- Jie gali atidaryti naujas kredito kortelių sąskaitas aukos vardu. Kai jie naudojami kreditinėmis kortelėmis ir neapmoka sąskaitų, aukų kredito ataskaitoje pranešama apie nesumokėtas sąskaitas;
- Jie gali informaciją naudoti neteisėtai prekybai narkotikais ar žmonėmis;
- Jie gali naudoti informaciją skambindami telefonu;
- Jie gali padirbti čekius arba kredito ar debeto korteles arba leisti atlikti elektroninius pervedimus kitu vardu ir išsekvoti banko sąskaitą;
- Jie gali pateikti bankroto bylą kitu vardu, kad išvengtų susidariusių skolų arba išvengtų iškeldinimo;
- Jie gali nusipirkti automobilį imdami paskolą kito asmens vardu;
- Jie gali gauti asmens tapatybę patvirtinantį dokumentą, pvz., vairuotojo pažymėjimą, išduotą su jų nuotrauka, aukos vardu;
- Jie gali nurodyti aukos vardą policijai.

Atsižvelgiant į visus šiuos atvejus, fizinėje erdvėje mes galime išskirti tokius dažniausiai pasitaikančius atvejus. Visų pirma, tai būtų veiksmai, atliekami su asmens

kreditine kortele. Tai gali būti tiek tokios kreditinės kortelės pasisavinimas, tiek veiksmų atlikimai su ja (atsiskaitymai, pervedimai). Taip pat galima turint pavyzdį tiesiog padirbti tokią asmens mokėjimo kortelę ir toliau ja naudotis. Antra, veiksmai gali būti atliekami turint informacijos, kurią asmuo gali tiesiog pamatyti ar nusifotografuoti, pavyzdžiui, parduotuvėje atsiskaitinėjant banko kortele, kitam asmeniui nusifotografavus jūsų kortelės numerį, vardą ir pavardę, kortelės galiojimo datą bei CV kodą, jis gali atlikti mokėjimus internetiniu būdu. Trečia kategorija būtų susijusi su asmens duomenimis. Tai reiškia, jog asmuo gali pasisavinti jūsų asmens tapatybę identifikuojantį dokumentą ir su juo atlikti pačius įvairiausias veiksmus – nuo paskolos paėmimo, buto nuomos sutarties iki įsidarbinimo sutarties sudarymo ar tokio dokumento palikimo kaip užstato, nuomojantis transporto priemonę. Galiausiai, asmuo taip pat gali suklastoti jūsų asmens dokumentus ir jais naudotis pačiais įvairiausiais būdais (May, 2004, p. 2). Vienas iš įdomiausių atvejų, paplitusių Jungtinėse Amerikos Valstijose ir šiuo metu, yra dokumentų pasisavinimas ir (ar) veikimas kito asmens vardu, siekiant gauti medicininę pagalbą ar medicininės paslaugas (Biegelman, 2009, p. 1).

Kalbant apie konkrečius realiai įvykusius atvejus, viena iš paskutiniųjų didelio masto duomenų vagysčių yra susijusi su „Facebook“ bei „LinkedIn“ socialiniais tinklais, kuomet 2021 metų pradžioje buvo pranešta apie pirmąjį incidentą – internete paviešinti 533 milijonų vartotojų asmens duomenys. Tuo metu įsilaužėlių forume gana nesunkiai ir net nemokamai buvo prieinami tokie „Facebook“ vartotojų duomenys kaip profilių adresai, telefonų numeriai, vardai ir pavardės, gimimo data, dalies elektroninio pašto adresai. Netrukus po šio atvejo buvo pranešta apie tokio pat pobūdžio incidentą su 500 milijonų „LinkedIn“ vartotojų asmens duomenimis (Teise.Pro, 2021).

Pažymint Lietuvoje įvykusius incidentus, vienas iš svarbiausių – 2017 metais įvykdytas įsilaužimas į „Grožio chirurgijos“ klinikos duomenų bazę. Tuo metu pasisavinti ne tik asmeniniai klientų duomenys, tačiau ir asmenų nuotraukos prieš ir po plastinių operacijų. Nukentėję klinikos pacientai buvo šantažuojami sumokėti nuo 50 iki 800 eurų, kitaip jų informacija būtų paviešinta. Tuo tarpu iš klinikos savininkų buvo reikalaujama 500 tūkstančių eurų bitcoin kriptovaliuta. Teigiama, kad buvo pavogti duomenys, priklausantys daugiau nei 22 tūkstančiams klinikos klientų; dalis nukentėjusiųjų – užsienio piliečiai. Nustatyta, kad į „Grožio chirurgijos“ klientų duomenų bazę įsilaužta panaudojus buvusio klinikos darbuotojo prisijungimo duomenis (BNS, 2019).

Vienas iš naujausių ir didžiausio masto įvykių – 2021 metų vasario mėnesį žiniasklaidą apskriejo žinia, kad daugiau nei 110 tūkstančių Lietuvoje registruotų automobilių dalijimosi paslaugos „CityBee“ vartotojų duomenys viešai paskelbti viename

internetiniame forume. Kibernetinių įsilaužėlių pamėgtoje erdvėje buvo skelbiami trejų metų senumo „CityBee“ klientų duomenys, tarp kurių vardai ir pavardės, asmens kodai, telefonų numeriai, elektroninio pašto adresai, gyvenamosios vietos adresai, mokėjimo kortelės detalės, vairuotojų pažymėjimo numeriai bei užšifruoti slaptažodžiai. Teigiama, jog incidentas įvyko nusikaltėliams neteisėtai pasisavinus dokumentą, kuris 2018 m. buvo laikinai naudotas techniniais tikslais, o už tokią veiką Valstybinė duomenų apsaugos inspekcija skyrė 110 tūkstančių eurų administracinę baudą (VDAI, 2021).

Taigi, apibendrinant, galime teigti, jog tapatybės vagystė gali pasireikšti dviem formomis: tapatybės vagystė fizinėje erdvėje ir tapatybės vagystė elektroninėje erdvėje. Abejomis formomis atliekama tapatybės vagystė sukelia itin daug žalos, tačiau šiuo metu daugėjant tokių nusikaltimų, atliekamų elektroninėmis ir informacinėmis ryšių priemonėmis, platesnė analizė pateikiama toliau.

2.2. Tapatybės vagystės elektroninėje erdvėje įvykdymo būdai

Tapatybės vagystė elektroninėje aplinkoje – pavojinga, struktūriškai išplėtota neteisėta veika, kurią atlieka kibernetinis nusikaltėlis, turintis tikslą įgyti asmeninę elektroninę informaciją, kurią išduoda finansų įstaiga, administracinė institucija, socialinio tinklo puslapis ir pan. Papildoma paskata tokios informacijos rinkimui dažniausiai būna panaudoti gautą informaciją kitiems nusikaltimams daryti ir (ar) platinti pavogtą informaciją. Dėl sparčiai augančio interneto naudojimo ir sparčiai besivystančios programinės įrangos, kuri dar labiau palengvina nelegalaus asmeninės informacijos rinkimą, sustabdyti elektroninės tapatybės vagystės procesą darosi nepaprastai sunku. Norint sukurti reikšmingas technologines ir teises priemones, skirtas kovoti su tokio pobūdžio elektroniniais nusikaltimais, būtina nurodyti, kokie yra populiariausi privačios elektroninės informacijos rinkimo būdai. Taip pat svarbu pažymėti, kad dažnai žmonės parduoda pasisavintą informaciją internetu, įsigyja ją iš kitų nusikaltėlių arba tiesiog išplatina ją neatlygintinai. (Bryan et al., 2009, p. 27).

Sukčių nuomone, pavogtos informacijos pirkimas iš kibernetinių nusikaltėlių yra saugesnis, taip pat nereikia pačiam daryti pirminių nusikalstamų veikų (informacijos surinkimo), o šie aspektai dažniausiai yra paskatinimas įsigyti tokią informaciją. Nurodoma, kad tapatybės vagystė dažniausiai atliekama vartotojui atliekant elektroninio autentifikavimo procesą, dėl to, kad vartotojai, norėdami gauti prieigą prie elektroninės informacinės sistemos, turi pateikti identifikuojančią informaciją (Štītīlis, et al., 2011, p. 120).

Kibernetinė erdvė suteikia galimybę kiekvienam rinkti asmeninę informaciją apie kitus bei didelę šios informacijos dalį – už tam tikrą kainą, galima rasti ir internete (Dodge, 2001, p. 1). Iš esmės beveik visuose apžvelgtuose moksliniuose šaltiniuose pateikiama ta pati elektroninės tapatybės vagystės atlikimo klasifikacija, pateikiami žinomiausi tapatybės vagystės įvykdymo būdai (Atefeh, 2013, p. 52-54):

- 1) Sukčiavimas (angl. *Phishing*). Ši gerai žinoma taktika paprastai apima apgaulingos svetainės sukūrimą, sukurtą taip, kad atrodytų kaip teisėta banko ar kitos finansų institucijos svetainė, o po to elektroninių laiškų, kurie, atrodo, buvo išsiųsti iš tos teisėtos institucijos, siuntimas elektroniniu paštu;
- 2) Įsilaužimas į tinklą (angl. *Network Intrusion*). Kitas paplitęs finansinės informacijos vagystės būdas yra tiesioginis įsilaužimas į mažmenininko ar kito tokios informacijos turėtojo tinklą;
- 3) Trojos arkliai (angl. *Trojan Horses*). Vienas iš sudėtingiausių kenkėjiškų kodų tipų yra „raktų registravimo Trojos arklys“, ši programa automatiškai įsidiegia aukos kompiuteryje ir neveikia tol, kol auka aplanko vieną iš anksto nustatytų interneto svetainių URL eilučių (pavyzdžiui, banko svetainėje), raktų registratorius „aktyvuoja“ ir išsaugo pirmąsias kelias dešimtis aukos įvestų klavišų paspaudimų (eilutė, kurioje bus jo prisijungimo vardas ir slaptažodis), o tada siunčia šiuos duomenis atgal užpuolikui;
- 4) „Tikro pasaulio“ vagystė (angl. *“Real-World” Theft*). Šis tapatybės vagystės tipas, susijęs su realiu pasauliu, išskirtinai pristatomas dėl viso apžvelgiamo konteksto ryšio. Tai vis dar populiariausia finansinės informacijos vagystės priemonė: apima tokias taktikas kaip „skimerių“ įrengimas bankomatuose, kurie įrašo informaciją iš į aparatą įdėtų kortelių, o restoranų padavėjai vagia informaciją iš kredito kortelių, kuriomis buvo apmokėta už maistą. Dažniausiai vagis tiesiogiai nesinaudoja tokia informacija, o parduoda ją internete dešimtimis, šimtais ar net tūkstančiais pažeistų paskyrų;
- 5) Biometrinių sensorių klastojimas (angl. *Spoofing of biometric sensors*). Atpažinimo procesas atliekamas be asmens, turinčio teisėtą teisę tai veikti pagal tokias biometrines priemones. Pirmiausia iš asmens surenkama informacija, pavyzdžiui, nuotrauka, o vėliau ji neteisėtai panaudojama;
- 6) *Pharmingas* (angl. *Pharming*). Tokios atakos yra panašios į sukčiavimo atakas, nes jos skirtos išgauti konfidencialius duomenis iš aukų, apsimitant patikimu šaltiniu ir prašant informacijos. *Pharmingo* ir sukčiavimo skirtumai yra tie, kad per apsimitimo atakas aukos DNS pašalinamas į kenkėjišką serverį, jam lankantis

teisėtoje svetainėje, o sukčiavimo atakoje, reikalaujama, kad aukos būtų apgaulinėjamos socialine inžinerija, kad apsilankytų apgaulingoje svetainėje;

- 7) Šnipinėjimo programos (angl. *Spyware*). Šnipinėjimo programos yra kompiuterių programinė įranga, kurią naudojant galima rinkti ir pašalinti konfidencialią informaciją iš bet kurio kompiuterio be savininko žinios. Viskas, ką naršytojas daro internete, įskaitant jo slaptažodžius, gali būti pažeidžiama šnipinėjimo programų. Šnipinėjimo programos gali sukelti didelį pavojų tapti tapatybės vagystės auka;
- 8) Elektroninės skelbimų lentos (angl. *Electronic Bulletin Boards*). Pokalbių kambariai ir elektroninės skelbimų lentos tapo vietomis tapatybės vagystėms. Kai nusikaltėliai gauna asmens tapatybę identifikuojančią informaciją, pvz., kredito kortelių numerius ar socialinio draudimo numerius, jie lankosi įsilaužėlių pokalbių kambariuose ir skelbia pranešimus, kad turi perduoti asmeninės informacijos.

Fizinių ir teritorinių kliūčių pasaulyje visuomenės skirsto grėsmes į išorines ir vidines, o atsakomybę už kiekvienos iš jų pašalinimą paskiria atitinkamoms socialinėms institucijoms. Nors mums visada reikės institucijų, kurios kovotų su tradicinėmis realaus pasaulio grėsmių formomis, vis dėlto mums tikrai reikia ir strategijos, kaip kovoti su grėsmėmis, kylančiomis iš kibernetinės erdvės ar virtualaus pasaulio. Kurdami šią strategiją, turėtume peržiūrėti ir apsvarstyti klasikinės ir tradicinės vidinių ir išorinių grėsmių nomenklatūros tinkamumą ir įgyvendinamumą.

Atitinkamai, nustatyti elektroninio nusikaltimo vietą gali būti nelengva užduotis, kai nusikaltėlis galėjo nukreipti savo ryšį su auka per kompiuterius iš trijų ar keturių šalių su neaiškiais tinklais, kurie tyrėjams nepasiekiami. Be to, nusikaltėliai gali daug apsunkinti šifravimo būdus, užtikrinančius aukštą anonimiškumo lygį arba prisiimdami nekaltą asmens tapatybę. Be to, tapatybės vagystės internete mastas gali viršyti realaus pasaulio nusikalstamumo mastą pagal žalą, kurią padaro vienas nusikaltimas, laipsni.

Skirtingai nuo realaus pasaulio nusikaltimų, kai atskiroms aukoms padaroma įvairių rūšių žala, tapatybės vagystės internetu gali padaryti tiek individualios, tiek sisteminės žalos. Kibernetinė erdvė tapo svarbia nacionalinės ypatingos svarbos infrastruktūros dalimi (Brenner, 2004, p. 19). Nors tapatybės vagystė kenkia atskiroms aukoms, tuo neapsiriboja, tapatybės vagystės internete gali pakenkti ar net sunaikinti svarbiausią tautos infrastruktūrą. Dėl to tai yra daug didesnė grėsmė nei tradicinis, realus nusikalstamumas – tam tikra prasme tapatybės vagystės internete panaikina skirtumą tarp vidinių ir išorinių grėsmių.

3. ASMENS DUOMENŲ VAGYSTĖS ELEKTRONINĖJE ERDVĖJE KRIMINALIZAVIMAS

Šiame skyriuje bus aptariamas užsienio valstybių požiūris į asmens tapatybės vagystę – apibūdinama, kaip tokia veika vertinama skirtingose šalyse, nurodoma, kuriose šalyse ji laikoma kaip nusikalstama veika, o kuriose ji laikoma tik sudėtine kitų nusikalstamų veikų dalimi. Skyriuje teikiamos išvalgos ar tokia veika, kaip asmens tapatybės vagystė gali būti laikoma nusikaltimu asmens privataus gyvenimo pažeidžiamumui, kokias vertybes ir saugomus gėrius ji pažeidžia, bei kaip tai turėtų būti vertinama. Galiausiai, apibūdinama, kaip atskiri asmens duomenų vagystės elementai yra kriminalizuoti Lietuvos Respublikos Baudžiamajame kodekse.

3.1. Tapatybės vagystės kriminalizavimas užsienio valstybėse

Tapatybės vagystės nusikaltimai šiais laikais yra globali problema, kuri vystosi ir plėtojasi visame pasaulyje, su ja susiduria kone kiekviena valstybė. Pastaruoju metu yra matoma vis daugiau diskusijų, kuriose yra keliami klausimai – ar tokia veika kaip tapatybės vagystė turėtų būti kriminalizuota? Ar tokios veikos sudėties inkorporavimas į kiekvienos valstybės baudžiamuosius įstatymus padėtų kovoti su tokiu nusikaltimu?

Pabrėžtina tai, jog šis nusikaltimas dažnu atveju yra daromas vienoje valstybėje, kuomet konkreči žala atsiranda kitos valstybės jurisdikcijoje. Tuomet susiduriame su problema, jog daugelyje valstybių tapatybės vagystė nėra kriminalizuota veika, tai nėra laikoma teisės pažeidimu, o dažnu atveju yra kaip kitų nusikalstamų veikų sudedamoji dalis, susijusi su duomenų slaptumo pažeidimais, plėšimu, sukčiavimu ar kitomis nusikalstamomis veikomis. Tuo tarpu kitos valstybės laikosi nuomonės, jog tokios veikos yra specifinės, todėl tapatybės vagystės kriminalizavimas yra naudinga priemonė siekiant užkirsti kelią tapatybės vagystės sukeliams grėsmėms (Štītīlis, et al., 2011, p. 216). Atsižvelgiant į tai, žemiau aptariamas Jungtinių Amerikos Valstijų, Prancūzijos, Vokietijos, Latvijos ir Estijos teisinis reguliavimas tapatybės vagystės srityje. Šios šalys pasirinktos dėl to, jog JAV yra viena iš pirmųjų šalių iniciavusi elektroninių nusikaltimų kriminalizavimą bei turinti sukaupusi didelę patirtį šioje srityje, yra vienas iš sektinų pavyzdžių. Prancūzija ir Vokietija paimtos dėl to, jog yra vienos iš kontinentinės teisės atstovių, Latvija ir Estija pasirinktos dėl Baltijos šalių regiono analizės.

Jungtinės Amerikos Valstijos turi sukaupusios didžiulę patirtį kovojant su elektroniniais nusikaltimais, yra viena iš Konvencijos dėl elektroninių nusikaltimų (2001) iniciatorių¹ ir ėmėsi daugybės priemonių, siekiant užkirsti kelią tapatybės nusikaltimams.

2021 m. asmenys Jungtinėse Amerikos Valstijose pateikė daugiau pranešimų apie tapatybės vagystę (25 % visų gautų pranešimų) visomis formomis nei bet kokio kito tipo skundų. Tokių pranešimų buvo pateikta beveik pusantro milijono. Šis nusikaltimas, remiantis 2021 m. gautais pranešimais, labiausiai paplitęs Rod Ailando, Kanzaso, Ilinojaus, Luizianos ir Džordžijos valstijose (Federal Trade Commissio, 2021).

Pirmos užuomazgos kriminalizuoti tapatybės vagystę prasidėjo 1998 m., kuomet JAV Kongresas įtvirtino tokios veikos sudėtį Tapatybės vagystės ir apsimitinėjimo atgrasymo akte (angl. *The Identity Theft and Assumption Deterrence Act*). 2004 m. tapatybės vagystės sudėtis buvo įtvirtinta Jungtinių Amerikos Valstijų baudžiamojo įstatymo 18 skirsnio 1 dalies 47 skyriaus 1028 straipsnio a dalies 7 punkte (United States Code, 1926). Remiantis šia įtvirtinta nuostata, veika laikoma nusikaltimu, kuris yra atliekamas tada, kai kas nors tyčia perduoda, laiko, naudoja, neturėdamas tam teisės, kito asmens identifikavimo priemonės, turėdamas tikslą įvykdyti arba tam kad padarytų, bet kokią neteisėtą veiką, kuri būtų Federacijos teisės pažeidimas arba kuri būtų sunkus nusikaltimas pagal galiojančius Valstijos ar vietinius teisės aktus (ibid).

Tais pačiais 2004 m. Kongresas paskelbė Tapatybės vagystės bausmės stiprinimo aktą (angl. *The Identity Theft Penalty Enhancement Act*). Šiuo dokumentu buvo įvesta sąvoka „šiurkšti tapatybės vagystė“ ir taip nurodomos sunkinamos nusikalstamos veikos aplinkybės. Tokia tapatybės vagystės forma buvo įtvirtinta Jungtinių Amerikos Valstijų baudžiamojo įstatymo 18 skirsnio 1 dalies 47 skyriaus 1028A straipsnyje (United States Code, 1926). Joje nurodoma, jog toks nusikaltimas gresia tuomet, kai asmens tapatybė naudojama nusikaltimams, susijusiems su imigracijos taisyklių pažeidimu, socialinio draudimo išmokomų vagystėmis bei vidaus terorizmu.

Atsižvelgiant į tai, galima pabrėžti, jog Jungtinės Amerikos Valstijos jau nuo 2004 m. yra įsitvirtinusios tokios nusikalstamos veikos, kaip asmens tapatybės vagystė, sudėtį, turi apsibrėžusi sunkinančias aplinkybes bei turi priemones kovai su tokios nusikalstamos veikos plitimu šalyje.

Tapatybės vagystės, kaip atskiros veikos, **Vokietijos** baudžiamuosiuose įstatymuose įtvirtinta nėra. Atsižvelgiant į tai, jog tapatybės vagystė gali būti kitų nusikalstamų veikų

¹ Konvenciją dėl elektroninių nusikaltimų JAV ratifikavo 2006 m. rugsėjo 29 d., šalyje ji įsigaliojo nuo 2007 m. sausio 1 d.

sudėtyje, Vokietijoje veika ir yra vertinama priklausomai nuo to, kaip nusikaltėlis gauna prieigą prie tapatybės duomenų.

Tai gali būti daroma naudojant vieną iš labiausiai paplitusių būdų asmens duomenis gauti – „Phishing“, o tai būtų laikoma baudžiamuoju nusikaltimu pagal 2000 m. Vokietijos baudžiamojo kodekso 202b straipsnį. Remiantis 202a straipsniu yra galimybė baudžiamajai atsakomybei kilti už „Duomenų šnipinėjimą“. Šiame straipsnyje kalbama apie tai, jog „Tas, kas, neturėdamas tam leidimo, apeidamas prieigos apsaugą gauna sau ar kitam prieigą prie duomenų, kurie nebuvo jam skirti ir buvo specialiai apsaugoti nuo neteisėtos prieigos, baudžiamas laisvės atėmimu ne ilgesniam kaip trejų metų laikotarpiui arba bauda“ (German Criminal Code, 1998). Taip pat naudojant tokius tapatybės duomenis nesąžiningais tikslais, tai gali būti laikoma nusikalstama veikla pagal Vokietijos baudžiamojo kodekso 263 straipsnį (sukčiavimas) arba Vokietijos baudžiamojo kodekso 263a (kompiuterinis sukčiavimas). Už abu nusikaltimus gresia laisvės atėmimas iki penkerių metų, o ypač sunkiais atvejais – iki 10 metų. Atsižvelgiant į konkrečius bylos faktus, kito asmens tapatybės naudojimas gali būti laikomas baudžiamuoju nusikaltimu, numatytu šio kodekso 267 straipsnyje (dokumentų klastojimas) arba 269 straipsnyje (įrodomosios reikšmės duomenų klastojimas) Vokietijos baudžiamojo kodekso. Už abu nusikaltimus gresia laisvės atėmimas iki penkerių metų, o ypač sunkiais atvejais – iki 10 metų.

Atsižvelgiant į tai, galime teigti, kad Vokietijoje taip pat nėra įtvirtintos atskiros tapatybės vagystės nusikalstamos veikos sudėties, o ji yra viena iš kitų nusikalstamų veikų sudedamoji dalis.

Prancūzijos baudžiamajame kodekse taip pat nėra įtvirtintos vienos nusikalstamos veikos, susijusios su asmens tapatybės vagyste.

Visų pirma, reikėtų pažymėti, jog veikos, susijusios su asmens tapatybe bei dokumentų klastojimu yra įtvirtintos Prancūzijos baudžiamojo kodekso skyriuje „Klastojimas“, tačiau šiuose straipsniuose mes randame nuostatas, susijusias su oficialių valstybės dokumentų klastojimu, pirkimu, įgijimu. Labiausiai su tapatybės vagyste susijusi nusikalstama veika yra įtvirtinta Prancūzijos baudžiamojo kodekso IV skirsnio I dalies 434-23 straipsnyje, kuris teigia, jog: „Kito asmens vardo prisiėmimas aplinkybėmis, dėl kurių tam asmeniui buvo iškelta baudžiamoji byla arba dėl kurių jis galėjo būti patrauktas baudžiamojon atsakomybėn, baudžiamas penkerių metų laisvės atėmimu ir 75 000 eurų bauda“ (France Criminal Code, 1994, p. 104). Tačiau pabrėžtina, jog ši veika yra itin siaura ir kalbama tik apie pasinaudojimą kito asmens vardu (sukonkretinta pasisavinamų duomenų sąvoka).

Galime daryti išvadą, jog tapatybės vagystė, kaip tokia, Prancūzijoje nėra įtvirtinta kaip atskira nusikalstama veika, o taip pat laikoma tik kitų nusikalstamų veikų sudedamoji dalis.

Vienoje iš Baltijos šalių – **Latvijoje**, tapatybės vagystė, kaip atskira nusikalstama veika kriminalizuota nėra.

Latvijos baudžiamajame kodekse labiausiai atitinkanti norma yra susijusi su bendrais asmens duomenimis ir jų panaudojimu, kai yra sukeliama žala. Šio kodekso 145 straipsnio „Neteisėta veikla, susijusi su fizinių asmenų duomenimis“ 1 dalyje yra reglamentuojama, jog: „Už neteisėtą veiklą, susijusią su fizinio asmens duomenimis, jeigu ji padarė didelę žalą, taikoma baudžiamoji atsakomybė – laisvės atėmimas iki dvejų metų arba laikinas laisvės atėmimas, arba viešieji darbai, arba bauda“ (Latvia Criminal Code, 1998, p. 51). Taip pat antroje dalyje matome ir sunkinančias aplinkybes, jei duomenys pasisavinami keršto, turto įsigijimo ar šantažo tikslais: „Už neteisėtą veiklą, susijusią su fizinio asmens duomenimis, jeigu asmens duomenų tvarkymo administratorius ar operatorius juos vykdė keršto, turto įsigijimo ar šantažo tikslais, taikoma baudžiamoji atsakomybė – laisvės atėmimas iki ketverių metų arba laikinas laisvės atėmimas, viešieji darbai arba bauda“ (ibid).

Atsižvelgiant į tai, galime teigti, jog Latvijoje yra kriminalizuota neapibrėžta veika – neteisėta veikla, susijusi su fizinio asmens duomenimis, į kurią šiuo atveju gali patekti ir tapatybės vagystė. Tačiau pabrėžtina, jog sąvoka neteisėta veikla yra gana siaura.

Kitoje Baltijos šalyje – **Estijoje**, tapatybės vagystė nusikaltimu yra laikoma jau nuo 2009 metų, kuomet buvo įtvirtinta Estijos baudžiamojo kodekso 157² straipsnyje „Nelegalus kito asmens tapatybės naudojimas“. Jame nurodoma: „Asmens duomenų, kuriais remiantis nustatoma ar galima nustatyti kito asmens tapatybę, perdavimas, leidimas susipažinti su duomenimis ar jais naudotis be to asmens sutikimo, siekiant sąmoningai suklaidinti tą asmenį, darant prielaidą, kad tas asmuo yra tapatus, jeigu dėl to padaryta žala kito įstatymo saugomo asmens teisėms ar interesams arba nuslėpti nusikalstamą veiką, baudžiama pinigine bauda arba laisvės atėmimu iki trejų metų“ (Estonia Criminal Code, 2001). Taip pat galime pažymėti ir kitas nusikalstamas veikas, kurios būna sietinos su tapatybės vagyste – Estijos baudžiamojo kodekso 209 straipsnis (sukčiavimas) bei 344-349 straipsniai, susiję su asmens dokumentų klastojimu, jų gaminimu, naudojimu.

Taigi, galime teigti, jog viena iš Baltijos regiono valstybių jau nuo 2009 metų tikslingai kovoja su tapatybės vagystės nusikaltimu bei už tokią veiką skiria atitinkamas sankcijas. Atsižvelgiant į tai, toks valstybės teisinis reguliavimas kaimynėje šalyje gali būti laikomas itin tinkamu pavyzdžiu.

Galiausiai, reikėtų pabrėžti, jog išnagrinėjus šių penkių valstybių jurisdikcijas galime matyti, jog tapatybės vagystė yra vertinama skirtingai – tik dvejose iš aukščiau nagrinėtų valstybių mes matome, jog tokia veika yra laikoma atskiru nusikaltimu ir yra įtvirtinta atskirame baudžiamojo įstatymo straipsnyje. Tuo tarpu kitos valstybės tokią veiką traktuoja kaip kitų nusikalstamų veikų sudedamąją dalį. Tačiau būtent dėl tokių skirtumų, nesutapimų traktuojant padarytas nusikalstamas veikas, yra sunkinamas tokių veikų susekimas ir ištyrimas, apsunkinamas baudžiamojo persekiojimo ne tik nacionaliniu, bet ir tarptautiniu lygmeniu procesas. Tuo tarpu neišaiškinus ar išaiškinus tokią veiką per vėlai yra sudaroma galimybė atsirasti dar sunkesniems ir sunkiau išaiškinamiems nusikaltimams, kuriems tapatybės vagystė gali būti tik viena iš sudedamųjų dalių. Blogiausiu atveju, tokios veikos, daromos skirtingose šalyse, pasekmėms atsirandant kitose šalyse ir nesutampant reguliavimui, gali likti ir visai neištirtos.

3.2. Asmens duomenų vagystė kaip nusikaltimas asmens privataus gyvenimo pažeidžiamumui

Visų pirma išgirdus sąvoką „asmens duomenys“ ar „tapatybės vagystė“ kyla klausimas, su kuo šie žodžiai yra susiję, kokias vertybes jie saugo? Tam, kad pasisavinti kito asmens tapatybę reikia kito asmens duomenų. Atsižvelgiant į tai, asmens duomenys yra ne kas kita, kaip asmens privatus gyvenimas, kuriuo jis nesidalina viešai. Remiantis Lietuvos Aukščiausiojo Teismo praktika – neteisėtas informacijos apie privatų asmens gyvenimą rinkimas visų pirma sietinas su informacijos gavimo būdo bei pažeisto asmens privatumo įvertinimu (Lietuvos Aukščiausiojo Teismo 2018 m. gegužės 31 d. nutartis baudžiamojoje byloje; Lietuvos Aukščiausiojo Teismo 2020 m. sausio 7 d. nutartis baudžiamojoje byloje). Čia matome išskirtą asmens privatumą bei jo pažeidimą.

Teisė į privatų gyvenimą yra fundamentali tiek Lietuvos Respublikos Konstitucijoje (1992), tiek Žmogaus teisių ir pagrindinių laisvių apsaugos konvencijoje (1950) (toliau – **Konvencija**) (8 straipsnis), tiek Europos Sąjungos pagrindinių teisių chartijoje (2012) (7, 8 straipsniai) ir tokia teisė gali būti ribojama tik išimtiniais atvejais. Konstitucijos 22 straipsnio 1 dalyje nustatyta, kad žmogaus privatus gyvenimas neliečiamas; informacija apie privatų asmens gyvenimą gali būti renkama tik motyvuotu teismo sprendimu ir tik pagal įstatymą (3 dalis). Konstitucijos 22 straipsnio 4 dalyje suformuluotas bendrasis privataus gyvenimo gynimo principas, pagal kurį įstatymas ir teismas saugo, kad niekas nepatirtų savavališko ar neteisėto kišimosi į jo asmeninį ir šeiminių gyvenimą, kėsینimosi į jo garbę ir orumą. Lietuvos Respublikos Konstitucinis Teismas savo nutarimuose ne kartą yra konstatavęs, kad pagal Konstituciją riboti asmens teisės ir laisvės galima, jeigu yra

laikomasi šių sąlygų: tai daroma įstatymu; apribojimai yra būtini demokratinėje visuomenėje siekiant apsaugoti kitų asmenų teises bei laisves ir Konstitucijoje įtvirtintas vertybes, taip pat konstituciškai svarbius tikslus; apribojimais nėra paneigiama teisių ir laisvių prigimtis bei esmė; yra laikomasi konstitucinio proporcingumo principo (Lietuvos Respublikos Konstitucinio Teismo 2005 m. gegužės 13 d., 2010 m. vasario 26 d., 2011 m. birželio 21 d., 2014 m. gegužės 9 d. nutarimai). Privataus gyvenimo neliečiamumas suponuoja asmens teisę į privatumą, kuri apima asmeninio, šeimos ir namų gyvenimo, garbės ir reputacijos neliečiamumą, asmens fizinę ir psichinę neliečiamybę, asmeninių faktų slaptumą, draudimą skelbti gautą ar surinktą konfidencialią informaciją ir kt. (Lietuvos Respublikos Konstitucinio Teismo 1999 m. spalio 21 d., 2000 m. gegužės 8 d., 2002 m. rugsėjo 19 d., 2002 m. spalio 23 d., 2003 m. kovo 24 d. nutarimai).

Europos Žmogaus Teisių Teismas (toliau – EŽTT) savo sprendimuose ne kartą yra pasisakęs dėl privataus gyvenimo sąvokos aiškinimo, dėl to, kokia informacija ir kokiais būdais renkama, net ir viešame kontekste, gali patekti į asmens privataus gyvenimo sferą. Pavyzdžiui, EŽTT 1992 m. gruodžio 16 d. sprendime, priimtame byloje N. prieš Vokietiją, nurodė, kad nėra nei galimybės, nei būtinybės pateikti išsamią (baigtinę) „privataus gyvenimo“ sąvokos apibrėžtį; kad būtų per daug siaura šią sąvoką apiboti „artimiausia asmens aplinka“, kurioje asmuo gali savo nuožiūra gyventi savo asmeninį gyvenimą, visiškai pašalinant iš šios sąvokos išorinį pasaulį, kurio ši aplinka neapima. Šis teismas 2004 m. birželio 24 d. sprendime, priimtame byloje V. H. prieš Vokietiją, dar kartą pabrėžęs esminę privataus gyvenimo apsaugos svarbą kiekvieno žmogaus asmenybės raidos požiūriu, pažymėjo, kad ši apsauga apima ne tik privačią šeimos, bet ir socialinę erdvę, kad kiekvienas asmuo (net jei jis ir yra žinomas plačiajai visuomenei) turi turėti galimybę naudotis teise į teisėtą lūkestį dėl savo privataus gyvenimo apsaugos ir gerbimo.

Atsižvelgiant į tai, mes matome, jog asmens duomenys gali būti prilyginami privačiai asmens informacijai. Vienas iš garsiausių tapatybės vagystės ekspertų Jungtinėse Amerikos Valstijose John D. Sileo (2005, p. 32) pateikia duomenis, pagal kuriuos, jo manymu, galima nustatyti žmogaus tapatybę: pilnas vardas, socialinio draudimo numeris, bankų sąskaitų numeriai, gimimo data, adresas, motinos mergautinė pavardė, kompiuterio slaptažodžiai, bankomatų PIN kodai, kreditinių kortelių numeriai, vairuotojo pažymėjimo numeris, telefono numeris, mobiliojo telefono numeris, elektroninio pašto adresas, kompiuterio IP adresas, garažo durų kodai, transporto priemonės numeris, šeimos narių vardai ir informacija apie juos, nuotrauka, nykščio antspaudas, akies tinklainės raštas, balso tembras, DNR, ūgis, svoris, plaukų ir akių spalva, etninė priklausomybė, pilietybė, lytis, profesija,

pajamos, religija. Tačiau net ir matant sąrašą reikia paminėti, jog tai yra tik keletas dalykų, pagal kuriuos galima nustatyti asmens tapatybę – jų gali būti daug daugiau.

Pagal Lietuvos Respublikos baudžiamojo kodekso (2000) (toliau – **BK**) 167 straipsnio 1 dalį atsako tas, kas neteisėtai rinko informaciją apie privatą asmens gyvenimą. Šios nusikalstamos veikos objektas yra asmens privataus gyvenimo neliečiamumas, dalykas – informacija, kurios turinį sudaro žinios apie privatą žmogaus gyvenimą. Nusikaltimas objektyviai pasireiškia neteisėtu informacijos apie privatą asmens gyvenimą rinkimu, neteisėtais veiksmais kėsiniama į asmens privataus gyvenimo neliečiamumą. Šiame baudžiamajame įstatyme nurodytos nusikalstamos veikos sudėtis yra formalioji, nusikaltimas laikomas baigtu atlikus veiksmus, kuriais neteisėtai buvo renkama informacija apie privatą žmogaus gyvenimą. Nusikaltimas padaromas tiesiogine tyčia – asmuo, darydamas pavojingą veiką, suvokia pavojingą daromos veikos pobūdį ir nori taip veikti (Lietuvos Respublikos baudžiamojo kodekso komentaras..., 2009, p. 236-237).

BK 167 straipsnio 1 dalyje nusikalstamos veikos aprašymas formalia sudėtimi nereiškia, kad, sprendžiant dėl konkrečios veikos kvalifikavimo pagal šį straipsnį, nereikalaujama įvertinti panaudotų konkrečių neteisėto informacijos rinkimo priemonių, nustatyti, kaip ir į kokią privataus asmens gyvenimo sritį jomis buvo įsiterpta. Pažymėta, kad privataus gyvenimo sąvoka yra gana plati, BK 167 straipsnyje nedetalizuojama, todėl apie tai, kas yra konkretaus asmens privataus gyvenimo dalis, kokia informacija patenka į konkretaus asmens privataus gyvenimo sferą, teismas sprendžia įvertinęs byloje nustatytą aplinkybių ir faktų visumą. Informacijos rinkimo samprata apima visus įmanomus tam skirtu neteisėto veikimo būdus – asmens sekimą, jo paties ar jo būsto stebėjimą, pokalbių klausymąsi ir kitus (Lietuvos Aukščiausiojo Teismo 2014 m. gegužės 6 d. nutartis baudžiamojoje byloje; Lietuvos Aukščiausiojo Teismo 2021 m. lapkričio 10 d. nutartis baudžiamojoje byloje).

Remiantis BK 168 straipsnio 1 dalimi, atsako tas, kas be asmens sutikimo viešai paskelbė, pasinaudojo ar kitų asmenų labai panaudojo informaciją apie kito žmogaus privatą gyvenimą, jeigu tą informaciją jis sužinojo dėl savo tarnybos ar profesijos arba atlikdamas laikiną užduotį, arba ją surinko darydamas BK 165–167 straipsniuose numatytą veiką. Objektyviai ši veika pasireiškia informacijos apie kito žmogaus privatą gyvenimą, sužinotos dėl tarnybos, profesijos arba laikinos užduoties atlikimo, arba surinktos aukščiau nurodytuose straipsniuose numatytomis veikomis, viešas paskelbimas, pasinaudojimas ja ar jos panaudojimas kitų asmenų labai neturint to žmogaus sutikimo. Pabrėžtina, kad šiuo atveju nusikalstama veika dviem būdais: 1) žinias apie kito asmens privatą gyvenimą kaltininkas gauna atlikdamas savo darbą, t. y. jis informaciją sužino; 2) aktyviai ir

nusikalstamai veikia su tikslu surinkti informaciją apie to asmens privatą gyvenimą, t. y. informaciją renka aktyviais veiksmais. Taip pat apibūdinant pasinaudojimo informacija sąvoką sutinkame tokį apibrėžimą – „tokios informacijos panaudojimas kaltininko savanaudiškais ar kitokiais interesais, siekiant paveikti tą žmogų kaip esamą ar būsimą klientą, daryti įtaką jo elgesiui, nugalėti jį konkurse <...> ir kt.“ (Lietuvos Respublikos baudžiamojo kodekso komentaras...2009, p. 241).

Taigi, atsižvelgus į atliktą analizę, galime daryti išvadą, jog taip, asmens duomenų vagystė, tiksliau, tapatybės vagystė elektroninėje erdvėje turėtų būti vertinama kaip asmens privataus gyvenimo pažeidimas. Tačiau BK XXIV skyriuje „Nusikaltimai privataus gyvenimo neliečiamumui“ mes turime įtvirtintas normas, kurios kalba apie neteisėtą informacijos apie privatą asmens gyvenimą rinkimą, panaudojimą, bet „panaudojimo“ sąvoka šiuo atveju yra apibrėžiama žymiai švelniau nei tikroje tapatybės vagystėje, neminint nei tikrųjų panaudojimo būdų, nei tokių veiksmy padarinių. Šiose normose mes nematome, jog asmuo duomenis rinktų su tikslu apsimesti kitu žmogumi, panaudoti duomenis, kad galėtų veikti kito asmens vardu ir tai darytų tyčia. Taip pat šiose normose mes nematome padarinių, užbaigtumo momento, o susiduriame labiau su informacijos apie asmenį rinkimu ir naudojimu, o ne informacijos, su tikslu būti tuo asmeniu rinkimu ir naudojimu.

Apibendrinant tai, kas išdėstyta anksčiau, šiuo metu turimi BK 167-168 straipsniai, kalbantys apie asmens privataus gyvenimo pažeidimus, gali būti siejami tik su pirmąja tapatybės vagystės stadija – neteisėtu duomenų apie privatą žmogaus gyvenimą rinkimu. Atsižvelgiant į tai, minėti straipsniai gali būti laikomi tik kaip sudėtinė tapatybės vagystės dalis.

3.3. Atskirų asmens duomenų vagystės elementų kriminalizavimas Lietuvoje

Lietuva 2004 m. kovo 18 d. ratifikavo Konvenciją dėl elektroninių nusikaltimų (2001) ir tapo jos nare (Konvencija įsigaliojo nuo 2004 m. liepos 1 d.). Nors elektroninių nusikaltimų, tokių kaip tapatybės vagystė elektroninėje erdvėje, daugėja, tačiau Lietuvoje mes vis dar neturime daug su tuo susijusios teismų praktikos, mokslinių tyrimų, atliktų elektroninių nusikaltimų srityje ir taip susiduriame su teikiamos informacijos trūkumu. Tuo labiau, tokia veika dažnu atveju net nėra suprantama pačių žmonių – dažniausiai tokios veikos kaip elektroniniai laiškai, telefoniniai skambučiai prisistatant asmens giminaičiais ar pareigūnais, yra vertinami ne kaip tapatybės vagystė, tačiau kaip sukčiavimas (Swedbank, 2021) ar tiesiog pačių asmenų neapdairumas (pasitaiko ir tokių atvejų, kad žmonės gali net ir nesužinoti, kad jų tapatybė buvo pavogta, kol nesusiduriama su realia žala).

Tačiau žiūrint ir iš formaliosios pusės, reikėtų pabrėžti tai, jog net ir norint inkriminuoti tokią veiką, Lietuvoje teisės aktai nenumato vieno konkretaus nusikaltimo, nusižengimo ar teisiškai apibrėžto veiksmo, kuris būtų įvardijamas kaip tapatybės vagystė (Visuotinė lietuvių enciklopedija).

Pirmiausia apžvelkime BK normas, kurios gali būti susijusios su tapatybės vagystės sudėtinėmis dalimis. Visų pirma, BK 182 straipsnyje yra įtvirtinta sukčiavimo, kaip nusikalstamos veikos, sudėtis: „tas, kas apgaule savo ar kitų naudai įgijo svetimą turtą ar turtinę teisę, išvengė turtinės prievolės arba ją panaikino <...>“; 2 dalyje turime kvalifikuotą nusikaltimo sudėtį – „tas, kas apgaule savo ar kitų naudai įgijo didelės vertės svetimą turtą ar turtinę teisę arba didelės mokslinės, istorinės ar kultūrinės reikšmės turinčias vertybes arba išvengė didelės vertės turtinės prievolės, arba ją panaikino, arba sukčiavo dalyvaudamas organizuotoje grupėje <...>“. Tuo tarpu BK 207 straipsnis nurodo specifiškesnę sukčiavimo nusikaltimo sudėtį – kreditinį sukčiavimą: „tas, kas apgaule gavo kreditą, paskolą, tikslinę paramą, subsidiją, dotaciją, laidavimo ar banko garantijos raštus arba kitus kreditinius įsipareigojimus <...>“. BK 198 straipsnyje kriminalizuotas neteisėtas elektroninių duomenų perėmimas ir panaudojimas: „tas, kas neteisėtai stebėjo, fiksavo, perėmė, įgijo, laikė, pasisavino, paskleidė ar kitaip panaudojo neviešus elektroninius duomenis <...>“; taip pat 2 dalyje nurodoma ir kvalifikuota nusikaltimo sudėtis – jei minėti veiksmai buvo atliekami su strateginę reikšmę nacionaliniam saugumui arba didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinčiais neviešais elektroniniais duomenimis. BK 198¹ straipsnyje numatyta baudžiamoji atsakomybė už neteisėtą prisijungimą prie informacinės sistemos: „tas, kas neteisėtai prisijungė prie informacinės sistemos pažeisdamas informacinės sistemos apsaugos priemones, baudžiamas viešaisiais darbais arba bauda, arba areštu, arba laisvės atėmimu iki dvejų“, o jei prisijungta buvo prie strateginę reikšmę nacionaliniam saugumui arba didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinčios informacinės sistemos, – bauda arba areštu, arba laisvės atėmimu iki trejų metų. BK XXX skyrius apibrėžia nusikaltimus elektroninių duomenų ir informacinių sistemų saugumui. Nuo 2004 m. BK yra įtvirtinta ir neteisėto disponavimo įrenginiais, programine įranga, slaptažodžiais, kodais ir kitokiais duomenimis nusikalstama veika (BK 198² straipsnis). Šiame straipsnyje nurodoma, jog: „tas, kas nusikalstamais tikslais ar kitaip neteisėtai gamino, gabeno, importavo, pardavė, suteikė prieigą ar kitaip platino, įgijo ar laikė įrenginius ar programinę įrangą, tiesiogiai skirtus ar pritaikytus daryti nusikalstamas veikas, taip pat slaptažodžius, kodus ar kitokius panašius duomenis, skirtus prisijungti prie informacinės sistemos ar jos dalies, baudžiamas viešaisiais darbais arba bauda, arba areštu, arba laisvės atėmimu iki ketverių metų“. Galiausiai, išskiriamos kelios

nusikalstamos veikos, kurios susijusios su elektroninėmis mokėjimo priemonėmis ir disponavimu jomis – BK 214 straipsnis įtvirtina baudžiamąją atsakomybę už netikros elektroninės mokėjimo priemonės gaminimą, tikros elektroninės mokėjimo priemonės klastojimą ar neteisėtą disponavimą elektronine mokėjimo priemone arba jos duomenimis; 215 straipsnyje kaip nusikalstama veika nurodomas neteisėtas elektroninės mokėjimo priemonės ar jos duomenų panaudojimas. Be to, tapatybės vagystės veiksmai gali atsispindėti ir BK 300 straipsnyje, kuris įtvirtina dokumento suklastojimo ar disponavimo suklastotu dokumentu sudėtį. Šiame straipsnyje išskiriamas tiek dokumentas, kaip toks, neišskiriant jokių konkrečių požymių, tiek valstybės išduoti asmens dokumentai ir disponavimas jais: asmens tapatybės kortele, pasu, vairuotojo pažymėjimu ar valstybinio socialinio draudimo pažymėjimu (veikos, atliktos su tokiais asmens dokumentais, remiantis BK 300 straipsnio 2 dalimi laikomos kvalifikuota tokios nusikalstamos veikos sudėtimi).

Išanalizavus BK esančias teises normas bei atlikus doktrininę analizę galime įžvelgti nebent tam tikrų tapatybės vagystės elektroninėje erdvėje elementų, kurie gali būti vertinami kaip pavojingos veikos. Tapatybės vagystės pirmoji stadija – su tapatybe susijusios informacijos gavimą – yra įtvirtinta BK 166, 167, 198, 198¹, 214 straipsniuose. Tuo tarpu antroji stadija (laikymas, perdavimas) – iš dalies patenka į 198 ir 214 straipsnių veikimo sritį, tačiau šioje stadijoje esantis pagrindinis elementas – su tapatybe susijusios informacijos turėjimas – BK nėra kriminalizuotas. Šiuo atveju baudžiamąją atsakomybę užtraukia tik neviešų elektroninių duomenų ir svetimų, netikrų ar suklastotų elektroninių mokėjimo priemonių laikymas (BK 198² straipsnis). Tapatybės vagystės trečioji stadija – su tapatybe susijusios informacijos panaudojimas siekiant įvykdyti nusikaltimą – patenka į BK 182, 207, 215, 300 straipsnių apimtį. Taigi, galima teigti, jog šiuo atveju reikėtų kalbėti apie nusikalstamų veikų daugetą (Štitalis, *et al.*, 2011, p. 242).

Atsižvelgiant į tai, kas išanalizuota aukščiau, kyla klausimas ar nebūtų reikalinga turėti tokį straipsnį, kuriame galėtume matyti vieną nusikalstamą veiką, už kurią būtų baudžiama? Matome, jog tokia nusikalstama veika, kaip tapatybės vagystė yra padaroma aiški ne tik moralinė, bet ir materialinė žala asmeniui, be to, tai yra aiškus vienos iš pamatinių žmogaus laisvių – teisės į privatų gyvenimą, įtvirtintos Lietuvos Respublikos Konstitucijos 22 straipsnyje – pažeidimas. Paminėtina, jog baudžiamasis įstatymas nustato konkrečius minėtos konstitucinės normos pažeidimų būdus ir sankcijas už jas (Vaišvila, 1998). Tačiau tiek BK skyriuje, kalbančiame apie nusikaltimus asmens gyvenimo neliečiamumui, tiek kituose aptartuose BK straipsniuose ar jų dalyse mes matome tik atskirus elementus, kuriuos „sujungti“ į vieną visumą ne retai gali būti tikras iššūkis – tačiau kitaip nėra ir negali būti atskleidžiama tikroji tapatybės vagystės sudėtis. Taigi, šiuo atveju

susiduriame su teisės taikymo spraga, kuomet turime akivaizdų teisės pažeidimą, tačiau neturime racionalios ir Lietuvos įstatymuose įtvirtintos bausmės už jo padarymą.

4. GALIMAS ASMENS TAPATYBĖS VAGYSTĖS, KAIP NUSIKALSTAMOS VEIKOS, SUDĖTIES MODELIS

Nusikalstamos veikos sudėties požymis turiniu ir forma iš esmės skiriasi nuo nusikalstamos veikos, baudžiamosios teisės normos ir baudžiamojo įstatymo straipsnio požymių. Reikia pažymėti, kad tik suvokus nusikalstamos veikos sudėties požymio esmę, galima tinkamai kvalifikuoti veiką kaip nusikalstamą (Veršekys, 2012, p. 203).

Atsižvelgiant į tai, jog nusikalstamos veikos sudėtį sudaro tam tikri požymiai, kurie skirstomi į objektyvius ir subjektyvius nusikalstamos veikos sudėties požymius, šio skyriaus tikslas – atlikti tapatybės vagystės elektroninėje erdvėje sudėties požymių analizę ir pateikti BK specialiosios dalies pakeitimo projektą, konstruojant tapatybės vagystės elektroninėje erdvėje sudėties modelį.

4.1. Tapatybės vagystės elektroninėje erdvėje sudėties objektyvieji požymiai

Visų pirma, reikėtų aptarti, kas yra laikoma objektyviaisiais požymiais. Prie objektyviųjų priskiriami šie fakultatyvieji nusikalstamos veikos sudėties požymiai: nusikalstamos veikos dalykas, objektas, padarymo būdas, laikas, vieta, priemonės, aplinkybės, specialaus subjekto požymis (Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2007 m. birželio 28 d. apžvalga Nr. 27).

Kalbant apie nusikalstamos veikos dalyką turėtume paminėti, jog **dalykas** yra pažeidžiamos baudžiamojo įstatymo saugomos vertybės. Tapatybės vagystė elektroninėje erdvėje yra kiek platesnė nei tapatybės vagystė fizinėje erdvėje, kadangi ji nėra nukreipta vien tik prieš kažkokį konkretų asmenį, siekiant pasisavinti jo dokumentus ar kitus reikšmingus daiktus, tačiau atlikdamas šią veiką kaltininkas veikia ir prieš informacines sistemas bei elektroninių ryšių tinklus. Tuo tarpu kalbant apie nusikalstamos veikos **objektą** turėtume įvertinti BK 178 straipsnyje įtvirtinto nusikaltimo – vagystės – sudėtį. Paminėtina, kad susiduriame su problema, jog yra laikomasi požiūrio, jog vagystės objektas yra visų rūšių ir formų nuosavybė, o turtas – turintys vertę bei fizinius parametrus (gabaritus, svorį, skaičių, kiekį) daiktai. Tai reiškia, pavyzdžiui, namų apyvokos daiktai, transporto ir gamybos priemonės, asmeniniai daiktai, taip pat pinigai ir vertybiniai popieriai (Lietuvos Aukščiausiojo Teismo Senato 2005 m. birželio 23 d. nutarimas Nr. 52). Todėl darytina išvada, jog vagystės dalyku gali būti tik materialus turtas, kuris turi ekonominę vertę, o šiuo atveju – informacija nepatenka į BK 178 straipsnio reglamentavimą ir negali

būti vagystės objektu. Atsižvelgiant į tai, jog tapatybės vagystės metu žala yra padaroma pasisavinus asmens duomenis ar kitą informaciją, kurios dėka gali būti nustatoma to asmens tapatybė, asmens tapatybės objektu turėtų būti laikomi duomenys, atskleidžiantys asmens tapatybę, neišskiriant ar informacija yra laikoma elektroninėje erdvėje, ar materialioje laikmenoje.

Padarymo būdas šioje nusikalstamoje veikoje pasireiškia veikimu, tai reiškia, jog asmuo, darantis tokią veiką ją atlieka sąmoningai ir valingai, imasi tam tikrų konkrečių veiksmų, jog įgytų kitam asmeniui priklausančius asmens duomenis ir (ar) tam tikrą informaciją, kuria remiantis būtų galima nustatyti žmogaus tapatybę, o vėliau atliktų dažniausiai neteisėtus veiksmus, apsimesdamas tuo asmeniu. Taigi tapatybės vagystė elektroninėje erdvėje pasireiškia alternatyviais padarymo būdais, tokiais kaip neteisėtas įgijimas, laikymas, pasisavinimas, fiksavimas, stebėjimas, perėmimas, disponavimas ar kitoks neteisėtas duomenų ir (ar) informacijos apie kitą asmenį panaudojimas.

Tapatybės vagystėje nėra svarbus nei **padarymo laikas**, nei **vieta**, kadangi nusikaltimas padaromas elektroninėje erdvėje, kurioje nėra skiriama padarymo vieta. Taip pat neturėtų būti išskiriamas ir laiko kriterijus, kadangi laikas reikšmės dėl tapatybės vagystės kvalifikavimo neturi. Kalbant apie **priemonės**, tapatybės vagystės elektroninėje erdvėje atveju jomis galima laikyti informacines ir ryšio technologijas, kurių pagalba galima rinkti, kaupti bei atlikti kitus veiksmus su kito asmens duomenimis ir (ar) informacija, pasiekti jo kompiuteryje esančią informaciją ar atlikti kitus efektyvius veiksmus net neturint tiesioginio kontakto su nusikalstamos veikos auka. **Specialaus subjekto** šiuo atveju taip pat nėra, kadangi asmuo duomenis gali gauti ne tik išimtinai atlikdamas savo tarnybines pareigas, tačiau ir bet kokiais kitais atvejais.

Galiausiai, kalbant apie padarinius, tapatybės vagystės sudėtis – **formali**, kadangi žala atsiranda vos tik yra pasikėsinama pasisavinti kito asmens duomenis, kadangi tai jau yra laikoma asmens privataus gyvenimo pažeidimu. Nėra būtina, jog asmuo pasinaudotų tais gautas duomenimis ir (ar) informacija, atsakomybė kiltų vien už tokios informacijos rinkimą ar kitos alternatyvios veikos atlikimą. Toks vertinimas yra pasirinktas dėl to, jog tokia nusikalstama veika kėsinama į pamatines žmogaus vertybes, pažeidžiama asmens duomenų apsauga, o išskirtiniais atvejais duomenys apie asmenį gali būti renkami tik su jo sutikimu ar konkrečiau įstatymo pagrindu.

4.2. Tapatybės vagystės elektroninėje erdvėje sudėties subjektyvieji požymiai

Subjektyvieji nusikalstamos veikos sudėties požymiai apibūdina žmogaus vidinę, psichinę būseną, jo valią ir tikslus atliekant tam tikrą veiką. Šiems požymiams priskirtini: kaltė,

tikslas, motyvai (Lietuvos Aukščiausiojo Teismo 2022 m. vasario 23 d. nutartis baudžiamojoje byloje). Be to, subjektyvioji nusikaltimo sudėtis turėtų aptarti ir kriterijus, taikomus subjektui.

Taigi, pirmiausia turėtume apibūdinti siūlomus kriterijus subjektui. Tapatybės vagystės **subjektu** yra fizinis asmuo, pakaltinamas, bei sulaukęs BK 13 straipsnio 1 dalyje nurodyto amžiaus (16 metų), nuo kurio asmuo galėtų būti traukiamas baudžiamojon atsakomybėn. Tokios nusikalstamos veikos subjektu gali būti ir juridinis asmuo, jei yra įrodoma, jog juridinis asmuo yra atsakingas už neteisėtą asmens duomenų rinkimą, saugojimą, panaudojimą ir (ar) kitas alternatyvias veikas, nurodytas tapatybės vagystės nusikaltimo sudėtyje. Apibūdinant kaltę, reikia paminėti, jog **kaltė** yra asmens, padariusio pavojingą veiką, vidinis (psichinis) santykis su objektyviaisiais nusikalstamos veikos sudėties požymiais. Ji yra būtinoji kiekvienos nusikalstamos veikos sudėties dalis, todėl turi būti įrodinėjama kiekvienoje baudžiamojoje byloje (Piesliakas, 2009, p. 336). Tapatybės vagystė šiuo atveju padaroma tik tiesiogine tyčia, kadangi iš pačios nusikaltimo sudėties matome, jog turi būti aiškus nusikalstamos veikos suvokimas, supratimas, aiškūs žingsniai bei noras atlikti būtent tokius veiksmus.

Pažymint dėl tapatybės vagystės **tikslo**, reikėtų apžvelgti du aspektus. Visų pirma, tapatybės vagystė dažniausiu atveju yra atliekama su tikslu gautus duomenis ir (ar) informaciją panaudoti kitais nusikalstamais tikslais. Tai reiškia, kad asmuo, pasisavinęs kito asmens duomenis ir veikdamas jo vardu atlieka nusikalstamas veikas ar teisės pažeidimus. Atsižvelgiant į tai, galima daryti prielaidą, jog tapatybės vagystės nusikaltimo sudėtyje (dispozicijoje) neturėtų būti įtrauktas tikslas būtent įvykdyti kitas nusikalstamas veikas ar teisės pažeidimus. Tuomet tapatybės vagystės nusikaltimu ir būtų laikomi tokie veiksmai, o neįrodžius šio esminio kriterijaus, negalėtume taikyti baudžiamosios atsakomybės. Tačiau šiais laikais mes kalbame apie tapatybės vagystę kaip apie asmens privatumo pažeidimą, kai vien žmogau asmeninės informacijos rinkimu, turėjimu, saugojimu yra sukeliama žala. Net ir apsimetimas kitu asmeniu vien atliekant tokius veiksmus, kaip elektroninio pašto dėžutės sukūrimas, prisijungimas prie banko informacinės sistemos ar net prie asmens socialinių tinklų, kadangi taip pamatomi asmens privatus duomenys, susirašinėjimai ar net identifikuojamasi to asmens vardu. Praktikoje taip pat pasitaiko ir atvejų, kai duomenis yra pardavinėjami tretiesiems asmenims, kurie naudojami tokiais duomenimis ir (ar) informacija bei realizuoja priešingus teisei veiksmus. Galiausiai, tokie duomenys ir (ar) informacija gali būti panaudojami ne iškart, o renkami sistemingai ir naudojami saviems tikslas ar parduodami ir vėliau, praėjus tam tokiam laikui tarpui. Taigi, kalbant apie tapatybės vagystės, kaip nusikaltimo, sudėtį ir tokios

nusikalstamos veikos kvalifikavimą, turėtume neišskirti tikslo, jog duomenys ir (ar) informacija turi būti panaudota nusikalstamai veikai ir (ar) priešingoms teisėms veikoms, tačiau ir tuomet, kai informacija ar (ir) asmens duomenys yra renkami, gaunami, atliekamos kitos alternatyvios veikos, tačiau nėra atliekama nusikalstama veika, nes tai jau yra priešingas teisei veiksmas, kuriuo yra pažeidžiama asmens privataus gyvenimo apsauga. Galiausiai, aptariant veikos motyvus, galėtume teigti, jog **motyvai** gali būti patys įvairiausi ir neturėtų būti išskiriami vien išskirtiniai motyvai. Vieni asmenys gali bandyti tokiais duomenimis pasinaudoti šmeižto, reputacijos sugadinimo tikslais, kiti – bandyti pasisavinti asmens turtą ir (ar) turtines teises. Galiausiai, galimi ir tokie motyvai kaip tiesiog smalsumo patenkinimas, t. y. prisijungimas prie kitam asmeniui priklausančios elektroninio pašto dėžutės ar socialinių tinklų, siekiant sužinoti asmens privačią informaciją, perskaityti jo susirašinėjimus, laiškus ar sužinoti konfidencialią informaciją.

4.3. Lietuvos Respublikos baudžiamojo kodekso specialiosios dalies pakeitimo projektas

Šio darbo tikslas – išsiaiškinti ar tikslinga būtų Lietuvos Respublikos baudžiamajame kodekse kriminalizuoti tapatybės vagystę kaip atskirą veiką. Visų pirma, norint atlikti išvadas ar tikslinga bei reikalinga kriminalizuoti asmens tapatybės vagystę kaip atskirą veiką, turime įvertinti ar ši veika atitinka kriterijus, pagal kuriuos veikos turėtų būti kriminalizuojamos. Remiantis profesoriaus Gintaro Švedo (2012) nuomone, pagrindiniai kriterijai, kuriuos būtina įvertinti priimant tam tikros veikos kriminalizavimo (decriminalizavimo) sprendimą, yra veikos pavojingumas, jos paplitimas, *ultima ratio* principas, baudžiamosios teisės veikimo sritis ir ribos.

Kalbant apie tokios veikos, kaip asmens tapatybės vagystės, pavojingumą, turėtume pabrėžti, jog tokios veikos mastas ir padaroma žala gali būti itin didelė, veika dažniausiu atveju neapsiriboja vienu asmeniu ir jo duomenų pasisavinimu – ypač kalbant apie tokios veikos padarymą elektroninėje erdvėje, dažnai tam prireikia ir didesnės grupės veikimo, atliekant skirtingus vaidmenis bei įvykdant specialių žinių reikalaujančias užduotis. Kaip ir aptarta aukščiau, tokia veika gali būti atliekama pačiais įvairiausiais būdais – nuo asmens tapatybės dokumento pasisavinimo iki masinės elektroninės bankininkystės prisijungimo duomenų vagystės, taip pažeidžiant ne tik asmens finansinius interesus, tačiau ir privataus gyvenimo apsaugą. Nepaisant to, tokios veikos kaip plėšimas, vagystė, baudžiamosios teisės teorijoje yra įvardijamos kaip „blogis savaime“ (*mala en se*) (ibid, p. 17).

Aptariant tokios veikos paplitimą, asmens duomenys bei asmens tapatybė visais laikais buvo itin svarbi vertybė kiekvieno žmogaus gyvenime. Atėjus į šį technologijų amžių, tokios veikos padarymui atsirado tik dar daugiau priemonių, įrankių, padedančių veiksmus atlikti greičiau, efektyviau, prieiti prie slaptesnės informacijos bei išlikti sunkiau surandamam, atliekant skirtingus veiksmus skirtingų šalių jurisdikcijose. Šiuo metu Lietuvoje neturime tikslios statistikos, kuri apibūdintų būtent asmens tapatybės vagystės paplitimą, tačiau matome, jog asmenys itin dažnai susiduria su elektroniniais nusikaltimais, kurių viena iš dažniausių esmių ir yra susijusi su asmenų duomenų pasisavinimu (Swedbank, 2021). Pavyzdžiui, vien šių metų (sausio – kovo mėnesiais) Lietuvoje jau yra užregistruotos 349 nusikalstamos veikos elektroninių duomenų ir informacinių sistemų saugumui (per 2021 metus – 705 nusikalstamos veikos) (Informatikos ir ryšių departamentas..., 2022).

Sekantis kriterijus – *ultima ratio* principas bei jo taikymas praktikoje. Šis principas kalba apie tai, jog tam tikro elgesio draudimas su baudžiamosios teisės pagalba turi būti griežčiausia (*ultima ratio*) valstybės reakcijos į nepageidaujamą elgesį forma (Dambrauskienė, 2015, p. 118). Kitaip sakant, nepageidaujamo elgesio draudimas baudžiamojoje teisėje galimas tik tuo atveju, kai jis neturi alternatyvių poveikio priemonių kitose teisės šakose (pavyzdžiui, drausminė, civilinė, administracinė atsakomybė ir pan.) (Fedosiuk, 2012, p. 717). Šiuo konkrečiu atveju mes matome situaciją, kuomet tokios veikos kaip asmens tapatybės vagystės reguliavimo mes neturime nei vienoje kitoje teisės šakoje, įskaitant ir baudžiamąją justiciją.

Galiausiai, aptariant paskutinįjį kriterijų – baudžiamosios teisės veikimo sritis ir ribas, pažymėtina, kad kuomet baudžiamoji teisė viršija ribas, tuomet galimas neigiamas poveikis, kuris pertekliniai suvaržytų net pačias pamatines žmogaus teises. Tačiau iš šios veikos kriminalizavimo perspektyvos mes galime pastebėti, jog būtent veikos padarymu yra padaroma daug didesnė žala ir pažeidžiamos itin svarbios ir fundamentalios teisės – teisė į asmens privataus gyvenimo apsaugą, tokio gyvenimo neliečiamumą ir galiausiai, tiesiog saugumo jausmą ne tik dėl asmens duomenų, tačiau ir pačios tapatybės.

Taigi, atsižvelgiant į aukščiau analizuotus tapatybės vagystės elektroninėje erdvėje, kaip atskiro nusikaltimo, subjektyviuosius ir objektyviuosius požymius bei aptartus kriminalizavimui taikomus kriterijus, toliau šioje dalyje siūlomas atskiros veikos įtvirtinimo BK projektas.

Pirmiausia, turėtume pabrėžti, nors jog ir šiame darbe dėl ribotos apimties pagrinde kalbama apie asmens tapatybės vagystę elektroninėje erdvėje, tačiau kalbant apie tokios naujos veikos kriminalizavimą, į nusikalstamos veikos sudėtį turėtume įtraukti ir asmens

tapatybės vagystę atliekamą fizinėje erdvėje. Tai turėtų būti atliekama dėl to, nes tapatybės vagystės įvykdymas elektroninėje erdvėje informacinių ir ryšio technologijų pagalba nėra išskiriamas kaip didesnę žalą padaranti ar didesnę pavojingumą turinti veika, kadangi ir fizinėje erdvėje pasisavinami duomenys ar (ir) informacija gali sukelti itin dideles pasekmes, pavyzdžiui, asmens tapatybės dokumento pasisavinimas, su kuriuo asmuo yra identifikuojamas fizinėje erdvėje.

Antra, turėtume paminėti tai, jog turėtume įsitvirtinti tokią sąvoką, kaip asmens tapatybė – siūloma, jog asmens tapatybė būtų apibrėžiama – asmens duomenų visuma, kuria remiantis gali būti nustatyta konkretaus asmens tapatybė. Tuo tarpu asmens duomenys – bet kokia informacija, susijusi su gyvu asmeniu, kurio tapatybė yra nustatyta arba gali būti nustatyta (Europos Komisija, 2007).

Autorės nuomone, įvertinus BK esančių veikų sudėtis, kurios yra tapatybės vagystės nusikaltimo sudedamosios dalys, nėra tinkama keisti vieną iš jau esančių nusikalstamų veikų sudėčių. Vertintinas BK 198 straipsnio 1 dalies pakeitimas, „neviešų elektroninių duomenų“ sąvoką keičiant tik „duomenų“ sąvoka, tačiau nusikalstama veika, kurios dispozicija skambėtų kaip: „tas, kas neteisėtai stebėjo, fiksavo, perėmė, įgijo, laikė, pasisavino, paskleidė ar kitaip panaudojo duomenis“ labiau vertintina kaip BK 167-168 straipsnių apibūdinimas, nesusijęs su pasinaudojimu tokiais duomenimis, siekiant apsimesti ir identifikuoti kitu asmeniu, o tai ir yra esminis tokios nusikalstamos veikos tikslas.

Taigi šiuo darbu būtų siūloma papildyti BK nauju straipsniu, apibrėžiančiu asmens tapatybės vagystės, kaip savarankiškos nusikalstamos veikos, sudėtį. Reikėtų paminėti tai, jog šiuo atveju pasirinkta tiek tokios veikos atlikimą elektroninėje, tiek fizinėje erdvėje vertinti kaip nusikalstamą veiką, neišskiriant kažkurios iš jų kaip pavojingesnės ar sukeliančios didesnę žalą. Tuo pačiu vertinant tikslą, neturėtų būti išskiriamas tikslas, jog duomenys (ir) ar informacija pasisavinti nusikalstamos veikos tikslais vertinama kaip kvalifikuoto nusikalstamos veikos požymis, kadangi atlikus nusikalstamą veiką, tai būtų galima vertinti kaip asmens tapatybės vagystės bei kitos atliktos nusikalstamos veikos sutaptį. Galiausiai, reikėtų pabrėžti ir tai, jog atsižvelgiant į itin plačią asmens tapatybės vagysčių įvairovę, pobūdį, rezultatus bei atlikimo būdus, įstatymų leidėjas turėtų įtvirtinti platų sankcijų pasirinkimą, kadangi kiekvieną kartą tokia veika turėtų būti vertinama itin individualiai ir už jos atlikimą būtų paskirtos itin proporcingos ir teisingos priemonės.

Atsižvelgiant į tai, kas išdėstyta aukščiau, bei pabrėžiant tokios nusikalstamos veikos pobūdį – vagystė, siūlytina, jog BK specialiosios dalies straipsnis, kuris įtvirtinta asmens tapatybės vagystę, kaip nusikaltimą, turėtų atrodyti:

178¹ straipsnis. Asmens tapatybės vagystė

1. Tas, kas neteisėtai įgijo, laikė, paskleidė, perėmė, fiksavo, disponavo ar kitaip neteisėtai panaudojo asmens duomenis ir (ar) informaciją apie kitą asmenį, siekiant pasisavinti tapatybę ir apsimesti kitu asmeniu, kurio duomenys ir (ar) asmeninė informacija buvo pasisavinta, baudžiamas <...>;
2. Už šiame straipsnyje numatytą veiką atsako ir juridinis asmuo.

IŠVADOS

1. Tapatybės vagystės terminas kilo ne iš teisėkūros išraiškos, teisminės išmonės ar akademinės abstrakcijos. Priešingai, tai yra itin senas šaknis turintis reiškinys, kuris siauriausia prasme visuomenėje yra suprantamas, kaip neteisėtas asmens duomenų pasisavinimas. Tuo tarpu, asmens tapatybės vagystės sąvoka Lietuvos teisiniame reguliavime taip pat nėra tiesiogiai apibrėžta ar oficialiai įtvirtinta. Taigi, įvertinus užsienio ir Lietuvos literatūros šaltinius, nurodoma bendrinė tapatybės vagystės sąvoka, kuri turi būti suprantama kaip – „neteisėti veiksmai pasitelkiant kito asmens duomenis ir (ar) informaciją, kurie suteikia galimybę identifikuoti kitą asmenį, turint tikslą apsimesti tuo asmeniu“. Tuo tarpu specifinė tapatybės vagystės elektroninėje erdvėje sąvoka turėtų skambėti kaip: „tapatybės vagystės rūšis, kai tapatybės vagystė atliekama nuotoliu, pasinaudojant informacinėmis ir ryšio technologijomis“.
2. Tapatybės vagystės yra įvykdomos fizinėje erdvėje ir (ar) elektroninėje erdvėje. Šiame darbe buvo nuodugniai analizuojamos elektroninėje erdvėje įvykdomos asmens duomenų bei tapatybės vagystės, nes ši nusikalstama veika yra atliekama vis dažniau ir gali būti atliekama pačiais įvairiausiais metodais, kurie kinta ir tobulėja kartu su technologijų pažanga. Dažniausi ir šiuo metu labiausiai paplitę tapatybės vagystės metodai elektroninėje erdvėje yra šie: sukčiavimas (angl. *Phishing*), įsilaužimas į tinklą (angl. *Network Intrusion*), trojos arkliai (angl. *Trojan Horses*), biometrinių sensorių klastojimas (angl. *Spoofing of biometric sensors*).
3. Asmens tapatybės vagystę laikant globalia problema bei atlikus užsienio šalių analizę matomas skirtingas tokios veikos vertinimas – vienos valstybės, tokios kaip Jungtinės Amerikos Valstijos bei Estija, suprasdamos tokios veikos pavojingumą asmens tapatybės vagystę laiko atskira nusikalstama veika, įtvirtinta jų baudžiamuosiuose įstatymuose, tuo tarpu kitos – Prancūzija, Vokietija ir Latvija tokią veiką laiko atskirų nusikalstamų veikų sudėtine dalimi. Kaip bebūtų, matoma, jog tokios nusikalstamos veikos atskiras kvalifikavimas itin reikalingas tikslingesniam ir efektyvesniam tokių veikų ištyrimui bei prevencijai, kadangi tokiems veiksmais itin reikšmingas šalių bendradarbiavimas.
4. Asmens tapatybės vagystė turėtų būti kvalifikuojama kaip nusikalstama veika – sąmoningas, valingas, priešingas teisei ir saugomoms vertybėms žmogaus elgesys, pasireiškiantis objektyviaisiais ir subjektyviaisiais požymiais, apibrėžiančiais tapatybės vagystės sudėtį. Taip pat ši veika atitinka ir visus kriminalizavimo kriterijus – veikos pavojingumą, jos paplitimą, *ultima ratio* principą ir baudžiamosios teisės veikimo sritį ir ribas.

5. Lietuvoje tokia nusikalstama veika nėra kriminalizuota, tačiau tam tikri tapatybės vagystės elektroninėje erdvėje atvejai patenka į kitų nusikalstamų veikų sudėtį. Tačiau visose iš šių veikų matomi neatitikimai, kurie neatspindi tikrojo asmens tapatybės vagystės tikslo, veiksmų bei padarinių, todėl kritikuotinas toks įstatymų leidėjo nusikalstamos veikos susiaurinimas – egzistuojančių Lietuvos Respublikos baudžiamojo kodekso specialiosios dalies normų reglamentavimo sritis neapima visų minėtos veikos elementų.

PASIŪLYMAI

Remiantis atlikta tarptautinių ir nacionalinių teisės aktų, Lietuvos ir užsienio mokslininkų formuojama doktrina, tapatybės vagystės sudėties požymių analize, kriminalizavimo kriterijais bei atsižvelgiant į suformuluotas išvadas, teikiami šie pasiūlymai:

1. Asmens tapatybės vagystę siūlytina apibrėžti kaip bet kokius neteisėtus veiksmus su kito asmens duomenimis ir (ar) asmenine informacija, leidžiančia identifikuoti kitą asmenį (tokių duomenų ir (ar) informacijos apie kitą asmenį įgijimas, laikymas, paskleidimas, perėmimas, fiksavimas, disponavimas ar kitas neteisėtas panaudojimas), su tikslu pasisavinti tapatybę ir apsimesti kitu asmeniu, kurio duomenys ir (ar) informacija buvo pasisavinta. Tuo tarpu tapatybės vagystę elektroninėje erdvėje ir (ar) fizinėje erdvėje laikyti asmens tapatybės vagystės rūšimis.
2. Atsižvelgiant į tapatybės vagystės, kaip savarankiškos nusikalstamos veikos požymių analizę, bei kriterijus kvalifikavimui, siūloma papildyti Lietuvos Respublikos baudžiamojo kodekso specialiąją dalį nauju straipsniu, numatančiu baudžiamąją atsakomybę už asmens tapatybės vagystę:

178^l straipsnis. Asmens tapatybės vagystė

1. *Tas, kas neteisėtai įgijo, laikė, paskleidė, perėmė, fiksavo, disponavo ar kitaip neteisėtai panaudojo asmens duomenis ir (ar) informaciją apie kitą asmenį, siekiant pasisavinti tapatybę ir apsimesti kitu asmeniu, kurio duomenys ir (ar) asmeninė informacija buvo pasisavinta, baudžiamas <...>;*
 2. *Už šiame straipsnyje numatytą veiką atsako ir juridinis asmuo.*
3. Galiausia, dėl itin plačios asmens tapatybės vagysčių įvairovės, pobūdžio, rezultatų bei atlikimo būdų, įstatymų leidėjui siūlytina įtvirtinti platų sankcijų pasirinkimą, kadangi kiekvieną kartą tokia veika turėtų būti vertinama itin individualiai ir už jos atlikimą turi būti paskirtos itin proporcingos bei teisingos priemonės.

ŠALTINIŲ SĄRAŠAS

Teisės norminiai aktai

Tarptautiniai teisės aktai

1. Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija (1950). *Valstybės žinios*, 1995, 40-987.

Europos Sąjungos teisės aktai

2. 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. OL L 119/1.
3. Europos Sąjungos pagrindinių teisių chartija (2009). *Europos Sąjungos oficialusis leidinys*, 2012, 326/02.
4. Konvencija dėl elektroninių nusikaltimų (2001). *Valstybės žinios*, 2004, 36-1188.

Lietuvos teisės aktai

5. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas (1996). *Valstybės žinios*, 63-1479.
6. Lietuvos Respublikos baudžiamasis kodeksas (2000). *Valstybės žinios*, 89-2741.
7. Lietuvos Respublikos asmens tapatybės kortelės ir paso įstatymas (2014). *Teisės aktų registras*, 21281.

Užsienio valstybių teisės aktai

8. Estijos baudžiamasis kodeksas (2001) [interaktyvus]. Prieiga per internetą: <https://www.legislationline.org/documents/section/criminal-codes/country/33/Denmark/show> [žiūrėta 2022 m. kovo 15 d.].
9. Jungtinių Valstijų kodeksas (1947) [interaktyvus]. Prieiga per internetą: <https://uscode.house.gov/browse.xhtml> [žiūrėta 2022 m. kovo 15 d.].
10. Latvijos baudžiamasis kodeksas (1998) [interaktyvus]. Prieiga per internetą: <https://www.legislationline.org/documents/section/criminal-codes/country/19/Latvia/show> [žiūrėta 2022 m. kovo 15 d.].
11. Prancūzijos baudžiamasis kodeksas (2005) [interaktyvus]. Prieiga per internetą: <https://www.legislationline.org/documents/section/criminal-codes/country/30/France/show> [žiūrėta 2022 m. kovo 15 d.].

12. Tapatybės vagystės baudmės padidinimo įstatymas (2004) [interaktyvus]. Prieiga per internetą: <https://www.congress.gov/bill/108th-congress/house-bill/1731/text> [žiūrėta 2022 m. kovo 22 d.].
13. Tapatybės vagystės ir apsimetinėjimo atgrasymo aktas (1998) [interaktyvus]. Prieiga per internetą: <https://www.congress.gov/bill/105th-congress/senate-bill/512/text> [žiūrėta 2022 m. kovo 22 d.].
14. Vokietijos baudžiamasis kodeksas (1998) [interaktyvus]. Prieiga per internetą: https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html [žiūrėta 2022 m. kovo 15 d.].

Specialioji literatūra

Monografijos, vadovėliai ir kiti leidiniai

15. Biegelman, T. M. (2009). *Identity Theft Handbook. Detection, Prevention, and Security* New Jersey.
16. Brenner, S. (2004). *Cybercrime Metrics: Old Wine, New Bottles*. Virginia, Virginia Journal of Law and Technology.
17. Bryan K., et al. (2009). *Cyber Fraud: Tactics, Techniques and Procedures*. Auerbach Publications, Florida.
18. Bullot, J. N. (2014). *Explaining Person Identification: An Inquiry Into the Tracking of Human Agents*. The Tracking and Identification of Human Agents, Volume 6, Issue 4, p. 567-584.
19. Collins, J. (2005). *Preventing Identity Theft Into Your Business*. New Jersey, John Wiley.
20. Copes, H. and Vieraitis, L. (2012). *Identity Theft: Assessing Offenders' Strategies and Perceptions of Risk*. The Oxford Handbook of Crime and Public Policy.
21. Dambrauskienė A. (2015). *Ultima ratio principio samprata*. *Teisė*, 2015, 97, 116-134.
22. Dodge, M. (2001). *Mapping Cyberspace*. N.Y, Routledge.
23. Fedosiuk, O. (2012). *Baudžiamoji atsakomybė kaip kraštutinė priemonė (ultima ratio): teorija ir realybė*. *Jurisprudencija*, 2012, 19 (2), 715-738.
24. Gercke, M. (2011). *Legal Approaches to Criminalize Identity Theft*. UNODC, Handbook on Identity-related Crime. New York: United Nations.
25. Higgins, H.E. (2010). *Cybercrime: An Introduction to an Emerging Phenomena*. Louisville.

26. Hoffman, K. S. and McGinley, T. G. (2010). *Identity Theft: a Reference Handbook*. Santa Barbara, Calif: ABC-CLIO.
27. Irshad, S. and Soomro, T. (2018). *Identity Theft and Social Media* [interaktyvus] IJCSNS International Journal of Computer Science and Network Security, VOL.18 No.1. Prieiga per internetą: http://search.ijcsns.org/07_book/html/201801/201801006.html [žiūrėta 2022 m. kovo 7 d.].
28. Jaishankar, K. (2008). *Space Transition Theory of cyber crimes*. Crimes of the Internet. Upper Saddle River, NJ: Prentice Hall. p. 283-301.
29. Jaquet-Chiffelle, D. O. (2009). *The Future of Identity in the Information Society*. Springer.
30. Kalpokas V. ir Marcinauskaitė R. (2012). *Tapatybės vagystė elektroninėje erdvėje: technologiniai aspektai ir baudžiamasis teisinis vertinimas. Teisės problemos*, 2012, 3 (77), 30-52.
31. Lawson, P. (2011). *Identity-related Crime Victim Issues: A Discussion Paper*. UNODC, Handbook on Identity-related Crime p. 107-168.
32. May, J. (2004). *Preventing Identity Theft*. N.Y., Security Resources Unlimited.
33. Piesliakas V. (2009). *Lietuvos baudžiamoji teisė. Pirmoji knyga*. Vilnius: Justitia.
34. Prapiestis, J. (2004). *Lietuvos Respublikos baudžiamojo kodekso komentaras (II)*. Vilnius: Registrų centras.
35. Sileo, J. D. (2005). *Stolen lives: identity theft prevention made simple*. DaVinci Publishing.
36. Štītīlis D. ir kt. (2011). *Tapatybės vagystė elektroninėje erdvėje: socialiniai, elektroninio verslo ir teisinio reguliavimo aspektai*. Kolektyvinė mokslo monografija. Vilnius: Mykolo Romerio universitetas.
37. Švedas G. (2012). *Veikos kriminalizavimo kriterijai: teorija ir praktika. Vilniaus universiteto leidykla*. 2012, 82, 12-25.
38. Švedas G., Bieliūnas E. ir ir Abramavičius A. (2010). *Lietuvos Respublikos baudžiamojo kodekso komentaras. 2 dalis. III tomas*. Vilnius: Registrų centras.
39. Tajpour, A. (2013). *Identity Theft and Fraud Type* [interaktyvus]. International Journal of Information Processing and Management. Prieiga per internetą: https://www.researchgate.net/publication/273259976_Identity_Theft_and_Fraud_Type [žiūrėta 2022 m. kovo 15 d.].
40. Vaišvila, A. (1998). *Baudžiamoji justicija – juridinė asmens teisinio statuso identifikacija. Teisės problemos* 3–4 (21, 22): 131.

41. Veršekys, P. (2012). *Nusikalstamos veikos sudėties požymio samprata ir ją lemiantys veiksniai*. *Teisė*, 2012, 82, 198-214.

Teismų praktika

Lietuvos teismų sprendimai

42. Lietuvos Respublikos Konstitucinio Teismo 1999 m. spalio 21 d. nutarimas. *Valstybės žinios*, 90-2662.
43. Lietuvos Respublikos Konstitucinio Teismo 2000 m. gegužės 8 d. nutarimas. *Valstybės žinios*, 39-1105.
44. Lietuvos Respublikos Konstitucinio Teismo 2002 m. rugsėjo 19 d. nutarimas. *Valstybės žinios*, 93-4000.
45. Lietuvos Respublikos Konstitucinio Teismo 2002 m. spalio 23 d. nutarimas. *Valstybės žinios*, 104-4675.
46. Lietuvos Respublikos Konstitucinio Teismo 2003 m. kovo 24 d. nutarimas. *Valstybės žinios*, 29-1196.
47. Lietuvos Respublikos Konstitucinio Teismo 2005 m. gegužės 13 d. nutarimas. *Valstybės žinios*, 63-2235.
48. Lietuvos Respublikos Konstitucinio Teismo 2010 m. vasario 26 d. nutarimas. *Valstybės žinios*, 25-1179.
49. Lietuvos Respublikos Konstitucinio Teismo 2011 m. birželio 21 d. nutarimas. *Valstybės žinios*, 76-3672.
50. Lietuvos Respublikos Konstitucinio Teismo 2014 m. gegužės 9 d. nutarimas. *Valstybės žinios*, 5321.
51. Lietuvos Aukščiausiojo Teismo 2018 m. gegužės 31 d. nutartis baudžiamojoje byloje Nr. 2K-7-84-489/2018.
52. Lietuvos Aukščiausiojo Teismo 2020 m. sausio 7 d. nutartys baudžiamojoje byloje Nr. 2K-52-942/2020.
53. Lietuvos Aukščiausiojo Teismo 2022 m. vasario 23 d. nutartis baudžiamojoje byloje Nr. 2K-35-719/2022.
54. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2007 m. birželio 28 d. apžvalga „Dėl teismų praktikos skiriant bausmes (BK 54–64 straipsniai)“, *Teismų praktika*. Nr. 27.
55. Lietuvos Aukščiausiojo Teismo Senato 2005 m. birželio 23 d. nutarimas Nr. 52 „Dėl teismų praktikos vagystės ir plėšimo baudžiamosiose bylose“.

Europos Žmogaus Teisių Teismo sprendimai

56. *Niemietz prieš Vokietiją* [EŽTT], Nr. 13710/88, [1992-12-16].
ECLI:CE:ECHR:1992:1216JUD001371088.
57. *Von Hannover prieš Vokietiją* [EŽTT], Nr. 59320/00, [2004-06-24].
ECLI:CE:ECHR:2004:0624JUD005932000.

Kiti šaltiniai

58. A Digital Agenda of Europe [interaktyvus]. Prieiga per internetą: <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF> [žiūrėta 2022 m. kovo 25 d.].
59. Allstate Identity Protection. *A step-by-step guide to identity theft* [interaktyvus]. Prieiga per internetą: <https://www.allstateidentityprotection.com/content-hub/how-does-identity-theft-work> [žiūrėta 2022 m. kovo 9 d.].
60. Bendrojo Duomenų Apsaugos Reglamento (BDAR) 29 straipsnio darbo grupės nuomonė 4/2007 dėl asmens duomenų sąvokos [interaktyvus]. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_lt.pdf [žiūrėta 2022 m. kovo 25 d.].
61. Delfi, BNS. „Grožio chirurgijos“ duomenų vagystės byla gražinta prokurorui [interaktyvus]. Prieiga per internetą: <https://www.delfi.lt/news/daily/law/grozio-chirurgijos-duomenu-vagystes-byla-grazinta-prokurorui.d?id=80705667> [žiūrėta 2022 m. sausio 11 d.].
62. Federal Trade Commission. *Consumer sentinel network* [interaktyvus]. Prieiga per internetą: https://www.ftc.gov/system/files/ftc_gov/pdf/CSN%20Annual%20Data%20Book%202021%20Final%20PDF.pdf [žiūrėta 2022 m. vasario 16 d.].
63. Geys W. (2021). The Real Social Media Addiction Stats for 2022. Influencer Marketing Hub [blog], 30 December. Prieiga per internetą: <https://influencermarketinghub.com/social-media-addiction-stats/#toc-0> [žiūrėta 2022 m. kovo 6 d.].
64. Informatikos ir ryšių departamentas. Ataskaitos: duomenys apie nusikalstamas veikas, padarytas Lietuvos Respublikoje (Forma_1G) 2022 m. sausis – kovas [interaktyvus]. Prieiga per internetą: https://www.ird.lt/lt/reports/view_item_datasource?id=9714&datasource=69472 [žiūrėta 2022 m. vasario 16 d.].
65. Informatikos ir ryšių departamentas. Ataskaitos: duomenys apie nusikalstamas veikas, padarytas Lietuvos Respublikoje (Forma_1G) 2021 m. sausis – gruodis

- [interaktyvus]. Prieiga per internetą: https://www.ird.lt/lt/reports/view_item_datasource?id=9563&datasource=66822 [žiūrėta 2022 m. vasario 16 d.].
66. Lyzhina, S. *The unsolved riddle of princess Anastasia* [interaktyvus]. Prieiga per internetą: <https://english.pravda.ru/history/6156-nicholas/> [žiūrėta 2022 m. vasario 3 d.].
67. Swedbank. *Tyrimas: gyventojų susidūrimai su sukčiais tapo ir dažnesni, ir brangesni* [interaktyvus]. Prieiga per internetą: <https://blog.swedbank.lt/pranesimai-spaudai-saugumas/tyrimas-gyventoju-susidurimai-su-sukciais-tapo-ir-daznesni-ir-brangesni> [žiūrėta 2022 m. vasario 16 d.].
68. Teise.pro. *Asmens duomenų saugumo incidentai „Facebook“ ir „LinkedIn“ socialiniuose tinkluose* [interaktyvus]. Prieiga per internetą: <https://www.teise.pro/index.php/2021/04/13/asmens-duomenu-saugumo-incidentai-facebook-ir-linkedin-socialiniuose-tinkluose/> [žiūrėta 2022 m. sausio 11 d.].
69. The Cross-Border Crime Forum. *Identity-Related Crime: A Threat Assessment* [interaktyvus]. Prieiga per internetą: <https://www.ojp.gov/ncjrs/virtual-library/abstracts/identity-related-crime-threat-assessment> [žiūrėta 2022 m. vasario 3 d.].
70. United States Secret Service. *Take charge – fighting back against identity theft* [interaktyvus]. Prieiga per internetą: <https://www.hsdl.org/?view&did=695104> [žiūrėta 2022 m. kovo 9 d.].
71. Valstybinė duomenų apsaugos inspekcija. *Automobilių nuomos bendrovei skirta bauda dėl duomenų saugumo pažeidimo pagal Bendrąjį duomenų apsaugos reglamentą* [interaktyvus]. Prieiga per internetą: <https://vdai.lrv.lt/lt/naujienos/automobiliu-nuomos-bendrovei-skirta-bauda-del-duomenu-saugumo-pazeidimo-pagal-bendraji-duomenu-apsaugos-reglamenta> [žiūrėta 2022 m. sausio 11 d.].
72. Visuotinė lietuvių enciklopedija. *Tapatybės vagystės sąvoka* [interaktyvus]. Prieiga per internetą: <https://www.vle.lt/straipsnis/tapatybes-vagyste/> [žiūrėta 2022 m. vasario d.].

SANTRAUKA

Asmens duomenų vagystės, kaip nusikalstamos veikos, teorinės ir praktinės problemos

Andra Mažrimaitė

Magistro darbe analizuojamas asmens tapatybės vagystės, kaip nusikalstamos veikos, kriminalizavimo poreikis bei galimybės Lietuvoje. Visų pirma, aptariama asmens tapatybės vagystė sąvoka bei įvertinama ar asmens duomenis ir asmens tapatybę galima laikyti tapačiomis sąvokomis. Aptariamas asmens tapatybės vagystės istorinis vystymasis bei tai, kaip keičiantis laikotarpiams ir tobulėjant technologijoms vystėsi ir stiprėjo asmens tapatybės vagysčių atvejai. Paminima, jog šiais laikais tapatybės vagystės tapo itin dažnu ir nekontroliuojamu nusikaltimu, nes informacija apie asmenis yra prieinama visur. Be to, internetas itin palengvina tapatybės vagystės vykdymą. Darbe įvardijamos ir apibrėžiamos pagrindinės tapatybės vagystės formos, kadangi būtent šių veikų gilesnė analizė atspindi tokių veikų mastą ir padaromą žalą. Trečiajame šio darbo skyriuje pirmiausia atliekama užsienio šalių analizė pateikiant vertinimą, kaip tapatybės vagystė yra kriminalizuojama užsienio valstybėse, tokiose kaip Jungtinės Amerikos Valstijos, Prancūzija, Vokietija, Estija bei Latvija. Pereinant prie Lietuvos analizės – magistro darbe analizuojamas atskirų asmens duomenų vagystės elementų kriminalizavimas Lietuvoje bei atliekamas vertinimas ar asmens tapatybės vagystė gali būti vertinama kaip nusikaltimas asmens privataus gyvenimo pažeidžiamumui – daroma išvada, jog Lietuvos Respublikos Baudžiamojo kodekso 167-168 straipsniai, kalbantys apie asmens privataus gyvenimo pažeidimus, gali būti siejami tik su pirmąja tapatybės vagystės stadija – neteisėtu duomenų apie privatų žmogaus gyvenimą rinkimu. Galiausiai, atsižvelgiant į tai, jog magistro darbe įvertinama, kad Lietuvoje asmens tapatybės vagystė nėra laikoma savarankiška nusikalstama veika, paskutinėje darbo dalyje analizuojamas galimas asmens tapatybės vagystės, kaip nusikalstamos veikos, sudėties modelis. Išskiriami bei išsamiai aptariami objektyvieji ir subjektyvieji požymiai bei pateikiamas Lietuvos Respublikos baudžiamojo kodekso specialiosios dalies pakeitimo projektas.

SUMMARY

Theoretical and Practical Problems of Identity Theft as Criminal Act

Andra Mažrimaitė

This master thesis analyzes the need and possibilities for the criminalization of identity theft as a criminal act in Lithuania. In particular, the concept of identity theft is discussed and it is assessed whether personal data and identity can be regarded as identical concepts. The historical development of identity theft and the way in which personal identity theft has evolved and intensified as periods change and technology evolves are discussed. It is mentioned that identity theft has become an extremely common and uncontrollable crime these days, as information about individuals is available everywhere. In addition, the internet makes it much easier to commit identity theft. This work identifies and defines the main forms of identity theft, as a deeper analysis of these acts reflects the scale of such acts and the damage they cause. The third chapter of this paper first analyzes foreign countries by providing an assessment of how identity theft is criminalized in foreign countries such as the United States, France, Germany, Estonia, and Latvia. Turning to the analysis of Lithuania, the master's thesis analyzes the criminalization of individual elements of personal data theft in Lithuania and assesses whether the theft of a person's identity can be considered a crime against a person's privacy. It is concluded that Articles 167-168 of the Criminal Code of the Republic of Lithuania, which deal with violations of a person's private life, can be related only to the first stage of identity theft – the illegal collection of data about a person's private life. Finally, taking into account that the master's thesis concludes that identity theft is not considered an independent criminal offense in Lithuania, the last part of the thesis analyzes a possible model of identity theft as a criminal offense. Objective and subjective features are singled out and discussed in detail, and a possible draft amendment to the special part of the Criminal Code of the Republic of Lithuania is presented.