MYKOLO ROMERIO UNIVERSITETAS

SOCIALINĖS INFORMATIKOS FAKULTETAS

ELEKTRONINIO VERSLO KATEDRA

INGA DAUPARAITĖ

Informatikos teisė

TAPATYBĖS VAGYSTĖS ELEKTRONINĖJE ERDVĖJE TEISINIAI ASPEKTAI

Magistro baigiamasis darbas

Darbo vadovas –

doc. dr. Darius Štitilis

Vilnius, 2009

TURINYS

ĮVADAS **3**
1. TAPATYBĖS VAGYSTĖS ELEKTRONINĖJE ERDVĖJE SAMPRATA **7**
1.1. Elektroninė erdvė ir tapatybės vagystė kaip visuomenei pavojinga veika **7**
1.2. Tapatybės samprata ir tapatybės nustatymas **11**
1.3. Tapatybės vagystės sąvokų įvairovė **17**
1.4. Skyriaus apibendrinimas **23**
2. TAPATYBĖS VAGYSTĖS ELEKTRONINĖJE ERDVĖJE FORMOS IR BŪDAI **25**
2.1. Tapatybės vagystės elektroninėje erdvėje formos **25**
2.2. Asmens duomenims kylantys pavojai elektroninėje erdvėje **30**
2.3. Tapatybės vagystės elektroninėje erdvėje įvykdymo būdai **34**
2.4. Skyriaus apibendrinimas **40**
3. TAPATYBĖS VAGYSTĖS ELEKTRONINĖJE ERDVĖJE KRIMINALIZAVIMAS **41**
3.1. Tapatybės vagystės kriminalizavimas užsienio valstybėse **41**
3.2. Tapatybės vagystė kaip tarptautinė ir regioninė problema **44**
3.3. Tapatybės vagystės vertinimas Lietuvoje **46**
3.4. Atskirų tapatybės vagystės elementų kriminalizavimas Lietuvoje **51**
3.5. Skyriaus apibendrinimas **54**
4. TAPATYBĖS VAGYSTĖS ELEKTRONINĖJE ERDVĖJE SUDĖTIES MODELIS **56**
4.1. Tapatybės vagystės elektroninėje erdvėje sudėties objektyvieji požymiai **56**
4.2. Tapatybės vagystės elektroninėje erdvėje sudėties subjektyvieji požymiai **60**
4.3. Lietuvos Respublikos baudžiamojo kodekso specialiosios dalies pakeitimo projektas **62**
4.4. Skyriaus apibendrinimas **64**
IŠVADOS **66**
PASIŪLYMAI **69**
LITERATŪRA **71**
SANTRAUKA **77**
SUMMARY **79**

ĮVADAS

Šiuolaikinė informacinė visuomenė jau nebeįsivaizduoja savo gyvenimo be informacinių ir ryšio technologijų, kuriomis naudojantis tampa prieinama elektroninė erdvė. Elektroninė erdvė – tai ne kas kita, kaip mūsų visuomenės atspindys; tai puiki terpė ne tik teisėtiems tikslams pasiekti, bet ir pavojingoms, priešingoms teisei veikoms atlikti bei jas atliekančių subjektų išradingumui parodyti: efektyvūs veiksmai (informacijos siuntimas, gavimas, saugojimas, apdorojimas – visi veiksmai, atliekami su informacinėmis sistemomis) yra atliekami per atstumą, pasinaudojant informacinėmis technologijomis, pačiais įvairiausiais, paprastam elektroninės erdvės naudotojui dažniausiai ne visada suprantamais ir (ar) pastebimais, būdais.

Nors informacinės technologijos ir socialiniai teisiniai reiškiniai (taip pat ir nusikalstamos, pavojingos veikos) elektroninėje erdvėje visų pirma turi būti reglamentuojami remiantis tokiais pačiais teisės principais kaip ir tradiciniai, neginčytina yra tai, kad elektroninėje erdvėje susiklostantys visuomeniniai santykiai turi unikalių, specifinių bruožų. Todėl nusikalstamos, pavojingos veikos elektroninėje erdvėje yra tikras iššūkis teisėsaugos institucijoms, grėsmė privatumui, asmens duomenų apsaugai, turtinėms teisėms ir interesams, o elektroninės erdvės globalus pobūdis lemia tai, kad nacionalinės teisinės iniciatyvos reglamentuojant elektroninę erdvę ir su ja susijusius socialinius reiškinius gali būti ne visada veiksmingos.

Per pastaruosius dešimt metų išaugo verslo teikiamų elektroninių paslaugų vartotojams mastas: daugelis verslo subjektų perkėlė savo veiklą (visą arba dalį jos) į elektroninę erdvę, finansų institucijos savo klientams siūlo elektroninės bankininkystės paslaugas, vartotojai įgyja vis daugiau patirties pirkdami prekes ar paslaugas internetu. Tačiau naudojantis elektroninėmis paslaugomis, vienas iš didžiausių pavojų, su kuriuo dažnai susiduria vartotojai, yra tapatybės vagystė elektroninėje erdvėje.

Tema aktuali tuo, kad tapatybės vagystė elektroninėje erdvėje yra naujas socialinis – teisinis 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.

Daugiausia teisinio neaiškumo sukelia tai, jog nei teisės aktuose ar teismų praktikoje, nei doktrinoje nėra įtvirtintos vienos bendros sąvokos tapatybės vagystės ar tapatybės vagystės elektroninėje erdvėje reiškiniui įvardyti: sutinkamos „tapatybės klastotės“, „piktnaudžiavimo tapatybe“, „tapatybės nusikaltimų“ sąvokos, kurios dažnai vartojamos kaip tapatybės vagystės sinonimai ir kurių turinys nagrinėjamame kontekste nėra aiškiai apibrėžtas.

Tapatybės vagystės atvejų daugėja, o pats reiškinys dėl nuolatinės informacinių ir ryšio technologijų pažangos įgyja naujų formų, kurios iš fizinės erdvės vis didesne apimtimi persikelia į

elektroninę erdvę. Pažymėtina, jog pirmieji tapatybės vagystės atvejai pasitaikė dar gerokai anksčiau nei atsirado internetas. Paprastai tradicinė tapatybės vagystė buvo – ir vis dar yra – atliekama panaudojant tokius metodus kaip „šiukšlių rinkimas“, mokėjimo kortelės vagystė, dingsties ieškojimas, „žiūrėjimas per petį“, duomenų nuskaitymas nuo kortelių apgaulės būdu arba kompiuterio vagystė. Tačiau per pastaruosius kelerius metus minėti metodai gerokai patobulėjo dėl sparčios interneto, informacinių bei ryšio technologijų plėtros, kuri, pavyzdžiui, suteikia galimybę tapatybės vagystės subjektams panaudoti duomenų vagystės metodą kenkėjiškų programų[1] ar nepageidaujamų elektroninio pašto žinučių pagalba.

Globalus elektroninės erdvės pobūdis ir specifinės jos savybės leidžia teisės pažeidėjams veikti pakankamai saugioje aplinkoje, nukreipti savo veiksmus bet kuria linkme ir veikti bet kurioje vietoje. Todėl ir tapatybės vagystė elektroninėje erdvėje yra globali problema: pasauliniu lygiu vyksta diskusijos, ar ši veika turėtų būti kriminalizuota ir ar tokios veikos sudėties įtraukimas į valstybių baudžiamuosius įstatymus padėtų efektyviau kovoti su šiuo reiškiniu. Daugelyje valstybių tapatybės vagystė *per se* apskritai nėra laikoma teisės pažeidimu, o patenka į įvairias išimtis, susijusias su duomenų slaptumu, apsauga ar klastote, už kuriuos galima asmenį patraukti baudžiamojon atsakomybėn. Tuo tarpu kitos valstybės laikosi nuomonės, jog tokios veikos yra specifinės, todėl tapatybės vagystės kriminalizavimas yra naudinga priemonė siekiant užkirsti kelią tapatybės vagystės sukeliamoms grėsmėms.

Taigi išsiskiria dvi konfrontuojančios pozicijos: vieni teigia, jog tapatybės vagystė turėtų būti kvalifikuojama kaip atskira, savo sudėtį turinti nusikalstama veika, t.y. siūlo šią veiką kriminalizuoti, argumentuodami, jog tais atvejais, kai užsienio valstybė neturi įstatymų, kriminalizuojančių tapatybės vagystę elektroninėje erdvėje, yra apsunkinamos informaciją renkančios valstybės galimybės rinkti tapatybės vagystės elektroninėje erdvėje įrodymus atitinkamoje užsienio valstybėje. Teisėsaugos institucijoms tokiu atveju nėra suteikiama pakankamai įgaliojimų veiksmingai kovoti su tokio pobūdžio veikomis, apsunkinamas tokių veikų susekimas, tyrimas ir baudžiamasis persekiojimas nacionaliniu bei tarptautiniu lygiu. Nesant galimybės rinkti įrodymus elektroniniu pavidalu, nėra užtikrinamas greitas ir patikimas tarptautinis bendradarbiavimas, kad būtų sustabdyti veiksmai, nukreipti prieš kompiuterinių sistemų, tinklų ir kompiuterinių duomenų konfidencialumą, vientisumą ir prieinamumą, ir nebūtų leidžiama tokių sistemų, tinklų ir duomenų netinkamai naudoti.

---

[1] Kenkėjiška programa šiame magistro baigiamajame darbe turėtų būti suprantama plačiąja prasme, t.y. kaip programinė įranga ar jos dalis, specialiai sukurta neteisėtai prisijungti ar sudaryti sąlygas neteisėtai prisijungti prie informacinės sistemos ar elektroninių ryšių tinklo, sutrikdyti ar pakeisti (įskaitant perimti valdymą) informacinės sistemos ar elektroninių ryšių tinklo veikimą, sunaikinti, sugadinti, ištrinti ar pakeisti elektroninius duomenis, panaikinti ar apriboti galimybę naudotis elektroniniais duomenimis, sudaryti sąlygas neteisėtai pasisavinti ar kitaip panaudoti neviešus elektroninius duomenis tokios teisės neturintiems asmenims (Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus 2009 m. kovo 20 d. įsakymu Nr. IV-348 patvirtintų Nacionalinio elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimų padalinio veiklos nuostatų 2.8 p.).

Šios pozicijos oponentai tapatybės vagystę traktuoja kaip priemonę teisės pažeidimams ir (ar) nusikalstamoms veikoms atlikti ir teigia, jog ši veika patenka į jau kriminalizuotas veikas reglamentuojančių straipsnių veikimo sritį, todėl tapatybės vagystės kriminalizavimas nėra būtinas.

Pažymėtina ir tai, jog daugelyje šalių (ne išimtis ir Lietuvos Respublika) tapatybės vagystė ir (ar) tapatybės vagystė elektroninėje erdvėje nėra kvalifikuojama kaip atskira nusikalstama veika, o remiantis valstybių, kuriose tapatybės vagystė yra kriminalizuota, teisės aktais, taip ir nėra aišku, kokie objektyvieji ir subjektyvieji požymiai turėtų būti įtraukti į šios veikos sudėtį.

Magistro baigiamojo darbo **tyrimo objektas** – tapatybės vagystė elektroninėje erdvėje kaip socialinis – teisinis reiškinys.

Tyrimo dalykas – tarptautinės teisės, Europos Sąjungos, Lietuvos Respublikos ir užsienio šalių teisės normos, reglamentuojančios tapatybės vagystę elektroninėje erdvėje ir su ja susijusius visuomeninius teisinius santykius, taip pat doktrina, kurioje analizuojami šie klausimai.

Tyrimo tikslas – išnagrinėti tapatybės vagystės elektroninėje erdvėje kaip socialinio – teisinio reiškinio teisinius aspektus. Tikslui pasiekti keliami šie **uždaviniai**:

1) apžvelgti tapatybės vagystę elektroninėje erdvėje, šios veikos sampratų įvairovę ir pateikti vieną bendrą sąvoką, kuri tiksliausiai apibūdintų šį socialinį – teisinį reiškinį;
2) aptarti tapatybės vagystės elektroninėje erdvėje, kaip vienos iš tapatybės vagystės rūšių, atlikimo būdus, jų specifiką ir šios veikos padarinius;
3) išnagrinėti tapatybės vagystės elektroninėje erdvėje kriminalizavimo aspektus;
4) išskirti ir išanalizuoti tapatybės vagystės elektroninėje erdvėje požymius bei pateikti šios veikos sudėties modelį.

Hipotezės:

1) tapatybės vagystė elektroninėje erdvėje yra kompleksinis, visuomenei pavojingas socialinis – teisinis reiškinys, pasižymintis formų ir atlikimo būdų įvairove;
2) siekiant efektyviai kovoti su šiuo reiškiniu, tapatybės vagystė elektroninėje erdvėje turi būti kvalifikuojama kaip savarankiška nusikalstama veika.

Magistro baigiamojo darbo **metodologinis pagrindas**: *analizės* (tapatybės vagystės elektroninėje erdvėje reiškinys išskaidomas į atskiras sudėtines dalis, požymius, savybes, kurie kiekvienas nagrinėjami atskirai, kad būtų atskleisti ir aptarti tiriamojo objekto ypatumai), *lingvistinis* (analizuojamas atitinkamų teisės aktų normų turinys), *loginis* (atskleidžiamos problemos, pateikiami galimi jų sprendimo būdai), *lyginamasis* (analizuojama tarptautinių, Europos Sąjungos, užsienio valstybių teisės aktų specifika lyginant su Lietuvos Respublikos baudžiamojo kodekso ir kitų nacionalinių teisės aktų nuostatomis), *dokumentų analizės* (atliekama atitinkamų teisės aktų, doktrininių teiginių analizė), *ekspertų vertinimo* (siekiama suprasti tapatybės vagystę elektroninėje erdvėje kaip socialinį teisinį reiškinį bei pateikti interpretacinį, holistinį šio reiškinio paaiškinimą),

istorinis (nagrinėjama tapatybės vagystės elektroninėje erdvėje evoliucija, aiškinamos šios pavojingos veikos priežastys ir pasekmės), *analitinis – kritinis* (akcentuojami esamo tapatybės vagystės elektroninėje erdvėje teisinio reguliavimo trūkumai, atliekamos teisės norminių aktų trūkumų įžvalgos), *apibendrinimo* (pateikiami tapatybės vagystės elektroninėje erdvėje bendrieji esminiai požymiai ir savybės, apibendrinama naudota literatūra, gauti empiriniai tyrimo duomenys, formuluojami pagrindiniai magistro baigiamojo darbo ir empirinio tyrimo teiginiai, mokslinės sąvokos, daromos galutinės išvados) metodai.

Darbo tema iš esmės plačiau nagrinėta tik užsienio autorių. Chris Reed, John Angel, Penny Duquenoy, Simon Jones, Barry G. Blundell, David Bainbridge, Jay Forder, Dan Svantesson, Judge Mohamed Chawki, Mohamed S. Abdel Wahab ir kiti šią temą nagrinėjo teisiniu aspektu, tuo tarpu John D. Sileo, Bob Sullivan šį reiškinį analizavo labiau iš socialinių perspektyvų. Minėti autoriai akcentavo didėjantį tapatybės vagysčių elektroninėje erdvėje skaičių, bandė pateikti galimus šios problemos sprendimo variantus, tačiau daugiausia dėmesio savo darbuose jie skyrė apskritai elektroniniams nusikaltimams, jurisdikcijos problemoms, o kalbėdami apie tapatybės vagystę elektroninėje erdvėje pateikdavo lakonišką sąvoką, pabrėždami, kad tai yra viena iš elektroninių nusikaltimų rūšių. Lietuvių autoriai – Mindaugas Kiškis, Rimantas Petrauskas, Irmantas Rotomskis, Darius Štitilis ir kiti – savo darbuose daugiausia dėmesio skyrė elektroninių nusikaltimų sampratai, rūšims, subjektams ir daromai žalai, 2001 m. Konvencijos dėl elektroninių nusikaltimų teisės normų analizei, o apie tapatybės vagystę elektroninėje erdvėje, kaip ir užsienio autoriai, užsiminė itin glaustai: tik tiek, kad tai yra vienas iš elektroninių nusikaltimų. Lietuvoje tik 2009 m. pabaigoje pasirodė pirmasis straipsnis[2], kuriame analizuojama tapatybės vagystė elektroninėje erdvėje ir pagrindiniai šios veikos požymiai. Vis dėlto pažymėtina, jog pasirinkta tema nebuvo išsamiai analizuota nei Lietuvos, nei užsienio šalių autorių.

Magistro baigiamajame darbe remiamasi užsienio autorių doktrina, tarptautinių, Europos Sąjungos, nacionalinių ir užsienio valstybių teisės aktų, reglamentuojančių tapatybės vagystę elektroninėje erdvėje, nuostatomis, tarptautinių, regioninių ir užsienio valstybių institucijų ir organizacijų atliktais tyrimais. Kadangi mokslinėje literatūroje nepakankamai atskleisti teisiniai tapatybės vagystės elektroninėje erdvėje aspektai, nėra atliktas išsamus šio socialinio – teisinio reiškinio įvertinimas, darbe aptariama tapatybės vagystės sampratų įvairovė, siekiant pateikti vieną, tiksliausiai šį reiškinį apibūdinančią sąvoką; atliekama lyginamoji šios veikos kriminalizavimo analizė ir teisinis įvertinimas; analizuojama, ar tapatybės vagystė elektroninėje erdvėje gali būti (turi būti) kvalifikuojama kaip savarankiška nusikalstama veika.

---

[2] **Štitilis D., Laurinaitis M.** Tapatybės vagystė elektroninėje erdvėje// Informacijos mokslai: mokslo darbai. – Vilnius, 2009, T. 50. P. 240-248.

1. TAPATYBĖS VAGYSTĖS ELEKTRONINĖJE ERDVĖJE SAMPRATA

Terminas „tapatybės vagystė“ bene kiekvieną dieną linksniuojamas užsienio valstybėse, pabrėžiant, jog šis reiškinys yra itin pavojingas ir galintis sukelti pačius įvairiausius neigiamus padarinius kiekvienam – tiek fiziniam, tiek ir juridiniam asmeniui. Tuo tarpu Lietuvoje tapatybės vagystė yra mistifikuojama: kartkartėmis, dažniausiai finansinių institucijų tinklapiuose, pasirodo pavieniai pranešimai, įspėjantys, jog minėtos institucijos savo klientų niekada neprašo patikslinti asmeninės prisijungimo prie šių institucijų informacinių sistemų informacijos. Tokių pranešimų tikslas – paskatinti elektroninės erdvės naudotojus būti budrius ir netapti internetinių sukčių aukomis.

Tačiau problema yra kur kas didesnė ir keleto atidumą skatinančių pranešimų per metus nepakanka efektyviam visuomenės švietimui apie vieną iš pavojingiausių reiškinių, susijusių su asmens duomenų ir privatumo apsauga. Todėl pirmiausia teisėsaugos, finansų sektoriaus ir kitos institucijos privalo tinkamai įvertinti kompleksinį, sudėtingą tapatybės vagystės reiškinį ir imtis atitinkamų veiksmų, kad maksimaliai būtų sumažinta tapatybės vagystės rizika.

Vertėtų atsisakyti požiūrio, jog tapatybės vagystė yra kažkas neapčiuopiamo ir tas kažkas gali nutikti bet kam, tik ne apdairiam, savo asmens duomenis ir asmeninę informaciją saugančiam elektroninės erdvės naudotojui. Nuo šios pavojingos veikos gali nukentėti bet kas. Tačiau šiame magistro baigiamajame darbe daugiausia dėmesio bus skiriama tapatybės vagystei, nukreiptai prieš fizinius asmenis, kurie šiuolaikinėje informacinėje visuomenėje kiekvieną dieną neišvengiamai susiduria su informacinėmis ir ryšio technologijomis.

Pirmo skyriaus tikslas – pateikti tapatybės vagystės sąvoką ir atskleisti šio reiškinio pavojingumą, aptariant tapatybės vagystės rūšis bei analizuojant šį reiškinį įvardijančių sąvokų įvairovę.

1.1. Elektroninė erdvė ir tapatybės vagystė kaip visuomenei pavojinga veika

Informacinė visuomenė, kuriai stebėtinai didelį poveikį daro informacinės ir ryšio technologijos, nuolat linksniuoja „interneto“ ir „elektroninės erdvės“ sąvokas, kurios, atrodo, niekuo nesiskiria, todėl vartojamos lygiagrečiai, kaip sinonimai. Tačiau iš principo tarp šių dviejų sąvokų negalima dėti lygybės ženklo, t.y. elektroninės erdvės nereikėtų tapatinti su internetu, kuris turėtų būti suprantamas tik kaip viena iš elektroninės erdvės paslaugų. Vis dėlto, šios dvi sąvokos labai dažnai vartojamos kaip sinonimai ir globali elektroninė erdvė tapatinama su internetu, kuris dar vadinamas tinklų tinklu. Kaip pabrėžia Darius Štitilis, yra manoma, kad vienas tinklas – internetas – neegzistuoja, jį sudaro grupės privačių bei viešųjų, tarpusavyje sujungtų tinklų. Todėl, pavyzdžiui, vietinis kompiuterių tinklas,

neprijungtas prie interneto, taip pat sudaro elektroninę erdvę[3]. Šiame magistro baigiamajame darbe sąvokos „internetas“ ir „elektroninė erdvė“ bus vartojamos kaip sinonimai.

Per pastaruosius dešimt metų internetas tapo atskira kompleksine infrastruktūra, kurioje vyksta konvergencija tarp audiovizualinių visuomenės informavimo, leidybos ir telekomunikacinių priemonių. Ši pigi ir vientisa komunikacijos sistema ne tik skatina jau esančių ir naujų pramonės šakų plėtrą, bet ir suteikia galimybę visuomenei skleisti kultūrą ir žinias. Šiandien internetas didina verslo subjektų komercines galimybes, jo pagalba galima tiesiogiai teikti viešąsias paslaugas, atnaujinti asmeninę ir socialinę veiklą. Internetas iš esmės pakeitė tiek pasaulinę ekonomiką, tiek pačią visuomenę, ir beveik nekyla abejonių, kad jo poveikis ateityje tik didės.

Numatydama galimą interneto reikšmės didėjimą, Ekonominio bendradarbiavimo ir plėtros organizacija (angl. *Organization for Economic Cooperation and Development*, toliau – OECD) dar 1998 m. pabrėžė elektroninių transakcijų svarbą pasaulinei ekonomikai ir pačiai visuomenei. Tačiau OECD taip pat įspėjo savo nares apie tokias tamsiąsias pokyčių puses, kaip naujų grėsmių, galinčių padaryti žalos klientams ir vartotojams elektroninėje erdvėje, atsiradimas. Elektroninėje erdvėje santykiai „akis – į – akį“ neegzistuoja, todėl gana sudėtinga nustatyti tikrąją asmens tapatybę atliekant elektronines transakcijas, tuo tarpu sukčiauti tokioje aplinkoje yra kur kas lengviau nei fizinėje erdvėje[4].

Pastaruoju metu vis didesne problema, su kuria elektroninėje erdvėje susiduria šiuolaikinė informacinė visuomenė, tampa tapatybės vagystė. Šis socialinis – teisinis reiškinys sparčiai plinta ir bent jau kol kas atrodo sunkiai sustabdomas: tiesiog stulbinančiai daugėja nukentėjusiųjų nuo tapatybės vagystės skaičius, jos sukeliama žala ir nukentėjusiųjų patirti nuostoliai skaičiuojami jau ne tūkstančiais ir net ne milijonais Jungtinių Amerikos Valstijų dolerių, o kur kas didesnėmis sumomis. Tuo tarpu teisėsaugos institucijos atrodo bejėgės kovoje su tapatybės vagystėmis užsiimančiais asmenimis, kurių sąjungininkėmis tampa nuolat besivystančios informacinės ir ryšio technologijos, įgalinančios atlikti pavojingas veikas vis sudėtingesniais ir paprastam elektroninės erdvės naudotojui vis sunkiau pastebimais būdais. Globalus elektroninės erdvės pobūdis ir specifinės jos savybės leidžia teisės pažeidėjams veikti pakankamai saugioje aplinkoje, nukreipti savo veiksmus bet kuria linkme ir veikti bet kurioje vietoje. Taip pat sudaromos puikios sąlygos pažeidėjams išlikti anonimiškiems, sukelti gerokai didesnę žalą didesniam vartotojų skaičiui per trumpesnį laiką nei veikiant fizinėje erdvėje. Be to, vienu metu galima atlikti keletą neteisėtų ir pavojingų veikų, o tokių veikų subjektu gali būti bet kas – netgi asmenys, nesulaukę reikiamo amžiaus, kad teisės aktų pagrindu kiltų atsakomybė.

---

[3] **Štitilis D.** Prekių ženklų naudojimas elektroninėje erdvėje: teisiniai aspektai// Jurisprudencija: mokslo darbai. – Vilnius, 2003, Nr. 41 (33). P. 141.

[4] **Online Identity Theft** – OECD, 2009. P. 15.
Prieinama internete: http://browse.oecdbookshop.org/oecd/pdfs/browseit/9309021E.PDF [žiūrėta 2009 06 02]

Aptariamas reiškinys pavojingas dar ir dėl to, kad yra kompleksinis – susijęs su vartotojų teisių, saugumo, privatumo, taisyklių, reglamentuojančių nepageidaujamos informacijos gavimą, pažeidimais.

Elektroninės erdvės specifika ir nuolatinė informacinių ir ryšio technologijų plėtra yra pagrindinės prielaidos naujoms pavojingoms veikoms atsirasti, jų įvykdymo būdams tobulėti. Dėl veikų, įvykdomų elektroninėje erdvėje, globalaus pobūdžio, latentiškumo, specifiškumo valstybės yra bejėgės efektyviai kovoti su tokiomis veikomis izoliuotai nuo kitų valstybių, todėl vien tik nacionalinio mechanizmo, kad būtų užkirstas kelias tokioms veikoms, nepakanka. Tačiau dėl minėtų priežasčių ir skirtingo tokio pobūdžio veikų vertinimo, sunku sukurti ir tarptautinį ar regioninį kovos su veikomis, atliekamomis elektroninėje erdvėje, mechanizmą, kuris būtų bendras visoms valstybėms ar bent jau daugeliui iš jų.

Tapatybės vagystė – viena iš pavojingų veikų, kurios gali būti atliekamos elektroninėje erdvėje ir kurių pavojingumas dažnai yra kur kas didesnis nei analogiškų veikų, atliekamų fizinėje erdvėje. Didžiausia problema, siekiant efektyviai kovoti su šia veika, yra ta, kad didžiuliu greičiu augant šio socialinio – teisinio reiškinio mastams, vis dar vyksta diskusijos, kas turėtų būti įvardijama tapatybės vagyste, ir ar ši veika turėtų būti kriminalizuota. Sąvokos apibrėžimai, dažniausiai naudojami statistiniais tikslais, skirtingose valstybėse skiriasi, be to, daugeliu atveju terminai „tapatybės vagystė“ ir „tapatybės klastotė“ vartojamos kaip sinonimai. Todėl pirmiausia valstybės, siekdamos efektyviai kovoti su neigiamų padarinių visuomenei sukeliančiais reiškiniais, turėtų juos tiksliai įvardyti ir visapusiškai įvertinti, o po to sukurti veiksmų planą ir vystyti tarptautinį bendradarbiavimą.

Pabrėžtina ir tai, kad patys asmenys dažnai nesuvokia, kokie svarbūs ir vertingi yra jų asmens duomenys, ir tokiais duomenimis disponuoja nesilaikydami elementarių saugumo taisyklių. Asmens duomenys reikalingi kiekviename gyvenimo žingsnyje: reikia įrodyti savo tapatybę norint atidaryti banko sąskaitą, gauti mokėjimo korteles, pajamas, paskolas, įkeisti turtą, gauti prekes ar paslaugas, kreipiantis dėl socialinių pašalpų ar išmokų ir pan. Todėl tapatybės vagystė ir yra pavojinga tuo, kad kitas asmuo, žinodamas jūsų asmeninius duomenis ir asmeninio gyvenimo detales, gali juos panaudoti labai įvairiai, dažniausiai turėdamas savanaudiškų ir neteisėtų ketinimų.

Tapatybės vagystės atveju nukentėjęs asmuo susiduria su įvairiomis problemomis, pavyzdžiui, sulaukia kreditorių reikalavimų dėl prievolių, kurių šalimi nebuvo, įvykdymo; gauna pranešimą apie išnaudotą kredito limitą; susiduria su nesėkmėmis ieškodamas darbo, norėdamas išsinuomoti būstą, nusipirkti automobilį ar pasiimti paskolą; toks asmuo gali būti netgi suimtas už nusikalstamas veikas, kurių nepadarė ir pan. Galimi tokios veikos padariniai tik patvirtina faktą, jog tai visuomenei itin pavojinga veika, kuri gali būti atliekama įvairiai – nuo neteisėto mokėjimo kortelės panaudojimo iki visiško kito asmens tapatybės perėmimo ir užvaldymo. Potencialių nukentėjusiųjų ratas taip pat gana platus, ypač jei tapatybės vagyste siekiama pasinaudoti finansų sistemoje: nuo valstybinių ir privačių institucijų, tvarkančių didelius asmens duomenų kiekius, iki finansinių paslaugų teikėjų ir vartotojų.

Veika pavojinga dar ir tuo, kad, viena vertus, problemos sprendimas labai priklauso nuo to, kas bus laikoma tapatybės vagyste, antra vertus, ne visada lengva įvertinti šios veikos sukeliamus padarinius. O padariniai, kaip minėta, gali būti labai įvairūs: tiesioginiai nuostoliai, pavyzdžiui, fizinių asmenų santaupų praradimas; tapatybės vagysčių atvejų tyrimo išlaidos verslo subjektams; išlaidos, susijusios su prevencijos priemonėmis, siekiant išvengti tapatybės vagysčių ateityje ir susigrąžinti prarastą reputaciją; netiesioginių nuostolių pavyzdžiais gali būti asmens reputacijos sumenkinimas, duomenų apie teistumą įrašymas asmens byloje ir pan.

Pabrėžtina ir tai, kad dėl latentiškumo, būdingo visoms pavojingoms veikoms, atliekamoms elektroninėje erdvėje, tapatybės vagystės elektroninėje erdvėje atveju teisėsaugos institucijoms sunku identifikuoti ir patraukti atsakomybėn tokias veikas įvykdžiusius asmenis. Oficialiai šių institucijų skelbiami statistiniai duomenys neatspindi visų tapatybės vagysčių atvejų, nes dažniausiai apie juos net nesužinoma. Tokį šių veikų latentiškumą lemia kelios priežastys: pirma, patiems informacinių technologijų naudotojams dažnai trūksta žinių, kad pastebėtų, jog jų tapatybė buvo pavogta (natūralus latentiškumas); antra, pačios aukos, net nukentėjusios nuo tapatybės vagystės elektroninėje erdvėje, vengia apie tai pranešti (dirbtinis latentiškumas), nes nenori atskleisti informacijos apie savo darbą, bijodamos viešumo arba prarasti gerą vardą, investuotojus, visuomenės pasitikėjimą (pavyzdžiui, bankai); trečia, aukos gali nepranešti dėl įsitikinimo, jog teisėsaugos institucijos tokios veikos atveju paprasčiausiai yra bejėgės.

Kalbant apie tapatybės vagystės praktinius pavyzdžius, galima paminėti keletą skandalų, susijusių su šiuo visuomenei pavojingu reiškiniu, kurie per paskutinius kelerius metus kilo Jungtinėje Karalystėje ir susilaukė pasaulinio susidomėjimo. 2007 m. pabaigoje buvo dingę du diskai, kuriuose buvo saugoma informacija apie 25 mln. britų, gaunančių valstybės socialines išmokas. Pusę milijono svarų (apie 2,1 mln. litų) kainavusi paieškos operacija buvo nesėkminga. Tų pačių metų gruodį taip pat paaiškėjo, jog viena JAV bendrovė pametė diskus, kuriuose buvo sukaupti duomenys apie maždaug 3 mln. britų, turinčių gauti vairuotojo pažymėjimus. 2008 m. iš vieno Gynybos ministerijos darbuotojo buvo pagrobtas kompiuteris, kuriame, kaip teigiama, buvo duomenys apie 600 tūkst. žmonių, siekiančių tarnauti Didžiosios Britanijos kariuomenėje. Tų pačių metų rugsėjį paaiškėjo, kad dingo diskas, kuriame buvo saugomi asmeniniai 5 tūkst. šalies kalėjimų darbuotojų duomenys, nors skubaus tyrimo metu buvo išsiaiškinta, kad diskas, kuriame buvo saugomi valstybės tarnautojų duomenys, dingo dar prieš metus[5]. Galima tik spėlioti, kam buvo panaudoti tokie didžiuliai šalies piliečių asmeninių duomenų kiekiai, o šie pavyzdžiai puikiai atskleidžia, kokiais mastais gali būti atliekama tapatybės vagystė ir koks gali būti potencialių nukentėjusiųjų skaičius.

---

[5] **Dingo kaip į vandenį**. Dienraštis Kauno diena, 2008 m. rugsėjo 8 d. Straipsnis prieinamas internete: http://kauno.diena.lt/dienrastis/pasaulis/dingo-kaip-i-vandeni-121179 [žiūrėta 2009 05 31]

Paminėtinas ir Lietuvoje įvykęs precedentas: 2009 m. spalio 13 d. visuomenės informavimo priemonėse mirgėjo antraštės, jog Lietuvos bankai masiškai blokuoja mokėjimo korteles dėl galimos duomenų vagystės. Kaip paaiškėjo, Lietuvos komerciniai bankai ėmėsi skubių apsaugos priemonių po to, kai į juos kreipėsi „MasterCard“ ir „Visa“ bedrovės, kurios pranešė, kad kai kurių klientų duomenys galėjo būti pavogti, todėl būtina žmonėms pakeisti mokėjimo korteles ir jų apsaugos duomenis. Tokių apsaugos priemonių ėmėsi „Swedbank“, „Nordea“, SEB ir „Danske“ bankai. Neoficialiais duomenimis, „Visa“ ir „MasterCard“ bendrovės nurodė blokuoti korteles, kuriomis buvo atsiskaitoma Ispanijoje. Minėtų bankų klientai, bandę atsiskaityti mokėjimo kortelėmis, nemaloniai nustebo: jiems buvo pranešta, kad kortelės neaptarnaujamos ir žmonės turėtų nedelsiant kreiptis į bankus; žmonėms buvo aiškinama, kad korteles ir jų apsaugos duomenis reikia pakeisti dėl galimos duomenų vagystės. „Danske“ bankas Lietuvoje blokavo daugiau kaip 600 kortelių, kiti bankai pranešė sąskaitas įšaldę mažesniam skaičiui klientų: „Swedbank“ blokavo apie 400 kortelių, SEB – 150[6].

Bankų atstovai primena, jog siekiant visiško duomenų saugumo mokėjimo kortele turi naudotis tik tas asmuo, kurio vardu ji yra išduota, ir PIN[7] kodas turi būti žinomas tik pačiam klientui (t.y. mokėjimo kortelės PIN kodą reikia saugoti atskirai nuo mokėjimo kortelės, ant mokėjimo kortelės ar ant kartu su ja laikomų daiktų nerašyti mokėjimo kortelės PIN kodo, įsiminus PIN kodą nedelsiant sunaikinti PIN kodo voką ir pan.). Klientas jokiais atvejais neturi atskleisti PIN kodo tretiesiems asmenims, net jei tai banko darbuotojai. Be to, klientai raginami būti dėmesingi naudojantis mokėjimo kortele, ypač atsiskaitant nežinomoje ar neįprastoje vietoje – užsienyje, internetu ar telefonu. Būnant užsienyje siūloma naudotis tik patikimų ir žinomų bankų bankomatais, pavyzdžiui, bankomatais, įrengtais bankų padaliniuose – tokiu atveju, kilus neaiškumams besinaudojant bankomatu, iš karto yra galimybė kreiptis į banko padalinio darbuotoją pagalbos.

1.2. Tapatybės samprata ir tapatybės nustatymas

Prieš pradedant analizuoti tapatybės vagystės sąvokų įvairovę, pirmiausia bent trumpai reikia aptarti pačios tapatybės sampratą, jos svarbą ir tapatybės nustatymo procesą.

---

[6] **Lietuvos bankai masiškai blokuoja mokėjimo korteles dėl galimos duomenų vagystės**. Dienraštis Lietuvos rytas, 2009 m. spalio 13 d. Straipsnis prieinamas internete: http://www.lrytas.lt/-12554330001253616142-lietuvos-bankai-masi%C5%A1kai-blokuoja-mok%C4%97jimo-korteles-d%C4%97l-galimos-duomen%C5%B3-vagyst%C4%97s-papildyta.htm [žiūrėta 2009 10 13]
Dėl galimos duomenų vagystės bankai blokuoja korteles. Dienraštis 15 min, 2009 m. spalio 13 d. Straipsnis prieinamas internete: http://www.15min.lt/naujiena/aktualu/pinigai/58/59976/ [žiūrėta 2009 10 13]
Bankai blokuoja korteles dėl galimos duomenų vagystės. Informacinis portalas Delfi: http://www.delfi.lt/news/economy/business/bankai-blokuoja-korteles-del-galimos-duomenu-vagystes.d?id=24664003 [žiūrėta 2009 10 13]

[7] PIN (angl. *personal identification number*) – asmens tapatybės numeris.

Tapatybė yra neatsiejama nuo asmens savojo aš ir individualumo suvokimo ir gali būti apibūdinama pagal tai, kaip ji nustatoma, pavyzdžiui, remiantis tam tikrais identifikatoriais. Identifikatoriai gali būti kelių rūšių: fiziniai arba biometriniai identifikatoriai, tokie kaip nuotraukos, akies rainelė, pirštų atspaudai, balso tembras; rašytiniai identifikatoriai apima asmens tapatybės patvirtinimo dokumentus – pasą, asmens tapatybės kortelę, gimimo liudijimą, taip pat prie šios kategorijos galima priskirti ir vairuotojo pažymėjimą; finansiniai identifikatoriai (pavyzdžiui, banko sąskaita, kreditinės kortelės informacija, darbo istorija) dažniausiai naudojami asmens tapatybės nustatymui verslo institucijų, bankų informacinėse sistemose, atliekant elektroninius pirkimus, mokėjimus, naudojantis elektroninėmis paslaugomis.

Vienas iš garsiausių tapatybės vagystės ekspertų Jungtinėse Amerikos Valstijose John D. Sileo[8] savo knygoje „Pavogti gyvenimai: nesudėtinga tapatybės vagystės prevencija“ (angl. *Stolen lives: identity theft prevention made simple*) teigia, kad tapatybė yra ne kas kita, kaip savęs apibūdinimas – mama, žmona, pianistas, autorius ir pan. Bet kai kalbame apie privatumą ir tapatybės vagystę, dėmesys turi būti kreipiamas į tapatybę, susijusią su asmens duomenimis – tai, pagal ką mus atpažįsta įvairios kompanijos, asociacijos ar valdžios institucijos. Autoriaus teigimu, tapatybę sudaro bet koks vardas, numeris ar kitas požymis, kuris suteikia informaciją apie mus arba kuriuo pasinaudojus galima prieiga prie kitų asmens duomenų[9].

Kai kalbama apie tapatybę, neišvengiamai susiduriama su sąvoka „asmens duomenys“. Todėl kyla klausimas: ar tapatybė gali būti suprantama kaip asmens duomenų sinonimas? Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas asmens duomenis apibrėžia kaip bet kokią informaciją, susijusią su fiziniu asmeniu – duomenų subjektu, kurio tapatybė yra žinoma arba gali būti tiesiogiai ar netiesiogiai nustatyta pasinaudojant tokiais duomenimis kaip asmens kodas, vienas arba keli asmeniui būdingi fizinio, fiziologinio, psichologinio, ekonominio, kultūrinio ar socialinio pobūdžio požymiai[10]. Įstatymo 2 str. 8 d. įtvirtinta ypatingų asmens duomenų sąvoka – tai duomenys, susiję su fizinio asmens rasine ar etnine kilme, politiniais, religiniais, filosofiniais ar kitais įsitikinimais, naryste profesinėse sąjungose, sveikata, lytiniu gyvenimu, taip pat informacija apie asmens teistumą. Minėto įstatymo teisės normų analizė leidžia daryti išvadą, kad asmens duomenų sąvoka yra labai plati ir apima daug duomenų, kurie *prima facie* turi menką ryšį su konkrečiu asmeniu, tačiau kuriais remiantis gali būti nustatyta asmens tapatybė.

Jau minėtas John D. Sileo pateikia sąrašą dalykų, kuriais remiantis gali būti nustatyta asmens tapatybė: pilnas vardas, socialinio draudimo numeris, bankų sąskaitų numeriai, gimimo data, adresas,

---

[8] Informacija apie John D. Sileo: http://www.thinklikeaspy.com/about-john-sileo.php [žiūrėta 2009 05 31]
[9] **Sileo J. D.** Stolen lives: identity theft prevention made simple, 2005. P. 31.
[10] **Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo** 2 str. 1 d. [aktuali redakcija nuo 2009-01-01]. Prieinama internete: http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=314940&p_query=&p_tr2= [žiūrėta 2009 04 25]

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 ekspertas pabrėžia, kad pateikiamas sąrašas nėra baigtinis[11].

Be minėtų duomenų, padedančių nustatyti asmens tapatybę, galima išskirti ir duomenis, kuriais asmens tapatybė nustatoma išskirtinai tik elektroninėje erdvėje. Asmuo elektroninėje erdvėje gali būti identifikuojamas naudojant elektroninio parašo technologiją, pagal kompiuterio tinklo plokštės MAC[12] adresą, kompiuterio IP adresą[13], *wireless*[14] stotelės adresą, domeno vardą ir pan.

Lietuvos ekspertų, kurių interesų sritis apima ir tapatybės vagystę, teigimu, tapatybė fizinėje erdvėje yra visiškai kitokia nei elektroninėje erdvėje. Fizinėje erdvėje savo tapatybę asmuo patvirtina vienu iš privalomų elementu – asmens dokumentu. Elektroninėje erdvėje tapatybę gali atstoti vardas ir slaptažodis. Vardas – kokio nors objekto sutartinis, tą objektą vienareikšmiškai identifikuojantis pavadinimas. Jis sistemoje turi būti unikalus. Slaptažodis – ženklų seka, žinoma tik paslaugos teikėjui ir jos vartotojui, pagal kurią paslaugos teikėjas patikrina į jį besikreipiančio tapatybę. Iš sąvokų matyti, kad elektroninėje erdvėje tapatybė sutapatinama su prisijungimo vardu ir slaptažodžiu ir visos saugumo užtikrinimo priemonės, tokios kaip skaitmeniniai sertifikatai ir kt., iš esmės atitinka asmens tapatybę elektroninėje erdvėje. Ekspertai nurodo, jog tapatybės nustatymo būdai elektroninėje erdvėje yra slaptažodžio valdymas vartotojo kompiuteryje, tapatybės nustatymas interneto paslaugų *proxy*[15] serveryje, tapatybę nustato trečioji šalis (naudojami specialūs protokolai), tapatybę nustato šalis, kuri yra viena iš pasitikėjimo grupės narių (pavyzdžiui, elektroninio deklaravimo sistemos Lietuvoje atveju pasitikėjimo šalis yra bankas, kuris identifikuoja vartotoją elektroninėje erdvėje).

Kalbant apie asmens identifikavimą elektroninėje erdvėje, svarbu paminėti, kad Lietuvoje nuo 2009 m. sausio 1 d. yra išduodamos asmens tapatybės kortelės, leidžiančios identifikuoti asmenį elektroninėje erdvėje. Naujosios asmens tapatybės kortelės ypatumas yra tas, kad joje yra integruotos dvi elektroninės laikmenos (lustai) – kontaktinė ir nekontaktinė. Nekontaktinėje laikmenoje fiksuojami asmens biometriniai duomenys: piliečio veido atvaizdas ir pirštų atspaudai, kurie leidžia lengviau apsaugoti kortelę nuo klastojimo bei sumažina galimybę ja pasinaudoti kitiems asmenims. Nekontaktinėje laikmenoje įrašytieji asmens duomenys apsaugoti nuo nuskaitymo nuotoliniu būdu,

---

[11] **Sileo J. D.** Stolen lives: identity theft prevention made simple, 2005. P. 32.
[12] MAC (angl. *Media Access Control*) adresas – tai tinklo plokštės identifikatorius.
[13] IP (*Internet Protocol*) adresas – kompiuterio identifikatorius tinkle, t.y. unikalus skaičius, naudojamas vienareikšmei duomenų paketo siuntėjo ir gavėjo identifikacijai.
[14] *Wireless* – bevielis ryšys.
[15] *Proxy* serveris – tai tarpinis serveris tarp kompiuterio ir interneto svetainės, kurią norima pasiekti, serverio.

nuo duomenų pakeitimo (bandymai pakeisti duomenis atpažįstami), nuo laikmenos pakeitimo kita (laikmenos „klonavimo“), pirštų atspaudus gali nuskaityti tiktai teisėta, sertifikuota įranga. Tuo tarpu asmens tapatybei patvirtinti elektroninėje erdvėje kontaktinėje laikmenoje įrašyti asmens atpažinimo elektroninėje erdvėje sertifikatas[16] ir kvalifikuotas, elektroniniam parašui skirtas, sertifikatas[17]. Tokiu būdu vartotojui suteikiama galimybė pasirašyti elektroninius dokumentus saugiu elektroniniu parašu, taip pat galimybė informacinėms sistemoms, kitiems paslaugų teikėjams identifikuoti asmenį jungiantis prie informacinių sistemų ir registrų, siunčiant duomenis internetu. Asmens atpažinimo elektroninėje erdvėje sertifikatas gali būti naudojamas jungiantis prie elektroninių paslaugų standartinės interneto naršyklės priemonėmis arba jungiantis prie specializuotos informacinės sistemos kokios nors organizacijos viduje. Teikiama asmens atpažinimo elektroninėje erdvėje galimybe galima naudotis tiktai tuo atveju, jei elektroninės paslaugos ar interneto portalai aiškiai deklaruoja tokią galimybę ir turi realizuotą reikiamą ir saugią sąsają vartotojo atpažinimui sertifikatu.

Pažymėtina, jog elektroninės erdvės sritys, kuriose asmuo identifikuojamas, yra labai įvairios: interneto svetainės, prekių ir paslaugų teikimas, elektroninio parašo sertifikato išdavimas, asmens dokumentų išdavimas ir kt. Todėl tapatybės svarbos supratimas ir tinkamas įvertinimas yra labai svarbus visais gyvenimo atvejais, nes fizinių ir juridinių asmenų atpažinimas ir diferenciacija yra paremta tam tikra identifikavimo forma, o asmens ir verslo subjektų ar valstybės institucijų dialogas be tapatybės nustatymo procedūrų vargu ar iš viso įmanomas. Visos priemonės, leidžiančios identifikuoti asmenį, nesvarbu, ar identifikavimo procesas vyksta elektroninėje ar fizinėje erdvėje, reikalingos asmenų santykiams su valstybės, privataus sektoriaus institucijomis ar tarp pačių asmenų realizuoti.

Aptariant asmens identifikavimą elektroninėje erdvėje, atskirai reikėtų aptarti asmens kodo, kuris yra vienas iš pagrindinių asmens tapatybės identifikatorių, panaudojimą. Asmens kodas – tai unikali skaitmenų seka[18]. Tokia asmens kodo struktūra atskleidžia asmeninę informaciją ir yra unikali bei nekeičiama identifikavimo priemonė, skirta duomenims apie asmenį kaupti gyventojų registre. Taip

---

[16] Remiantis Lietuvos Respublikos asmens tapatybės kortelės įstatymo 1 str. 1 d. ir 4 str. 1 d. **asmens atpažinimo elektroninėje erdvėje sertifikatas** yra apibrėžiamas kaip elektroninis liudijimas su įrašytais duomenimis apie pilietį (vardas (vardai), pavardė, lytis, gimimo data, asmens kodas, pilietybė) ir vidaus reikalų ministro nustatytais techniniais duomenimis ir patvirtinantis arba leidžiantis nustatyti asmens tapatybę elektroninėje erdvėje.

[17] Remiantis Lietuvos Respublikos asmens tapatybės kortelės įstatymo 1 str. 2 d., 4 str. 1 d. ir Lietuvos Respublikos elektroninio parašo įstatymo 2 str. 15 d. **kvalifikuotas sertifikatas** yra suprantamas kaip sertifikatas, kurį sudarė Vyriausybės ar jos įgaliotos institucijos nustatytus reikalavimus atitinkantis sertifikavimo paslaugų teikėjas. Šiame sertifikate yra tokie duomenys: užrašas, kad tai yra kvalifikuotas sertifikatas; sertifikavimo paslaugų teikėjo ir jo buveinės šalies identifikatoriai; pasirašančio asmens vardas ir pavardė arba slapyvardis; pasirašančio asmens specialūs atributai, jei tai reikalinga atsižvelgiant į numatomus sertifikato naudojimo tikslus; parašo tikrinimo duomenys, atitinkantys pasirašančio asmens turimus parašo formavimo duomenis; sertifikato galiojimo pradžios ir pabaigos terminai; sertifikato identifikatorius, suteiktas sertifikavimo paslaugų teikėjo; sertifikavimo paslaugų teikėjo saugus elektroninis parašas; sertifikato naudojimo paskirties apribojimai, jei tai nustatyta; leistina operacijų piniginė vertė, kada sertifikatas gali būti naudojamas, jei tai nustatyta. Sertifikate gali būti įrašyti duomenys apie pilietį (vardas (vardai), pavardė, lytis, gimimo data, asmens kodas, pilietybė) ir vidaus reikalų ministro nustatyti techniniai duomenys.

[18] **Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo** 7 str. 1 d. [aktuali redakcija nuo 2009-01-01]. Prieinama internete:
http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=314940&p_query=&p_tr2= [žiūrėta 2009 04 25]

pat pažymėtina, kad asmens kodas yra patogus požymis vienareikšmiškai identifikuoti asmenį visuose valstybės registruose ir informacinėse sistemose (dažnai ir privačiose), susieti asmenį su kitais šiose sistemose tvarkomais duomenimis. Tačiau asmens kodo naudojimas elektroninėje erdvėje kelia grėsmę, kad asmens kodo paplitimas leis sujungti įvairiose informacinėse sistemose tvarkomus asmens duomenis, o naudojamas atviru pavidalu kelia grėsmę, kad asmens tapatybė elektroninėje erdvėje gali būti pasisavinta.

Jungtinės Karalystės ministrų kabinetas 2002 m. ataskaitoje[19] išskyrė dviejų tipų tapatybės elementus – priskirtus ir biografinius. Remiantis šia ataskaita, įgyti tapatybės elementai, tokie kaip asmens vardas, gimimo data, informacija apie tėvus, yra asmens gimimo padarinys, t.y. nulemti paties gimimo fakto. Tuo tarpu biografiniai elementai atsiranda po gimimo. Į šią kategoriją patenka informacija apie asmens santykius su visuomene, kuri atsispindi iš tam tikrų dokumentų, pavyzdžiui, sudaromų rinkėjų sąrašų, išduodamų santuokos liudijimų, įgytą išsilavinimą ar specialią kvalifikaciją patvirtinančių dokumentų, darbo patirties istorijos.

Taigi fizinėje erdvėje asmens tapatybę nustatyti yra gana paprasta – tereikia paprašyti asmens tapatybę patvirtinančio dokumento ir įsitikinti, kad pateiktas dokumentas nėra suklastotas ar naudojamas neteisėtais tikslais. Tuo tarpu elektroninėje erdvėje asmens tapatybės nustatymo procedūra yra kur kas sudėtingesnė, nes tarp asmens ir institucijos, į kurią asmuo kreipiasi pasinaudodamas informacinėmis ir ryšio technologijomis, įsiterpia daugybė tarpininkų. Todėl elektroninėje erdvėje susiduriama ne tik su asmens tapatybės nustatymo mechanizmo įgyvendinimu, bet ir su vartotojų teisių, asmens duomenų ir privatumo apsaugos užtikrinimo klausimais. Dėl minėtų priežasčių reikia imtis papildomų priemonių, reikalingų asmens duomenų perdavimo saugumui užtikrinti, kad trečiosios šalys, neturinčios teisės susipažinti su tokiais duomenimis ar asmeninio pobūdžio informacija, negalėtų tokiais duomenimis ar informacija pasinaudoti.

Kalbant apie asmens tapatybės nustatymo procesą elektroninėje erdvėje, reikia pabrėžti, kad asmenų autentifikacija pirmiausia yra susijusi su individo tapatybės patikrinimu tam, kad būtų užtikrinta prieigos kontrolė prie tam tikrų resursų. Šis procesas yra susijęs su pačios sistemos saugumo užtikrinimu. Autentifikacija daugiausia yra paremta tuo, kuo asmuo naudojasi, pavyzdžiui, asmens tapatybės kortelė, pasas, kortelės, su integruotomis mikroschemomis; tuo, ką asmuo žino, pavyzdžiui, slaptažodis, PIN kodas, atsakymas į tam tikrą klausimą; arba tuo, kuo asmuo yra, pavyzdžiui, asmeniui būdingi bruožai – psichologiniai arba elgsenos (žr. schemą 1). Pirmasis ir antrasis autentefikacijos būdai turi keletą privalumų: yra sąlyginai nebrangūs, paprasti įdiegti ir patogūs vartotojui. Be to, slaptažodžiai ar kortelės, su integruotomis mikroschemomis, nesunkiai gali būti pakeisti pastaruosius pamiršus ar praradus. Daugelis sistemų, kurių veikimo principai paremti minėtais autentifikacijos

[19] United Kingdom Cabinet Office, *Identity Fraud: A Study*, Economic and Domestic Secretariat, London. Prieinama internete: http://www.identitycards.gov.uk/downloads/id_fraud-report.pdf [žiūrėta 2009 05 31]

būdais, dažniausiai blokuoja prisijungimą prie sąskaitų, keletą kartų neteisingai įvedus slaptažodį ar PIN kodą. Tačiau kortelės su integruotomis mikroschemomis, slaptažodžiai gali būti lengvai prarasti ar pavogti, taip pat jais gali būti dalijamasi, taigi aukštas saugumo lygis nėra užtikrinamas. Kadangi žinojimu ir naudojimusi paremtos autentifikacijos procedūros nėra labai patikimos, jos dažniausiai naudojamos kartu. Geriausias pavyzdys yra bankomatai, kurių atveju vyksta dviejų faktorių autentifikacija, reikalaujanti ne tik vartotojo PIN kodo (to, ką asmuo žino), bet ir fizinės kortelės (to, ką asmuo turi ir naudojasi).

Grynai techniniu požiūriu, tapatybė elektroninėje erdvėje yra tiktai skaitmeninis pseudonimas, kuris reprezentuoja asmenį. Todėl turi būti ir atitinkamos priemonės, kad būtų įrodyta, jog skaitmeninis pseudonimas tikrai priklauso konkrečiam asmeniui, teigiančiam, jog pseudonimas priklauso būtent jam. Kai naudojamas pseudonimas, visada privalo būti užtikrinama, kad jis naudojamas būtent to asmens, kuriam priklauso. Technologijos turėtų užtikrinti, kad asmuo galės nevaržomai naudotis skaitmeniniu pseudonimu, o kiti asmenys tokios galimybės neturės. Skirtingos technologijos siekia minėto tikslo, tačiau bent jau kol kas visada išlieka nesėkmės rizika.



1 schema. **Asmens autentifikacija, atliekama informacinių technologijų sistemų**

Šaltinis: Leenes (ed.), FIDIS network, deliverable 5.2b, ID-related crime: towards a common ground for interdisciplinary research, May 2006[20]. P. 80.

[20] Prieinama internete: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp5-del5.2b.ID-related_crime.pdf [žiūrėta 2009 06 01]

Taigi apibendrinant technologinį tapatybės patvirtinimo elektroninėje erdvėje aspektą, dar kartą pabrėžtina, kad informacinių technologijų sistemos asmenis sugeba atpažinti pagal tam tikrus identifikatorius: pagal tai, kas asmuo yra (panaudojant biometrinius metodus); pagal tai, kuo asmuo naudojasi, arba pagal tai, ką asmuo žino. Kiekviena identifikatorių kategorija iliustruoja, kas gali būti naudojama kaip konkretaus pseudonimo elektroninėje erdvėje įrodymas (patvirtinimas). Elektroninėje erdvėje autentifikacija dažniausiai yra paremta dviem metodais: tuo, ką asmuo turi, ir tuo, ką asmuo žino, kurie gali būti naudojami kartu siekiant užtikrinti didesnį saugumo lygį naudojantis informacinėmis sistemomis.

1.3. Tapatybės vagystės sąvokų įvairovė

Neteisėtos ir pavojingos veikos, kurios yra susijusios su asmens tapatybe ir asmenine informacija, dažniausiai apima suklastotos tapatybės naudojimą. Įvairiais būdais gali būti klastojamos tiek fizinių (gyvų, ligotų, ar net mirusių), tiek ir juridinių asmenų tapatybės, pavyzdžiui, Australijos ir Azijos politinių tyrimų centras, išskiria tapatybės klastotę (netikros, neegzistuojančios tapatybės sukūrimas); manipuliavimą tapatybe (asmens tapatybės pakeitimas, pakeičiant vieną ar daugiau tapatybės nustatymo elementų, pavyzdžiui, gali būti pakeičiamas vardas, gimimo data, adresas ir pan.); tapatybės vagystę (apsimetimas kitu asmeniu, kuris vėliau gali sudaryti sąlygas neteisėtiems veiksmams atlikti)[21].

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. Kai kurios valstybės pasirinko tapatybės vagystę traktuoti plačiąja prasme, t.y. apimant tapatybės vagystės atvejus tiek elektroninėje, tiek ir fizinėje erdvėje. Tačiau tik nedaugelis valstybių tapatybės vagystę laiko specifiniu teisės pažeidimu. Dėl tokio požiūrių skirtumo, skiriasi ir tapatybės vagystės teisinė prigimtis priklausomai nuo valstybių jurisdikcijos, kuri lemia teisinius prevencijos, patraukimo atsakomybėn ir skiriamų sankcijų skirtumus.

Tapatybės vagystė gali būti traktuojama kaip neteisėta veika, pasireiškianti daugeliu aspektų. Dažniausiai ji yra teisės pažeidimų ir nusikaltimų grandinės dalis. Be to, tapatybės vagystė gali sukelti įvairių padarinių. Toks šio reiškinio sudėtingumas ir lėmė skirtingą teisinį valstybių vertinimą: tapatybės vagystė gali būti kvalifikuojama kaip specifinis nusikaltimas, civilinės teisės pažeidimas ar

---

[21] ACPR, *Standardisation of definitions of identity crime terms: A step towards consistency*, Report Series No 145.3, March 2006. P. 7. Prieinama internete: http://www.acpr.gov.au/pdf/ACPR145_3.pdf [žiūrėta 2009 04 19]

kaip pasirengimas įvykdyti kitus nusikaltimus, tokius kaip sukčiavimas, klastojimas, terorizmas ar pinigų plovimas. Siekiant efektyviai kovoti su šiuo neigiamu reiškiniu, visų pirma būtina jį įvardyti.

OECD siūlo tokį tapatybės vagystės apibrėžimą: tapatybės vagystė yra tada, kai asmuo, neturėdamas tam teisės, įgyja, perduoda, laiko ar naudoja asmeninę informaciją apie fizinį ar juridinį asmenį, turėdamas tikslą įvykdyti arba tam, kad padarytų sukčiavimą arba kitus nusikaltimus[22].

Jungtinėse Amerikos Valstijose tapatybės vagystė traktuojama kaip specifinis nusikaltimas, kai kas nors tyčia perduoda, laiko, naudoja, neturėdamas tam teisės, kito asmens identifikavimo priemones, turėdamas tikslą įvykdyti arba tam, kad padarytų bet kokią neteisėtą veiką, kuri būtų Federacijos teisės pažeidimas arba kuri būtų sukus nusikaltimas pagal galiojančius Valstijos ar vietinius teisės aktus[23]. Iš šios normos matyti, kad tapatybės vagystė Jungtinėse Amerikos Valstijose *per se* laikoma nusikaltimu.

Jungtinėje Karalystėje apgaulė (angl. *fraud*) nebuvo laikoma specifiniu nusikaltimu. Tačiau remiantis 2006 m. Apgaulės Aktu, kuris įsigaliojo 2007 m. sausio 15 d., apgaulė tapo atskiru įstatymiškai įtvirtintu nusikaltimu, kuris apima ir apgaulę, įvykdytą elektroninėje erdvėje. Šis teisės aktas numato, kad apgaulė gali būti įvykdyta trimis būdais:

1) melagingai kreipiantis (nesąžiningai, turint tikslą gauti naudos, padaryti arba sukelti pavojų patirti nuostolių);

2) nepavykus atskleisti informacijos;

3) piktnaudžiaujant įgaliojimais[24].

Taip pat įtvirtinti nauji nusikaltimai, tokie kaip nesąžiningas paslaugų gavimas, jei už jas atliekami mokėjimai, pavyzdžiui, elektroninėje erdvėje apgaulės būdu pasinaudojant mokėjimo kortele; priemonių, įskaitant bet kokių programų ar asmens duomenų, laikomų elektronine forma, skirtų apgaulei įvykdyti ir kurios yra susijusios su tapatybės klastote, turėjimas; taip pat tokių priemonių gaminimas ir siūlymas, žinant, kad jos sukurtos ar pritaikytos atlikti apgavikiškus veiksmus[25]. Taigi pagal minėtą Jungtinės Karalystės teisės aktą tapatybės vagystė laikoma sudedamąja teisės pažeidimų arba nusikaltimų dalimi.

Australijoje, išskyrus Kvinslendą ir Pietų Australiją, tapatybės vagystė nelaikoma atskiru nusikaltimu, Kanadoje – taip pat. **Kanadoje** neteisėtą kito asmens tapatybės nustatymo duomenų panaudojimą apima baudžiamajame kodekse įtvirtintų nusikaltimų, tokių kaip apsimetimas kitu

---

[22] **Online Identity Theft** – OECD, 2009. P. 16.
Prieinama internete: http://browse.oecdbookshop.org/oecd/pdfs/browseit/9309021E.PDF [žiūrėta 2009 06 02]

[23] **United States Code** („U. S. C“), Title 18, Part I, Chapter 47, Section 1028 (a) (7). Prieinama internete: http://www.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00001028----000-.html [žiūrėta 2009 05 31]

[24] **Fraud Act 2006**. Prieinama internete:
http://www.opsi.gov.uk/acts/acts2006/pdf/ukpga_20060035_en.pdf [žiūrėta 2009 04 14]

[25] Out-Law news, Phishing kits banned by new Fraud Act, 13 November 2006. Straipsnis prieinamas internete: www.out-law.com/page-7469 [žiūrėta 2009 05 31]

asmeniu ar klastojimas, dispozicijos. Tačiau pasiruošimo įvykdyti nusikaltimą, pavyzdžiui, informacijos, padedančios nustatyti asmens tapatybę, rinkimas, turėjimas ir perdavimas paprastai nepatenka į įtvirtintų nusikaltimų sudėtis[26].

Kalbant apie tapatybės vagystę, dažnai sutinkamas „tapatybės klastotės“ terminas. Ypač daug dėmesio šių veikų prevencijai skiriama Jungtinėje Karalystėje. Jungtinės Karalystės vidaus reikalų ministerijos Tapatybės klastotės valdymo komitetas pasiūlė taip apibrėžti „tapatybės vagystės“ ir „tapatybės klastotės“ sąvokas:

- ***tapatybės vagystė*** įvyksta tada, kai gaunama pakankamai informacijos apie tapatybę tam, kad būtų lengviau įvykdyti tapatybės klastotę, nepriklausomai nuo to, ar auka yra gyva ar mirusi;
- ***tapatybės klastotė*** įvyksta tada, kai panaudojama netikra tapatybė ar kieno nors kito tapatybės duomenys tam, kad būtų padaryta neteisėta veika arba išvengta įsipareigojimų (atsakomybės) melagingai teigiant, kad jis arba ji buvo tapatybės klastotės auka, pavyzdžiui, netikros tapatybės arba kito asmens tapatybės duomenų (vardo, adreso, gimimo datos ir kt.) panaudojimas komercinei ar piniginei naudai gauti, prekėms įsigyti arba prieiti prie tam tikros įrangos ar paslaugų (banko sąskaitos atidarymas, paskolos prašymas arba prašymas išduoti mokėjimo kortelę)[27].

Sukčiavimų prevencijos organizacija Jungtinėje Karalystėje CIFAS pateikia tokius minėtų sąvokų apibrėžimus: ***tapatybės vagystė*** (dar žinoma kaip apsimetimas kitu asmeniu) yra neteisėtas kito asmens tapatybės (vardo, gimimo datos, gyvenamosios vietos adreso) pasisavinimas be jo žinios ar sutikimo. Šie tapatybės duomenys naudojami prekėms ir paslaugoms gauti tokio asmens vardu. ***Tapatybės klastotė*** – tai neteisėtai pasisavintos tapatybės panaudojimas nusikalstamai veikai padaryti, apgaulės būdu gauti prekes ir paslaugas. Paprastai tokia veika apima pavogtų ar suklastotų tapatybės dokumentų, tokių kaip pasas ar vairuotojo pažymėjimas, panaudojimą[28].

Iš apibrėžimų matyti, kad Jungtinės Karalystės vidaus reikalų ministerijos Tapatybės klastotės valdymo komitetas ir CIFAS pateikia kiek skirtingus apibrėžimus, tačiau turinio prasme jie yra panašūs. Minėtų institucijų ataskaitose ir pranešimuose terminai „tapatybės vagystė“ ir „tapatybės klastotė“ dažnai vartojami kaip sinonimai. Tačiau atlikus šių dviejų sąvokų turinio analizę, jas galima atriboti remiantis dviem pagrindiniais kriterijais – veiksmai su turimais duomenimis ir informacija, kuria remiantis galima identifikuoti kitą asmenį, ir tikslas, kuriuo tokie duomenys ir informacija buvo renkami. Tapatybės vagystės atveju pakanka paties neteisėto minėtų duomenų gavimo fakto, nepriklausomai nuo to, kokiu tikslu šie duomenys buvo gauti ir ar jie bus kaip nors panaudoti ateityje.

---

[26] **Kanados teisingumo departamento oficialus tinklapis**: http://www.justice.gc.ca/ [žiūrėta 2009 05 31]
Ten pat, http://www.justice.gc.ca/eng/news-nouv/nr-cp/2007/doc_32178.html [žiūrėta 2009 05 31]
Ten pat, http://www.justice.gc.ca/eng/news-nouv/nr-cp/2009/doc_32348.html [žiūrėta 2009 05 31]
Ten pat, http://www.justice.gc.ca/eng/news-nouv/nr-cp/2009/doc_32347.html [žiūrėta 2009 05 31]
[27] **Interneto tinklapis „Tapatybės vagystė; netapk auka“, sukurtas bendradarbiaujant Jungtinės Karalystės vyriausybei ir privačiam sektoriui**: http://www.identitytheft.org.uk/identity-crime-definitions.asp [žiūrėta 2009 05 31]
[28] **CIFAS interneto svetainė**: http://www.cifas.org.uk/default.asp?edit_id=561-56 [žiūrėta 2009 05 31]

Tuo tarpu tapatybės klastotės atveju duomenys ir informacija apie kitą asmenį yra renkami tam, kad jais pasinaudojus būtų galima gauti kokios nors apčiuopiamos, dažniausiai finansinės, naudos – jais pasinaudojant atliekama nusikalstama veika, pavyzdžiui, sukčiavimas, dokumentų klastojimas, pinigų plovimas ir pan. Taigi apibendrinant tapatybės vagystės ir tapatybės klastotės santykį, remiantis anksčiau minėtų organizacijų dokumentų analize, galima daryti išvadą, jog tapatybės vagystė yra priemonė tapatybės klastotei įvykdyti.

Toks terminų „tapatybės vagystė“ ir „tapatybės klastotė“ alternatyvus vartojimas kritikuotinas, nes remiantis anksčiau pateikta sąvokų turinio analize pats terminas „tapatybės klastotė“ šiame kontekste yra netikslus: klastoti – tai daryti ką nors netikra siekiant apgauti. Klastojimas gali būti dviejų rūšių: materialinis, kuris pasireiškia kaip netikro dokumento pagaminimas ar neteisėtas tikro dokumento turinio pakeitimas veikiant jo materialinę formą, pavyzdžiui, nuotraukos pakeitimas, vienos informacijos ištrynimas ir kitos įrašymas, parašo, antspaudo padirbimas ir pan., ir intelektinis, kuris pasireiškia kaip melagingos informacijos įrašymas į tikrą dokumentą. Klastojimo rūšių apibrėžimuose sutinkamas „tikro dokumento“ terminas turėtų būti suprantamas kaip dokumentas, surašytas ar kitaip pagamintas asmens, turinčio teisę tai padaryti, pavyzdžiui, sutartis, patvirtinta notaro, pasas, išduotas pasų poskyrio, pažymėjimas, surašytas atitinkamos institucijos, kvitas, išduotas banko ir pan. Regioninių ir nacionalinių organizacijų rekomendacinio pobūdžio teisės aktuose tapatybės klastotė apibrėžiama kaip netikros tapatybės ar kieno nors kito tapatybės duomenų panaudojimas tam, kad būtų padaryta neteisėta veika arba išvengta įsipareigojimų (atsakomybės) melagingai teigiant, kad jis arba ji buvo tapatybės klastotės auka. Tačiau tapatybės klastotė turėtų apimti tik tuos veiksmus, kuriais sukuriama netikro, realiai neegzistuojančio asmens tapatybė. Šiuo atveju tokia veika patektų į dokumentų klastojimą reglamentuojančių normų veikimo sritį.

Siekiant išvengti „tapatybės vagystės“ ir „tapatybės klastotės“ terminų sukeliamos painiavos, kurį sukelia minėtų sąvokų turinio netikslumai, siūlytina išskirti dvi tapatybės vagystės rūšis pagal turimą tikslą:

1) piktnaudžiavimą tapatybe, kai atliekami įvairūs veiksmai su kito asmens duomenimis ir (ar) asmenine informacija, siekiant apsimesti tuo asmeniu, iš kurio buvo gautos jį identifikuojančios priemonės, tačiau *neturint tikslo įvykdyti nusikalstamą veiką.* „Piktnaudžiavimo“ terminas pabrėžia veiksmų neleistinumo aspektą: net jei tokiais veiksmais realiai jokia žala ar nuostoliai nesukeliami, pats veiksmų atlikimo faktas yra priešingas teisei ir dažniausiai patenka į neteisėto asmens duomenų tvarkymo, už kurį paprastai numatoma administracinė atsakomybė, kategoriją. Tokios veikos pavyzdžiais galėtų būti prisijungimas prie socialinio tinklapio, informacinės sistemos, duomenų bazės, elektroninio pašto dėžutės naudojantis kito asmens prisijungimo duomenimis;

2) tapatybės vagystę (tapatybės pasisavinimas nusikalstamais tikslais), kai atliekami įvairūs veiksmai su kito asmens duomenimis ir (ar) asmenine informacija, siekiant apsimesti tuo asmeniu, iš

kurio buvo gautos jį identifikuojančios priemonės, ir *turint tikslą atlikti nusikalstamas veikas* – baudžiamuosius nusižengimus ir (ar) nusikaltimus, pavyzdžiui, sukčiauti, klastoti ir pan.

Chris Reed ir John Angel tapatybės vagystę apibūdina kaip asmens tapatybės nustatymo duomenų[29] gavimą pasinaudojant įvairiais slaptais metodais. Tokios veiklos tikslas – gauti duomenų apie asmenį tam, kad būtų galima imtis tolesnių nesąžiningų veiksmų, įskaitant naudojimąsi esamomis privilegijomis arba sukuriant naujas, pasinaudojant kito asmens tapatybe. Taip pat tapatybės vagystė gali būti pasirengimas įvykdyti klastojimą, tačiau nusikalstamos veikos gali būti kaip alternatyvūs tikslai[30].

Dar 2004 m. Bob Sullivan savo knygoje „Tavo blogasis dvynys: paskui tapatybės vagystės epidemiją“ (angl. *„Your evil twin: behind the identity theft epidemic“*) pabrėžė, kad tapatybės vagystė yra kur kas rimtesnis nusikaltimas nei buvo manyta iki tol ir yra pagrindinė priemonė terorizmui įvykdyti[31].

Penny Duquenoy, Simon Jones ir Barry G. Blundell tapatybės vagystę traktuoja kaip vieną iš greičiausiai plintančių elektroninių nusikaltimų, kuris apima ne tik mokėjimo kortelių numerių vagystę, bet ir socialinio draudimo ar socialinės apsaugos numerių, banko sąskaitų duomenų, adresų ir bet kokių kitų asmeninių duomenų, kuriuos asmuo gali naudoti savo tapatybei patvirtinti, vagystę. Šie duomenys gali būti panaudoti kaip visuma suklastoti tapatybei arba apsimesti kitu asmeniu užgrobiant pastarojo tapatybę, turint tikslą įvykdyti vagystę, klastotę ar kitus piktavališkus veiksmus[32]. Reikia atkreipti dėmesį, kad šie autoriai, pateikdami tapatybės vagystės apibrėžimą, iš esmės pateikia tapatybės vagystės elektroninėje erdvėje, kuri yra viena iš tapatybės vagystės rūšių, sąvoką, įvardydami ją kaip elektroninį nusikaltimą. Būtent įvykdymo vieta ir būdai, kuriais atliekami neteisėti veiksmai, yra pagrindiniai kriterijai, pagal kuriuos atribojamos dvi tapatybės vagystės rūšys: tapatybės vagystė fizinėje erdvėje ir tapatybės vagystė elektroninėje erdvėje. Apie tai plačiau rašoma 2 skyriaus 1 poskyryje „Tapatybės vagystės elektroninėje erdvėje formos“ ir 2 skyriaus 3 poskyryje „Tapatybės vagystės elektroninėje erdvėje įvykdymo būdai“.

Bob Sullivan tapatybės vagystę traktuoja kaip nusikaltimą, kuris kyla iš informacinės politikos struktūros – tai paaiškina, kodėl šį nusikaltimą taip lengva įvykdyti ir taip sunku patraukti kaltą asmenį atsakomybėn[33].

Pateiktas tapatybės vagystės sąvokas vienija keletas aspektų. Visų pirma, jose tapatybės vagystė akcentuojama kaip problema, susijusi su asmenine informacija. Dabartinė mūsų visuomenė tampa vis

---

[29] Tokie duomenys gali ne visada identifikuoti asmenį, pavyzdžiui, kas jūs esate; jie gali autentifikuoti, pavyzdžiui, ar jūs esate tikrasis vartotojas, ar autorizuoti, pavyzdžiui, ką jūs galite daryti, asmenį nebūtinai nustatant konkretaus individo tapatybę.
[30] **Computer Law: the law and regulation of information technology** / Edited by Reed C., Angel J., 2007. P. 558.
[31] **Sullivan B**. Your evil twin: behind the identity theft epidemic, 2004. P. 10.
[32] **Duquenoy P. et al.** Ethical, legal and professional issues in computing, 2008. P. 39.
[33] Ten pat. P. 12.

labiau priklausoma nuo asmeninės informacijos, reikalingos identifikuoti asmenis įvairiose gyvenimo situacijose. Pavyzdžiui, asmeninė informacija naudojama atsiskaitant su prekių tiekėjais, interneto paslaugų teikėjais, mobiliojo ryšio operatoriais; norint gauti prieigą prie finansinių institucijų, sveikatos organizacijų, mokyklų, valstybės institucijų sąskaitų, oficialių dokumentų sistemų ir pan.

Antra, esminiai tapatybės elementai remiasi nekintančiais ir patikrinamais požymiais, kurie paprastai oficialiai teikiami ir registruojami valstybės institucijų. Tai tokie asmens požymiai, kaip lytis, vardas, pavardė, gimimo data ir vieta, tėvų vardai ir pavardės, kai kuriose valstybėse – ir socialinio draudimo numeris. Tačiau asmenį galima identifikuoti ir remiantis daugybe kitų požymių, pavyzdžiui, kompiuterio vartotojo vardas ir slaptažodis, interneto puslapis, asmeninis tinklaraštis, IP adresas, elektroninio pašto adresas, banko sąskaitos numeris, PIN kodas ir kt.

Trečia, daugeliu atvejų, apibrėžiant tapatybės vagystę, nurodomas ir ryšys su sukčiavimu ar kitu nusikaltimu, t.y. dažniausiai teisės pažeidėjai, atlikdami tokio pobūdžio neteisėtus veiksmus, siekia padaryti įvairaus pobūdžio teisės pažeidimus. Tikslai gali būti labai įvairūs: gauti paskolą, pinigų, finansinės ar materialinės naudos, paslaugų, darbo privilegijų arba bet ko, kas turi vertę, pasinaudojant nukentėjusiojo duomenimis be jo sutikimo ar žinios. Piktnaudžiavimo tapatybe atveju pažeidėjai gali ne patys naudotis nukentėjusiojo tapatybe, o atlygintinai perduoti ją trečiajai šaliai, kuri, pavyzdžiui, įvykdys sukčiavimą, arba sukurti naujus neteisėtus asmens tapatybės dokumentus (pavyzdžiui, gimimo liudijimą, asmens tapatybės kortelę, pasą ar vairuotojo pažymėjimą).

Jau buvo trumpai užsiminta, kad tapatybės vagystė elektroninėje erdvėje yra tik viena iš sudėtingo tapatybės vagystės reiškinio rūšių. Taigi kalbant apie tapatybės vagystę elektroninėje erdvėje ypač svarbi reikšmė tenka elektroninei erdvei ir jos specifikai. Elektroninė erdvė turėtų būti suprantama kaip efektyvūs veiksmai (pavyzdžiui, informacijos siuntimas, gavimas, saugojimas, apdorojimas, t.y. visi veiksmai, atliekami su informacinėmis sistemomis) per atstumą, pasinaudojant informacinėmis technologijomis.

Per pastaruosius dešimt metų smarkiai išaugo verslo teikiamų elektroninių paslaugų vartotojams mastas. Tai lėmė kelios priežastys: daugelis verslo subjektų perkėlė savo veiklą (visą arba dalį jos) į elektroninę erdvę, finansų institucijos savo klientams siūlo elektroninės bankininkystės paslaugas, vartotojai įgyja vis daugiau patirties pirkdami prekes ir (ar) paslaugas internetu. Tačiau naudojantis elektroninėmis paslaugomis, vienas iš didžiausių pavojų, su kuriuo dažnai susiduria vartotojai, yra tapatybės vagystė elektroninėje erdvėje. Tai didina vartotojų nepasitikėjimą, susirūpinimą savo asmeninių duomenų saugumu, kai kurie vartotojai prioritetą teikia analogiškoms paslaugoms, teikiamoms tradicine forma, dėl ko nukenčia elektroninių mokėjimų, elektroninės bankininkystės paslaugos ir viso elektroninės komercijos sektoriaus plėtra.

Kalbant apie situaciją Lietuvoje, reikia pastebėti, jog nei teisės aktuose ar teismų praktikoje, nei doktrinoje taip pat nėra įtvirtintos tapatybės vagystės ar tapatybės vagystės elektroninėje erdvėje

sąvokos. Tapatybės vagystę galima bandyti aiškinti remiantis atskirų šios sąvokos elementų lingvistine analize. Pavyzdžiui, Dabartinės lietuvių kalbos žodynas[34] „tapatybę“ apibrėžia kaip tapatumą, t.y. identiškumą, tolygumą. Lietuvių kalbos žodyne[35] įtvirtinta iš esmės turinio prasme analogiška sąvoka – objekto (šiuo atveju – asmens) lygybė pačiam sau arba kitam objektui, tolygumas, vienodumas. Taigi tapatybės vagystė galėtų būti suprantama kaip duomenų, leidžiančių identifikuoti asmenį, pasisavinimas. Tuo tarpu tapatybės vagystė elektroninėje erdvėje galėtų būti suprantama kaip tapatybės vagystės atlikimas per atstumą, t.y. pasinaudojant informacinėmis ir ryšio technologijomis, dėl kurių nuolatinės pažangos tobulėja ir atsiranda naujų tapatybės vagystės elektroninėje erdvėje įvykdymo būdų. Vis dėlto toks lingvistinis sąvokos aiškinimas laikytinas pernelyg neinformatyviu ir neatskleidžiančiu tapatybės vagystės reiškinio esmės ir pagrindinių šios visuomenei pavojingos veikos požymių. Plačiau sąvokos „tapatybės vagystė“ ir „tapatybės vagystė elektroninėje erdvėje“ bei šių sąvokų turinio problematika Lietuvos kontekste aptariama 3 skyriaus 3 poskyryje „Tapatybės vagystės vertinimas Lietuvoje“.

1.4. Skyriaus apibendrinimas

Pastaruoju metu vis didesne problema, su kuria susiduria šiuolaikinė informacinė visuomenė, tampa tapatybės vagystė, ypač viena iš jos rūšių – tapatybės vagystė elektroninėje erdvėje. Šis socialinis – teisinis reiškinys sparčiai plinta ir bent jau kol kas atrodo sunkiai sustabdomas.

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. Nors tapatybės vagystė yra tarptautinio pobūdžio problema, tačiau nei tarptautiniuose, nei regioniniuose privalomos galios teisės aktuose nepateikiama tapatybės vagystės ar tapatybės vagystės elektroninėje erdvėje sąvoka. Šios veikos apibrėžimą siūlo kai kurios tarptautinės ir nacionalinės užsienio valstybių organizacijos, tačiau šių organizacijų teisės aktai yra tik rekomendacinio pobūdžio, o jų pateikiamas ataskaitas ir tyrimus galima vertinti tik kaip tam tikras gaires valstybėms narėms.

Nacionaliniu lygiu tapatybės vagystės sąvoka suprantama gana skirtingai, o tapatybės vagystės elektroninėje erdvėje sąvoka iš viso nepateikiama. Kai kurios valstybės pasirinko tapatybės vagystę traktuoti plačiąja prasme, t.y. apimant tapatybės vagystės atvejus tiek elektroninėje, tiek ir fizinėje erdvėje. Dažniausiai akcentuojama, jog tapatybės vagystė yra teisės pažeidimų ir nusikaltimų

---

[34] **Dabartinės lietuvių kalbos žodyno elektroninė versija**, prieinama internete: http://www.autoinfa.lt/webdic/ [žiūrėta 2009 06 02]

[35] **Lietuvių kalbos žodyno elektroninė versija**, prieinama internete: http://lkz.mch.mii.lt/Zodynas/Visas.asp [žiūrėta 2009 06 02]

grandinės dalis. Toks reiškinio sudėtingumas lėmė skirtingą teisinį valstybių vertinimą: tapatybės vagystė gali būti kvalifikuojama kaip specifinis nusikaltimas, civilinės teisės pažeidimas ar kaip pasirengimas įvykdyti kitus nusikaltimus, tokius kaip sukčiavimas, klastojimas, terorizmas ar pinigų plovimas. Mokslinėje literatūroje tapatybės vagystės sąvoka taip pat nepateikiama: išskiriami tik kai kurie sampratos fragmentai, be to, pasirinktas tapatybės vagystės traktavimas plačiąja prasme.

Atlikus tarptautinių, regioninių ir nacionalinių užsienio valstybių institucijų rekomendacinio pobūdžio teisės aktų ir užsienio mokslininkų formuojamos doktrinos analizę, siūlytinas toks tapatybės vagystės apibrėžimas: ***tapatybės vagystė*** *– tai bet kokie neteisėti veiksmai su kito asmens duomenimis ir (ar) asmenine informacija, leidžiančia identifikuoti kitą asmenį (tokių duomenų ir (ar) asmeninės informacijos perėmimas, įgijimas, laikymas, naudojimas, paskleidimas, disponavimas ar kitokių veiksmų atlikimas), turint tikslą apsimesti tuo asmeniu, iš kurio buvo gautos jį identifikuojančios priemonės, tam, kad būtų galima atlikti teisės pažeidimus ir (ar) nusikalstamas veikas.* Tuo tarpu ***tapatybės vagystė elektroninėje erdvėje*** galėtų būti suprantama kaip *tapatybės vagystės rūšis, kai tapatybės vagystė atliekama per atstumą, t.y. pasinaudojant informacinėmis ir ryšio technologijomis.*

Be to, tikslinga išskirti dvi tapatybės vagystės rūšis pagal šios veikos padarymo metu turimą tikslą:

1) piktnaudžiavimą tapatybe, kai atliekami įvairūs veiksmai su kito asmens duomenimis ir (ar) asmenine informacija, siekiant apsimesti tuo asmeniu, iš kurio buvo gautos jį identifikuojančios priemonės, tačiau *neturint tikslo įvykdyti nusikalstamą veiką*. Tokios veikos pavyzdžiais galėtų būti prisijungimas prie socialinio tinklapio ir bendravimas kito asmens vardu, prisijungimas prie informacinės sistemos, duomenų bazės ir domėjimasis joje esančiais kito asmens duomenimis ir (ar) asmenine informacija, jo turimu turtu, esamais įsiskolinimais, išlaidų ir pajamų balansu, prisijungimas prie elektroninio pašto dėžutės naudojantis kito asmens prisijungimo duomenimis ir svetimų laiškų skaitymas ar net rašymas naudojantis svetima elektroninio pašto dėžute ir pan.;

2) tapatybės vagystė (tapatybės pasisavinimas nusikalstamais tikslais), kai atliekami įvairūs veiksmai su kito asmens duomenimis ir (ar) asmenine informacija, siekiant apsimesti tuo asmeniu, iš kurio buvo gautos jį identifikuojančios priemonės, ir *turint tikslą atlikti nusikalstamas veikas* – baudžiamuosius nusižengimus ir (ar) nusikaltimus, pavyzdžiui, sukčiauti, klastoti ir pan.

Dažnai tapatybės vagystės kontekste sutinkamas tapatybės klastotės terminas: regioniniuose ir nacionaliniuose rekomendacinio pobūdžio teisės aktuose tapatybės klastotė apibrėžiama kaip netikros tapatybės ar kieno nors kito tapatybės duomenų panaudojimas tam, kad būtų padaryta neteisėta veika arba išvengta įsipareigojimų (atsakomybės) melagingai teigiant, kad jis arba ji buvo tapatybės klastotės auka. Tačiau tapatybės klastotė turėtų apimti tik tuos veiksmus, kuriais sukuriama netikro, realiai neegzistuojančio asmens tapatybė. Tokiu atveju ši veika patektų į dokumentų klastojimą reglamentuojančių normų veikimo sritį.

2. TAPATYBĖS VAGYSTĖS ELEKTRONINĖJE ERDVĖJE FORMOS IR BŪDAI

Tapatybės vagystė pagal įvykdymo vietą ir atlikimo būdą skirstoma į dvi rūšis: tapatybės vagystę fizinėje erdvėje ir tapatybės vagystę elektroninėje erdvėje. Abi šios veikos rūšys gali pasireikšti analogiškomis formomis, skiriasi tik būdas, kuriuo buvo gauti kito asmens duomenys bei asmeninė informacija, leidžianti identifikuoti asmenį, ir vieta, kurioje tokia veika buvo atlikta. Pirmuoju atveju naudojamos paprastos, ypatingų žinių nereikalaujančios priemonės (angl. *low-tech*), o veiksmai atliekami fizinėje erdvėje, patiriant tiesioginį kontaktą su nukentėjusiuoju. Antruoju atveju veikiama elektroninėje erdvėje naudojantis informacinėmis ir ryšio technologijomis (angl. *high-tech*), neteisėti veiksmai yra atliekami per atstumą, o tokios veikos įvykdymo būdai yra gana sudėtingi, reikalaujantys specifinių žinių ir dažniausiai nepastebimi paprastam elektroninės erdvės naudotojui.

Šiame skyriuje bus aptariama tapatybės vagystės elektroninėje erdvėje pasireiškimo formų ir įvykdymo būdų įvairovė, trumpai apžvelgiami tapatybės vagystės fizinėje erdvėje įvykdymo būdai bei pavojai, kylantys asmens duomenims ir asmeninei informacijai elektroninėje erdvėje.

2.1. Tapatybės vagystės elektroninėje erdvėje formos

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. Šiame poskyryje tapatybės vagystės formos taip pat bus aptariamos vadovaujantis tapatybės vagystės plačiąja prasme samprata, nes, kaip jau buvo minėta ir kaip bus matyti iš pateikiamos tapatybės vagystės formų įvairovės, abi tapatybės vagystės rūšys gali pasireikšti analogiškomis formomis.

Tapatybės vagystės atvejų vis daugėja, o pats reiškinys dėl nuolatinės informacinių ir ryšio technologijų pažangos įgyja vis naujų formų, kurios iš fizinės erdvės vis didesne apimtimi persikelia į elektroninę erdvę. Dėl šių priežasčių tapatybės vagystės formų baigtinį sąrašą galima sudaryti tik esamam momentui.

Dažniausiai išgirdus terminą „tapatybės vagystė“ pirma mintis kyla apie sukčiavimą ar kitas neteisėtas veikas finansų sektoriuje. Tačiau toks tapatybės vagystės suvokimas yra gana siauras ir neatskleidžiantis šio pavojingo reiškinio sudėtingumo, nes tapatybės vagystė gali pasireikšti įvairiomis formomis, kurių išskyrimas ir analizė yra svarbūs minėto reiškinio kompleksiškumui, sudėtingumui ir sritims, kuriose tapatybės vagystė gali pasireikšti, atskleidimui ir tinkamam įvertinimui.

Jungtinių Amerikos Valstijų Federalinė prekybos komisija išskiria tokias tapatybės vagystės formas, kurios dar gali būti įvardijamos kaip pavogtos tapatybės panaudojimo būdai [36]:

1) sukčiavimas, susijęs su kreditinėmis kortelėmis:

- kreditinių kortelių sąskaitų atidarymas nukentėjusiojo asmens vardu: kai pasinaudojama kreditine kortele, nukentėjusiojo nuo tapatybės vagystės skolos ataskaitoje atsiranda įrašai apie neapmokėtas sąskaitas;
- gali būti pakeistas adresas, kuriuo asmuo gauna sąskaitas, tam, kad daugiau neapmokėtų sąskaitų nebegautų, o kaltininkas galėtų apmokėti mokesčius naudodamasis nukentėjusiojo sąskaita. Kai sąskaitos siunčiamos kitu adresu, kartais gali būti sunku greitai išsiaiškinti kilusią problemą.

2) sukčiavimas, susijęs su telefono ar komunalinėmis paslaugomis:

- gali būti sudaromos telefono ar bevielio ryšio sutartys nukentėjusiojo vardu, mokami mokesčiai naudojantis nukentėjusiojo sąskaitomis;
- nukentėjusiojo asmens duomenys gali būti panaudoti siekiant gauti komunalines paslaugas, tokias kaip elektros, šilumos energija, kabelinė televizija ir pan.

3) sukčiavimas bankininkystės ir finansų sektoriuje:

- gali būti klastojami čekiai panaudojant nukentėjusiojo vardą ar sąskaitos numerį;
- gali būti atidaromos banko sąskaitos ir išrašomi netikri čekiai;
- gali būti klonuotas bankomato arba debetinės kortelės numeris ir atliekamos elektroninės piniginės operacijos ištuštinant nukentėjusiojo sąskaitas;
- gali būti paimama paskola nukentėjusiojo vardu.

4) sukčiavimas valstybiniame sektoriuje:

- gali būti gautas vairuotojo pažymėjimas ar asmens tapatybės kortelė su nukentėjusiojo vardu, tačiau su kaltininko nuotrauka;
- nukentėjusiojo asmens duomenys ir socialinio draudimo numeris gali būti panaudoti siekiant gauti valstybės pašalpas ar socialines išmokas;
- nukentėjusiojo asmeninė informacija gali būti panaudota siekiant nesąžiningai susigrąžinti mokesčius.

5) kiti sukčiavimo atvejai:

- naudodamasis nukentėjusiojo socialinio draudimo numeriu kaltininkas gali siekti įsidarbinti;
- pasinaudojus nukentėjusiojo asmens duomenimis gali būti išsinuomotas namas arba gaunamos medicininės paslaugos;
- nukentėjusiojo asmeninė informacija gali būti perduoda policijai arešto metu. Jei kaltininkas nepasirodo teisme ir neprisipažįsta, arešto orderis išduodamas nukentėjusiojo vardu ir kt.

---

[36] **Federalinės prekybos komisijos tinklapis, skirtas kovai su tapatybės vagyste**: http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html [žiūrėta 2009 04 26]

Atkreiptinas dėmesys, jog informacinės visuomenės nariai dažnai naudojasi elektroninėmis paslaugomis, kurios galėtų būti apibrėžiamos kaip teisės aktais reglamentuojamas gyventojų, verslo subjektų ir valdžios institucijų bendravimo procesas, kurio esmė – elektroninio verslo ir viešojo administravimo funkcijų realizavimas tarp šių paslaugų teikėjų ir gavėjų, vykdomas paslaugų gavėjo buvimo vietoje skaitmeniniu pavidalu, nuotoliniu būdu per internetą bei kitomis telekomunikacijų priemonėmis. Naudojantis elektroninėmis paslaugomis galima ne tik prisijungti prie elektroninės bankininkystės sistemos, bet ir deklaruoti pajamas, pateikti prašymus dokumentų išdavimui ar net įregistruoti juridinį asmenį. Todėl asmenys, išmanantys informacines ir ryšio technologijas, turintys specialių įgūdžių ir priešingų teisei ketinimų, elektroninę erdvę laiko sąlyginai saugia aplinka, suteikiančia galimybes didelio masto nusikalstamoms veikoms įvykdyti. Tereikia gauti keletą asmenį tam tikros institucijos informacinėje sistemoje identifikuojančių elementų, kad pastarieji, naudojantis elektroninėmis paslaugomis ir elektroninės erdvės suteikiamomis galimybėmis, būtų panaudoti įvairiais būdais ir sukeltų nukentėjusiajam neigiamų padarinių.

Čikagos Džono Maršalo teisės mokyklos teisės profesoriaus David E. Sorkin teigimu, tapatybės vagystė šiuo metu dažniausiai pasireiškia tokiomis formomis[37]:

1) **medicininė tapatybės vagystė** (angl. *Medical Identity Theft*): tai viena iš greitai plintančių apgaulės formų, kurios įgyvendinimą labai palengvina elektroninės erdvės savybės, o privatumą reglamentuojantys teisės aktai tai laiko sunkiai išsprendžiama problema. Pažeidėjai, gavę informaciją apie pacientą, gali padaryti didelės žalos: jie aukos vardu gali gauti tam tikros naudos, pavyzdžiui, apsilankymas pas gydytoją, medicininis gydymas, nuolaidos receptiniams vaistams.

2) **kompiuterinė tapatybės vagystė** (angl. *Computer Identity Theft*): interneto atsiradimas ir evoliucija sudarė puikias galimybes tapatybės vagystę įvykdyti pasinaudojant kompiuteriu. Šiuo atveju pažeidėjai savo aukas bando suklaidinti pasinaudodami suklastotais interneto tinklapiais arba elektroniniu paštu: naudodamiesi šiomis priemonėmis apsimeta esantys, pavyzdžiui, mokesčių surinkimo institucijų atstovai arba banko darbuotojai ir prašo patikslinti informaciją apie gyvenamosios vietos adresą, socialinio draudimo numerį, banko sąskaitų informaciją ir pan. Asmenys, atsakę į tokio pobūdžio klausimus, yra apgaunami – sukčius akimirksniu, pasinaudodamas gautais asmeniniais duomenimis, ištuština aukos kreditines korteles ir banko sąskaitas. Taip pat galimi atvejai, kai asmenys patys sukelia grėsmę savo asmeniniams duomenims be interneto įsikišimo, pavyzdžiui, parduodant nebereikalingą kompiuterį jo kietajame diske gali būti pakankamai asmeninės informacijos, kurios gali pakakti nusikalstamų ketinimų turinčiam asmeniui pasisavinti aukos sunkiai uždirbtus pinigus ir netgi tapatybę. Pabrėžtina, kad net iš kompiuterio ištrinta informacija technologijas

---

[37] **Teisės profesoriaus David E. Sorkin sukurtas tinklapis**: http://www.spamlaws.com/passport-identity-theft.html [žiūrėta 2009 05 31]

išmanančio asmens gali būti nesunkiai atkurta ir taip atskleistos, pavyzdžiui, elektroninio pašto žinutės, aukos vardas, pavardė, gimimo data ir kita jautri asmeninė informacija.

3) vairuotojo pažymėjimo tapatybės vagystė (angl. *Driver's License Identity Theft*): gali būti įvykdoma keliais būdais, pavyzdžiui, pateikiant dokumentus vairuotojo pažymėjimui gauti kito asmens vardu arba įvykdžius tapatybės vagystę. Tai sunkus nusikaltimas, kuris gali būti susijęs su daugeliu kitų nusikalstamų veikų, tokių kaip klastojimas, disponavimas suklastotomis tapatybės kortelėmis, dokumentų klastojimas vairuotojo pažymėjimui gauti, neteisėtas vairuotojo pažymėjimo naudojimas ir pan.

4) kreditinių kortelių tapatybės vagystė (angl. *Credit Cards Identity Theft*): sąlygoja ne tik neatsakingas kreditinių kortelių naudojimas ir pirkimo išsimokėtinai galimybė – bet kas gali tapti tokios tapatybės vagystės auka.

5) tapatybės vagystė elektroninėje erdvėje (angl. *Internet Identity Theft*): nuo „tradicinės" tapatybės vagystės skiriasi daugeliu aspektų. Pavyzdžiui, fizinėje erdvėje gali būti pavagiama piniginė, kurioje yra vairuotojo pažymėjimas, kreditinės, medicininės kortelės, kurių duomenimis nusikaltėlis gali pasinaudoti neteisėtiems mokėjimams atlikti ar dokumentų klastojimui. Tuo tarpu tapatybės vagystė elektroninėje erdvėje gali likti iš viso nepastebėta, t.y. aukos gali net nesužinoti, kad jų asmeninė informacija buvo pavogta, o kai sužino, dažniausiai jau būna per vėlu. Pradedantysis interneto vartotojas dažnai nežino, kad kompiuteris savo kietajame diske kaupia ir saugo daugybę asmeninės informacijos. Tokio pobūdžio informacija taip pat gali būti saugoma interneto naršyklės talpykloje, paieškos istorijoje ar laikinuosiuose interneto dokumentuose (angl. *Temporary Files*). Nors išvardytų priemonių tikslas yra palengvinti naudojimąsi interneto tinklu, jos taip pat fiksuoja tokią informaciją kaip vartotojų vardai, slaptažodžiai, adresai, kreditinių kortelių numeriai. Tokia vartotojo kompiuteryje saugoma informacija gali būti pavogta dviem būdais: pirma, pažeidėjas gali gauti prieigą perimdamas duomenis, siunčiamus neapsisaugojusio vartotojo, antra, galima įdiegti kenkėjišką programą, kuri sukurta tam, kad surinktų ir pažeidėjams pristatytų informaciją.

6) finansinė tapatybės vagystė (angl. *Financial Identity Theft*): apgavikas panaudoja kito asmens tapatybės nustatymo duomenis (tokius kaip vardas, socialinio draudimo ar banko sąskaitos numeris) apgaulei įvykdyti ir taip aukai sukelia finansinius nuostolius. Šiuo atveju tapatybės vagystė įvykdoma apgaulės būdu atidarant naują kreditinės kortelės ar banko sąskaitą. Kai išnaudojamas kredito limitas, auka lieka su neapmokėtomis sąskaitomis ir skolomis. Taip pat pažeidėjas gali perimti asmens tapatybę, kuri įgalina lengvai atidaryti banko sąskaitas, naudotis kreditinėmis kortelėmis, įsigyti transporto priemonę, įkeisti nekilnojamąjį turtą ar netgi įsidarbinti.

7) socialinio draudimo tapatybės vagystė (angl. *S. S Identity Theft*): pažeidėjai, žinodami socialinio draudimo numerį, gali sužinoti daugiau asmeninės informacijos apie auką, taip pat,

panaudoti jį, pavyzdžiui, paskolai gauti. Auka apie tokio tipo tapatybės vagystę dažniausiai sužino tada, kai sulaukia kreditorių reikalavimų dėl piniginių sandorių, kurių auka nesudarė, apmokėjimo.

8) banko operacijų tapatybės vagystė (angl. *Banking Identity Theft*): šiuo atveju banko klientai dažniausiai elektroniniu paštu informuojami, kad buvo pasikėsinta prisijungti prie jų banko sąskaitos, todėl siekiant užtikrinti saugumo reikalavimus prašoma paspausti ant nuorodos ir laikantis nurodytų taisyklių patvirtinti savo prisijungimo prie elektroninės banko sistemos duomenis. Nuoroda nukreipia klientą į suklastotą banko internetinį tinklapį, kuris atrodo identiškas originaliam. Tada kliento prašoma įvesti savo asmeninius duomenis, kuriais vėliau gali pasinaudoti apgavikas.

9) korporacinė tapatybės vagystė (angl. *Corporate Identity Theft*): sukelia neigiamas pasekmes verslo subjektams, pavyzdžiui, gavus prieigos duomenis prie verslo subjektų informacinės sistemos, gali būti pakeistas verslo vietos adresas, paskirtas kitas kompanijos vadovas, priimti nauji darbuotojai. Tokie apgaulės būdu „įdarbinti“ asmenys nesunkiai gali atsidaryti sąskaitas banke, nurodyti prekes pristatyti kitu adresu ir pan. – taip gali būti sugriauta verslo subjekto reputacija tuo pačiu metu paliekant neįvykdytus įsipareigojimus.

10) tapatybės vagystė klonuojant tapatybę (angl. *Identity Theft Cloning*): tai turėtų būti viena iš labiausiai bauginančių tapatybės vagystės atmainų. Šiuo atveju vietoj jūsų asmeninės informacijos vagystės finansinei naudai gauti ar tam, kad būtų įvykdytas kitas nusikaltimas jūsų vardu, „tapatybės klonai“ gyvena ir dirba taip, kaip jūs. Jie gali apmokėti sąskaitas, susižadėti, susituokti ar net sukurti šeimą kaip jūs. Kitaip tariant, tapatybės klonavimas reiškia, kad apsišaukėlis tiesiog gyvena jūsų gyvenimą tik kitoje vietoje. Pažeidėjai stengiasi surinkti kuo daugiau informacijos apie auką, pavyzdžiui, išsiaiškinti gimimo vietą, gatvę, kurioje auka užaugo, lankytą mokyklą, santykius su kitais moksleiviais, informaciją, susijusią su aukos tėvais ir kitais šeimos nariais, aukos nuolatinę gyvenamąją vietą, socialinio draudimo numerį ir t.t. Trumpiau tariant, „tapatybės klonai“ stengiasi apie auką sužinoti kiek galima daugiau informacijos tam, kad sugebėtų atsakyti į klausimus apie aukos gyvenimą, kurį gyvena jie. Dažniausiai tokie pažeidėjai yra kriminaliniai nusikaltėliai, besislapstantys nuo teisėsaugos institucijų, arba asmenys, kenčiantys nuo psichologinių problemų.

11) baudžiamoji tapatybės vagystė (angl. *Criminal Identity Theft*): apgavikas pasinaudoja nukentėjusiojo nuo tapatybės vagystės vardu arešto metu ar atliekant ikiteisminį tyrimą. Asmeninė informacija, kurią apgavikai pateikia teisėsaugos institucijoms, gali apimti vairuotojo pažymėjimą, gimimo datą ar socialinio draudimo numerį. Taip pat apgavikas gali suklastoti atitinkamą leidimą, kuriame būtų jo nuotrauka, bet kito asmens duomenys. Dažniausiai toks asmuo nesąžiningai įsigyja asmens tapatybės kortelę ar vairuotojo pažymėjimą aukos vardu, kuriuos vykstant ikiteisminiam tyrimui gali pateikti teisėsaugos pareigūnams. Ši tapatybės vagystės forma gali būti įvykdyta ir tada, kai panaudojami apgavikų draugų ar giminių vardai ir adresai, neparodant nuotraukos. Dažnai to pakanka, kad apsimetėlis išvengtų įtarimų arba jam būtų panaikintas areštas. Po to, kai apsimetėlis

pasirašo šaukimą į teismą ir pasižadėjimo atvykti pranešimą ir nustatytu laiku teisme nepasirodo, teisėjas priima sprendimą atvesdinti kaltinamąjį. Vietoj jo atvesdinamas nieko neįtariantis ir nekaltas kitas asmuo. Taip pat gali būti, kad apsimetėlis atvyks į teismo posėdį be aukos žinios. Tokiu atveju įrašas apie teistumą įtraukiamas į aukos asmens bylą duomenų bazėse.

12) paso tapatybės vagystė (angl. *Passport Identity Theft*): pasas – tai asmens dokumentas, patvirtinantis asmens tapatybę bei pilietybę ir skirtas vykti į užsienio valstybes, todėl dažnai tampa sukčių taikiniu. Pavogtas pasas gali būti parduodamas juodojoje rinkoje, kuri egzistuoja daugelyje valstybių ir labiausiai klesti dėl nelegalios imigracijos ir kitų neteisėtų veikų.

Profesoriaus siūlomas tapatybės vagystės formų sąrašas kritikuotinas, nes nedaromas skirtumas tarp sąvokų „forma“ ir „rūšis“. Rūšis turėtų būti suprantama kaip skirstymo pakopa, vienetas, išskirtas remiantis tam tikrais kriterijais – klasifikacijos pagrindu. Pavyzdžiui, tapatybės vagystė, pagal jos įvykdymo būdą ir atlikimo vietą gali būti skirstoma į tapatybės vagystę, atliekamą fizinėje erdvėje, ir tapatybės vagystę elektroninėje erdvėje; pagal įvykdymo tikslą – į tapatybės vagystę siekiant įgyvendinti nusikalstamus ketinimus (tapatybės pasisavinimas nusikalstamais tikslais) ir piktnaudžiavimą tapatybe, kai tokio tikslo nėra. Tuo tarpu „forma“ šiame kontekste turėtų būti suprantama kaip tapatybės vagystės reiškinio pasireiškimo būdas, atsižvelgiant į tai, kokioje srityje ar sektoriuje neturint tam teisės buvo panaudoti asmens duomenys ir (ar) asmeninė informacija, leidžianti identifikuoti kitą asmenį, t.y. tą asmenį, iš kurio buvo gautos jį identifikuojančios priemonės.

Trumpai apžvelgus formas, kuriomis dažniausiai pasireiškia tapatybės vagystė, būtų klaidinga teigti, jog viena tapatybės vagystės forma yra pavojingesnė už kitą. Jau pats tapatybės reiškinys yra kompleksiškas ir pavojingas nepriklausomai nuo jo pasireiškimo formos, nes kėsinimosi objektas yra asmens duomenys ir (ar) asmeninė informacija, kurios pagalba galima identifikuoti asmenį. Todėl iš esmės nesvarbu, kokia forma pasireiškia tapatybės vagystė, nes rezultatas kiekvienu atveju bus tas pats – kitas asmuo, neturėdamas tam teisės, turės galimybę pasinaudoti nukentėjusiojo asmens duomenimis ir (ar) informacija apie šį asmenį, o pačiam nukentėjusiajam iškils potencialus pavojus susidurti su neigiamomis pasekmėmis įvairiose gyvenimo srityse.

2.2. Asmens duomenims kylantys pavojai elektroninėje erdvėje

Siekiant visapusiškai išnagrinėti tapatybės vagystės elektroninėje erdvėje teisinius aspektus, būtina aptarti tam tikras elektroninės erdvės savybes, kurios sukelia potencialią riziką, kad tretieji asmenys, neturintys teisės susipažinti su tam tikra informacija, vis dėlto turės galimybę tai padaryti.

Naudojantis elektronine erdve galima naudotis neišsenkančiu informacijos kiekiu, tačiau kompiuteris interneto pagalba tampa pasiekiamas iš bet kurio kito kompiuterio. Dėl šios priežasties

iškyla grėsmė tapti piktų kėslų turinčių asmenų aukomis. Naršant internete nuolat yra rizika susidurti su vienu iš šių pavojų:

1) gali būti prarasti duomenys arba pažeistas asmens privatumas: informacija jūsų kompiuteryje gali būti sugadinta (sunaikinta ar iškraipyta) arba paviešinta internete;

2) kompiuteris gali būti apkrėstas virusu arba kirminu: įsilaužėlis jūsų kompiuteryje gali įdiegti programas, kurios pačios plinta internetu, gadina sistemines bylas ar kaip nors kitaip paveikia jūsų kompiuterį;

3) kompiuteris gali būti paverstas „zombiu“: įsilaužėlis gali jūsų kompiuterį panaudoti be jūsų žinios savo kėslams, pavyzdžiui, įdiegęs specialias programas, siųsti iš jūsų kompiuterio nepageidaujamas elektroninio pašto žinutes, panaudoti jį atakoms prieš kitus kompiuterius ir pan.[38]

Pati elektroninė erdvė pasižymi vartotojų gausa, sparčiais struktūros ir formos pokyčiais, informacijos tvarkymo decentralizavimu, teritorinių apribojimų nepaisymu ir pan.[39] Tokie įrankiai kaip paieškos sistemos, „slapukai“ (angl. *cookies*), elektroninės parduotuvės, elektroniniai atsiskaitymai, žaidimai, sveikatos diagnozė on-line[40], elektroninis paštas, pokalbių svetainės – tai tik keletas elektroninių paslaugų pavyzdžių, kurie visi pasižymi potencialia galimybe itin greitai ir efektyviai rinkti bei platinti asmens duomenis ir (ar) asmeninę informaciją, kurių pagalba, kaip jau buvo minėta anksčiau, galima nustatyti asmens tapatybę[41].

Galima pritarti Mindaugui Civilkai, kad asmens duomenų judėjimas, anksčiau vykęs tik su asmens duomenų subjekto žinia, šiuo metu vis dažniau tampa pasyvus ir slaptas, o didžiausią pavojų asmeninės informacijos konfidencialumui kelia šie išskirtinai su interneto paplitimu ir raida susiję reiškiniai:

1) naršymo duomenų rinkimas ir tvarkymas (angl. *browsing chaterring*): bet kokio apsilankymo internete metu naršyklė lankomos svetainės serveriui persiunčia informaciją, duomenis, kurie gali būti charakterizuojantys ir pakankamai individualizuojantys konkretų interneto puslapį aplankiusį asmenį (vartotoją), pavyzdžiui, priklausomai nuo konkrečios naršyklės, šie duomenys gali būti: operacinės sistemos pavadinimas ir jos versija, naršyklės pavadinimas ir jos versijos numeris, ieškomo puslapio pavadinimas, pasirinkta kalba, netgi programinė įranga, naudojama vartotojo kompiuteryje;

---

[38] **Lietuvos Respublikos ryšių reguliavimo tarnybos Tinklų ir informacijos saugumo skyriaus interneto tinklapis, skirtas informacijos saugai elektroninėje erdvėje**: http://www.esaugumas.lt/index.php?-229839978 [žiūrėta 2009 10 25]

[39] **J. R. Reidenberg, P. M. Schwartz**. Data protection law and on-line services: regulatory responses. ARETE Study, P. 4, 5. Prieinama internete: http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/regul_en.pdf [žiūrėta 2009 05 31]

[40] On-line – anglų kalbos terminas, kurio lietuviškas atitikmuo – tiesioginės kreipties režimas, t.y. darbo kompiuteriniame tinkle būdas, kai vienas asmuo iš savo kompiuterio siunčia elektroninius duomenų pranešimus į tinkle esantį kito subjekto ar interneto tarpininko kompiuterį, kuris iš karto apdoroja užklausą ir automatiškai atsiunčia besikreipiančiam subjektui atsakomąjį elektroninį duomenų pranešimą.

[41] **Civilka M.** Asmens duomenų teisinis reguliavimas interneto kontekste, p. 4.
Prieinama internete: http://media.search.lt/GetFile.php?OID=92932&FID=269994 [žiūrėta 2009 05 31]

2) nematomos nuorodos į kitus tinklapius (angl. *invisible hyperlinks*), kurios suteikia galimybę prieiti prie duomenų, esančių visai kitame serveryje negu tas, į kurį iš pradžių dėl tokios informacijos buvo kreiptasi;

3) „slapukai“ (angl. *cookies*): tai maži duomenų paketai, sukuriami interneto puslapio serverio ir laikomi vartotojo kompiuterio kietajame diske. Jie buvo sukurti siekiant padėti vartotojo – serverio santykiams, duomenų rinkimui ir gali būti serverio vertinami dabartinio ir vėlesnio apsilankymo tinklapyje metu. „Slapukai“ gali būti efektyviai naudojami palengvinti naršymo duomenų ir savanoriškai atskleistos informacijos rinkimą bei panaudojimą. Tai padaroma kiekvienam vartotojui suteikiant unikalų kodą ir saugant šį numerį „slapuke“. Šis kodas yra atkuriamas kiekvieną kartą aplankant tą konkretų tinklapį. Vėliau apie vartotoją surinkta informacija gali būti susieta su šiuo unikaliu kodu[42].

Visais šiais atvejais eiliniam interneto vartotojui nepastebimu būdu apie jį yra renkami ir kaupiami didžiuliai asmeninės informacijos kiekiai, kurių panaudojimo sritys iki galo nėra aiškios. Be to, iškyla dar vienas problemiškas klausimas: ar naršymo duomenys, IP adresas, „slapukai“ gali būti traktuojami kaip asmens duomenys?

Kai įeinama į tinklapį, iš vartotojo kompiuterio į serverį yra perduodama informacija apie vartotojo IP adresą, pagal kurį per domenų vardų sistemą gali būti nustatytas domeno vardas ir subjekto, kuris įregistravo domeno vardą, vardas (pavadinimas), buvimo vieta; informacija apie naršyklę, operacinę ir kompiuterinę sistemą; informacija apie vartotojo apsilankymo laiką, prieš tai aplankytą tinklapį; vartotojo elektroninio pašto adresas, o jei buvo naudojama paieškos sistema – ir visos užklausos. Lankymosi internete metu generuojami duomenys apie aplankytus tinklapius, juose praleistą laiką, siųstą ir gautą informaciją.

Tačiau kai kalbama apie IP adresą, kaip asmenį identifikuojantį požymį, būtina išskirti ir aptarti dvi IP adresų kategorijas – dinaminius (judrius) ir statinius (fiksuotus) IP adresus. Dinaminiai IP adresai nurodo duomenų judėjimo maršrutą, kurį apibrėžto apsilankymo tikslais kiekvienam naudotojo kompiuteriui priskiria interneto paslaugų teikėjas. Šiuo atveju tretieji asmenys IP adreso pagalba gali nustatyti tik interneto paslaugų teikėjo tapatybę. Vis dėlto, interneto paslaugų teikėjas IP adresą gali susieti su konkrečiu interneto vartotoju ar kompiuteriu – taip atsiranda galimybė identifikuoti interneto vartotoją. Interneto svetainės gali reikalauti, kad interneto vartotojas nurodytų savo vardą ir (arba) elektroninio pašto adresą – taip svetainės valdytojas gali nurodytam vardui priskirti IP adresą ir stebėti jį visų internete atliekamų operacijų metu. Bet jei vartotojas neatskleidžia jokios informacijos ir tarp serverio bei vartotojo interneto paslaugų teikėjo nėra jokio ryšio, identifikuoti įmanoma tik interneto paslaugų teikėją. Tuo tarpu fiksuoti IP adresai kiekvieno apsilankymo internete metu visuomet

---

[42] Ten pat, p. 4.

identifikuoja vieną ir tą patį konkretų kompiuterį. Tačiau ar tai, kad kompiuteris buvo identifikuotas, reiškia ir tai, kad identifikuojamas ir konkretus asmuo? Tai dar viena problema, kylanti naudojantis elektronine erdve, nes minėtu atveju identifikavus kompiuterį nebūtinai juo naudojasi vienas ir tas pats asmuo (pavyzdžiui, šeimos nariai naudojasi vienu kompiuteriu). Konkretus asmuo galėtų būti identifikuojamas, susiejus fiksuotą IP adresą su kitais duomenimis.

Analizuojant „slapukų“ funkcijas ir paskirtį, galima padaryti išvadą, jog informacija, surinkta „slapukų“ pagalba, neturėtų būti laikoma asmenine informacija. „Slapukai“ patys savaime neidentifikuoja konkretaus asmens, nes duomenys, surinkti „slapukų“ pagalba, yra labiau susiję su konkretaus kompiuterio panaudojimu nei su interneto vartotoju. Tačiau, pavyzdžiui, tiesioginės rinkodaros kompanijos *DoubleClick* „slapukus“ susieja su kitais duomenimis, esančiais *DoubleClick* duomenų sistemoje, tokiais kaip: valstybė, kurioje gyvena interneto naudotojas; interneto domenas (adresas), kuriam priklauso interneto naudotojas; įmonės, kurioje dirba interneto vartotojas, sritis; įmonės, kurioje dirba interneto vartotojas, apyvarta; internetinių paslaugų teikėjas; interneto vartotojo naudojama naršyklė; paieškos sistemose įvesti žodžiai ar jų junginiai[43]. Todėl šiuo atveju nekyla abejonių, kad tokie duomenys yra požymiai, būdingi konkretaus vartotojo ekonominiam, kultūriniam ar socialiniam identitetui, o „slapukai“ laikytini asmens duomenimis.

Akcentuotina tai, kad dažniausiai su problemomis susiduriama tada, kai tą patį kompiuterį ne visada naudoja tas pats asmuo, taip pat tada, kai įvairios reklamos agentūros mėgina asmens tapatybę nustatyti pagal konkretaus vartotojo vartojimo įpročius.

Pažymėtina, jog internetas buvo kuriamas kaip atviras tinklas. Jo veikimas yra pagrįstas TCP/IP protokolų[44] pagrindu, tačiau vien tik TCP/IP protokolai neužtikrina konfidencialumo, sąžiningumo, autentiškumo ar prieinamumo. Duomenų paketai gali būti persiunčiami kaip paprastas tekstas, t.y. neužšifruoti, ir tokiu atveju užpuolėjas gali juos pakeisti ar ištrinti. Taip pat gali būti perduodami suklastoti duomenų paketai su klaidinga siuntėjo informacija. Tai tėra tik kelios iš daugybės saugumo problemų, kurių nebuvo numatę ir iki šiol nėra išsprendę TCP/IP protokolai.

Apibendrinant galima teigti, jog šiame poskyryje pateikiamų pavojų, kylančių asmens duomenims elektroninėje erdvėje, sąrašas nėra baigtinis. Kiekvieną kartą vartotojui prisijungus prie interneto apie jį (dažniausiai jam net nežinant) yra surenkama daugybė informacijos, kurios rinkimo ir panaudojimo tikslai nėra aiškūs, tad visada išlieka rizika tapti potencialia teisės į privatumą ir duomenų apsaugą pažeidimo auka.

---

[43] ***DoubleClick*** **kompanijos tinklapis**: http://www.doubleclick.com/privacy/ [žiūrėta 2009 05 31]

[44] TCP/IP protokolai (angl. *Transmission control protocol*/*Internet Protocol*) – tai taisyklės ir susitarimai, apibrėžiantys kompiuterio perduodamo duomenų srauto skaidymo į paketus, perdavimo tinklu tam tikru maršrutu ar maršrutais ir gaunamų duomenų surinkimo iš paketų būdus.

2.3. Tapatybės vagystės elektroninėje erdvėje įvykdymo būdai

Tapatybės vagystės, kaip neteisėtos veikos, padarymo būdas gali būti suprantamas kaip subjekto elgesys iki neteisėtos veikos padarymo, neteisėtos veikos padarymo metu ir po neteisėtos veikos padarymo, paliekantis tam tikrus pėdsakus. Tai kompleksas subjekto veiksmų ruošiantis, darant ar slepiant neteisėtą veiką.

Pabrėžtina tai, kad pirmieji tapatybės vagystės atvejai pasitaikė dar gerokai anksčiau nei atsirado internetas. Paprastai tradicinė tapatybės vagystė buvo – ir vis dar yra – atliekama panaudojant tokius metodus kaip „šiukšlių rinkimas“, mokėjimo kortelės vagystė, dingsties ieškojimas, „žiūrėjimas per petį“, duomenų nuskaitymas nuo kortelių apgaulės būdu arba kompiuterio vagystė. Tačiau per pastaruosius metus minėti metodai gerokai patobulėjo dėl sparčios interneto, informacinių bei ryšio technologijų plėtros, kuri suteikia galimybę tapatybės vagystės subjektams kompiuteriuose įdiegti kenkėjiškas programas ar panaudoti duomenų vagystės metodą kenkėjiškų programų ar nepageidaujamų elektroninio pašto žinučių pagalba. Dėl minėtų priežasčių dauguma tapatybės vagyčių yra atliekama elektroninėje erdvėje pačiais įvairiausiais metodais, kurie kinta ir tobulėja kartu su technologijų pažanga.

Galima išskirti tokius tapatybės vagystės būdus, nepriklausomai nuo to, ar ji yra atliekama fizinėje ar elektroninėje erdvėje:

1) „**žiūrėjimas per petį**“ (angl. *shoulder surfing*): būnant netoli kito asmens stebima, kaip pastarasis įveda PIN kodą, slaptažodį, vartotojo vardą ar kitus asmeninius duomenis, arba klausomasi pokalbio, kai tokio pobūdžio duomenys perduodami telefonu;

2) „**šiukšlių rinkimas**“ (angl. *dumpster diving*): tarp šiukšlių ieškoma sąskaitų ar kitų dokumentų, kuriuose būtų nurodytas asmens vardas ar kita asmeninė informacija;

3) vagystė (angl. *stealing*): gali būti pavogtas elektroninis laiškas, įskaitant sąskaitų, kreditinių kortelių duomenis, kreditinių kortelių pasiūlymus, mokestinę informaciją, arba piniginė ar rankinė tam, kad būtų galima pasinaudoti jose esančiais kito asmens dokumentais;

4) kyšininkavimas (angl. *bribing*): stengiamasi papirkti darbuotojus, kurie gali prieiti prie asmeninės informacijos (pavyzdžiui, dirbančius valstybės institucijose, bankuose, kredito kompanijose ir pan.);

5) dingsties ieškojimas (angl. *pretexting*): prisidengiant melaginga dingstimi siekiama gauti informacijos apie kitą asmenį iš bankų, telefono ryšio operatorių, kredito kompanijų ir kitų institucijų;

6) duomenų nuskaitymas nuo kortelių apgaulės būdu (angl. *skimming*): specialių įrenginių, kurie gali nuskaityti ir išsaugoti mokėjimo kortelių duomenis, kai jomis atsiskaitoma, naudojimas;

7) duomenų vagystė (angl. *phishing*): apsimetant finansine ar kokia nors kita institucija (tarkim, loto kompanija) siunčiamos nepageidaujamos elektroninio pašto žinutės arba staiga ir

netikėtai pateikiami reklaminiai pasiūlymai (angl. *pop-up advertisements*), kuriais vartotoją stengiamasi suklaidinti ir įtikinti nurodyti asmeninę informaciją;

8) adreso pakeitimas (angl. *changing your address*): gyvenamosios vietos adreso pakeitimo formos užpildymas, po kurio visos sąskaitos ir kitas paštas pristatomas kitu adresu, kur asmeninė informacija tampa lengvai prieinama.

Aptarti tapatybės vagystės metodai, kaip jau minėta, naudojami atlikti šią pavojingą veiką nepriklausomai nuo to, ar ji padaroma fizinėje, ar elektroninėje erdvėje. Tačiau būtina paminėti, kad dėl elektroninės erdvės specifikos, galima išskirti būdus, kuriais tokio pobūdžio veika gali būti atliekama tik elektroninėje erdvėje, į pagalbą pasitelkiant informacines ir ryšio technologijas bei specialią programinę įrangą ar atitinkamus įrenginius. Pažymėtina ir tai, kad tapatybės vagystės subjektas, gavęs tam tikrus duomenis apie kitą asmenį fizinėje erdvėje, disponuodamas jais gali stengtis gauti daugiau to asmens duomenų elektroninėje erdvėje ir atvirkščiai.

Kalbant apie tapatybės vagystę elektroninėje erdvėje, dažniausiai su ja susiduriama tada, kai elektroninės erdvės naudotojai dalyvauja autentifikavimo procese. Šiame procese vartotojai, norėdami gauti prieigą prie atitinkamų informacinių sistemų, turi patvirtinti savo tapatybę. Čia ir kyla grėsmė tapti tapatybės vagystės auka, nes ne visi asmenys laikosi būtinų asmens duomenų apsaugos principų ir taisyklių, dažnai elgiamasi neapdairiai, neatidžiai ar nesuvokiama, kokią žalą gali sukelti internetinis sukčius, pasinaudojęs vartotojo neatsargumu ir gavęs jo asmens duomenis ar kitą asmeninę informaciją. Be to, turi būti užtikrinamas atsiskaitymų, duomenų tvarkymo[45] (t.y. bet kokio veiksmo, atliekamo su duomenimis) ir ryšio kanalų saugumas. Todėl, atsižvelgiant į tapatybės patvirtinimo elektroninėje erdvėje ypatybes, įvertinant informacinės sistemos ir programinės įrangos procesus, prieigos ir autentifikavimo procedūras, galima paminėti FIDIS pasiūlytą tapatybės vagystės (klastotės) įvykdymo būdų, klasifikaciją[46]:

I. Tapatybės vagystė:

1) tiesioginė ryšio, jungiančio asmenį ir autentifikavimo duomenis, ataka atliekant vieną ar kelis toliau išvardytus žingsnius:

• *panaudojant kompiuterinius kirminus*, kurie įdiegia kenkėjiškas programas (pavyzdžiui, *key logger*[47]). Tokiu būdu autentifikavimo duomenys yra tiesiogiai paimami iš asmens, manipuliuojant jo

---

[45] Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo 2 str. 4 d. duomenų tvarkymas apibrėžiamas kaip bet kuris su asmens duomenimis atliekamas veiksmas: rinkimas, užrašymas, kaupimas, saugojimas, klasifikavimas, grupavimas, jungimas, keitimas (papildymas ar taisymas), teikimas, paskelbimas, naudojimas, loginės ir (arba) aritmetinės operacijos, paieška, skleidimas, naikinimas ar kitoks veiksmas arba veiksmų rinkinys.

[46] **Leenes** (ed.), FIDIS network, deliverable 5.2b, ID-related crime: towards a common ground for interdisciplinary research, May 2006, p. 83. Prieinama internete: http://www.fidis.net/resources/deliverables/forensic-implications/int-d52b000/doc/29/ [žiūrėta 2009 05 31]

[47] *Key logger* – anglų kalbos terminas, apibūdinantis programą arba techninę įrangą, kuri fiksuoja kiekvieną kompiuterio klaviatūros paspaudimą.

įvesties įrenginiais (dažniausiai vietiniu kompiuteriu). Tokia ataka vykdoma nesiremiant jokiais atrankos metodais ir yra nukreipta prieš daugelį įvesties įrenginių be tiesioginio kreipimosi į asmenį;

• *socialinė inžinerija*: naudojantis ryšio priemonėmis (pavyzdžiui, telefonu, elektroniniu paštu), autentifikavimo duomenys iš vartotojo gaunami tiesiogiai, vartotojui pateikiant įtikinančią priežastį atskleisti prašomus duomenis, tarkim, nurodant, kad tokie duomenys reikalingi įmonės informacinių technologijų departamento administraciniam personalui patikrinimo tikslais. Tokia ataka yra nukreipta prieš konkretų asmenį;

• *Trojos arkliai*[48] *ir kitos kenkėjiškos programos, siunčiamos elektroniniu paštu kaip priedai* (angl. *attachments*): pirmiausia neapibrėžtam vartotojų skaičiui išsiunčiama nepageidaujama elektroninio pašto žinutė, kurios priede yra kenkėjiška programa. Vartotojui perskaičius minėtą laišką ir atidarius laiško priedą, kenkėjiška programa automatiškai įdiegiama į vartotojo kompiuterį ir pradeda rinkti autentifikavimo duomenis;

• *apgaulės taktika prieš (biometrinius) jutiklius* (angl. *spoofing of (biometric) sensors*): veiksmai atliekami be asmens, su kuriuo tokie jutikliai susieti, žinios. Pirmiausia iš asmens gaunami reikalingi biometriniai duomenys, tokie kaip, pavyzdžiui, akių nuotrauka, kuri po to atspausdinama ir neteisėtai panaudojama. Ataka yra nukreipta prieš konkretų asmenį.

2) netiesioginė ataka, nukreipta prieš duomenis:

• *su asmeniu susijusių identifikatorių, duomenų, suteikiančių asmeniui tam tikras teises atlikti kai kuriuos veiksmus duomenų apdorojimo sistemoje, nuorodų paieška*: ataka gali būti nukreipta prieš visą duomenų bazę arba tik prieš tam tikrus duomenų įrašus;

• *manipuliavimas nuorodų duomenimis, susijusiais su asmeniu*: autentifikavimo duomenų perdavimas peradresuojamas taip, kad juos gautų internetinis sukčius, o ne informacinių technologijų sistemos, prie kurių turi teisę prisijungti teisėtas vartotojas;

• *duomenų vagystė* (angl. *phishing*): daugeliui vartotojų, pavyzdžiui, banko klientams, išsiunčiamos nepageidaujamos elektroninio pašto žinutės, kurios atrodo taip, tarsi būtų gautos iš patikimos (šiuo atveju – banko) institucijos. Dažniausiai žinutėje raginama paspausti ant pateikiamos nuorodos, kuri nukreipia į suklastotą internetinį tinklapį, iš pirmo žvilgsnio atrodantį lygiai taip pat, kaip originalus institucijos tinklapis. Tokia ataka yra nukreipta prieš ryšį tarp informacinės sistemos ir autentifikavimo duomenų (žr. 2 schemą, Ryšys 3). Suklastotame tinklapyje vartotojas apgaulės būdu įtikinamas įvesti savo autentifikavimo duomenis.

---

[48] Trojos arklys (angl. *Trojan horse*) – tai slaptas specialių programų įvedimas į svetimą programinę įrangą; naujos programos pradeda atlikti naujas, teisėto savininko neplanuotas funkcijas. Programa įrašoma šalia kitos programos arba įvedama į jos vidų ir tik tada pagrindinė programa atlieka vienokio ar kitokio pobūdžio pakeitimus; bendros pagrindinės programos funkcijos dėl to nesikeičia. Paprastai tokios programos yra sukurtos taip, kad pradėtų veikti praėjus tam tikram laikui arba atlikus tam tikrą operacijų skaičių.

II. „Žmogus viduryje“ (angl. *man in the middle*) **atakos**: leidžia atlikti tiek tiesiogines, tiek netiesiogines atakas. Šios rūšies atakų metu perimami komunikavimo duomenys, kuriais keičiasi vartotojas ir sistema. Atakos yra labai veiksmingos ir, be kita ko (pavyzdžiui, duomenų pakeitimo galimybės), suteikia galimybę įvairiais būdais atlikti tapatybės vagystę:

1) tapatybės vagystė, atliekama ieškant autentifikavimo duomenų, kai asmuo komunikacijos procese dalyvauja nesilaikydamas saugumo reikalavimų (žr. 2 schemą, tiesioginė Ryšys 1 ataka);

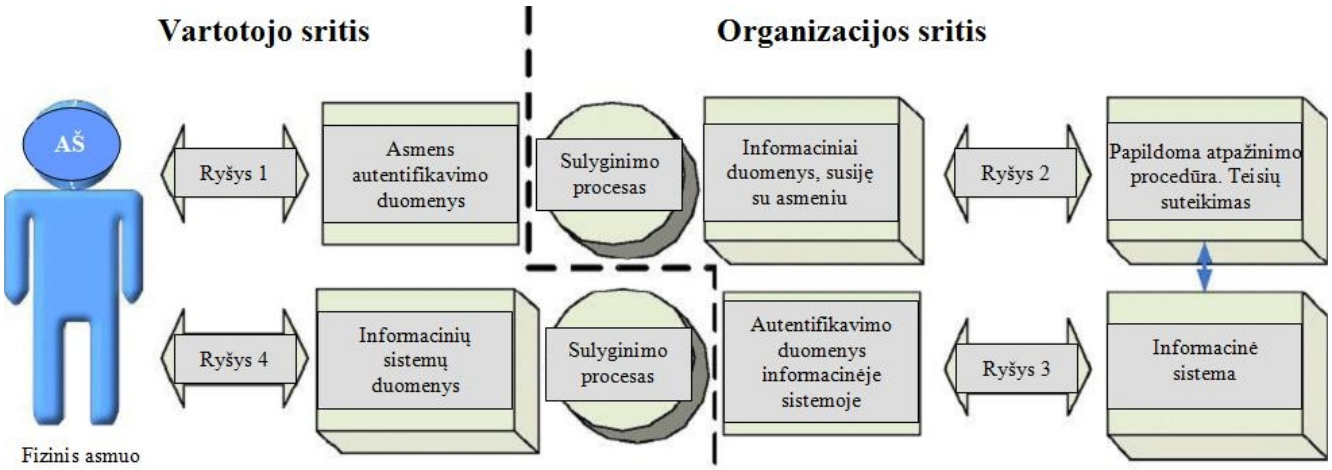
2) atsakomosios (angl. *replay*) ***atakos***: manipuliuojama interneto protokolo paketu, talpinančiu autentifikavimo duomenis su siuntėjo adresu. Toks protokolas yra persiunčiamas gaunančiajai sistemai. Ataka yra nukreipta prieš specialių įvesties įrenginių naudotoją (žr. 2 schemą, tiesioginė Ryšys 1 ataka);

3) tapatybės vagystė, atliekama peradresuojant pranešimą į suklastotą interneto tinklapį (pavyzdžiui, panaudojant apgaulės taktiką domenų vardų sistemos atžvilgiu (angl. *DNS-spoofing*)): Suklastotame interneto tinklapyje vartotojas apgaulės būdu įtikinamas įvesti savo autentifikavimo duomenis (žr. 2 schemą, netiesioginė Ryšys 3 ataka).

III. Nesąžiningas tapatybės perdavimas arba nesąžiningas apsikeitimas tapatybėmis: šiuo atveju asmuo bendrininkauja su internetiniu sukčiumi, sąmoningai duodamas jam savo autentifikavimo duomenis ir suvokdamas, kad šie duomenys bus panaudojami neteisėtai (žr. 2 schemą, ataka nukreipta prieš Ryšys 1).

IV. Tapatybės sukūrimas: internetinis sukčius paprastai pasinaudoja tam tikrais registracijos aspektais ir savo manipuliacinius veiksmus nukreipia prieš Ryšys 1 arba Ryšys 2 (žr. 2 schemą) tam, kad suardytų tarp jo, kaip fizinio asmens, ir duomenų, suteikiančių asmeniui tam tikras teises atlikti kai kuriuos veiksmus duomenų apdorojimo sistemoje, veiksmų grandinę. Taip internetinis sukčius, neturėdamas tam teisės, kurį laiką gali naudotis informacine sistema.

Elektroninėje erdvėje dėl įvairių sistemų ir programinės įrangos procesų prieiga prie informacinės sistemos ir autentifikavimo procesas yra sudėtingi, autentifikavimo procese dalyvauja keletas elementų ir įvairūs tarpininkai. Kiekvienas tarpininkas, pradedant nuo vartotojo ir baigiant institucija, teikiančia elektronines paslaugas ir turinčią informacinę sistemą, elektroninėje erdvėje vykstančio autentifikavimo proceso grandinėje pats savaime yra silpnoji grandis. Dėl šios priežasties yra nuolatinis pavojus, kad bus pasikėsinta į asmens duomenis ar asmeninę informaciją, perduodamą elektroninių ryšių tinklais ir būtiną efektyviam informacinės visuomenės narių tarpusavio komunikavimui. Todėl svarbu užtikrinti tapatybės nustatymo ir patvirtinimo proceso grandinės vientisumą.



2 schema. **Asmenų autentifikavimo procedūra informacinėse sistemose**

Šaltinis: Report on Identity Theft/Fraud, 2007[49].

Silpniausios grandinės dalys yra vartotojai, interneto paslaugų teikėjai, subjektai, atsakingi už duomenų tvarkymą, veikiantys kaip trečioji šalis, lygiai taip pat kaip duomenų bazės, valdomos valstybinio ir privataus sektoriaus institucijų. Bene pati silpniausia minėtos grandinės dalis yra patys vartotojai. Socialinės inžinerijos metodai, tokie kaip duomenų vagystė, yra nukreipiami prieš asmenis, kurie nepaiso saugos reikalavimų, o tokių asmenų naudojimasis neapsaugotu interneto ryšiu gali būti prilyginamas nerūpestingumui.

Techninės ir programinės įrangos gamintojai, kūrėjai bent jau kol kas nėra pajėgūs sukurti gaminio, kuris būtų absoliučiai apsaugotas nuo trečiųjų šalių įsikišimo. Dėl šios priežasties daugybė tapatybės vagysčių elektroninėje erdvėje yra atliekama prieigos taškų lygmenyje (darbo vieta, PDA[50], mobilieji telefonai, interneto kavinės ir pan.), pasinaudojant minėtų technologijų silpnosiomis vietomis (pavyzdžiui, panaudojant kompiuterinius kirminus, virusus, kitas kenkėjiškas programas).

Interneto paslaugų teikėjai taip pat užima nemenką vaidmenį tapatybės nustatymo ir patvirtinimo proceso grandinės vientisumo užtikrinime: neužtikrinant duomenų perdavimo saugumo, sudaromos palankios sąlygos tapatybės vagystei įvykdyti. Trečiosios šalys internete taip pat gali sudaryti palankias galimybes neteisėtiems ir pavojingiems veiksmams elektroninėje erdvėje atlikti, pavyzdžiui, domenų vardų registravimo procese gali būti tam tikrų spragų, kuriomis sėkmingai gali pasinaudoti

[49] **Report on Identity Theft/Fraud**. Fraud Prevention Expert Group. Brussels, 22 October 2007. Prieinama internete: http://ec.europa.eu/internal_market/fpeg/docs/id-theft-report_en.pdf [žiūrėta 2009 04 26]

[50] *Personal digital assistant* – anglų kalbos terminas, vartojamas mažiems, rankiniams įrenginiams, kurie suteikia galimybę naudotis įprastinėmis asmeninio kompiuterio funkcijomis, apibūdinti. Lietuviškas termino atitikmuo – delninukas.

apgavikai, atlikdami grobikiškus veiksmus spausdinimo klaidų (angl. *typographical error squatting*[51]) metodų pagalba. Verslo subjektai, vykdantys veiklą elektroninėje erdvėje, yra pagrindiniai vartotojų duomenų patikėtiniai (finansinės institucijos, bankai, paieškos sistemos, elektroninio pašto paslaugų teikėjai), todėl, jei šių subjektų informacinės sistemos nėra pakankamai apsaugotos, apgavikas gali nesunkiai į jas įsilaužti ir prieiti prie jose esančių duomenų.

Atsižvelgiant į tai, kas išdėstyta, ir siekiant išskirti būdus, būdingus tik tapatybės vagystei elektroninėje erdvėje, pažymėtina, kad dažniausiai tapatybės vagystės elektroninėje erdvėje atliekamos naudojant tokius metodus:

1) duomenų vagystė (angl. *phishing*, terminas kilęs nuo žodžių junginio *„fishing for your password“* – slaptažodžio žvejyba): tai vis dažniau pasitaikantis reiškinys, nuo kurio gali nukentėti bet kuris interneto vartotojas. Duomenų vagystė – tai tokia sukčiavimo forma prieš organizacijas ar privačius asmenis, kai pasinaudojant nepageidaujamomis elektroninio pašto žinutėmis ar falsifikuotais internetiniais tinklapiais siekiama išgauti prisijungimo prie informacinių sistemų slaptažodžius ar kitus konfidencialius duomenis;

2) falsifikuoti internetiniai tinklalapiai (angl. *scam*): tai atakos, kurios pagrįstos padirbtu kokios nors institucijos (pvz., banko) tinklalapiu. Tinklapis yra tiksliai nukopijuotas arba gali būti pavogtas ir atrodo bei funkcionuoja visiškai taip pat, kaip ir reali svetainė. Tokių tinklapių gaminimu bei naudojimu užsiima įsilaužėliai, norintys gauti priėjimą, pavyzdžiui, prie bankų informacinių sistemų;

3) nepageidaujamos elektroninio pašto žinutės (angl. *spam*): tiksliai apibrėžti nepageidaujamų elektroninio pašto žinučių sąvoką nėra paprasta, kadangi galimos skirtingos to paties reiškinio interpretacijos. Dažniausiai sutinkamas šios sąvokos apibūdinimas – nepageidaujamos elektroninio pašto žinutės, siunčiamos dideliais kiekiais be vartotojo sutikimo;

4) apgaulės taktika (angl. *spoofing*): apgaulės taktika reiškia, kad, siekiant išsiųsti nepageidaujamą informaciją plačiam gavėjų ratui, naudojamas netikras elektroninis paštas;

5) šnipinėjimo programinė įranga (angl. *spyware*): tai tokios programos, kurios, dažniausiai nežinant vartotojui, renka informaciją apie lankomas interneto svetaines, vartotojo vardą, elektroninio pašto adresus, programas ar bylas, esančias kompiuteryje, arba registruoja vartotojo atliekamus veiksmus internete, pavyzdžiui, dirbant su banko sąskaitomis, ir siunčia šiuos duomenis tretiesiems asmenims – programų gamintojams ar kitiems suinteresuotiems asmenims – be vartotojo leidimo ir netgi be jo žinios (pvz., *key logging*);

---

[51] *Typographical error squatting* – anglų kalbos terminas, apibūdinantis metodą, kai teksto įvedimo metu (naudojantis kompiuterio klaviatūra) padaroma klaida, nepaisant to fakto, kad vartotojas tiksliai žino, ką jis turi įvesti. Taip paprastai atsitinka dėl operatoriaus nepatyrimo naudojant įvedimo raktų rinkinius galiniame kompiuteryje (angl. *keyboarding*), skubėjimo, neatidumo ar nerūpestingumo.

6) duomenų nuskaitymas nuo kortelių apgaulės būdu (angl. *skimming*): tai vienas iš labiausiai paplitusių mokėjimo kortelių klastojimo ir sukčiavimo būdų, kai duomenys nuo kortelių su magnetine juostele nuskaitomi atsiskaitymo metu restoranuose, parduotuvėse ar kitose vietose, o po to suklastojama nauja kortelė.

2.4. Skyriaus apibendrinimas

Tapatybės vagystės atvejų daugėja, o pats reiškinys dėl nuolatinės informacinių ir ryšio technologijų pažangos įgyja naujų formų, kurios iš fizinės erdvės vis didesne apimtimi persikelia į elektroninę erdvę. Dauguma elektroninės erdvės įrankių, pavyzdžiui, paieškos sistemos, „slapukai“ (angl. *cookies*), elektroninės parduotuvės, elektroniniai atsiskaitymai, žaidimai ir sveikatos diagnozė on-line, pasižymi potencialia galimybe itin greitai ir efektyviai rinkti bei platinti asmens duomenis. Didžiausią pavojų asmeninės informacijos konfidencialumui kelia šie išskirtinai su interneto paplitimu ir raida susiję reiškiniai: naršymo duomenų rinkimas ir tvarkymas (angl. *browsing chaterring*); nematomos nuorodos į kitus tinklapius (angl. *invisible hyperlinks*) ir „slapukai“ (angl. *cookies*). Visais šiais atvejais eiliniam interneto vartotojui nepastebimu būdu apie jį yra renkami ir kaupiami didžiuliai asmeninės informacijos kiekiai, kurių panaudojimo sritys iki galo nėra aiškios.

Elektroninės erdvės sritys, kuriose asmuo identifikuojamas, yra labai įvairios, o asmens tapatybės nustatymo procedūra sudėtinga: tarp asmens ir institucijos, į kurią asmuo kreipiasi, įsiterpia daugybė tarpininkų, todėl elektroninės erdvės naudotojui, dalyvaujančiam autentifikavimo procese, kyla potenciali rizika tapti tapatybės vagystės auka. Taigi yra nuolatinis pavojus, kad bus pasikėsinta į asmens duomenis ir (ar) asmeninę informaciją, perduodamą elektroninių ryšių tinklais ir būtiną efektyviam informacinės visuomenės narių tarpusavio komunikavimui.

Pirmieji tapatybės vagystės atvejai pasitaikė gerokai anksčiau nei atsirado internetas, kai ši veika buvo – ir vis dar yra – atliekama panaudojant tokius metodus kaip „šiukšlių rinkimas“, mokėjimo kortelės vagystė, dingsties ieškojimas, „žiūrėjimas per petį“, duomenų nuskaitymas nuo kortelių apgaulės būdu arba kompiuterio vagystė. Per pastaruosius kelerius metus minėti metodai gerokai patobulėjo dėl sparčios interneto, informacinių bei ryšio technologijų plėtros, kuri suteikia galimybę tapatybės vagystės subjektams kompiuteriuose įdiegti kenkėjiškas programas ar panaudoti duomenų vagystės metodą kenkėjiškų programų ar nepageidaujamų elektroninio pašto žinučių pagalba. Dėl minėtų priežasčių tapatybės vagystės elektroninėje erdvėje yra atliekamos įvairiais metodais, kurie kinta ir tobulėja kartu su technologijų pažanga. Šiuo metu dažniausiai naudojami yra šie būdai: duomenų vagystė (angl. *phishing*), falsifikuoti internetiniai tinklalapiai (angl. *scam*), nepageidaujamos elektroninio pašto žinutės (angl. *spam*), apgaulės taktika (angl. *spoofing*), šnipinėjimo programinė įranga (angl. *spyware*), duomenų nuskaitymas nuo kortelių apgaulės būdu (angl. *skimming*).

3. TAPATYBĖS VAGYSTĖS ELEKTRONINĖJE ERDVĖJE KRIMINALIZAVIMAS

Tapatybės vagystė elektroninėje erdvėje yra globali problema, todėl ypač svarbi užsienio teisėsaugos institucijų pagalba siekiant efektyviai kovoti su šia visuomenei pavojinga veika. Tačiau tais atvejais, kai užsienio valstybė neturi įstatymų, kriminalizuojančių tapatybės vagystę elektroninėje erdvėje, yra apsunkinamos informaciją renkančios valstybės galimybės rinkti tapatybės vagystės elektroninėje erdvėje įrodymus atitinkamoje užsienio valstybėje ir patraukti atsakomybėn kaltus asmenis. Todėl svarbu, kad valstybės vienodai traktuotų tapatybės vagystę elektroninėje erdvėje, o tai yra neišvengiamai susiję su tapatybės vagystės elektroninėje erdvėje kriminalizavimo problema.

Šio skyriaus tikslas – įrodyti, kad tapatybės vagystė elektroninėje erdvėje turėtų būti kriminalizuota. Siekiant šio tikslo skyriuje pateikiama valstybių, kuriose tapatybės vagystė yra kriminalizuota, apžvalga, Europos Komisijos ir OECD argumentai dėl tapatybės vagystės elektroninėje erdvėje kriminalizavimo, analizuojama situacija Lietuvoje, remiantis atlikta ekspertų apklausa, sistemiškai nagrinėjamos Lietuvos Respublikos baudžiamojo kodekso normos, į kurių reglamentavimo sritį patenka tam tikri tapatybės vagystės elementai.

3.1. Tapatybės vagystės kriminalizavimas užsienio valstybėse

Tapatybės nusikaltimai yra pasaulinė problema, su kuria susiduria daugelis valstybių. Todėl pastaruoju metu netyla diskusijos, ar tapatybės vagystė turėtų būti kriminalizuota ir ar tokios veikos sudėties įtraukimas į valstybių baudžiamuosius įstatymus padėtų efektyviau kovoti su šiuo reiškiniu. Pabrėžtina, kad daugelyje valstybių tapatybės vagystė *per se* apskritai nėra laikoma teisės pažeidimu, o patenka į įvairias išimtis, susijusias su duomenų slaptumu, apsauga ar klastote, už kuriuos galima asmenį patraukti baudžiamojon atsakomybėn. Tuo tarpu kitos valstybės laikosi nuomonės, jog tokios veikos yra specifinės, todėl tapatybės vagystės kriminalizavimas yra naudinga priemonė siekiant užkirsti kelią tapatybės vagystės sukeliamoms grėsmėms.

Jungtinėje Karalystėje tapatybės nusikaltimai, kaip specifiniai teisės pažeidimai, nėra išskiriami, o tapatybės vagystė laikoma sudedamąja teisės pažeidimų arba nusikaltimų dalimi. Tačiau Kredito pramonės sukčiavimų prevencijos organizacija (toliau – CIFAS) tapatybės vagystės kriminalizavimu laiko 2006 m. Jungtinės Karalystės Tapatybės kortelių akto 25 ir 26 skyrius, kuriuose įtvirtinamos naujos nusikalstamų veikų sudėtys, susijusios su suklastotų dokumentų turėjimu ir disponavimu, kuris apima ir autentiškus dokumentus, jei šie buvo gauti neteisėtu būdu ar išduoti ne tam asmeniui be

pateisinamos priežasties[52], ir Apgaulės aktą, kuris įtvirtino apgaulę, kaip savarankišką teisės pažeidimą, kuris gali būti atliekamas trim būdais: melagingai kreipiantis (nesąžiningai, turint tikslą gauti naudos, padaryti arba sukelti pavojų patirti nuostolių); nepavykus atskleisti informacijos; piktnaudžiaujant įgaliojimais[53]. Taip pat įtvirtinti nauji nusikaltimai, tokie kaip nesąžiningas paslaugų gavimas, jei už jas atliekami mokėjimai, pavyzdžiui, elektroninėje erdvėje apgaulės būdu pasinaudojant mokėjimo kortele; priemonių, įskaitant bet kokių programų ar asmens duomenų, laikomų elektronine forma, skirtų apgaulei įvykdyti ir kurios yra susijusios su tapatybės klastote, turėjimas; taip pat tokių priemonių gaminimas ir siūlymas, žinant, kad jos sukurtos ar pritaikytos atlikti apgavikiškus veiksmus[54]. Organizacija pabrėžia, kad iki kriminalizavimo sukčiai kuo puikiausiai suvokė, jog tapatybės klastotė yra puikus būdas gauti finansinės naudos, nes teisėsaugos institucijos negali už šią veiką patraukti atsakomybėn. Laikomasi nuomonės, kad tapatybės vagystės kriminalizavimas paskatins giliau pažvelgti į problemą: teisėsaugos institucijos ištirs daugiau tapatybės vagystės atvejų, nukentėjusieji galės pareikšti savo nuomonę ir bus pripažįstami nusikaltimo aukomis, o atsakomybė už tokią veiką bus sugriežtinta siekiant labiau atkreipti dėmesį į svarstomą problemą.

Australijoje, išskyrus Kvinslendą ir Pietų Australiją, tapatybės vagystė nelaikoma atskiru nusikaltimu, Kanadoje – taip pat. Kanadoje neteisėtą kito asmens tapatybės nustatymo duomenų panaudojimą apima baudžiamajame kodekse įtvirtintų nusikaltimų, tokių kaip apsimetimas kitu asmeniu ar klastojimas, dispozicijos. Tačiau pasiruošimo įvykdyti nusikaltimą, pavyzdžiui, informacijos, padedančios nustatyti asmens tapatybę, rinkimas, turėjimas ir perdavimas, paprastai nepatenka į įtvirtintų nusikaltimų sudėtis. Šiuo metu Kanadoje svarstymui pateiktas Tapatybės vagystės bilis, kaip teisės aktas, kurio tikslas – užpildyti Baudžiamojo kodekso spragas ir užtikrinti, kad informacijos, kuria remiantis galima nustatyti asmens tapatybę, rinkimas, laikymas ir perdavimas nėra apimamas kitų teisės pažeidimų sudėčių. Pagal naująjį teisės aktą kiekviena iš minėtų trijų veikų užtraukia baudžiamąją atsakomybę ir už tai numatoma laisvės atėmimo bausmė iki penkerių metų[55].

Jungtinėse Amerikos Valstijose (toliau – JAV) Pajėgos, nukreiptos prieš tapatybės vagystę (angl. *Identity Theft Task Force*), remia pastangas skatinti kitas valstybes, OECD nares, imtis veiksmų, kad tapatybės vagystė būtų kriminalizuota. Kadangi tapatybės vagystė yra pasaulinio lygio problema, itin svarbus tampa užsienio valstybių tarptautinis bendradarbiavimas. Tais atvejais, kai užsienio valstybė

---

[52] **Interneto tinklapis „Tapatybės vagystė; netapk auka“, sukurtas bendradarbiaujant Jungtinės Karalystės vyriausybei ir privačiam sektoriui**: https://www.identitytheft.org.uk/criminal-offences.asp [žiūrėta 2009 06 03]

[53] **Fraud Act 2006**. Prieinama internete: http://www.opsi.gov.uk/acts/acts2006/pdf/ukpga_20060035_en.pdf [žiūrėta 2009 04 14]

[54] Out-Law news, Phishing kits banned by new Fraud Act, 13 November 2006. Straipsnis prieinamas internete: www.out-law.com/page-7469 [2009 06 02]

[55] **Kanados teisingumo departamento oficialus tinklapis**: http://www.justice.gc.ca/ [žiūrėta 2009 05 31]
Ten pat, http://www.justice.gc.ca/eng/news-nouv/nr-cp/2007/doc_32178.html [žiūrėta 2009 05 31]
Ten pat, http://www.justice.gc.ca/eng/news-nouv/nr-cp/2009/doc_32348.html [žiūrėta 2009 05 31]
Ten pat, http://www.justice.gc.ca/eng/news-nouv/nr-cp/2009/doc_32347.html [žiūrėta 2009 05 31]

nėra numačiusi baudžiamosios atsakomybės už tapatybės vagystę, apsunkinama tyrimą atliekančios valstybės galimybė rinkti įrodymus ir atlikti baudžiamąjį persekiojimą už tapatybės vagystės nusikaltimą, turintį užsienio elementą[56]. Paminėtina tai, kad JAV ėmėsi daugybės priemonių, siekdamos užkirsti kelią tapatybės nusikaltimams. 1998 m. JAV Kongresas Tapatybės vagystės ir apsimetinėjimo atgrasymo akte[57] (angl. *Identity Theft and Assumption Deterrence Act*) įtvirtino specifinės nusikalstamos veikos sudėtį. Tapatybės vagystė buvo įtvirtinta JAV baudžiamajame kodekse, pagal kurį tokia veika traktuojama kaip specifinis nusikaltimas, atliekamas tada, kai kas nors tyčia perduoda, laiko, naudoja, neturėdamas tam teisės, kito asmens identifikavimo priemones, 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[58]. Bausmė, numatoma už tokį nusikaltimą, yra laisvės atėmimas iki penkerių metų, o jei nusikaltimas padarytas sunkinančiomis aplinkybėmis[59] – laisvės atėmimas iki penkiolikos metų. Reikia paminėti ir tai, kad Tapatybės vagystės ir apsimetinėjimo atgrasymo aktas numato centralizuotą pagalbą aukoms, skundų pateikimo tvarką ir vartotojų mokymo paslaugas nukentėjusiems nuo tapatybės vagystės. Tai reiškia, kad aukoms nereikia kreiptis į kelias susijusias institucijas – vietoj to yra sukurtas „jungtinis apgaulės pavojaus“ (angl. *joint fraud alert*) mechanizmas, už kurio įgyvendinimą yra atsakingos trys didžiausios kredito ataskaitas teikiančios institucijos. Nukentėjusieji gali sulaukti pagalbos net jei apkaltinamasis nuosprendis už tapatybės vagystę ir nėra priimtas. Paminėtina ir tai, kad 2003 m. Teisingų ir tikslių kredito transakcijų aktu[60] (angl. *Fair and Accurate Credit Transactions Act*) buvo patvirtintos tam tikros priemonės, skirtos vartotojų apsaugai:

- vartotojai, pateikę užklausą, gali nemokamai gauti kredito ataskaitą, kuri padėtų jiems patikrinti savo finansinę informaciją ir imtis priemonių kilus pavojui;
- vartotojai, pajutę apgaulės pavojų, gali specialiai pažymėti savo sąskaitas, kad kredito ataskaitas teikiančios institucijos užblokuotų potencialiai apgaulingą vartotojo kredito ataskaitų informaciją. Įspėjimo signalas apie galimą apgaulę galioja 90 dienų nuo to momento, kai vartotojas įrodo savo tapatybę, be to, yra galimybė pratęsti minėtą terminą iki septynerių metų, skaičiuojamą nuo to momento, kai vartotojas parašo pareiškimą policijai;

---

[56] **Scoping Paper on Online Identity Theft**: Ministerial Background Report. DSTI/CP (2007)3/Final. P. 14. Prieinama internete: http://www.oecd.org/dataoecd/35/24/40644196.pdf [žiūrėta 2009 06 04]

[57] **Identity Theft and Assumption Deterrence Act**, 1998. Prieinama internete: http://www.ftc.gov/os/statutes/itada/itadact.htm [2009 06 04]

[58] **United States Code** („U. S. C“), Title 18, Part I, Chapter 47, Section 1028 (a) (7). Prieinama internete: http://www.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00001028----000-.html [žiūrėta 2009 05 31]

[59] Sunkinančios aplinkybės numatytos 2004 m. Bausmės už tapatybės vagystę padidinimo akte (angl. *Identity Theft Enhancement Penalty Act*). Prieinama internete: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ275.108.pdf [žiūrėta 2009 06 03]

[60] **Fair and Accurate Credit Transactions Act**, 2003. Prieinama internete: http://www.gpo.gov/fdsys/pkg/PLAW-108publ159/pdf/PLAW-108publ159.pdf [žiūrėta 2009 06 04]

- Aktas nustato nacionalinius standartus Jungtinėms Valstijoms, kurie reikalauja, kad verslo subjektai sutrumpintų sąskaitų numerius, pateikiamus kredito ir debeto kortelių kvituose;
- tapatybės vagystės aukos gali gauti apgaviko pateiktų paraiškų atidaryti banko sąskaitą ir aukos vardu įvykdytų transakcijų kopijas, kai tik policijai pateikiamas pareiškimas. Apkaltinamojo nuosprendžio priėmimas šiuo atveju nėra būtina sąlyga.

Be to, Federalinis bankas ir taupymo reguliavimo institucijos parengė Tinkamo informacijos apie vartotojus tvarkymo gaires[61] (angl. *Guidelines requiring the Proper Disposal of Consumer Information*), skirtas tinkamam Teisingų ir tikslių kredito transakcijų akto įgyvendinimui. Šios gairės finansines institucijas įpareigoja vystyti ir palaikyti tinkamus kontrolės mechanizmus tam, kad būtų užtikrintas tinkamas vartotojų informacijos, gaunamos iš vartotojų kredito ataskaitų, tvarkymas.

Europos valstybės taip pat pripažįsta, jog tapatybės nusikaltimai yra rimta problema, tačiau, pavyzdžiui, Prancūzijos, Vokietijos, Olandijos teisės aktai neįtvirtina teisės pažeidimo sudėties, kuri apimtų ir tapatybės nusikaltimus. Lygiai taip pat, kaip ir Kanadoje, šiose valstybėse yra priimti teisės aktai, kuriais remiantis gali būti atliekamas persekiojimas už tokias veikas, kaip klastotė arba neteisėtas duomenų panaudojimas, tačiau tapatybės nusikaltimas, kaip specifinis teisės pažeidimas, nėra įtvirtintas[62].

Būtina pabrėžti, kad tikriausiai mažiausiai įprastas požiūris į tapatybės vagystės problemą vyrauja Pietų Korėjoje. Pietų Korėjos vyriausybė ketina priimti teisės aktus, kurie finansinėms institucijoms nustatys pareigą kompensuoti vartotojų, kurie tapo klastotės ir tapatybės vagystės elektroninėje erdvėje aukomis, patirtą žalą. Tačiau jei vartotojai su savo duomenimis elgėsi neatsargiai, jie neturės teisės į tokią kompensaciją. Manoma, kad vyriausybei laikantis tokios pozicijos, finansų institucijos bus labiau atsakingos už aukšto lygio apsaugos sistemų palaikymą, siekdamos išvengti tapatybės vagystės[63].

3.2. Tapatybės vagystė kaip tarptautinė ir regioninė problema

Daugelis Europos valstybių (taip pat keletas ne Europos valstybių) yra prisijungusios prie 2001 m. Europos Tarybos konvencijos dėl elektroninių nusikaltimų[64] (toliau – Konvencija). Konvencijos 1

---

[61] **US Federal Register**, Volume 69, Number 248, Rules and Regulations, Page 77610-77621, December 28 2004. Prieinama internete: http://www.fdic.gov/news/news/financial/2005/fil705a.html [žiūrėta 2009 06 03]

[62] **Identity Crime: Discussion Paper.** Model Criminal Law Officer‘s Committee. 2007. P. 11. Prieinama internete: http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(4341200FE1255EFC59DB7A1770C1D0A5)~MCLOC-draft-identity-crime-discussion-paper-march+2007.pdf/$file/MCLOC-draft-identity-crime-discussion-paper-march+2007.pdf [žiūrėta 2009 06 03]

[63] **Bruce Schneier**. Korea Solves the Identity Theft Problem. December 14, 2005. Straipsnis prieinamas internete: http://www.schneier.com/blog/archives/2005/12/korea_solves_th.html [žiūrėta 2009 06 03]

[64] **Konvencija dėl elektroninių nusikaltimų**. Prieinama internete:

skirsnis numato baudžiamosios teisės pažeidimus, kurie turėtų būti kriminalizuoti valstybių nacionaliniame lygmenyje. Šios veikos daugeliu atvejų yra susijusios ir su tapatybės nusikaltimo įvykdymu. Konvencijos 2 str. įtvirtina neteisėtą prieigą prie kompiuterinių duomenų, 3 str. – neteisėtą duomenų perėmimą, 4 str. – poveikį duomenims, 5 str. – poveikį sistemai, 6 str. – netinkamą įtaisų naudojimą, kai ketinama juos panaudoti 2 – 5 str. apibūdintiems nusikaltimams. Konvencijos 7 str. ir 8 str. atitinkamai įtvirtina kompiuterinį klastojimą ir kompiuterinį sukčiavimą. Atlikus Konvencijos teisės normų analizę, galima teigti, kad tapatybės nusikaltimas pats savaime nėra įtvirtinamas kaip nusikaltimas jokiame Konvencijos straipsnyje ir netgi nėra reikalaujama, kad Konvenciją ratifikavusios valstybės nacionaliniame lygmenyje imtųsi kokių nors veiksmų, siekiant užkirsti kelią tapatybės nusikaltimams. Tačiau paminėtinas trečias Konvencijos skyrius, reglamentuojantis tarptautinį bendradarbiavimą: įtraukiant šį skyrių į Konvenciją buvo pripažinta, kad nusikaltimai, susiję su kompiuterinėmis sistemomis ir duomenimis, gali būti įvykdomi nepriklausomai nuo valstybių sienų, todėl sėkminga kova su tokiais nusikaltimais daugeliu atvejų priklauso nuo efektyvaus tarptautinio bendradarbiavimo.

Kalbant apie tarptautinį lygmenį, didžiulį darbą atliko ir specialų leidinį „Tapatybės vagystė elektroninėje erdvėje“[65] (angl. *Online Identity Theft*) pateikė OECD. Be to, paminėtina ir šios Organizacijos 2007 m. parengta ataskaita[66] apie tapatybės vagystę elektroninėje erdvėje. Šiuose darbuose organizacija akcentuoja tai, kad internetiniai sukčiai, naudodamiesi plačiai prieinamomis elektroninėmis priemonėmis, gana nesunkiai iš nieko bloga neįtariančių elektroninės erdvės naudotojų išvilioja asmens duomenis. Tokius duomenis sukčiai vėliau panaudoja neteisėtais tikslais, taip stiprindami nepasitikėjimą elektroninės bankininkystės paslaugomis ir mokėjimais, atliekamais elektroninėje erdvėje. Organizacija pateikia tapatybės vagystės, kaip pavojingos veikos, įvertinimą: apibrėžiama tapatybės vagystės sąvoka ir būdai, kuriais ji gali būti atliekama, bendrais bruožais apibūdinama, kokių veiksmų imtasi valstybėse narėse siekiant efektyviai kovoti su šiuo neigiamų pasekmių sukeliančiu reiškiniu, ir pateikiamos rekomendacijos, kuriose akcentuojama, kad kova su tapatybės vagyste turi būti vykdoma globaliu mastu. Organizacija siūlo kriminalizuoti tapatybės vagystę ir pabrėžia, kad priimdamos teisės aktus, numatančius baudžiamąją atsakomybę už nusikalstamas veikas, susijusias su tapatybės vagyste, OECD valstybės narės galėtų remtis įvairiapusiu požiūriu į nagrinėjamą problemą, kuris apimtų, pavyzdžiui, teisės aktų, numatančių galimybę pranešti

---

http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=228195&p_query=&p_tr2= [žiūrėta 2009 12 01]

[65] **Online Identity Theft** – OECD, 2009. P. 16.
Prieinama internete: http://browse.oecdbookshop.org/oecd/pdfs/browseit/9309021E.PDF [žiūrėta 2009 06 02]

[66] **Scoping Paper on Online Identity Theft**: Ministerial Background Report. DSTI/CP (2007)3/Final. P. 14. Prieinama internete: http://www.oecd.org/dataoecd/35/24/40644196.pdf [žiūrėta 2009 06 04]

apie duomenų apsaugos pažeidimus, skatinančius viešas bei privačias iniciatyvas siekiant rasti visapusį tapatybės vagystės problemos sprendimą, priėmimą.

Europos Sąjunga (toliau – ES) taip pat iškėlė klausimą dėl būtinybės kriminalizuoti tapatybės vagystę. Europos Komisija 2007 m. gegužės 22 d. priėmė komunikatą KOM (2007) 267 Bendrosios politikos, skirtos kovai su elektroniniais nusikaltimais, linkme[67]. Šiame teisės akte aptariant tikslinius teisės aktus, skirtus kovai su elektroniniais nusikaltimais, akcentuojama, kad ypatinga problema, kuriai gali reikėti teisės akto, susijusi su situacija, kai elektroniniai nusikaltimai padaromi pasinaudojant tapatybės vagyste. Komisija pabrėžia, kad paprastai tapatybės vagystė suprantama kaip asmens tapatybę atskleidžiančios informacijos panaudojimas, pavyzdžiui, kredito kortelės numeris, kaip priemonė padaryti kitus nusikaltimus, todėl labiausiai tikėtina, kad daugelyje valstybių narių nusikaltėlis būtų patrauktas baudžiamojon atsakomybėn ne už tapatybės vagystę, o už sukčiavimą arba kitą galimą nusikaltimą, kurie laikomi sunkesniais nusikaltimais. Taip pat Komisija atkreipia dėmesį, kad tapatybės vagystė nėra kriminalizuota visose valstybėse narėse, ir teigia, jog dažniausiai tapatybės vagystės nusikaltimą įrodyti lengviau negu sukčiavimo nusikaltimą, todėl tapatybės vagystės kriminalizavimas visose valstybėse narėse pagerintų ES teisėsaugos institucijų bendradarbiavimą[68].

3.3. Tapatybės vagystės vertinimas Lietuvoje

Siekiant išsiaiškinti situaciją, susijusią su tapatybės vagyste, Lietuvoje, buvo atliekamas kokybinis tyrimas taikant empirinį – ekspertų vertinimo – metodą (buvo atliekama ekspertų apklausa).

Tyrimo metodo pagrindimas. Ekspertų apklausa, kaip kokybinis tyrimo metodas, pasirinkta siekiant suprasti tapatybės vagystę elektroninėje erdvėje kaip socialinį teisinį reiškinį bei pateikti interpretacinį, holistinį šio reiškinio paaiškinimą. Kadangi tyrimo objektas labai specifinis, tyrimas buvo sąmoningai orientuotas į kompetentingus asmenis (teisėsaugos ir finansų institucijų atstovus, teisininkus – mokslininkus), galinčius turėti teorinių ir ypač praktinių žinių, susijusių su tiriamu objektu, ir suteikti būtiną informaciją tyrėją dominančiais klausimais. Dar viena priežastis, dėl ko buvo pasirinktas būtent toks tyrimo metodas, – siekis užtikrinti mokslinį objektyvumą.

Devyniems ekspertams, kiekvienam individualiai, buvo nurodyta problema, tyrimo objektas ir tikslas bei pateiktas klausimynas su tyrėją labiausiai dominančiais aspektais. Pagrindinė priežastis, lėmusi tokio sąlyginai nedidelio ekspertų skaičiaus pasirinkimą, yra ta, kad Lietuvos mastu gana sudėtinga rasti tokios specifinės srities specialistų, be to, net jei būtų apklaustas didelis skaičius

---

[67] **Europos Komisijos 2007 m. gegužės 22 d. komunikatas KOM (2007) 267 Bendrosios politikos, skirtos kovai su elektroniniais nusikaltimais, linkme**. Prieinama internete: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:LT:HTML [žiūrėta 2009 06 03]

[68] Ten pat, 3.3. straipsnis.

ekspertų, pavyzdžiui, penkiasdešimt, būtų vargu ar įmanoma suformuluoti konkrečias išvadas ir pateikti apibendrintus rezultatus dėl pernelyg skirtingų pozicijų. Atsižvelgiant į tai, jog ekspertų apklausa yra kokybinis, o ne kiekybinis tyrimo metodas, paprastai apklausiama ekspertų grupė, sudaryta iš 5 – 7 žmonių[69]. Pabrėžtina ir tai, kad rezultatų prasme atliktas empirinis tyrimas nėra pagrindinis, o ekspertų apklausos metu gauti rezultatai vertinami kitų rezultatų kontekste.

Tyrimo objektas – tapatybės vagystė elektroninėje erdvėje kaip socialinis – teisinis reiškinys.

Tyrimo tikslas – išnagrinėti tapatybės vagystės elektroninėje erdvėje kaip socialinio – teisinio reiškinio teisinius aspektus ir vertinimą Lietuvoje.

Tyrimo naujumas. Tokio pobūdžio tyrimus atlieka tarptautinės (pavyzdžiui, Ekonominio bendradarbiavimo ir plėtros organizacija), regioninės (pavyzdžiui, Europos Komisija), taip pat užsienio valstybių (pavyzdžiui, CIFAS (Sukčiavimų prevencijos organizacija Jungtinėje Karalystėje), FTC (Federalinė Prekybos Komisija JAV)) institucijos ir organizacijos. Kai kurios užsienio valstybės (pavyzdžiui, JAV, Didžioji Britanija) ypač daug dėmesio skiria visuomenės informavimui ir tapatybės vagystės, kaip visuomenei pavojingos veikos, prevencijai. Tuo tarpu Lietuvoje neadekvačiai vertinama šios veikos potenciali žala, per mažai skiriama dėmesio šio reiškinio visapusiškam įvertinimui ir panašaus pobūdžio tyrimai nėra atliekami.

Tyrimo reikšmė. Tyrimo metu gautos informacijos pagrindu atliekama tapatybės vagystės elektroninėje erdvėje teisinių aspektų analizė, aptariama situacija Lietuvoje; analizuojant ir apibendrinant ekspertų nuomones, formuluojamos mokslinės sąvokos, prognozuojamos minėto reiškinio kitimo tendencijos.

Atlikus tyrimą ir apibendrinus ekspertų nuomones, dar kartą akcentuotina, jog tapatybės vagystė yra pavojingas reiškinys: dažniausiai tapatybės vagystė naudojama palengvinti nusikaltimų, tokių kaip nelegali imigracija, terorizmas ir šnipinėjimas, šantažas, finansiniai nusikaltimai, atlikimą. Tačiau ne visais atvejais motyvas yra finansinės priežastys – tai gali būti ir asmens persekiojimas.

Ekspertų teigimu, nusikaltimas gali prasidėti suklastojus tapatybę, kuri tampa būsimų nusikaltimų pradžia. Taigi tapatybės vagystė neapsiriboja tik apsimetimu kitu asmeniu: ji taip pat apima melagingos dokumentacijos naudojimą, teigiantį neegzistuojantį ryšį su teisėtomis kompanijomis, neegzistuojančiomis korporacijomis ar sukčiavimui naudojamomis organizacijomis. Suklastotos, netikros tapatybės naudojamos įkuriant teisiškai tvarkingas kompanijas, o sukurtos netikros tapatybės – klastotės vėliau padeda išvengti atsakomybės, kilusios dėl neteisėtos tokių kompanijų veiklos.

Vertinant tapatybės vagystės fizinėje erdvėje ir tapatybės vagystės elektroninėje erdvėje pavojingumą, vienareikšmiškai atsakyti, kuri iš šių dviejų tapatybės vagystės rūšių yra pavojingesnė,

---

[69] **Tidikis R.** Socialinių mokslų tyrimų metodologija. P. 515.

gana sunku. Ekspertai pabrėžia, kad tapatybė fizinėje erdvėje yra visiškai kitokia nei elektroninėje erdvėje. Fizinėje erdvėje savo tapatybę asmuo patvirtina vienu iš privalomų elementu – asmens dokumentu, tuo tarpu elektroninėje erdvėje tapatybę gali atstoti vardas ir slaptažodis. Vardas – tai kokio nors objekto sutartinis, tą objektą vienareikšmiškai identifikuojantis pavadinimas. Jis sistemoje turi būti unikalus. Slaptažodis – tai ženklų seka, žinoma tik paslaugos teikėjui ir jos vartotojui, pagal kurią paslaugos teikėjas patikrina į jį besikreipiančio tapatybę. Iš sąvokų matyti, kad elektroninėje erdvėje tapatybė sutapatinama su prisijungimo vardu ir slaptažodžiu ir visos saugumo užtikrinimo priemonės, tokios kaip skaitmeniniai sertifikatai, iš esmės atitinka asmens tapatybę elektroninėje erdvėje.

Pačią ***tapatybės vagystę elektroninėje erdvėje*** ekspertai siūlo apibrėžti kaip *gavimą pagrindinių asmens tapatybę liudijančios informacijos elementų (elektroninėje erdvėje), siekiant apsimesti tuo asmeniu, su tikslu atlikti nusikaltimus*. Kai nėra tikslo atlikti nusikaltimus, veika gali būti apibrėžiama kaip piktnaudžiavimas tapatybe, o kai naudojamasi neegzistuojančio asmens tapatybe, veika turėtų būti įvardijama tapatybės klastote.

Situacija, kai asmuo tik norėjo apsimesti kažkuo kitu, t.y. pavogė kito asmens tapatybę, bet kitų neteisėtų ir pavojingų veiksmų neatliko ir finansinės naudos iš to negavo, ekspertų teigimu, turėtų būti vertinama kaip mažiau pavojinga veika ir galėtų būti laikoma piktnaudžiavimu tapatybe, atsižvelgiant į tai, kad minėtu atveju nėra nusikalstamo požymio. Tokiu atveju atitinkamai reikėtų spręsti ir atsakomybės klausimą. Deja, šiuo metu Lietuvos teisės aktai tokio pobūdžio veikos nereglamentuoja ir atsakomybės už tai nenumato.

Kalbant apie tapatybės vagystės elektroninėje erdvėje įvykdymo būdus, ekspertai pirmiausia pabrėžia, jog elektroninėje erdvėje tapatumo duomenis gauti yra lengviau nei fizinėje erdvėje, ir išskiria tokius pagrindinius tapatybės vagystės elektroninėje erdvėje atlikimo būdus:

1) įsibrovimas (angl. *hacking*): dažniausiai sukčius, apeidamas sistemos slaptažodžius, saugumo priemones, patenka į sistemą. Ypatingai stengiamasi pasinaudoti saugumo spragomis, neapsaugotas bevieliais, intraneto tinklais, taip pat ieškoma sistemų, kuriose didžioji dalis apsaugos funkcijų yra išjungtos;

2) šnipinėjimo programa (angl. *spyware*) – tai programinė įranga, kuri be asmens žinios renka ir siunčia jo asmeninius duomenis nurodytu adresu. Dažniausiai pažeidinėjami privatumo lygiai. Renkami ir fiksuojami asmens naršymo internete įpročiai, dažnai lankomų svetainių adresai. Rinkodaros kompanijos kasmet išleidžia milijonus dolerių bandydamos nustatyti vartotojų išlaidų įpročius. Naršymo įpročiai paprastai nusiunčiami reklamos kompanijai, kuri ateityje pateikia tuos įpročius atitinkančią reklamą;

3) slaptažodžio žvejyba (angl. *phishing, password fishing*): pasinaudojant nepageidaujamomis elektroninio pašto žinutėmis ar netikrais internetiniais tinklapiais bandoma išgauti prisijungimo prie

informacinių sistemų slaptažodžius, kitus asmeninius duomenis. Dažniausiai tokio sukčiavimo aukos būna banko klientai – siekiama sužinoti jų prisijungimo prie elektroninės bankininkystės sistemų slaptažodžius ar kreditinių kortelių duomenis. Gauta informacija gali būti panaudota pasipelnymo tikslais vykdant nusikalstamas veikas, neteisėtus prisijungimus prie informacinių sistemų, vagystes iš sąskaitų ar elektroninėje erdvėje atsiskaitant už prekes naudojant svetimas mokėjimo korteles. Taip pat egzistuoja trumpųjų žinučių sukčiavimai (angl. *SMiShing*), internetinės balso telefonijos sukčiavimai (angl. *vishing*), apgaulingas laiškas (angl. *scam*). Tai nėra baigtinis sukčiavimų sąrašas, kiti būdai bei metodai labai panašūs į aptartus anksčiau;

4) Trojos arklys (angl. *Trojans*) – tai programa, sprendžianti kokį nors naudingą uždavinį, tačiau iš tikrųjų atliekanti kitą darbą: naikina, sugadina kompiuteryje esančius duomenis, programas. Dažniausiai Trojos arkliai skirstomi į kirminams artimas programas, kurios platina savo kopijas kompiuterių tinkluose. Kita rūšis – nuotolinio valdymo programos, įprastos programoms, kurios naudojamos nuotoliniam sistemų administravimui. Pavojingiausios programos pasisavina informaciją, ją persiunčia tretiesiems asmenims, dažnai net naudoja paprastą elektroninį paštą ar svetaines;

5) apgaulinga IP taktika (angl. *pharming*): siekiama nukreipti vienos svetainės srautą į kitą. Gali būti atliekama pakeičiant aukos pagrindinio kompiuterio nustatymus arba pasinaudojus sričių vardų serverių (DNS) eksploatavimo pažeidimais. Pažeisti sričių vardų serveriai vadinami užnuodytais (angl. *DNS cache poisoning*);

6) pakartojimo ataka (angl. *replay attack*): mėginama prisijungti prie kompiuterio tinklo, siekiant pakartotinai išsiųsti vartotojo informaciją. Jeigu informacija koduojama, galima pakartoti tą patį duomenų siuntimą, tikintis, kad serveris patikės, jog tai tas pats vartotojas.

Pasaulyje egzistuoja daugelis kitų metodų, bet visi jie veikia panašiai, pasinaudojant tinklų, sistemų saugumo ir (ar) technologines spragas.

Ekspertų nuomone, tapatybės vagystė elektroninėje erdvėje turėtų būti kriminalizuota. Pagrindinis argumentas, pagrindžiantis tokią poziciją, yra tas, jog tapatybės vagystė elektroninėje erdvėje yra globali problema, todėl ypač svarbi užsienio valstybių teisėsaugos institucijų pagalba. Tais atvejais, kai užsienio valstybė neturi įstatymų, kriminalizuojančių tapatybės vagystę elektroninėje erdvėje, yra ženkliai apsunkinamos informaciją renkančios valstybės galimybės rinkti tapatybės vagystės elektroninėje erdvėje įrodymus atitinkamoje užsienio valstybėje. Todėl nacionaliniuose, regioniniuose ir tarptautiniuose teisės aktuose turėtų būti įtvirtintas tapatybės vagystės elektroninėje erdvėje baudžiamumas, o teisėsaugos institucijoms suteikta pakankamai įgaliojimų veiksmingai kovoti su tokio pobūdžio nusikalstamomis veikomis. Taip būtų palengvintas atliekamų veikų susekimas, tyrimas ir baudžiamasis persekiojimas nacionaliniu bei tarptautiniu lygiu, šių veikų įrodymus būtų galima rinkti elektroniniu pavidalu, taigi tokiu būdu būtų užtikrinamas greitas ir patikimas tarptautinis bendradarbiavimas, kad būtų sustabdyti veiksmai, nukreipti prieš kompiuterinių sistemų, tinklų ir

kompiuterinių duomenų konfidencialumą, vientisumą ir prieinamumą, ir nebūtų leidžiama tokių sistemų, tinklų ir duomenų netinkamai naudoti.

Kalbant apie tapatybės vagystę elektroninėje erdvėje, svarbu paminėti tarp baudžiamosios teisės ir informatikos teisės specialistų kylančią diskusiją dėl teisės panaudoti elektroninę mokėjimo priemonę perdavimo kitam asmeniui bei šio asmens svetimos mokėjimo priemonės panaudojimą kito (perdavusio) asmens vardu. Pažymėtina, kad nuomonės šiuo klausimu išsiskiria. Baudžiamosios teisės specialistų nuomone, tokia veika neturėtų būti laikoma nusikalstama, nes asmuo savo teisę panaudoti elektroninę mokėjimo priemonę kitam asmeniui perduoda laisva valia, niekieno neverčiamas, taigi nelieka ir pagrindinių nusikalstamos veikos charakteristikų – pavojingumo ir priešingumo teisei. Todėl ir 2005 m. gruodžio 29 d. Lietuvos Aukščiausiojo Teismo Senato (toliau – LAT Senato) nutarimo Nr. 55 „Dėl teismų praktikos nusikalstamų veikų finansų sistemai baudžiamosiose bylose (BK 214, 215, 219, 220, 221, 222, 223 straipsniai)“[70] 4 punktas, kuriame teigiama „kadangi paprastai mokėjimo instrumentas (pvz., banko mokėjimo kortelė) nuosavybės teise priklauso emitentui, t.y. mokėjimo instrumentą išdavusiai institucijai, kuri pagal mokėjimo instrumento naudojimosi sutartį tik jo turėtojui suteikia teisę naudotis mokėjimo instrumentu, todėl kiekvienam trečiajam (kitam) asmeniui jis yra svetimas BK 214 straipsnio prasme“, šiuo atžvilgiu yra kritikuotinas. Galima pateikti praktinį pavyzdį, kai tokia LAT Senato pozicija iš tiesų atrodo nelogiška: susirgus šeimos nariui ir pastarajam paprašius kito šeimos nario iš bankomato išimti tam tikrą sumą pinigų, pasinaudojant sergančiojo mokėjimo kortele, tokia situacija būtų kvalifikuojama kaip nusikalstama veika, kas, žiūrint iš socialinės, o ne iš griežtai teisinės perspektyvos, prasilenktų su sveika logika.

Informatikos teisės specialistai palaiko priešingą poziciją ir teigia, kad žmogus, naudodamas tokią kortelę, klastoja dokumentus pasirašydamas, t.y. aktyviais veiksmais išreikšdamas valią, pavyzdžiui, įvesdamas PIN kodą, kito asmens vardu.

Abi pozicijos yra gana įtikinančios. Vis dėlto, griežtai juridine prasme teisės panaudoti elektroninę mokėjimo priemonę perdavimas kitam asmeniui bei šio asmens svetimos mokėjimo priemonės panaudojimas kito (perdavusio) asmens vardu, turėtų būti vertinamas kaip nusikalstama veika. Tokią poziciją galima pagrįsti ir 2006 m. lapkričio 21 d. LAT kasacine nutartimi Nr. 2K-581/2006[71], kurioje Teismas konstatavo, kad baudžiamoji atsakomybė už svetimo mokėjimo instrumento panaudojimą ne didesnei kaip 1 MGL[72] dydžio finansinei operacijai inicijuoti kyla pagal BK 214 straipsnį, į kurio reglamentavimo sritį patenka neteisėtas disponavimas elektronine mokėjimo

---

[70] **2005 m. gruodžio 29 d. Lietuvos Aukščiausiojo Teismo Senato nutarimas Nr. 55 „Dėl teismų praktikos nusikalstamų veikų finansų sistemai baudžiamosiose bylose (BK 214, 215, 219, 220, 221, 222, 223 straipsniai)“**, 4 punktas. Prieinama internete: http://www.lat.lt/4_tpbiuleteniai/senos/nutartis.aspx?id=31289 [žiūrėta 2009 06 04]

[71] **2006 m. lapkričio 21 d. Lietuvos Aukščiausiojo Teismo kasacinė nutartis baudžiamojoje byloje Nr. 2K-581/2006**. Prieinama internete: http://www.lat.lt/3_nutartys/senos/nutartis.aspx?id=30503 [žiūrėta 2009 06 04]

[72] MGL – minimalus gyvenimo lygis, kuris lygus 130 litų. Šiuo metu vietoj minėtos sąvokos vartojamas „bazinės socialinės išmokos“ (santrumpa – BSI) terminas.

priemone arba jos duomenimis, tačiau tokio mokėjimo instrumento panaudojimas didesnei nei 1 MGL dydžio finansinei operacijai inicijuoti jau sudaro dviejų nusikaltimų sutaptį ir kvalifikuotinas pagal BK 214 ir 182 straipsnius (neteisėto disponavimo elektronine mokėjimo priemone arba jos duomenimis ir sukčiavimo sutaptis).

Mokėjimo instrumentas kaip bendroji sąvoka, vartojama kalbant apie tapatybės vagystę, apibūdina įvairius daiktus, teisėtai dalyvaujančius finansinėje apyvartoje ir skirtus atsiskaityti negrynaisiais pinigais. Tai – piniginiai vertybiniai popieriai (čekiai, vekseliai, obligacijos), nustatytos formos rašytiniai dokumentai ir elektroninės mokėjimo priemonės (plastikinės kortelės, kita įranga, leidžianti elektroniniu būdu duoti nurodymus kredito įstaigai dėl disponavimo sąskaitoje esančiais pinigais), kuriais naudojantis atliekami pavedimai – perkeliami negrynieji pinigai[73].

3.4. Atskirų tapatybės vagystės elementų kriminalizavimas Lietuvoje

Lietuvoje tam tikri tapatybės vagystės elektroninėje erdvėje elementai yra vertinami kaip pavojingos veikos, pavyzdžiui, Lietuvos Respublikos baudžiamojo kodekso[74] (toliau – LR BK) 198 str., reglamentuoja neteisėtą elektroninių duomenų perėmimą ir panaudojimą. 1 d. įtvirtinamos alternatyvios veikos, kurios užtraukia baudžiamąją atsakomybę: „neteisėtai stebėjo, fiksavo, perėmė, įgijo, laikė, pasisavino, paskleidė ar kitaip panaudojo neviešus elektroninius duomenis“. 2 d. įtvirtinama kvalifikuota nusikaltimo sudėtis, numatanti atsakomybę už strateginę reikšmę nacionaliniam saugumui arba didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinčių neviešų elektroninių duomenų perėmimą ir panaudojimą. Atsakomybė už šią veiką gali kilti tiek fiziniam, tiek juridiniam asmeniui.

Vis dėlto pabrėžtina, kad tapatybės vagystės elektroninėje erdvėje atveju reikia kalbėti apie nusikalstamų veikų daugetą,[75] t.y. šios pavojingos veikos atveju pavojingi ir priešingi teisei veiksmai gali būti kvalifikuojami kaip nusikalstamų veikų sutaptis pagal LR BK 198 str. ir kitus LR BK specialiosios dalies straipsnius, pavyzdžiui, 154 str. šmeižimas, 155 str. įžeidimas (nusikalstamos veikos garbei ir orumui); 166 str. asmens susižinojimo neliečiamumo pažeidimas, 167 str. neteisėtas informacijos apie privatų asmens gyvenimą rinkimas, 168 str. neteisėtas informacijos apie asmens privatų gyvenimą atskleidimas ir panaudojimas (nusikaltimai asmens privataus gyvenimo neliečiamumui); 173 str. rinkimų ar referendumo dokumento suklastojimas arba suklastoto rinkimų ar

---

[73] **Ušinskaitė D.** Mokėjimo instrumento sąvoka Lietuvos baudžiamojoje teisėje // Jurisprudencija: mokslo darbai, - Vilnius, 2004, Nr. 60 (52). P. 115-124.

[74] **Lietuvos Respublikos baudžiamasis kodeksas** [aktuali redakcija nuo 2008-06-27]. Prieinama internete: http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=323740&p_query=&p_tr2= [žiūrėta 2009 06 03]

[75] Tai teisinė situacija, kai asmuo padaro kelias nusikalstamas veikas, dėl kurių sprendžiamas jo patraukimo baudžiamojon atsakomybėn klausimas.

referendumo dokumento panaudojimas; 182 str. sukčiavimas, 186 str. turtinės žalos padarymas apgaule (nusikalstamos veikos nuosavybei, turtinėms teisėms ir turtiniams interesams); 207 str. kreditinis sukčiavimas, 214 str. netikros elektroninės mokėjimo priemonės gaminimas, tikros elektroninės mokėjimo priemonės klastojimas ar neteisėtas disponavimas elektronine mokėjimo priemone arba jos duomenimis, 215 str. neteisėtas elektroninės mokėjimo priemonės ar jos duomenų panaudojimas (nusikalstamos veikos finansų sistemai); 300 str. dokumento suklastojimas ar disponavimas suklastotu dokumentu, 304 str. melagingos informacijos pateikimas siekiant įgyti dokumentą (nusikalstamos veikos valdymo tvarkai, susijusios su dokumentų klastojimu).

Tuo tarpu kalbant apie tapatybės vagystę, atliekamą fizinėje erdvėje, Lietuvoje ji yra traktuojama kaip priemonė, pasiruošimas kitai neteisėtai veikai padaryti ir *per se* nusikalstama veika nėra laikoma. Todėl šiuo atveju, kai įvykdoma tapatybės vagystė ir kita su ja tiesiogiai susijusi nusikalstama veika, tokia situacija paprastai negali būti traktuojama kaip nusikalstamų veikų sutaptis, t.y. kaip tokia teisinė situacija, kai asmuo padaro kelias nusikalstamas veikas, numatytas viename ar keliuose skirtinguose baudžiamojo kodekso specialiosios dalies straipsniuose, iki priimant apkaltinamąjį nuosprendį dėl padarytų veikų, jei nėra juridinių kliūčių traukti asmenį baudžiamojon atsakomybėn bent už dvi iš padarytų nusikalstamų veikų[76]. Minėtu atveju tokia veika dažniausiai bus kvalifikuojama kaip vagystė ar plėšimas, kurių metu pasisavinami materialūs objektai, fiksuojantys asmens duomenis ar kitą asmeninę informaciją, kuriais pasinaudodamas nusikalstamos veikos subjektas gali įgyvendinti kitus nusikalstamus ketinimus, pavyzdžiui, atlikti sukčiavimą ar dokumentų klastojimą.

Atkreiptinas dėmesys, kad nors, kaip minėta, tam tikri tapatybės vagystė elektroninėje erdvėje elementai patenka į LR BK 198 str. 1 d. reglamentavimo sritį, atlikus šios normos analizę, galima teigti, kad problema yra išsprendžiama tik iš dalies, o 198 str. negali būti vertinamas kaip tapatybės vagystės elektroninėje erdvėje kriminalizavimas. Visų pirma, kritikuotinas įstatymų leidėjo aptariamos veikos objekto susiaurinimas, į normos dispoziciją įtraukiant tik neviešus elektroninius duomenis. O jei tam tikri duomenys yra viešai prieinami? Ar tokiu atveju asmuo gali rinkti, kaupti, sisteminti ar atlikti kitokius veiksmus su viešai prieinamais duomenimis apie kitus asmenis, o nusikalstamos veikos sudėties nebelieka? Arba dar: ar tapatybės vagystė, atliekama fizinėje erdvėje, ir į LR BK specialiąją dalį neįtraukta kaip savarankiška nusikalstama veika, visais atvejais pateks į vagystės ar plėšimo sudėtis? Juk, tarkim, kaip jau buvo minėta 2 skyriaus 3 poskyryje, tapatybės vagystė fizinėje erdvėje gali būti atliekama panaudojant tokius metodus kaip „žiūrėjimas per petį“, „šiukšlių rinkimas“, dingsties ieškojimas, kurie patys savaime nėra kvalifikuojami kaip nusikalstami veiksmai. Kaip tokiu atveju išspręsti problemą, kai tokio pobūdžio veiksmai nėra kriminalizuoti ir apskritai nėra laikomi teisės pažeidimu? Minėtais atvejais tokius veiksmus atlikęs asmuo liktų nenubaustas, nes Lietuvos

---

[76] **Piesliakas V.** Lietuvos baudžiamoji teisė. Kn. 2. P. 125.

Respublikoje nėra teisės akto, kurio normomis remiantis būtų galima patraukti asmenį atsakomybėn už tokių veiksmų atlikimą.

Pažymėtina ir tai, kad LR BK normos negali būti aiškinamos plečiamai, taigi LR BK 198 str. taip pat negalėtų būti taikomas. Toks teisinis reglamentavimas vertintinas kaip teisės spraga: sparčiai plintant tokiam visuomenei pavojingam reiškiniui, kaip tapatybės vagystė, Lietuvos Respublikos teisėsaugos institucijos yra bejėgės kovoti su tokio pobūdžio problema.

Taip pat kyla klausimas: kaip kvalifikuoti asmens veiksmus, kai neteisėta veika dar nepadaryta, tačiau pas asmenį aptinkama kito asmens (asmenų) asmeninė informacija ir (ar) asmens duomenys? O jei tapatybės vagystė atliekama turint tikslą įvykdyti kitą nusikalstamą veiką ar teisės pažeidimą, tai ar egzistuojančios teisės aktų normos apims visus tapatybės vagystės metu įgytų asmens duomenų ir (ar) asmeninės informacijos panaudojimo atvejus?

Šią probleminę situaciją galima iliustruoti parašo fizinėje erdvėje ir elektroninio parašo pavyzdžiais. Abejonių nekyla, kad fizinėje erdvėje savo valią patvirtinant kito asmens parašu tokie veiksmai patenka į LR BK 300 str. reglamentavimo sritį ir yra kvalifikuojami kaip dokumentų klastojimas. Tačiau kalbant apie valios išreiškimą elektroninėje erdvėje, kurioje, kaip jau aptarta 3 skyriaus 3 poskyryje, asmens valia informacinėje sistemoje išreiškiama įvedant atitinkamą vartotojo vardą ir slaptažodį ar PIN kodą, vieningos pozicijos, kaip reikėtų vertinti veiksmus, kai, tarkim, prie informacinės sistemos, naudodamasis tais pačiais prisijungimo duomenimis, jungiasi ne vienas asmuo, nėra. LR BK tokie veiksmai nėra kriminalizuoti, nors juridine prasme, kaip jau tai buvo aptarta anksčiau, tokie veiksmai turėtų būti kvalifikuojami kaip nusikalstama veika. Pradine išeities pozicija būtų galima laikyti Lietuvos Respublikos elektroninių ryšių įstatymo[77] (toliau – Įstatymo) 2 str. 1 ir 3 d. Įstatymo 2 str. 1 d. įtvirtinta, jog vienas iš principų, kuriais grindžiamas elektroninių ryšių veiklos reguliavimas, yra funkcinio lygiavertiškumo principas. Šio principo turinys yra įtvirtintas Įstatymo 2 str. 3 d., kurioje teigiama, jog funkcinio lygiavertiškumo principas reiškia, kad teisės normos turi būti kuo vienodžiau taikomos elektroninių ryšių tinklams ar paslaugoms, atliekantiems analogiškas funkcijas. Taigi, remiantis minėtomis Įstatymo normomis, kito asmens vartotojo vardo ir slaptažodžio panaudojimas turėtų būti kvalifikuojamas kaip klastojimas. Tačiau, kaip minėta, vienos nuomonės ar teismų praktikos šiuo klausimu kol kas nėra.

Kaip matyti iš sumodeliuotų ir trumpai aptartų probleminių ir teisės normų nereglamentuotų situacijų, LR BK specialiosios dalies normų, kriminalizuojančių atskirus, tačiau ne visus tapatybės vagystės elektroninėje erdvėje elementus, analizės, tapatybės vagystės elektroninėje erdvėje vertinimas yra gana kontraversiškas. Todėl siekiant išvengti situacijų, kai asmuo, neturėdamas tam teisės disponuoja kito asmens duomenimis ir (ar) asmenine informacija ir lieka už tai nenubaustas bei

---

[77] **Lietuvos Respublikos elektroninių ryšių įstatymas** [aktuali redakcija nuo 2009-03-15] Prieinama internete: http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=332292&p_query=&p_tr2= [žiūrėta 2009 07 06]

užkirsti kelią nusikalstamos veikoms, kurios potencialiai gali būti padarytos pasinaudojant tapatybės vagystės metu įgytais duomenimis ir (ar) informacija, tapatybės vagystę elektroninėje erdvėje siūlytina kriminalizuoti.

3.5. Skyriaus apibendrinimas

Tapatybės vagystė elektroninėje erdvėje yra globali problema, todėl ypač svarbi užsienio teisėsaugos institucijų pagalba siekiant efektyviai kovoti su šia visuomenei pavojinga veika. Tais atvejais, kai užsienio valstybė neturi įstatymų, kriminalizuojančių tapatybės vagystę elektroninėje erdvėje, yra apsunkinamos informaciją renkančios valstybės galimybės rinkti tapatybės vagystės elektroninėje erdvėje įrodymus atitinkamoje užsienio valstybėje ir patraukti atsakomybėn kaltus asmenis. Todėl svarbu, kad valstybės vienodai traktuotų tapatybės vagystę elektroninėje erdvėje, o tai yra neišvengiamai susiję su tapatybės vagystės elektroninėje erdvėje kriminalizavimo problema.

Pastaruoju metu netyla diskusijos, ar tapatybės vagystė turėtų būti kriminalizuota ir ar tokios veikos sudėties įtraukimas į valstybių baudžiamuosius įstatymus padėtų efektyviau kovoti su šiuo reiškiniu. Daugelyje valstybių tapatybės vagystė *per se* apskritai nėra laikoma teisės pažeidimu, o patenka į įvairias išimtis, susijusias su duomenų slaptumu, apsauga ar klastote, už kuriuos galima asmenį patraukti baudžiamojon atsakomybėn. Tuo tarpu kitos valstybės laikosi nuomonės, jog tokios veikos yra specifinės, todėl tapatybės vagystės kriminalizavimas yra naudinga priemonė siekiant užkirsti kelią tapatybės vagystės sukeliamoms grėsmėms.

Europos Komisija palaiko iniciatyvą kriminalizuoti tapatybės vagystę. 2007 m. gegužės 22 d. komunikate KOM (2007) 267 Bendrosios politikos, skirtos kovai su elektroniniais nusikaltimais, linkme pabrėždama, jog ypatinga problema, kuriai gali reikėti teisės akto, susijusi su situacija, kai elektroniniai nusikaltimai padaromi pasinaudojant tapatybės vagyste. Komisija atkreipia dėmesį, kad tapatybės vagystė nėra kriminalizuota visose valstybėse narėse, ir teigia, jog dažniausiai tapatybės vagystės nusikaltimą įrodyti lengviau negu sukčiavimo nusikaltimą, todėl tapatybės vagystės kriminalizavimas visose valstybėse narėse pagerintų ES teisėsaugos institucijų bendradarbiavimą. OECD taip pat siūlo kriminalizuoti tapatybės vagystę.

Lietuvoje tapatybės vagystė nėra kriminalizuota, tačiau tam tikri tapatybės vagystės elektroninėje erdvėje atvejai patenka į LR BK 198 str. reglamentavimo sritį. Vis dėlto, kritikuotinas įstatymų leidėjo nusikalstamos veikos objekto susiaurinimas, į normos dispoziciją įtraukiant tik neviešus elektroninius duomenis. Tapatybės vagystė, atliekama fizinėje erdvėje, apskritai nėra įtraukta į LR BK specialiąją dalį kaip savarankiška nusikalstama veika, nors pastaruoju metu dažnai nutinka taip, jog egzistuojančių LR BK normų reglamentavimo sritis neapima visų minėtos veikos elementų. Lietuvos teisės aktai nereglamentuoja situacijos, kai neteisėta veika dar nepadaryta, tačiau pas asmenį aptinkama kito

asmens (asmenų) asmeninė informacija ir (ar) asmens duomenys, o egzistuojančios teisės aktų normos neapima visų tapatybės vagystės metu įgytų asmens duomenų ir (ar) asmeninės informacijos panaudojimo atvejų. Kadangi tapatybės vagystė yra pavojinga veika, dažniausiai naudojama palengvinti tokių nusikaltimų, kaip nelegali imigracija, terorizmas, šnipinėjimas, šantažas, finansiniai nusikaltimai, atlikimą, siūlytina šią veiką kriminalizuoti.

Atlikus ekspertų apklausos metu gautos informacijos analizę, galima pritarti ekspertų siūlymui tapatybės vagystę elektroninėje erdvėje apibrėžti kaip gavimą pagrindinių asmens tapatybę liudijančios informacijos elementų (elektroninėje erdvėje), siekiant apsimesti tuo asmeniu, su tikslu atlikti nusikaltimus. Kai nėra tikslo atlikti nusikaltimus, veika gali būti apibrėžiama kaip piktnaudžiavimas tapatybe, o kai naudojamasi neegzistuojančio asmens tapatybe – tapatybės klastote. Taip pat reikėtų sutikti su ekspertų nuomone, jog tapatybė fizinėje erdvėje yra visiškai kitokia nei elektroninėje erdvėje: fizinėje erdvėje savo tapatybę asmuo patvirtina vienu iš privalomų elementu – asmens dokumentu, tuo tarpu elektroninėje erdvėje tapatybę gali atstoti prisijungimo vardas ir slaptažodis.

4. TAPATYBĖS VAGYSTĖS ELEKTRONINĖJE ERDVĖJE SUDĖTIES MODELIS

Nusikalstama veika baudžiamosios teisės kontekste suprantama kaip pavojinga ir baudžiamojo įstatymo uždrausta veika. Ji gali būti nagrinėjama įvairiais aspektais: kaip atitinkamas poelgis, kaip socialinio gyvenimo reiškinys, kaip asmens savybių, jo charakterio bruožų pasekmė. Šie aspektai suponuoja ir skirtingas nusikalstamos veikos tyrimo kryptis. Tačiau baudžiamoji teisė apsiriboja nusikalstamos veikos nagrinėjimu teisiniu aspektu, t.y. baudžiamajai teisei yra reikšmingas nusikalstamos veikos kaip atitinkamo poelgio požymių atskleidimas ir jų formalizavimas įstatyme. Šiuo aspektu nusikalstama veika apibrėžiama kaip sąmoningas ir valingas, pavojingas, priešingas teisei žmogaus elgesys išoriniame pasaulyje.

Žmogaus poelgį galima įvardyti nusikalstama veika tik tada, kai nustatyti visi nusikalstamos veikos sudėties požymiai. Nusikalstamos veikos sudėtis – tai teisinė žmogaus poelgio priešingumo baudžiamajai teisei išraiška[78]. Esminis terminų „nusikalstama veika“ ir „nusikalstamos veikos sudėtis“ skirtumas yra tas, kad nusikalstamos veikos terminas vartojamas apibrėžti objektyvios tikrovės reiškinį, uždraustą baudžiamuoju įstatymu, o nusikalstamos veikos sudėties terminas vartojamas teisiškai įvertinti objektyvios tikrovės reiškinį ir konkretų atvejį[79].

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

4.1. Tapatybės vagystės elektroninėje erdvėje sudėties objektyvieji požymiai

Objektyvieji nusikalstamos veikos sudėties požymiai – tai išorinė, akiai matoma šios veikos dalis. Jiems priskirtini: baudžiamojo įstatymo saugomos vertybės, pavojinga veika, nusikalstamos veikos dalykas, padarymo būdas, jos padarymo laikas, vieta ir priemonės, nusikalstamos veikos padarymo aplinkybės, pavojingi padariniai, priežastinis padarytos veikos ir kilusių (įstatyme numatytų) pavojingų padarinių ryšys, asmens, trauktino baudžiamojon atsakomybėn, amžius, specialaus subjekto požymis[80].

---

[78] **Piesliakas V.** Lietuvos baudžiamoji teisė. Kn. 1. P. 175.
[79] Ten pat, p. 178.
[80] Ten pat, p. 180, 181.

Kaip jau buvo minėta, tapatybės vagystė, remiantis LR BK, *per se* nėra laikoma nusikaltimu. Tam tikrais atvejais viena iš jos rūšių – tapatybės vagystė elektroninėje erdvėje – patektų į LR BK 198 str. reglamentavimo sritį. Tokia situacija sukelia teisinį neaiškumą, o aiškaus ir vienareikšmiško teisinio reguliavimo nebuvimas tapatybės vagystės atžvilgiu vertintinas kaip įstatymų leidėjo padaryta teisės spraga. Siekiant išspręsti šią problemą ir užtikrinti efektyvų tarptautinį bendradarbiavimą su užsienio valstybių teisėsaugos institucijomis, LR BK tikslinga įtvirtinti tapatybės vagystės, kaip savarankiškos nusikalstamos veikos, sudėtį.

Objektas. Kalbant apie bendruosius tapatybės vagystės kriminalizavimo aspektus, buvo minėta, jog tam tikri tapatybės vagystės elektroninėje erdvėje elementai patenka į LR BK 198 str. reguliavimo sritį. Tačiau analizuojant LR BK 198 str. įtvirtintos nusikalstamos veikos objektyviuosius požymius, matyti, kad šios veikos objektas – nevieši elektroniniai duomenys. Įstatymo leidėjas, į normos dispoziciją įtraukdamas tik tam tikrą elektroninių duomenų kategoriją, būtent, neviešus duomenis, nepagrįstai susiaurino tapatybės vagystės elektroninėje erdvėje objektą, nes pasikėsinimas gali būti nukreiptas ir į duomenis, kurie yra viešai prieinami – tokie veiksmai taip pat turėtų būti vertinami kaip tapatybės vagystė elektroninėje erdvėje. Pasikėsinimas į elektroninius duomenis, kaip į įstatymo saugomą vertybę, galimas tokius duomenis tvarkant informacinių ir ryšio technologijų pagalba. Tačiau, kaip jau buvo ne kartą minėta, tapatybės vagystė gali būti įvykdoma ne tik elektroninėje, bet ir fizinėje erdvėje, todėl kriminalizuotos turėtų būti abi tapatybės vagystės rūšys.

Dar viena problema, susijusi su baudžiamojo įstatymo saugoma vertybe – objektu, – yra ta, kad Lietuvos Respublikos baudžiamosios teisės teorijoje ir praktikoje laikomasi požiūrio, jog vagystės objektas yra visų rūšių ir formų nuosavybė, o turtas pagal LR BK 178 str. – tai turintys vertę bei fizinius parametrus (gabaritus, svorį, skaičių, kiekį) daiktai (pavyzdžiui, namų apyvokos daiktai, transporto ir gamybos priemonės, asmeniniai daiktai, taip pat pinigai ir vertybiniai popieriai)[81]. Taigi, remiantis LAT pozicija, vagystės dalykas yra svetimas materialus judamas (kilnojamo pobūdžio), turintis ekonominę vertę turtas, tuo tarpu informacija nepatenka į LR BK 178 str. reglamentavimo sritį, nes neatitinka materialumo požymio, todėl negali būti laikoma vagystės dalyku. Panašios pozicijos laikosi ir britų informacijos ir ryšių teisės profesorius dr. Ian Walden, teigiantis, jog sąvoka „tapatybės vagystė“ apskritai yra vartojama netinkamai, kadangi informacija pati savaime negali būti pavogta. Veika tokiu atveju kaip vagystė galėtų būti kvalifikuojama tik tuomet, jei duomenys, kuriais remiantis galima identifikuoti asmenį, yra kokioje nors apčiuopiamoje formoje, nuosavybės teise priklausančioje kitam asmeniui, pavyzdžiui, pavogta mokėjimo kortelė[82].

---

[81] **2005 m. birželio 23 d. Lietuvos Aukščiausiojo Teismo Senato nutarimas Nr. 52 „Dėl teismų praktikos vagystės ir plėšimo baudžiamosiose bylose“**, 4 punktas.
Prieinama internete: http://www.lat.lt/4_tpbiuleteniai/senos/nutartis.aspx?id=29259 [žiūrėta 2009 06 03]

[82] **Ian Walden.** Computer Crimes and Digital Investigations, 2007. P.116.

Toks požiūris kritikuotinas. Sparčiai vystantis informacinėms ir ryšio technologijoms, o visuomenei vis daugiau naudojantis elektronine erdve, vagystės dalykas turėtų apimti ne tik materialumo požymiais pasižymintį turtą, bet ir informaciją bei duomenis, kurių vertė dažnai yra kur kas didesnė nei fizinius parametrus turinčių ir materialumo požymį tenkinančių daiktų, o neteisėtai disponuojant tokia informacija ir (ar) duomenimis nukentėjusiajam gali būti padaryta didelė žala. Taigi tapatybės vagystės objektu turėtų būti laikoma informacija ir duomenys, kurių pagalba gali būti nustatyta asmens tapatybė, nesvarbu, ar tokia informacija ir duomenys yra elektroninėje formoje, ar išsaugoti materialioje laikmenoje.

Dalykas. Nusikalstamos veikos dalykas yra tai, ką veikiant pažeidžiamos baudžiamojo įstatymo saugomos vertybės. Fizinėje erdvėje atliekant tapatybės vagystę priešingi teisei veiksmai yra nukreipti prieš konkretų asmenį, tuo tarpu elektroninėje erdvėje – ne tik prieš konkretų asmenį (pavyzdžiui, panaudojant nepageidaujamas elektroninio pašto žinutes), bet ir prieš informacines sistemas bei elektroninių ryšių tinklus, kurių pagalba atliekamas duomenų tvarkymas. Taigi tapatybės vagystės elektroninėje erdvėje dalykas yra kur kas platesnis nei tapatybės vagystės fizinėje erdvėje.

Pavojinga veika. Tapatybės vagystė elektroninėje erdvėje turėtų būti kvalifikuojama kaip nusikalstama veika, t.y. kaip pavojinga ir baudžiamojo įstatymo uždrausta veika. Ji gali būti nagrinėjama įvairiais aspektais, tačiau šiame magistro baigiamajame darbe nusikalstama veika nagrinėjama apsiribojant baudžiamosios teisės teisiniais aspektais, t.y. šiuo atveju reikšmingas nusikalstamos veikos kaip atitinkamo poelgio požymių atskleidimas ir jų formalizavimas įstatyme. Šiuo aspektu nusikalstama veika suprantama kaip sąmoningas ir valingas, pavojingas, priešingas teisei žmogaus elgesys išoriniame pasaulyje.

Išoriškai kiekviena pavojinga veika gali pasireikšti dviem formomis: veikimu ir neveikimu. Veikimas yra pagrindinė kiekvienos pavojingos veikos padarymo forma, kuri pasireiškia įvairių veiksmų, kuriais kėsinamasi į baudžiamojo įstatymo saugomus teisinius gėrius, atlikimu. Kiekvieną veikimą sudaro sąmoningas ir valingas žmogaus kūno judesys. Tapatybės vagystė elektroninėje erdvėje taip pat padaroma veikimu, kai asmuo, sąmoningai ir valingai imasi tam tikrų veiksmų, kad naudodamasis atitinkamais metodais gautų duomenis ir kitą asmeninę informaciją, kuriais remiantis galima nustatyti kito asmens tapatybę, o vėliau apsimesdamas tuo asmeniu galėtų įgyvendinti savo tikslus (paprastai neteisėtus). Taigi tapatybės vagystė elektroninėje erdvėje atliekama aktyviais veiksmais: neteisėtai stebint, fiksuojant, perimant, įgyjant, laikant, pasisavinant, paskleidžiant ar kitaip panaudojant duomenis ir (ar) asmeninę informaciją apie kitą asmenį.

Padariniai. Tapatybės vagystės elektroninėje erdvėje sudėtis turėtų būti formali, t.y. normos dispozicijoje neturėtų būti reikalaujama, kad kiltų atitinkama žala, norint patraukti asmenį atsakomybėn. Atsakomybė padarius šią veiką kiltų vien už tokios veikos padarymą. Tokiu atveju atsakomybėn būtų traukiama už neteisėtą duomenų ir (ar) asmeninės informacijos apie kitą asmenį

gavimą, rinkimą, kaupimą, įgijimą ir pan., neatsižvelgiant į faktą, kad kaltininkas, atlikdamas veiksmus su kito asmens duomenimis ir (ar) asmenine informacija, nerealizavo jokių nusikalstamų ketinimų, t.y. neatliko jokios kitos nusikalstamos veikos. Pagrindinis argumentas, kodėl tapatybės vagystės elektroninėje erdvėje sudėtis turėtų būti formali, yra tas, kad šis reiškinys yra labai pavojingas ir glaudžiai susijęs su tokiais opiais klausimais kaip privatumo ir asmens duomenų apsauga. Situacija, kai duomenys ar asmeninė informacija apie kitą asmenį renkama neturint kokio nors konkretaus, dažniausiai nusikalstamo, tikslo, yra mažai tikėtina ir apskritai vargu ar įmanoma.

Padarymo būdas. Nusikalstamos veikos padarymo būdas, kaip jos sudėties požymis, labai glaudžiai susijęs su pavojingos veikos požymiu. Tai pavojingos veikos raiškos būdas ar jos padarymo metodas. Šis nusikalstamos veikos sudėties požymis dažnai naudojamas įstatymų leidėjo formuluojant nusikalstamų veikų sudėtis[83]. Tačiau atsižvelgiant į tai, kad tapatybės vagystė elektroninėje erdvėje gali būti atliekama įvairiais metodais, kurie savo ruožtu kinta ir tobulėja priklausomai nuo informacinių ir ryšių technologijų pažangos, teisės normos dispozicijoje, įtvirtinančioje tapatybės vagystės elektroninėje erdvėje sudėtį, būdų netikslinga įvardyti konkrečius metodus. Taip būtų išvengiama teisės normos veikimo srities apribojimo ir situacijų, kai pasinaudojus pažangesniais metodais, neliktų nusikalstamos veikos sudėties ir neteisėtus veiksmus atlikęs asmuo išvengtų atsakomybės.

Reikia akcentuoti ir tai, kad į tapatybės vagystės sudėtį nereikėtų įtraukti sąlygos „be asmens žinios ar sutikimo“, kaip privalomojo nusikalstamos veikos požymio. Net jei asmuo laisva valia kitam asmeniui perduoda, pavyzdžiui, elektroninės bankininkystės instrumentus (vartotojo vardą, slaptažodį, kodų kortelę), juridine prasme jau yra atliekama neteisėta veika. Kitas asmuo neteisėtai įgyja teisę disponuoti minėtais instrumentais, o tokia situacija vertintina kaip tapatybės vagystė – naudojantis, pavyzdžiui, elektronine bankininkyste banko informacinėje sistemoje toks asmuo identifikuojamas kaip pradinis vartotojas, kuriam buvo suteiktas elektroninės bankininkystės paslaugų paketas, nors šiuo paketu naudojas ne tas vartotojas.

Padarymo priemonės ir įrankiai. Dažnai terminai „priemonė“ ir „įrankis“ baudžiamosios teisės kontekste suvokiami kaip sinonimai. Tačiau skirtumas tarp šių sąvokų vis dėlto yra. Nusikalstamos veikos padarymo priemonės – tai materialūs daiktai, kurie patys nenaudojami nusikalstamai veikai padaryti, tačiau palengvina nusikalstamos veikos padarymą arba sudaro prielaidas jai padaryti; tuo tarpu įrankiai – tai materialaus pasaulio objektai, kuriais tiesiogiai padaroma nusikalstama veika. Tapatybės vagystės elektroninėje erdvėje atveju šias sąvokas dar sunkiau atriboti: veikiama elektroninėje erdvėje, todėl „įrankių“ sąvoka galėtų būti iš viso eliminuota.

---

[83] **Piesliakas V.** Lietuvos baudžiamoji teisė. Kn. 1. P. 298.

Tačiau atsižvelgiant į tai, kad įprastai vartojamos sąvokos sparčiai vystantis informacinėms ir ryšio technologijoms informacinėje visuomenėje įgauna naujas prasmes ir požymius, ir šiuo atveju, kalbant apie tapatybę elektroninėje erdvėje, galima atsiriboti nuo įrankio materialaus pobūdžio. Tokiu atveju į „įrankio“ kategoriją patektų nepageidaujamos elektroninio pašto žinutės, falsifikuoti interneto tinklapiai, kuriais naudojantis išgaunami prisijungimo prie informacinių sistemų slaptažodžiai ar kiti konfidencialūs duomenys, taip pat šnipinėjimo programinė įranga, kuri nežinant vartotojui renka informaciją apie lankomas interneto svetaines, vartotojo vardą, elektroninio pašto adresus, programas ar bylas, esančias kompiuteryje, arba registruoja vartotojo atliekamus veiksmus internete ir siunčia šiuos duomenis tretiesiems asmenims.

Nusikalstamos veikos padarymo priemone tapatybės vagystės elektroninėje erdvėje atveju laikytinos informacinės ir ryšio technologijos, įgalinančios internetinius sukčius veikti elektroninėje erdvėje, t.y. atlikti efektyvius veiksmus per atstumą, neturint tiesioginio kontakto su nukentėjusiuoju.

Subjektas. Tapatybės vagystės elektroninėje erdvėje subjektu gali būti bet kas – netgi asmuo, nesulaukęs reikiamo amžiaus, kad baudžiamojo įstatymo pagrindu kiltų atsakomybė. Todėl baudžiamajame įstatyme turėtų būti įtvirtintos atitinkamos bendrųjų normų išimtys, reglamentuojančios subjekto amžių, nuo kurio gali kilti baudžiamoji atsakomybė už tapatybės vagystę.

4.2. Tapatybės vagystės elektroninėje erdvėje sudėties subjektyvieji požymiai

Subjektyvieji nusikalstamos veikos sudėties požymiai apibūdina žmogaus vidinę – psichinę, savo elgesį suvokiančią, pateisinančią, nukreipiančią ir kontroliuojančią pusę. Šiems požymiams priskirtini: pakaltinamumas, kaltė, nusikalstamos veikos padarymo motyvas ir tikslas[84].

Pakaltinamumas. Baudžiamojon atsakomybėn traukiamas ne kiekvienas žmogus, padaręs pavojingą veiką, o tik toks, kuris pasižymi tam tikromis savybėmis. Viena iš jų yra pakaltinamumas. Baudžiamosios teisės subjektais gali būti tik sąmoningi, normalios psichikos žmonės, o baudžiamojo poveikio priemonės gali pasiekti tikslą tik tuo atveju, jei jos taikomos žmogui, turinčiam normalius psichinius gebėjimus, galinčiam laisvai orientuotis aplinkoje, suprasti savo poelgių esmę, numatyti jų padarinius, taigi sąmoningai pasirinkti teisingą elgesio variantą[85].

LR BK nepateikiama pakaltinamumo sąvoka, tačiau ji nesunkiai išvedama iš nepakaltinamumo apibrėžimo, įtvirtinto LR BK 17 str., todėl pakaltinamumas turi būti suprantamas kaip gebėjimas darant veiką suvokti daromos veikos pobūdį ir valdyti savo poelgį. Taip pat pabrėžtina, kad pakaltinamumas yra būtina kaltės sąlyga. Taigi tapatybės vagystės elektroninėje erdvėje atveju

---

[84] Ten pat, p. 180, 181, 319.
[85] Ten pat, p. 325.

atsakomybė kils tik pakaltinamam ir kaltam asmeniui, t.y. tokiam, kuris darydamas tokią nusikalstamą veiką suvokė jos pobūdį ir galėjo valdyti savo veiksmus.

Kaltė. 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[86].

LR BK skiriamos dvi kaltės formos: tyčinė ir neatsargi kaltė. Pabrėžtina tai, kad tapatybės vagystė elektroninėje erdvėje gali būti atliekama tik tiesiogine tyčia. Jau buvo minėta, kad siūlytina konstruoti formalią tapatybės vagystės elektroninėje erdvėje sudėtį, todėl tiesioginė tyčia šios veikos atžvilgiu turi būti suprantama taip, kaip ji įtvirtinta LR BK 15 str. 2 d. 1 p., kuriame teigiama, kad nusikaltimas ar baudžiamasis nusižengimas yra padarytas tiesiogine tyčia, jeigu jį darydamas asmuo suvokė pavojingą nusikalstamos veikos pobūdį ir norėjo taip veikti.

Nusikalstamos veikos padarymo tikslas. Nusikalstamos veikos padarymo tikslas – tai asmens siekiai, susiję su nusikalstamos veikos padarymu, priežastys, dėl ko jis nusprendė padaryti nusikalstamą veiką. Nusikalstamos veikos padarymo tikslas paprastai išreiškiamas LR BK straipsnių dispozicijose vartojant žodžius „siekiant“ arba „turint tikslą“[87]. Iš pirmo žvilgsnio gali pasirodyti, jog konstruojant tapatybės vagystės elektroninėje erdvėje dispoziciją, į ją nereikėtų įtraukti nusikalstamos veikos tikslo įvykdyti kitas nusikalstamas veikas ar teisės pažeidimus. Taip būtų išvengiama situacijų, kai neįrodžius nusikalstamų ar neteisėtų ketinimų (tokiu atveju nebūtų ir šios veikos sudėties), asmuo, atlikęs neteisėtus veiksmus, išvengtų atsakomybės. Tačiau atsižvelgiant į tai, kad tapatybės vagystė, remiantis nusikalstamų ketinimų kriterijumi, gali būti klasifikuojama į tapatybės vagystę (tapatybės pasisavinimą nusikalstamais tikslais) ir piktnaudžiavimą tapatybe, problemą galima išspręsti kriminalizuojant abi minėtas veikas. Tokiu atveju baudžiamoji atsakomybė kiltų ne tik tada, kai nusikalstama veika įvykdoma turint ketinimų įvykdyti kitas nusikalstamas veikas (atsakomybė už tapatybės vagystę – tapatybės pasisavinimą nusikalstamais tikslais), bet ir tada, kai asmuo atlieka įvairius veiksmus su kitą asmenį identifikuojančiais ar galinčiais identifikuoti duomenimis ir (ar) asmenine informacija (pavyzdžiui, tokio pobūdžio duomenis ir informaciją renka, sistemina ir pan.), tačiau nusikalstamų ketinimų, kuriuos galėtų realizuoti tokių duomenų ir (ar) asmeninės informacijos pagalba, neturi (atsakomybė šiuo atveju kiltų už piktnaudžiavimą tapatybe).

Tapatybės vagystės (tapatybės pasisavinimo nusikalstamais tikslais) atveju pradinis šios nusikalstamos veikos padarymo tikslas yra subjekto siekis apsimesti kitu asmeniu, t.y. identifikuotis elektroninėje erdvėje apsimetant pradiniu vartotoju, iš kurio buvo pasisavinti tokie duomenys ir asmeninė informacija kaip vartotojo vardas, slaptažodis, PIN kodas, kodų kortelės ir kita, bei atlikti nusikalstamas veikas – nusikaltimus ir (ar) baudžiamuosius nusižengimus. Tuo tarpu

---

[86] Ten pat, p. 336.
[87] Ten pat, p. 414, 415.

piktnaudžiaudamas tapatybe subjektas nesiekia įvykdyti jokios nusikalstamos veikos, o minėtus duomenis ir informaciją gali rinkti dėl įvairių priežasčių, pavyzdžiui, norėdamas prisijungti kito asmens vardu prie socialinių tinklapių ir bendrauti šio asmens vardu, prisijungti prie kito asmens elektroninio pašto dėžutės ir perskaityti svetimus laiškus, prisijungti prie banko informacinės sistemos ir stebėti kito asmens pajamas ir išlaidas, prisijungti prie Nekilnojamojo turto registro duomenų bazės ir domėtis, kokį nekilnojamąjį turtą turi konkretūs asmenys ir pan. Taip pat labai tikėtina, kad piktnaudžiavimo tapatybe subjektas renkamus duomenis ir informaciją apie tam tikrus asmenis gali atlygintinai perduoti tretiesiems asmenims, kurie pasinaudodami tokiais duomenimis ir (ar) informacija realizuos nusikalstamus ketinimus.

Kaip jau buvo minėta, vien pats faktas, kad asmuo, neturėdamas tam teisės, turi galimybę disponuoti kito asmens asmenine informacija, sudaro pagrįstą prielaidą, kad neteisėti ketinimai gali būti realizuoti ne iš karto, vos tik gavus tokio pobūdžio informaciją, bet praėjus tam tikram laiko tarpui, t.y. išlieka potenciali galimybė tokią informaciją panaudoti vėliau. Vis dėlto, kvalifikuojant veiką kaip tapatybės vagystę (tapatybės pasisavinimą nusikalstamais tikslais) ar piktnaudžiavimą tapatybe, reikėtų atsižvelgti į ketinimus, kuriuos subjektas turėjo nusikalstamos veikos padarymo metu.

4.3. Lietuvos Respublikos baudžiamojo kodekso specialiosios dalies pakeitimo projektas

Ankstesniuose šio skyriaus poskyriuose aptarus tapatybės vagystės elektroninėje erdvėje, kaip savarankiškos nusikalstamos veikos, objektyviuosius ir subjektyviuosius sudėties požymius, siūlytinas alternatyvus LR BK keitimas, susijęs su tapatybės vagystės elektroninėje erdvėje kriminalizavimu.

Pirmoji alternatyva – atsisakyti „neviešų elektroninių duomenų“ sąvokos, minimos LR BK 198 str., įtvirtinant tik „duomenų“ sąvoką, kuri apimtų ir duomenis, kuriais remiantis gali būti nustatyta asmens tapatybė. Šiuo atveju LR BK 198 str. 1 d. normos dispozicija skambėtų taip: „Tas, kas neteisėtai stebėjo, fiksavo, perėmė, įgijo, laikė, pasisavino, paskleidė ar kitaip panaudojo duomenis“. Tačiau tokia normos dispozicija vertintina kaip neįtvirtinanti esminių, tapatybės vagystei elektroninėje erdvėje būdingų požymių.

Kita galima LR BK keitimo alternatyva – LR BK papildyti nauju straipsniu, kuriame būtų įtvirtinta tapatybės vagystės, kaip savarankiškos nusikalstamos veikos, sudėtis, nepriklausomai nuo šios veikos įvykdymo būdo ir vietos, t.y. nedarant skirtumo tarp tapatybės vagystės elektroninėje erdvėje ir tapatybės vagystės fizinėje erdvėje. Siūloma teisės norma galėtų skambėti taip: „tas, kas neturėdamas tam teisės, perėmė, įgijo, laikė, naudojo, paskleidė, disponavo ar atliko kitokius veiksmus su asmens duomenimis ir (ar) asmenine informacija apie kitą asmenį, siekdamas identifikuotis kaip asmuo, iš kurio tokie duomenys ir (ar) asmeninė informacija buvo pasisavinti, tam, kad atliktų kitas nusikalstamas veikas“. Tačiau šiuo atveju į tokios normos reguliavimo sritį nepatektų tie atvejai, kai

asmuo atlieka įvairius veiksmus su kito asmens duomenimis ir (ar) asmenine informacija, siekdamas apsimesti tuo asmeniu, iš kurio buvo gautos jį identifikuojančios priemonės, tačiau *neturėdamas tikslo įvykdyti nusikalstamą veiką.*

Taigi siūlomas trečias ir, rodos, optimalus problemos sprendimo variantas – LR BK papildyti nauju straipsniu, kuriame būtų numatoma atsakomybė už skirtingas tapatybės vagystės rūšis. Tapatybės vagystės įvykdymas elektroninėje erdvėje informacinių ir ryšio technologijų pagalba turėtų būti įtvirtintas kaip kvalifikuojantis tapatybės vagystės (tapatybės pasisavinimo nusikalstamais tikslais) sudėties požymis atsižvelgiant į tai, kad ši veika pagal atlikimo būdų, gautų duomenų ir informacijos apie kitą asmenį panaudojimo sričių įvairovę, pavojingumo mastą ir latentiškumą turėtų būti vertinama kaip pavojingesnė veika nei tapatybės vagystė fizinėje erdvėje. Šiuo atveju kvalifikuotos nusikalstamos veikos sudėties įtvirtinimą lemtų būtent veikos įvykdymo būdas, kuris, kaip jau buvo minėta, yra glaudžiai susijęs su pavojingos veikos požymiu bei dažnai naudojamas įstatymų leidėjo formuluojant nusikalstamų veikų sudėtis. Šiai pozicijai pagrįsti galima pateikti keletą pavyzdžių, kur nusikalstamos veikos padarymo būdas lemia veikos pavojingumą ir yra įtvirtinamas kaip kvalifikuotos nusikalstamos veikos sudėties požymis: BK 178 str. 1 dalis reglamentuoja vagystę, o šio straipsnio 2 d. įtvirtina kvalifikuotą vagystės sudėtį, į straipsnio dispoziciją įtraukiant nusikalstamos veikos būdą – *įsibrovimą* į patalpą, saugyklą ar saugomą teritoriją („<...> pagrobė svetimą turtą įsibrovęs į patalpą, saugyklą ar saugomą teritoriją <...>“); BK 187 str. 1 d. reglamentuoja svetimo turto sunaikinimą ar sugadinimą, o minėto straipsnio 2 d. įtvirtina kvalifikuotą šios veikos sudėtį atsižvelgiant į veikos įvykdymo būdą – „<...> sunaikino ar sugadino svetimą turtą *visuotinai pavojingu būdu* arba *išardydamas ar sugadindamas įrenginį ar agregatą, jeigu dėl to galėjo nukentėti žmonės* <...>“ ir pan.

Vertinant tapatybės vagystės rūšių pavojingumą, manytina, jog tapatybės vagystė elektroninėje erdvėje yra pavojingesnė už tapatybės vagystę fizinėje erdvėje: fizinėje erdvėje apsisaugoti nuo tapatybės vagystės yra sąlyginai paprasta, tuo tarpu tapatybės vagystės elektroninėje erdvėje atveju – kur kas sudėtingiau dėl šios veikos įvykdymo būdų įvairovės ir dėl informacinių bei ryšio technologijų suteikiamų galimybių. Internetiniams sukčiams puikiai pavyksta pasinaudoti programinės įrangos spragomis, elektroninių paslaugų vartotojų nerūpestingumu ir neapdairumu, menkomis žiniomis apie elektroninėje erdvėje tykančius pavojus jų privatumui, asmens duomenims ir asmeninei informacijai, dėl ko sparčiai daugėja nukentėjusiųjų nuo tapatybės vagystės elektroninėje erdvėje skaičius. Patys nukentėjusieji dažnai tik po kurio laiko susivokia, jog tapo minėtos veikos aukomis. Reikia pabrėžti, jog informacinėmis ir ryšio technologijomis bei jų pažangos tendencijomis besidomintis ir šias technologijas išmanantis žmogus, turintis piktų, neteisėtų ketinimų, visada bus pranašesnis už paprastą elektroninės erdvės naudotoją.

Taigi grįžtant prie tapatybės vagystės rūšių kriminalizavimo, abiejų veikų sudėtyse turėtų būti įtvirtintas nusikalstamų ketinimų požymis. Tame pačiame straipsnyje be minėtų nusikalstamų veikų

sudėčių turėtų būti įtvirtinta ir piktnaudžiavimo tapatybe – kaip mažiau pavojingos veikos – sudėtis, joje nenumatant nusikalstamų ketinimų požymio ir kvalifikuojant tokio pobūdžio veiką kaip baudžiamąjį nusižengimą. LR BK specialiosios dalies straipsnis, reglamentuojantis tapatybės vagystę, galėtų atrodyti taip:

178(1) Tapatybės vagystė

1. Tas, kas, neturėdamas tam teisės, perėmė, įgijo, laikė, naudojo, paskleidė, disponavo ar atliko kitokius veiksmus su asmens duomenimis ir (ar) asmenine informacija apie kitą asmenį, siekdamas identifikuotis kaip asmuo, iš kurio tokie duomenys ir (ar) asmeninė informacija buvo pasisavinti, tam, kad atliktų kitas nusikalstamas veikas, baudžiamas...

2. Tas, kas padarė šio straipsnio 1 dalyje numatytą veiką pasinaudodamas informacinių ir ryšio technologijų pagalba, baudžiamas...

3. Tas, kas atliko šio straipsnio 1 ir (ar) 2 dalyje numatytus veiksmus, tačiau neturėjo tikslo įvykdyti nusikalstamą veiką, padarė baudžiamąjį nusižengimą ir baudžiamas...

4.4. Skyriaus apibendrinimas

Tapatybės vagystė turėtų būti kvalifikuojama kaip nusikalstama veika, t.y. kaip sąmoningas ir valingas, pavojingas, priešingas teisei žmogaus elgesys išoriniame pasaulyje, pasireiškianti objektyviaisiais ir subjektyviaisiais požymiais, apibrėžiančiais tapatybės vagystės sudėtį.

Šios veikos objektas – informacija ir duomenys, kurių pagalba gali būti nustatyta asmens tapatybė, nesvarbu, ar tokia informacija ir duomenys yra vieši ar nevieši, yra elektroninėje formoje, ar išsaugoti materialioje laikmenoje. Dalykas, priklausomai nuo šios veikos rūšies, pasireiškia tam tikra specifika: fizinėje erdvėje priešingi teisei veiksmai yra nukreipti prieš konkretų asmenį, tuo tarpu elektroninėje erdvėje – ne tik prieš konkretų asmenį, bet ir prieš informacines sistemas bei elektroninių ryšių tinklus, kurių pagalba atliekamas duomenų tvarkymas.

Aptariama pavojinga veika atliekama aktyviais veiksmais: neteisėtai stebint, fiksuojant, perimant, įgyjant, laikant, pasisavinant, paskleidžiant ar kitaip panaudojant duomenis ir asmeninę informaciją apie kitą asmenį. Pavojingų padarinių požymio šios veikos atveju neturėtų būti reikalauja, t.y. tapatybės vagystės sudėtis turėtų būti formali. Kadangi tapatybės vagystė elektroninėje erdvėje pasireiškia įvykdymo būdų įvairove, šią veiką reglamentuojančios teisės normos dispozicijoje pakaktų įtvirtinti, jog tokia veika gali būti atlikta pasinaudojant informacinėmis ir ryšio technologijomis.

Tapatybės vagystės elektroninėje erdvėje atveju reikėtų atsiriboti nuo veikos įvykdymo įrankio materialaus pobūdžio, į šią kategoriją įtraukiant nepageidaujamas elektroninio pašto žinutes, falsifikuotus interneto tinklapius, šnipinėjimo programinę įrangą, o šios nusikalstamos veikos padarymo priemone turėtų būti laikomos informacinės ir ryšio technologijos.

Tapatybės vagystės (tapatybės pasisavinimo nusikalstamais tikslais) elektroninėje erdvėje padarymo tikslas – apsimesti kitu asmeniu, t.y. identifikuotis apsimetant pradiniu vartotoju, bei atlikti nusikalstamas veikas. Tuo tarpu piktnaudžiavimo tapatybe atveju subjektas nesiekia įvykdyti jokios nusikalstamos veikos. Taigi nusikalstamos veikos tikslas šiuo atveju yra vienas iš požymių, lemiančių veikos pavojingumą.

Išanalizavus tapatybės vagystės kaip savarankiškos nusikalstamos veikos požymius, akcentuotinas šios veikos pavojingumas ir siūlytina tapatybės vagystę kriminalizuoti. Tam tikri tapatybės vagystės elektroninėje erdvėje atvejai patenka į LR BK 198 str. reglamentavimo sritį, tačiau dalis šios pavojingos veikos požymių kol kas nėra kriminalizuota. Toks teisinis reguliavimas laikytinas nepakankamu, todėl siūlytina LR BK papildyti nauju straipsniu, kuriame būtų numatoma atsakomybė už skirtingas tapatybės vagystės rūšis. Tapatybės vagystės (tapatybės pasisavinimo nusikalstamais tikslais) įvykdymas elektroninėje erdvėje informacinių ir ryšio technologijų pagalba turėtų būti įtvirtintas kaip kvalifikuojantis tapatybės vagystės (tapatybės pasisavinimo nusikalstamais tikslais) sudėties požymis atsižvelgiant į tai, kad tapatybės vagystė (tapatybės pasisavinimas nusikalstamais tikslais) elektroninėje erdvėje pagal atlikimo būdų, gautų duomenų ir informacijos apie kitą asmenį panaudojimo sričių įvairovę, pavojingumo mastą ir latentiškumą gali būti vertinama kaip pavojingesnė veika nei tapatybės vagystė (tapatybės pasisavinimas nusikalstamais tikslais) fizinėje erdvėje. Abiejose tapatybės vagystės (tapatybės pasisavinimo neteisėtais tikslais) sudėtyse turėtų būti įtvirtintas nusikalstamų ketinimų požymis. Tame pačiame straipsnyje turėtų būti įtvirtinta ir piktnaudžiavimo tapatybe – mažiau pavojingos veikos – sudėtis, joje nenumatant nusikalstamų ketinimų požymio ir kvalifikuojant tokio pobūdžio veiką kaip baudžiamąjį nusižengimą. LR BK specialiosios dalies straipsnis, reglamentuojantis tapatybės vagystę, galėtų atrodyti taip:

178(1) Tapatybės vagystė

1. Tas, kas, neturėdamas tam teisės, perėmė, įgijo, laikė, naudojo, paskleidė, disponavo ar atliko kitokius veiksmus su asmens duomenimis ir (ar) asmenine informacija apie kitą asmenį, siekdamas identifikuotis kaip asmuo, iš kurio tokie duomenys ir (ar) asmeninė informacija buvo pasisavinti, tam, kad atliktų kitas nusikalstamas veikas, baudžiamas...

2. Tas, kas padarė šio straipsnio 1 dalyje numatytą veiką pasinaudodamas informacinių ir ryšio technologijų pagalba, baudžiamas...

3. Tas, kas atliko šio straipsnio 1 ir (ar) 2 dalyje numatytus veiksmus, tačiau neturėjo tikslo įvykdyti nusikalstamą veiką, padarė baudžiamąjį nusižengimą ir baudžiamas...

Įstatymų leidėjas, atsižvelgdamas į tapatybės vagystės elektroninėje erdvėje įvykdymo būdų įvairovę, jų sudėtingumą, turėtų įtvirtinti platų sankcijų už šią veiką spektrą, kad kiekvienu konkrečiu atveju nusikalstamos veikos subjektui būtų paskirta proporcingumo ir teisėtumo kriterijus atitinkanti bausmė.

IŠVADOS

Atlikus tarptautinių, regioninių ir užsienio valstybių institucijų teisės aktų, užsienio mokslininkų formuojamos doktrinos analizę, nustatyta, kad tapatybės vagystė elektroninėje erdvėje yra kompleksinis, visuomenei pavojingas socialinis – teisinis reiškinys, pasižymintis formų ir atlikimo būdų įvairove, o siekiant efektyviai kovoti su šiuo reiškiniu, tapatybės vagystė elektroninėje erdvėje turi būti kvalifikuojama kaip savarankiška nusikalstama veika. Taigi magistro baigiamojo darbo įvade iškeltos hipotezės pasitvirtino.

Išnagrinėjus tapatybės vagystės elektroninėje erdvėje kaip socialinio – teisinio reiškinio teisinius aspektus ir atsižvelgiant į magistro baigiamojo darbo įvade iškeltus uždavinius, galima pateikti tokias **išvadas**:

1. Tapatybės vagystė yra kompleksinis socialinis – teisinis reiškinys, susijęs su vartotojų teisių, saugumo, privatumo, taisyklių, reglamentuojančių nepageidaujamos informacijos gavimą, pažeidimais. Nors ši veika yra tarptautinio pobūdžio problema, nei tarptautiniuose, nei regioniniuose privalomos galios teisės aktuose nepateikiama tapatybės vagystės ar tapatybės vagystės elektroninėje erdvėje sąvoka. Tapatybės vagystės apibrėžimą siūlo kai kurios tarptautinės ir nacionalinės organizacijos, tačiau šių organizacijų teisės aktai yra tik rekomendacinio pobūdžio, o pateikiamas ataskaitas ir tyrimus galima vertinti tik kaip tam tikras gaires valstybėms narėms.

2. Nacionaliniu lygiu tapatybės vagystės sąvoka suprantama gana skirtingai, o tapatybės vagystės elektroninėje erdvėje sąvoka iš viso nepateikiama. Kai kurios valstybės pasirinko tapatybės vagystę traktuoti plačiąja prasme, t.y. apimant tapatybės vagystės atvejus tiek elektroninėje, tiek ir fizinėje erdvėje. Šio reiškinio sudėtingumas lėmė skirtingą teisinį valstybių vertinimą: tapatybės vagystė gali būti kvalifikuojama kaip specifinis nusikaltimas, civilinės teisės pažeidimas ar kaip pasirengimas įvykdyti kitus nusikaltimus, tokius kaip sukčiavimas, klastojimas, terorizmas ar pinigų plovimas.

3. Tapatybės vagystė elektroninėje erdvėje gali būti atliekama pačiais įvairiausiais metodais, kurie kinta ir tobulėja kartu su technologijų pažanga. Dažniausiai naudojami yra šie metodai: duomenų vagystė (angl. *phishing*), falsifikuoti internetiniai tinklalapiai (angl. *scam*), nepageidaujamos elektroninio pašto žinutės (angl. *spam*), apgaulės taktika (angl. *spoofing*), šnipinėjimo programinė įranga (angl. *spyware*), duomenų nuskaitymas nuo kortelių apgaulės būdu (angl. *skimming*), įsibrovimas (angl. *hacking*), Trojos arkliai (angl. *Trojans*), apgaulingos IP taktikos (angl. *pharming*) ir pakartojimo atakos (angl. *replay attack*).

4. Tapatybės vagystė elektroninėje erdvėje yra globali problema, todėl ypač svarbi užsienio teisėsaugos institucijų pagalba siekiant efektyviai kovoti su šia visuomenei pavojinga veika. Daugelyje valstybių tapatybės vagystė *per se* apskritai nėra laikoma teisės pažeidimu, o patenka į įvairias išimtis,

susijusias su duomenų slaptumu, apsauga ar klastote, už kuriuos galima asmenį patraukti baudžiamojon atsakomybėn. Kitos valstybės laikosi nuomonės, jog tokios veikos yra specifinės, todėl tapatybės vagystės kriminalizavimas yra naudinga priemonė siekiant užkirsti kelią šios veikos sukeliamoms grėsmėms. Tais atvejais, kai užsienio valstybė neturi įstatymų, kriminalizuojančių tapatybės vagystę elektroninėje erdvėje, yra apsunkinamos informaciją renkančios valstybės galimybės rinkti tokios veikos įrodymus atitinkamoje užsienio valstybėje ir patraukti atsakomybėn kaltus asmenis. Todėl svarbu, kad valstybės vienodai traktuotų minėtą veiką, o tai yra neišvengiamai susiję su tapatybės vagystės elektroninėje erdvėje kriminalizavimo problema.

5. Lietuvos ekspertai tapatybės vagystę elektroninėje erdvėje siūlo apibrėžti kaip gavimą pagrindinių asmens tapatybę liudijančios informacijos elementų (elektroninėje erdvėje), siekiant apsimesti tuo asmeniu, su tikslu atlikti nusikaltimus. Kai nėra tikslo atlikti nusikaltimus, ekspertų nuomone, veika gali būti apibrėžiama kaip piktnaudžiavimas tapatybe, o kai naudojamasi neegzistuojančio asmens tapatybe, veika turėtų būti įvardijama tapatybės klastote.

6. Tapatybė fizinėje erdvėje yra visiškai kitokia nei elektroninėje erdvėje. Fizinėje erdvėje savo tapatybę asmuo patvirtina vienu iš privalomų elementu – asmens dokumentu, tuo tarpu elektroninėje erdvėje tapatybę gali atstoti vardas ir slaptažodis. Elektroninėje erdvėje tapatybė sutapatinama su prisijungimo vardu ir slaptažodžiu ir visos saugumo užtikrinimo priemonės, tokios kaip skaitmeniniai sertifikatai, iš esmės atitinka asmens tapatybę elektroninėje erdvėje.

7. Tapatybės vagystė turėtų būti kvalifikuojama kaip nusikalstama veika, t.y. kaip sąmoningas ir valingas, pavojingas, priešingas teisei žmogaus elgesys išoriniame pasaulyje, pasireiškianti objektyviaisiais ir subjektyviaisiais požymiais, apibrėžiančiais tapatybės vagystės sudėtį. Šios veikos objektas – informacija ir duomenys, kurių pagalba gali būti nustatyta asmens tapatybė, nesvarbu, ar tokia informacija ir duomenys yra vieši ar nevieši, yra elektroninėje formoje, ar išsaugoti materialioje laikmenoje. Dalykas, priklausomai nuo šios veikos rūšies, pasireiškia tam tikra specifika: fizinėje erdvėje priešingi teisei veiksmai yra nukreipti prieš konkretų asmenį, tuo tarpu elektroninėje erdvėje – ne tik prieš konkretų asmenį, bet ir prieš informacines sistemas bei elektroninių ryšių tinklus, kurių pagalba atliekamas duomenų tvarkymas. Veika atliekama aktyviais veiksmais: neteisėtai stebint, fiksuojant, perimant, įgyjant, laikant, pasisavinant, paskleidžiant ar kitaip panaudojant duomenis ir asmeninę informaciją apie kitą asmenį. Pavojingų padarinių požymio šios veikos atveju neturėtų būti reikalaujama, t.y. tapatybės vagystės sudėtis turėtų būti formali. Tapatybės vagystė elektroninėje erdvėje pasireiškia įvykdymo būdų įvairove, todėl šią veiką reglamentuojančios teisės normos dispozicijoje pakaktų įtvirtinti, jog tokia veika gali būti atlikta pasinaudojant informacinėmis ir ryšio technologijomis. Taip pat šios veikos atveju reikėtų atsiriboti nuo veikos įvykdymo įrankio materialaus pobūdžio, į šią kategoriją įtraukiant nepageidaujamas elektroninio pašto žinutes, falsifikuotus interneto tinklapius, šnipinėjimo programinę įrangą, o šios nusikalstamos veikos padarymo priemone turėtų būti

laikomos informacinės ir ryšio technologijos. Tapatybės vagystės (tapatybės pasisavinimo nusikalstamais tikslais) elektroninėje erdvėje atveju šios veikos padarymo tikslas – siekis apsimesti kitu asmeniu, t.y. identifikuotis elektroninėje erdvėje apsimetant pradiniu vartotoju, bei atlikti nusikalstamas veikas. Tuo tarpu piktnaudžiavimo tapatybe atveju subjektas nesiekia įvykdyti jokios nusikalstamos veikos. Taigi nusikalstamos veikos tikslas šiuo atveju yra vienas iš požymių, lemiančių veikos pavojingumą.

8. Tapatybės vagystė Lietuvoje nėra kriminalizuota, tačiau tam tikri tapatybės vagystės elektroninėje erdvėje atvejai patenka į LR BK 198 str. reglamentavimo sritį. Vis dėlto, kritikuotinas įstatymų leidėjo nusikalstamos veikos objekto susiaurinimas, į normos dispoziciją įtraukiant tik neviešus elektroninius duomenis. Tapatybės vagystė, atliekama fizinėje erdvėje, apskritai nėra įtraukta į LR BK specialiąją dalį kaip savarankiška nusikalstama veika, nors pastaruoju metu dažnai nutinka taip, jog egzistuojančių LR BK normų reglamentavimo sritis neapima visų minėtos veikos elementų. Taip pat Lietuvos teisės aktai nereglamentuoja situacijos, kai nusikalstama veika dar nepadaryta, tačiau pas asmenį aptinkama kito asmens (asmenų) asmeninė informacija ir (ar) asmens duomenys. Be to, egzistuojančios teisės aktų normos neapima visų tapatybės vagystės metu įgytų asmens duomenų ir (ar) asmeninės informacijos panaudojimo atvejų.

PASIŪLYMAI

Remiantis atlikta tarptautinių, regioninių ir nacionalinių institucijų rekomendacinio pobūdžio teisės aktų, užsienio valstybių privalomojo pobūdžio teisės aktų ir užsienio mokslininkų formuojamos doktrinos, ekspertinio tyrimo rezultatų, tapatybės vagystės sudėties požymių analize bei atsižvelgiant į suformuluotas išvadas, teiktini tokie **pasiūlymai**:

1. ***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) asmeninės informacijos perėmimas, įgijimas, laikymas, naudojimas, paskleidimas, disponavimas ar kitokių veiksmų atlikimas), turint tikslą apsimesti tuo asmeniu, iš kurio buvo gautos jį identifikuojančios priemonės, tam, kad būtų galima atlikti nusikalstamas veikas. Tuo tarpu* ***tapatybės vagystę elektroninėje erdvėje*** siūlytina apibrėžti kaip *tapatybės vagystės rūšį, kai tapatybės vagystė atliekama per atstumą, t.y. pasinaudojant informacinėmis ir ryšio technologijomis*.

2. ***Remiantis tikslo kriterijumi***, ***siūlytina išskirti*** dvi tapatybės vagystės rūšis:

1) piktnaudžiavimą tapatybe, kai atliekami įvairūs veiksmai su kito asmens duomenimis ir (ar) asmenine informacija, siekiant apsimesti tuo asmeniu, iš kurio buvo gautos jį identifikuojančios priemonės, tačiau *neturint tikslo įvykdyti nusikalstamą veiką*;

2) tapatybės vagystę *(tapatybės pasisavinimą nusikalstamais tikslais)*, kai atliekami įvairūs veiksmai su kito asmens duomenimis ir (ar) asmenine informacija, siekiant apsimesti tuo asmeniu, iš kurio buvo gautos jį identifikuojančios priemonės, ir *turint tikslą atlikti nusikalstamas veikas* – nusikaltimus ir (ar) baudžiamuosius nusižengimus.

3. Atsižvelgiant į tapatybės vagystės kaip savarankiškos nusikalstamos veikos požymių analizę, siūlytina papildyti LR BK specialiąją dalį nauju straipsniu, numatančiu baudžiamąją atsakomybę už skirtingas tapatybės vagystės rūšis:

178$^{(1)}$ Tapatybės vagystė

1. Tas, kas, neturėdamas tam teisės, perėmė, įgijo, laikė, naudojo, paskleidė, disponavo ar atliko kitokius veiksmus su asmens duomenimis ir (ar) asmenine informacija apie kitą asmenį, siekdamas identifikuotis kaip asmuo, iš kurio tokie duomenys ir (ar) asmeninė informacija buvo pasisavinti, tam, kad atliktų kitas nusikalstamas veikas, baudžiamas...

2. Tas, kas padarė šio straipsnio 1 dalyje numatytą veiką pasinaudodamas informacinių ir ryšio technologijų pagalba, baudžiamas...

3. Tas, kas atliko šio straipsnio 1 ir (ar) 2 dalyje numatytus veiksmus, tačiau neturėjo tikslo įvykdyti nusikalstamą veiką, padarė baudžiamąjį nusižengimą ir baudžiamas...

Įstatymų leidėjas, atsižvelgdamas į tapatybės vagystės elektroninėje erdvėje įvykdymo būdų įvairovę, jų sudėtingumą, turėtų įtvirtinti platų sankcijų už šią veiką spektrą, kad kiekvienu konkrečiu atveju nusikalstamos veikos subjektui būtų paskirta proporcingumo ir teisėtumo kriterijus atitinkanti bausmė.

4. Tapatybės vagystės (tapatybės pasisavinimo nusikalstamais tikslais) įvykdymą elektroninėje erdvėje informacinių ir ryšio technologijų pagalba siūlytina įtvirtinti kaip kvalifikuojantį tapatybės vagystės (tapatybės pasisavinimo nusikalstamais tikslais) sudėties požymį, atsižvelgiant į tai, kad tapatybės vagystė (tapatybės pasisavinimas nusikalstamais tikslais) elektroninėje erdvėje pagal atlikimo būdų, gautų duomenų ir informacijos apie kitą asmenį panaudojimo sričių įvairovę, pavojingumo mastą ir latentiškumą turėtų būti vertinama kaip pavojingesnė veika nei tapatybės vagystė (tapatybės pasisavinimas nusikalstamais tikslais) fizinėje erdvėje. Kvalifikuotos nusikalstamos veikos sudėties įtvirtinimą lemtų būtent veikos įvykdymo būdas, kuris yra glaudžiai susijęs su pavojingos veikos požymiu bei dažnai naudojamas įstatymų leidėjo formuluojant nusikalstamų veikų sudėtis.

LITERATŪRA

Tarptautiniai ir Europos Sąjungos teisės aktai

1. **Komisijos komunikatas** KOM/2007/267 galutinis/ **Bendrosios politikos, skirtos kovai su elektroniniais nusikaltimais, linkme** // {SEK(2007) 641}{SEK(2007) 642}, 22/5/2007. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:LT:HTML; [žiūrėta 2008 12 17]
2. **Konvencija dėl elektroninių nusikaltimų**. http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=228195&p_query=&p_tr2= [žiūrėta 2009 01 08]

Lietuvos Respublikos teisės aktai

1. **Lietuvos Respublikos baudžiamasis kodeksas** [aktuali redakcija nuo 2008-06-27]. http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=323740&p_query=&p_tr2= [žiūrėta 2009 01 08]
2. **Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo pakeitimo įstatymas.** http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=314801&p_query=&p_tr2= [žiūrėta 2009 01 08]
3. **Lietuvos Respublikos elektroninių ryšių įstatymas.** http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=332292&p_query=&p_tr2= [žiūrėta 2009 01 08]
4. **Lietuvos Respublikos informacinės visuomenės paslaugų įstatymas.** http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=277491&p_query=&p_tr2= [žiūrėta 2009 01 08]
5. **Lietuvos Respublikos asmens tapatybės kortelės įstatymas.** http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=324119&p_query=&p_tr2= [žiūrėta 2009 08 05]
6. **Nacionalinio elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimų padalinio veiklos nuostatai**, patvirtinti 2009 m. kovo 20 d. Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus įsakymu Nr. IV-348. https://www.cert.lt/doc/CERT-LT_nuostatai.pdf [žiūrėta 2009 10 17]

Lietuvos teismų praktika

1. 2005 m. birželio 23 d. Lietuvos Aukščiausiojo Teismo Senato nutarimas Nr. 52 „Dėl teismų praktikos vagystės ir plėšimo baudžiamosiose bylose“. Prieinama internete: http://www.lat.lt/4_tpbiuleteniai/senos/nutartis.aspx?id=29259 [žiūrėta 2009 06 03]
2. 2005 m. gruodžio 29 d. Lietuvos Aukščiausiojo Teismo Senato nutarimas Nr. 55 „Dėl teismų praktikos nusikalstamų veikų finansų sistemai baudžiamosiose bylose (BK 214, 215, 219, 220, 221, 222, 223 straipsniai)“. Prieinama internete: http://www.lat.lt/4_tpbiuleteniai/senos/nutartis.aspx?id=31289 [žiūrėta 2009 06 04]
3. 2006 m. lapkričio 21 d. Lietuvos Aukščiausiojo Teismo kasacinė nutartis baudžiamojoje byloje Nr. 2K-581/2006. Prieinama internete: http://www.lat.lt/3_nutartys/senos/nutartis.aspx?id=30503 [žiūrėta 2009 06 04]

Specialioji literatūra

1. **Bainbridge D.** Introduction to computer law / 5th ed. - Harlow: Pearson, Longman, 2004. - 553 p. – ISBN 0-582-47365-9
2. **Civilka M. ir kt.** Informacinių technologijų teisė. - Vilnius: NVO Teisės institutas, 2004. – 544 p. – ISBN 9955-9744-0-0
3. **Computer Law: the law and regulation of information technology** / Edited by Reed C., Angel J. - Oxford: Oxford University Press, 2007. - 610 p. – ISBN 978-0-19-920596-7
4. **Cybercrime and jurisdiction: a global survey** / Edited by Koops B. J., Brenner S. W. - The Hague: T.M.C. Asser Press, 2006. - 355 p. – ISBN 90-6704-221-8
5. **Duquenoy P. et al.** Ethical, legal and professional issues in computing. - London: Thomson, : Middesex University Press, 2008. - 253 p. – ISBN 978-1-84480-749-9
6. **Forder J., Svantenson D.** Internet and e-commerce law. - South Melbourne Oxford New York (N.Y.) : Oxford University Press, 2008. - 264 p. – ISBN 978-0-19-556053-4
7. **Ian Walden**. Computer Crimes and Digital Investigations. - Oxford: Oxford University Press, 2007. – 491 p. – ISBN 9780199290987
8. **Kiškis M. ir kt.** Teisės informatika ir informatikos teisė: vadovėlis. - Vilnius: Mykolo Romerio universitetas, 2006. – 267 p. – ISBN 9955-19-048-5
9. **Online Identity Theft** – OECD, 2009. – 137 p. – ISBN 978-92-64-05658-9. Prieinama internete: http://browse.oecdbookshop.org/oecd/pdfs/browseit/9309021E.PDF
10. **Piesliakas V.** Lietuvos baudžiamoji teisė. Kn. 1. Vilnius: Justitia, 2006. – 414 p. – ISBN 9955616199
11. **Piesliakas V.** Lietuvos baudžiamoji teisė. Kn. 2. Vilnius: Justitia, 2008. – 479 p. – ISBN 9789955616399

12. **Štitilis D.** Teisinės atsakomybės pagrindų nustatymo už neteisėtas veikas elektroninėje erdvėje problemos (rankraštis): daktaro disertacija: socialiniai mokslai, teisė (01 S). – Vilnius: Mykolo Romerio universitetas, 2002. - 190 p.
13. **Štitilis D. ir kt.** Kai kurie konvencijos dėl elektroninių nusikaltimų proceso teisės skirsnio įgyvendinimo Lietuvoje aspektai // Jurisprudencija: mokslo darbai. – Vilnius, 2005, Nr. 67 (59), p. 20 – 28. - ISSN 1392-6195
14. **Štitilis D.** Prekių ženklų naudojimas elektroninėje erdvėje: teisiniai aspektai// Jurisprudencija: mokslo darbai. – Vilnius, 2003, Nr. 41 (33), p. 141 – 154. – ISSN 1392-6195
15. **Štitilis D., Laurinaitis M.** Tapatybės vagystė elektroninėje erdvėje// Informacijos mokslai: mokslo darbai. – Vilnius, 2009, T. 50, p. 240-248. – ISSN 1392-0561
16. **Tidikis R.** Socialinių mokslų tyrimų metodologija. Vilnius: Lietuvos teisės universitetas, 2003. – 626 p. – ISBN 9955563265
17. **Ušinskaitė D.** Mokėjimo instrumento sąvoka Lietuvos baudžiamojoje teisėje // Jurisprudencija: mokslo darbai, - Vilnius, 2004, Nr. 60 (52). P. 115-124. – ISSN 1392-6195

Elektroniniai šaltiniai

1. **Bankai blokuoja korteles dėl galimos duomenų vagystės**. Informacinis portalas Delfi: http://www.delfi.lt/news/economy/business/bankai-blokuoja-korteles-del-galimos-duomenu-vagystes.d?id=24664003 [žiūrėta 2009 10 13]
2. **Bruce Schneier**. Korea Solves the Identity Theft Problem. December 14, 2005. Straipsnis prieinamas internete: http://www.schneier.com/blog/archives/2005/12/korea_solves_th.html [žiūrėta 2009 06 03]
3. Chawki J. M., Abdel Wahab M. S. Identity Theft in Cyberspace: Issues and Solutions // Lex Electronica, vol.11 n°1 (Printemps / Spring 2006) // http://www.lex-electronica.org/docs/articles_54.pdf [žiūrėta 2009 01 08]
4. **Chawki J. M.** Phishing in Cyberspace: Issues and Solutions // Computer Crime Research Center, August 19, 2006 // http://www.crime-research.org/articles/phishing-in-cyberspace-issues-and-solutions [žiūrėta 2009 01 08]
5. **CIFAS interneto svetainė**: http://www.cifas.org.uk/default.asp?edit_id=561-56 [žiūrėta 2009 05 31]
6. **Civilka M.** Asmens duomenų teisinis reguliavimas interneto kontekste. Prieinama internete: http://media.search.lt/GetFile.php?OID=92932&FID=269994 [žiūrėta 2009 05 31]
7. **Dabartinės lietuvių kalbos žodyno elektroninė versija**, prieinama internete: http://www.autoinfa.lt/webdic/ [žiūrėta 2009 06 02]

8. **Dėl galimos duomenų vagystės bankai blokuoja korteles**. Dienraštis 15 min, 2009 m. spalio 13 d. Straipsnis prieinamas internete: http://www.15min.lt/naujiena/aktualu/pinigai/58/59976/ [žiūrėta 2009 10 13]
9. **Dingo kaip į vandenį**. Dienraštis Kauno diena, 2008 m. rugsėjo 8 d. Straipsnis prieinamas internete: http://kauno.diena.lt/dienrastis/pasaulis/dingo-kaip-i-vandeni-121179 [žiūrėta 2009 05 31]
10. ***DoubleClick* kompanijos tinklapis**: http://www.doubleclick.com/privacy/ [žiūrėta 2009 05 31]
11. **Fair and Accurate Credit Transactions Act**, 2003. Prieinama internete: http://www.gpo.gov/fdsys/pkg/PLAW-108publ159/pdf/PLAW-108publ159.pdf [žiūrėta 2009 06 04]
12. **FIDIS** (Future of Identity in the Information Society) - a NoE (Network of Excellence) supported by the European Union: http://www.fidis.net/ [žiūrėta 2009 01 12]
13. **Fraud Act 2006**. Prieinama internete: http://www.opsi.gov.uk/acts/acts2006/pdf/ukpga_20060035_en.pdf [žiūrėta 2009 04 14]
14. **Identity Crime: Discussion Paper.** Model Criminal Law Officer‘s Committee. 2007. http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(4341200FE1255EFC59DB7A1770C1D0A5)~MCLOC-draft-identity-crime-discussion-paper-march+2007.pdf/$file/MCLOC-draft-identity-crime-discussion-paper-march+2007.pdf [žiūrėta 2009 01 12]
15. **Identity Fraud: A Study**. United Kingdom Cabinet Office, Economic and Domestic Secretariat, London. Prieinama internete: http://www.identitycards.gov.uk/downloads/id_fraud-report.pdf [žiūrėta 2009 05 31]
16. **Identity Theft and Assumption Deterrence Act**, 1998. Prieinama internete: http://www.ftc.gov/os/statutes/itada/itadact.htm [2009 06 04]
17. **Identity Theft Enhancement Penalty Act**, 2004. Prieinama internete: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ275.108.pdf [žiūrėta 2009 06 03]
18. **Identity theft: how to protect your name, your credit and your vital information and what to do when someone hijacks any of these** / The Silver Lake editors. - Silver Lake Publishing, 2004. - 288 p. - ISBN 1563437775, 9781563437779 // http://books.google.com/books?id=imqcowXV96MC&printsec=frontcover&dq=identity+theft+book&source=gbs_similarbooks_r&cad=0_1#PPP7,M1 [žiūrėta 2008 12 17]
19. **Identity Theft Survey Report, 2006.** Federeal Trade Commission. http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf [žiūrėta 2009 01 12]
20. **Informacija apie John D. Sileo**: http://www.thinklikeaspy.com/about-john-sileo.php

[žiūrėta 2009 05 31]

21. **Interneto tinklapis „Tapatybės vagystė; netapk auka“, sukurtas bendradarbiaujant Jungtinės Karalystės vyriausybei ir privačiam sektoriui**: http://www.identitytheft.org.uk/identity-crime-definitions.asp [žiūrėta 2009 05 31]
22. **JAV Federalinės prekybos komisijos tinklapis, skirtas kovai su tapatybės vagyste**: http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html [žiūrėta 2009 04 26]
23. **J. R. Reidenberg, P. M. Schwartz**. Data protection law and on-line services: regulatory responses. ARETE Study. Prieinama internete: http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/regul_en.pdf [žiūrėta 2009 05 31]
24. **Kanados teisingumo departamento oficialus tinklapis**: http://www.justice.gc.ca/ [žiūrėta 2009 06 03]
25. **Leenes** (ed.), FIDIS network, deliverable 5.2b, ID-related crime: towards a common ground for interdisciplinary research, May 2006. Prieinama internete: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp5-del5.2b.ID-related_crime.pdf [žiūrėta 2009 06 01]
26. **Lietuvos bankai masiškai blokuoja mokėjimo korteles dėl galimos duomenų vagystės**. Dienraštis Lietuvos rytas, 2009 m. spalio 13 d. Straipsnis prieinamas internete: http://www.lrytas.lt/-12554330001253616142-lietuvos-bankai-masi%C5%A1kai-blokuoja-mok%C4%97jimo-korteles-d%C4%97l-galimos-duomen%C5%B3-vagyst%C4%97s-papildyta.htm [žiūrėta 2009 10 13]
27. **Lietuvių kalbos žodyno elektroninė versija**, prieinama internete: http://lkz.mch.mii.lt/Zodynas/Visas.asp [žiūrėta 2009 06 02]
28. **Lietuvos Respublikos ryšių reguliavimo tarnybos Tinklų ir informacijos saugumo skyriaus interneto tinklapis, skirtas informacijos saugai elektroninėje erdvėje**: www.esaugumas.lt [žiūrėta 2009-10-17]
29. **Phishing kits banned by new Fraud Act**, 13 November 2006, Out-Law news. Prieinama internete: www.out-law.com/page-7469 [žiūrėta 2009 05 31]
30. **Portalas, skirtas apsaugai nuo tapatybės vagystės**: http://www.identity-theft-protection-made-easy.com/define-identity-theft.html [žiūrėta 2009 01 08]
31. **Report on Identity Theft/Fraud.** Fraud Prevention Expert Group. Brussels, 22 October 2007. Prieinama internete: http://ec.europa.eu/internal_market/fpeg/docs/id-theft-report_en.pdf [žiūrėta 2009 01 12]
32. **Scoping Paper on Online Identity Theft**: Ministerial Background Report. DSTI/CP (2007)3/Final. Prieinama internete: http://www.oecd.org/dataoecd/35/24/40644196.pdf

[žiūrėta 2009 06 04]

33. **Sileo J. D.** Stolen lives: identity theft prevention made simple. - DaVinci Publishing, 2005. - 173 p. - ISBN 0977059774, 9780977059775 // http://books.google.com/books?id=XuxRgXrtpMEC&dq=identity+theft+book&pg=PP1&ots=J8V5kQR83W&source=in&sig=o3GBCQGy0CBRJtkD8aDcxtYpf8M&hl=en&sa=X&oi=book_result&resnum=16&ct=result#PPA14,M1 [žiūrėta 2008 12 17]
34. **Standardisation of definitions of identity crime terms: A step towards consistency**. ACPR, Report Series No 145.3, March 2006. Prieinama internete: http://www.acpr.gov.au/pdf/ACPR145_3.pdf [žiūrėta 2009 04 19]
35. **Suler J.** The Online Disinhibition Effect // CyberPsychology and Behavior, 2004, 7, 321-326 // http://www-usr.rider.edu/~suler/psycyber/disinhibit.html [žiūrėta 2009 01 08]
36. **Sullivan B**. Your evil twin: behind the identity theft epidemic. - John Wiley and Sons, 2004. – 314 p. - ISBN 0471648108, 9780471648109 // http://books.google.com/books?id=SCf7swqny4MC&dq=identity+theft+book&pg=PP1&ots=7kI5__4qCX&source=in&sig=72eqowYNi9MIpiIcWsINW4Ry0T0&hl=en&sa=X&oi=book_result&resnum=15&ct=result#PPR7,M1. [žiūrėta 2008 12 17]
37. **Tapatybės vagystės tyrimų centro oficialus tinklapis**: www.idtheftcenter.org [žiūrėta 2009 01 08]
38. **Teisės profesoriaus David E. Sorkin sukurtas tinklapis** http://www.spamlaws.com/passport-identity-theft.html [žiūrėta 2009 05 31]
39. **Teisių į privatų gyvenimą informacinės agentūros interneto tinklapis**: http://www.privacyrights.org/identity.htm [žiūrėta 2009 01 08]
40. **United States Code** („U. S. C“). Prieinama internete: http://www.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00001028----000-.html [žiūrėta 2009 05 31]
41. **US Federal Register**, Volume 69, Number 248, Rules and Regulations, Page 77610-77621, December 28 2004. Prieinama internete: http://www.fdic.gov/news/news/financial/2005/fil705a.html [žiūrėta 2009 06 03]

Dauparaitė I. Tapatybės vagystės elektroninėje erdvėje teisiniai aspektai / Informatikos teisės magistro baigiamasis darbas. Vadovas doc. dr. D. Štitilis. – Vilnius: Mykolo Romerio universitetas, Socialinės informatikos fakultetas, 2009. – 80 p.

SANTRAUKA

Šiame magistro baigiamajame darbe nagrinėjami tapatybės vagystės elektroninėje erdvėje kaip socialinio – teisinio reiškinio teisiniai aspektai. Iškeliamos hipotezės, jog tapatybės vagystė elektroninėje erdvėje yra kompleksinis, visuomenei pavojingas reiškinys, pasižymintis formų ir atlikimo būdų įvairove, o siekiant efektyviai kovoti su šiuo reiškiniu, tapatybės vagystė elektroninėje erdvėje turi būti kvalifikuojama kaip savarankiška nusikalstama veika. Buvo prieita prie išvados, jog tapatybės vagystė elektroninėje erdvėje yra glaudžiai susijusi su vartotojų teisių, saugumo, privatumo, taisyklių, reglamentuojančių nepageidaujamos informacijos gavimą, pažeidimais bei pasižymi formų ir atlikimo būdų įvairove (dažniausiai yra naudojami duomenų vagystė, falsifikuoti internetiniai tinklalapiai, nepageidaujamos elektroninio pašto žinutės, apgaulės taktika, šnipinėjimo programinė įranga, duomenų nuskaitymas nuo kortelių apgaulės būdu, įsibrovimas, Trojos arkliai, apgaulinga IP taktika ir pakartojimo atakos), yra pavojinga ir turėtų būti kriminalizuota.

Nors tapatybės vagystė elektroninėje erdvėje yra tarptautinio pobūdžio problema, tačiau nėra visuotinai pripažįstamos tapatybės vagystės sąvokos. Be to, pasauliniu lygiu vyksta diskusijos, ar ši veika turėtų būti kriminalizuota ir ar tokios veikos sudėties įtraukimas į valstybių baudžiamuosius įstatymus padėtų efektyviau kovoti su šiuo reiškiniu. Daugelyje valstybių tapatybės vagystė *per se* apskritai nėra laikoma teisės pažeidimu, o patenka į įvairias išimtis, susijusias su neteisėta prieiga prie duomenų, sukčiavimu, klastojimu ir pan., už kuriuos galima asmenį patraukti baudžiamojon atsakomybėn. Tuo tarpu kitos valstybės laikosi nuomonės, jog tokios veikos yra specifinės, todėl tapatybės vagystės kriminalizavimas yra naudinga priemonė siekiant užkirsti kelią tapatybės vagystės sukeliamoms grėsmėms.

Paprastai tapatybės vagystė suprantama kaip asmens tapatybę atskleidžiančios informacijos panaudojimas, pavyzdžiui, kredito kortelės numeris, kaip priemonė padaryti kitus nusikaltimus, todėl labiausiai tikėtina, kad daugelyje valstybių nusikaltėlis būtų patrauktas baudžiamojon atsakomybėn ne už tapatybės vagystę, o už sukčiavimą arba kitą galimą nusikaltimą, kurie laikomi sunkesniais nusikaltimais. Tačiau dažniausiai tapatybės vagystės nusikaltimą įrodyti lengviau negu sukčiavimo nusikaltimą, taigi vienas iš efektyvių būdų kovoti su tapatybės vagyste elektroninėje erdvėje būtų šios pavojingos veikos kriminalizavimas.

Siekiant magistro baigiamajame darbe iškelto tikslo, apžvelgiama tapatybės vagystės sampratų įvairovė, tapatybės vagystės elektroninėje erdvėje atlikimo būdai ir formos, nagrinėjami probleminiai

šios veikos kriminalizavimo aspektai, atliekama tapatybės vagystės elektroninėje erdvėje požymių analizė, siūlomi galimi problemos sprendimo variantai.

Magistro baigiamąjį darbą sudaro keturi skyriai. Pirmame skyriuje aptariama tapatybės vagystės sąvokų įvairovė, tapatybės vagystės rūšys, atskleidžiamas šio reiškinio pavojingumas ir siūloma tapatybės vagystės sąvoka. Antrame skyriuje aptariama tapatybės vagystės elektroninėje erdvėje pasireiškimo formų ir įvykdymo būdų įvairovė, trumpai apžvelgiami tapatybės vagystės fizinėje erdvėje įvykdymo būdai bei pavojai, kylantys asmens duomenims ir asmeninei informacijai elektroninėje erdvėje. Trečiame skyriuje įrodinėjama, kad tapatybės vagystė elektroninėje erdvėje turėtų būti kriminalizuota, pateikiama valstybių, kuriose tapatybės vagystė yra kriminalizuota, apžvalga, Europos Komisijos ir OECD argumentai dėl tapatybės vagystės elektroninėje erdvėje kriminalizavimo, analizuojama situacija Lietuvoje, remiantis atlikta ekspertų apklausa, sistemiškai nagrinėjamos Lietuvos Respublikos baudžiamojo kodekso normos, į kurių reglamentavimo sritį patenka tam tikri tapatybės vagystės elementai. Ketvirtame skyriuje analizuojami tapatybės vagystės elektroninėje erdvėje kaip nusikalstamos veikos sudėties požymiai ir pateikiamas LR BK specialiosios dalies pakeitimo projektas, konstruojant tapatybės vagystės elektroninėje erdvėje sudėties modelį.

Magistro baigiamajame darbe ***tapatybės vagystę siūloma apibrėžti*** *kaip bet kokius neteisėtus veiksmus su kito asmens duomenimis ir (ar) asmenine informacija, leidžiančia identifikuoti kitą asmenį (tokių duomenų ir (ar) asmeninės informacijos perėmimas, įgijimas, laikymas, naudojimas, paskleidimas, disponavimas ar kitokių veiksmų atlikimas), turint tikslą apsimesti tuo asmeniu, iš kurio buvo gautos jį identifikuojančios priemonės, tam, kad būtų galima atlikti nusikalstamas veikas.* Tuo tarpu ***tapatybės vagystę elektroninėje erdvėje siūloma suprasti*** *kaip tapatybės vagystės rūšį, kai tapatybės vagystė atliekama per atstumą, t.y. pasinaudojant informacinėmis ir ryšio technologijomis*. Be to, ***remiantis tikslo kriterijumi***, ***siūloma išskirti*** dvi tapatybės vagystės rūšis: ***tapatybės vagystę*** *(tapatybės pasisavinimą nusikalstamais tikslais)* ir ***piktnaudžiavimą tapatybe*** (*kai atliekant tokio pobūdžio veiką, neturima tikslo įvykdyti nusikalstamą veiką*) ***bei kriminalizuoti tapatybės vagystę*** – ne tik elektroninėje, bet ir fizinėje erdvėje, – padarant atitinkamus pakeitimus LR BK specialiojoje dalyje.

Pagrindiniai žodžiai: tapatybė, tapatybės vagystė, tapatybės vagystė elektroninėje erdvėje, tapatybės klastotė, piktnaudžiavimas tapatybe, tapatybės vagystės elektroninėje erdvėje teisiniai aspektai, tarptautinis bendradarbiavimas, tapatybės vagystės kriminalizavimas, asmens duomenys ir asmeninė informacija, elektroninė erdvė, informacinės ir ryšio technologijos, informacinė visuomenė.

Dauparaitė I. Legal Aspects of Online Identity Theft / Master‘s Work in Informatics Law. Supervisor doc. dr. D. Štitilis. – Vilnius: Faculty of Social Informatics, Mykolas Romeris University, 2009. - 80 p.

SUMMARY

This Master‘s Work analyzes legal aspects of online identity theft as a social – legal phenomenon. Two hypotheses are held. The first one is that online identity theft is a complex and dangerous phenomenon to our society because of the ability to occur in various forms and be made in different ways. The second hypothesis is that in order to fight with online identity theft successfully it should be criminalized. Indeed, it has been come to a conclusion that online identity theft is concerned with violation of consumer protection rules, security and privacy and anti-spam rules and may be committed in various ways (e.g. phishing, scam, spam, spoofing, spyware, skimming, hacking, Trojans, pharming, replay attack, etc.). Also, it has been stated that online identity theft is dangerous and should be criminalized.

Although online identity theft is an international problem, there is no generally accepted definition of identity theft. Moreover, it is globally discussed whether identity theft should be criminalized or not. Only a few countries have adopted legislation that specifically addresses identity theft. In most other countries, it is a constituent element of common wrongs, and as such it is covered by a multitude of rules including unlawful access to data, fraud, forgery, *etc.* Other countries state that identity theft is specific and criminalization of it should be a useful mean to prevent society from threats, caused by identity theft.

Generally, identity theft is understood as the use of personal identifying information, e.g. a credit card number, as an instrument to commit other crimes. In most countries a criminal would most likely be prosecuted for the fraud or another potential crime rather than for the identity theft; the former being considered a more serious crime. However, it is often easier to prove the crime of identity theft than that of fraud, so one of the effective ways to fight with online identity theft should be criminalization of such a dangerous deed.

Trying to reach the main objective of this Master‘s Work various definitions of identity theft, types and methods of online identity theft are reviewed, different issues, concerned with online identity theft criminalization as well as features of online identity theft are analyzed and solutions for this problem are suggested.

This Master‘s Work consists of four chapters. In the first chapter identity theft definition is proposed, riskiness and types of identity theft are disclosed, various definitions of online identity theft are discussed. In the second chapter types and methods of online identity theft are analyzed, methods of off-line identity theft are reviewed and risks for data and personal information in cyberspace are

mentioned. In the third chapter it is argued that online identity theft should be criminalized, giving examples of foreign countries which have already criminalized identity theft, stating European Commission‘s and OECD arguments for the criminalization of online identity theft. In addition, in this chapter the situation in Lithuania is analyzed with reference to experts’ poll. Moreover, rules of Criminal Code of the Republic of Lithuania are also analyzed. In the fourth chapter, features of online identity theft as a criminal action are analyzed and the amendments to the special section of Criminal Code of the Republic of Lithuania are suggested, setting the composition model of online identity theft.

In conclusions, In this Master‘s Work it is stated, that ***identity theft should be defined*** *as any unlawful action with another person‘s data and (or) personal information which enables identify yourself as another person (e.g. interception, acquisition, possession, use, dissemination, disposition or other actions) in order to pretend of being the person from whom it was obtained his identifiers, so that other legal violations and (or) criminal acts could be committed*. While ***online identity theft should be understand*** *as a kind of identity theft, when identity theft is committed by means of information and communication technologies*. Moreover, it is suggested to ***set two kinds of identity theft based on criminal intention***: ***identity theft*** (*misappropriation of identity having criminal intention*) and ***misuse of identity*** (*when there is no criminal intention*). In addition to that, it is argued that online identity theft as well as off-line identity theft should be criminalized, making amendments to the special section of Criminal Code of the Republic of Lithuania.

Key Words: identity, identity theft, online identity theft, identity fraud, misuse of identity, legal aspects of online identity theft, international cooperation, criminalization of identity theft, data, personal information, cyber-space, information and telecommunications technologies, information society.