www.mruni.eu

TAPATYBĖS VAGYSTĖ ELEKTRONINĖJE ERDVĖJE: SOCIALINIAI, ELEKTRONINIO VERSLO IR TEISINIO REGULIAVIMO ASPEKTAI

Darius Štitilis
Paulius Pakutinskas
Marius Laurinaitis
Inga Dauparaitė

MYKOLO ROMERIO UNIVERSITETAS

MYKOLO ROMERIO UNIVERSITETAS

Darius Štitilis, Paulius Pakutinskas,
Marius Laurinaitis, Inga Dauparaitė

TAPATYBĖS VAGYSTĖ ELEKTRONINĖJE ERDVĖJE: SOCIALINIAI, ELEKTRONINIO VERSLO IR TEISINIO REGULIAVIMO ASPEKTAI

Kolektyvinė
mokslo monografija

Vilnius, 2011

UDK 342.7
Ta-113

Tyrimą finansavo Lietuvos mokslo taryba (sutarties Nr. MIP17/2010).

Recenzavo:

doc. dr. Irmantas Rotomskis, Mykolo Romerio universitetas

doc. dr. Antanas Keras

Autorių indėlis:

doc. dr. Darius Štitilis – 1.2.1, 1.2.2, 1.6, 3.1, 3.2.3, 3.5.2, 4.2.2, 4.2.3, 4.3, 4.4 dalys (10,83 autorinių lankų)

Paulius Pakutinskas – įvadas, 1.2.3, 1.7 (kartu su I. Dauparaite), 3.5.1 (kartu su I. Dauparaite), 5.2 (kartu su D. Štitiliu) dalys (2,11 autorinių lankų)

Marius Laurinaitis – 1.1, 1.3, 3.2.1, 4.1, 4.2.1 dalys (2,10 autorinių lankų)

Inga Dauparaitė – 1.4, 1.5, 2, 3.2.2, 3.3.1, 3.3.2 (kartu su D. Štitiliu), 3.4.1 (kartu su D. Štitiliu), 3.4.2 (kartu su D. Štitiliu), 5.1 dalys (7,06 autorinių lankų)

Mokslinis redaktorius:

doc. dr. Darius Štitilis

Mykolo Romerio universiteto Socialinės informatikos fakulteto Elektroninio verslo katedros 2011 m. spalio 10 d. posėdyje (protokolas Nr. 1ELVK-1) pritarta leidybai.

Mykolo Romerio universiteto Socialinės informatikos fakulteto tarybos 2011 m. spalio 17 d. posėdyje (protokolas Nr. 2SI-2) pritarta leidybai.

Mykolo Romerio universiteto mokslinių-mokomųjų leidinių aprobavimo spaudai komisijos 2011 m. spalio 28 d. posėdyje (protokolas Nr. 2L-19) pritarta leidybai.

ISBN 978-9955-19-374-6

Apie autorius

Darius Štitilis yra Mykolo Romerio universiteto Socialinės informatikos fakulteto Elektroninio verslo katedros docentas, daktaras (teisė, 01 S). Pagrindinės tyrimų sritys: informacinių technologijų teisė, elektroninės komercijos teisė, elektroniniai nusikaltimai, privatumo ir asmens duomenų teisinė apsauga, elektroninių duomenų saugumo teisinis reguliavimas. Asmeninis tinklalapis: http://stitilis.home.mruni.eu.

Paulius Pakutinskas yra socialinių mokslų daktaras (teisė, 01 S). Pagrindinės tyrimų sritys: interneto teisė, informacinių technologijų teisė, elektroninės komercijos teisė, elektroninių ryšių teisė.

Marius Laurinaitis yra Mykolo Romerio universiteto Ekonomikos ir finansų valdymo fakulteto Bankininkystės ir investicijų katedros lektorius. Pagrindinės tyrimų sritys: elektroninės mokėjimų sistemos, elektroniniai pinigai, mobilūs atsiskaitymai, pinigų plovimo prevencija.

Inga Dauparaitė yra teisės magistrė. Pagrindinė tyrimų sritis: informacinių technologijų teisė.

Įvadas

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. Ši veika, atsižvelgiant į jos įvykdymo būdų ir neigiamų padarinių įvairovę, galimą mastą ir latentiškumą, priskirtina vienai iš pavojingiausių ir labiausiai plintančių elektroninių pavojingų veikų rūšių, kurios aukos gali susidurti su įvairiais neigiamais padariniais – tiek finansinio, tiek moralinio pobūdžio. Tapatybės vagystė elektroninėje erdvėje gali sukelti pačių įvairiausių neigiamų pasekmių, pradedant nuo to, kad asmenys ar įmonės kurį laiką negali naudotis savo kompiuteriais, internete netikėtai susiduria su rasistinio ar pornografinio turinio informacija, tampa sukčiavimo aukomis ir patiria finansinių nuostolių, iki to, kad asmenys šantažuojami, iš jų tyčiojamasi, pažeidžiami nepilnamečių ir mažamečių interesai ir teisės. Dar daugiau – gali būti užblokuojami valstybės valdžios institucijų internetinių tinklalapių adresai arba internete paviešinama valstybės ir (ar) tarnybos paslaptį atskleidžianti informacija. Potenciali tapatybės vagystės elektroninėje erdvėje žala, pasikėsinimo objektas ir mastas, t. y. galimas nukentėjusiųjų skaičius, lemia jos pavojingumą – nuo grėsmės privatumui ir asmens duomenų apsaugai iki pavojaus valstybės interesams ir nacionaliniam saugumui.

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 (dėl to atsiranda poreikis elektroninėje erdvėje taikyti specifinius teisės principus, pavyzdžiui, technologijų neutralumo principą). 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, reglamentuojančios elektroninę erdvę ir su ja susijusius socialinius reiškinius, gali būti ne visada veiksmingos. Ši pavojinga veika toliau plinta, nes nėra veiksmingo teisinio ir kitokio atsako. Nusikaltėliai ir

pažeidėjai, vykdantys tapatybės vagystę elektroninėje erdvėje, dažnai lieka nenubausti. Taip pat nėra aiškiai suvokiama, kaip apsisaugoti nuo šio pavojingo reiškinio (prevencijos priemonių problema).

Tapatybės vagystė elektroninėje erdvėje kelia ir praktinių, ir teorinių problemų (įskaitant ir teisinio reguliavimo). Tiek mokslininkai, tiek praktikai ginčijasi dėl tapatybės vagystės elektroninėje erdvėje sąvokos, jos įvykdymo būdų ir kitų aspektų. Daug teisinio neaiškumo sukelia tai, kad nei teisės aktuose ar teismų praktikoje, nei doktrinoje nėra įtvirtinta vienos bendros tapatybės vagystės ar tapatybės vagystės elektroninėje erdvėje sąvokos šiam reiškiniui įvardyti: tai „tapatybės klastotės“, „piktnaudžiavimo tapatybe“, „tapatybės nusikaltimų“ sąvokos, kurios dažnai vartojamos kaip tapatybės vagystės sinonimai, kurių turinys nagrinėjamame kontekste nėra aiškiai apibrėžtas. Su tapatybės vagyste susijusių visuomeninių santykių teisinio reguliavimo klausimas taip pat dažnai keliamas tiek praktinėje, tiek mokslinėje literatūroje (Camp 2010; Williams 2006; Abagnale 2007; Collins 2006), nesutariama ir dėl teisinio reguliavimo būdų, ir dėl teisinio reguliavimo apimties (Higgins 2010; Brenner 2010; Wells 2010; Ghosh, Turrini 2010). Keliama įvairių idėjų dėl tapatybės vagystės elektroninėje erdvėje kriminalizavimo, manoma, kad esamų baudžiamųjų įstatymų normų nepakanka, kovojant su šiuo pavojingu reiškiniu, todėl reikia specialių baudžiamųjų normų, tačiau yra ir priešingų nuomonių.

Lietuvoje tapatybės vagystė elektroninėje erdvėje kaip socialinis teisinis reiškinys iš viso beveik nėra nagrinėtas (2009 metais buvo publikuotas straipsnis: Štitilis D., Laurinaitis M. 2009. Tapatybės vagystė elektroninėje erdvėje[1], *Informacijos mokslai* 50: 239–247), todėl ši tema neabejotinai yra nauja.

Autorių nuomone, būtina išnagrinėti tapatybės vagystę elektroninėje erdvėje kaip tokią, aptarti šio socialinio teisinio reiškinio sąvoką, pavojingumą, tendencijas, rūšis, įvykdymo būdus, teisinį reguliavimą (įskaitant teisinę atsakomybę) ir prevenciją. Todėl keltinas tyrimo tikslas – išnagrinėti tapatybės vagystės elektroninėje erdvėje socialinius, elektroninio verslo ir teisinės atsakomybės aspektus. Taigi, šioje kolektyvinėje mokslo monografijoje (toliau – monografija) aptariami šie pagrindiniai aspektai, susiję su tapatybės

[1] Straipsnyje nagrinėta tapatybė ir identifikavimas, tapatybės vagystės būdai ir formos, tapatybės vagystės elektroninėje erdvėje samprata ir kriminalizavimas. Atliktas tyrimas parodė, kad nėra bendros tapatybės vagystės elektroninėje erdvėje sampratos, tapatybės vagystės elektroninėje erdvėje būdai skiriasi, o tapatybės vagystės kriminalizavimo klausimu nėra vieningos pozicijos.

vagyste elektroninėje erdvėje. Tačiau reikia paminėti ir tai, kad monografija buvo rengiama įgyvendinant mokslinį projektą „Tapatybės vagystė elektroninėje erdvėje: socialiniai, e. verslo ir teisinio reguliavimo aspektai“, finansuojamą Lietuvos mokslo tarybos, ir įgyvendina konkrečius šio mokslinio projekto uždavinius[2]. Dėl šios priežasties monografijoje gali likti neaptartų kai kurių klausimų, susijusių su tapatybės vagyste elektroninėje erdvėje, pvz., tapatybės vagystės elektroninėje erdvėje tyrimas[3], jurisdikcija ir kt. Visgi nepaisant to, pasistengta sistemiškai perteikti pagrindinius tapatybės vagystės kaip socialinio teisinio reiškinio elektroninėje erdvėje aspektus ir su šiuo reiškiniu susijusių visuomeninių santykių teisinį reguliavimą bei prevenciją.

Monografijoje taikyti mokslinio tyrimo metodai. Atsižvelgdami į tiriamojo reiškinio sudėtingumą bei daugialypiškumą ir tai, kad buvo siekiama ištirti daugelį svarbių reiškinio aspektų, monografijos autoriai pritaikė daug vienas kitą papildančių mokslo tyrimo metodų. Autoriai plačiai taikė *empirinius tyrimo metodus (dokumentų analizės metodai, anketinis, ekspertų apklausos ir kitus),* tačiau siekiant įvairiapusiškai išanalizuoti mokslinę problemą neapsiribojama vien šiais tyrimo metodais, o nuosekliai taikomi ir *teoriniai (pavyzdžiui, lyginamasis, genezės, dedukcijos ir kiti).*

Atliekant tyrimus taikyti šie **empiriniai metodai**:

Dokumentų analizės metodas. Šis metodas taikomas daugelyje monografijos dalių. Autoriai tiria įvairius dokumentus, tačiau svarbiausiais laiko oficialius dokumentus, kurie yra patikimesnis informacijos šaltinis negu neoficialūs. Kaip atskirą dokumentų analizės porūšį, reikia išskirti plačiai taikomą *teisinių dokumentų analizę*. Monografijoje tiriami Lietuvos, užsienio ir tarptautiniai teisės norminiai aktai ir kiti dokumentai, susiję su tapatybės vagyste elektroninėje erdvėje. Analizuojant norminius teisės aktus, gautus iš patikimų Europos Sąjungos (*www.eur-lex.europa.eu*), Lietuvos (*www.lrs.lt*; *www.litlex.lt*) ir kitų duomenų bazių, nėra būtina atskirai vertinti dokumentų autentiškumo, patikimumo ir kitų kriterijų, kuriuos būtina patikrinti analizuojant daugelį kitokių dokumentų (pvz., rankraščių ir kt.).

[2] 1) Apžvelgti tapatybės vagystę elektroninėje erdvėje kaip socialinį-teisinį reiškinį ir pateikti šio reiškinio plitimo tendencijas; 2) Aptarti tapatybės vagystės elektroninėje erdvėje atlikimo būdus, jų specifiką ir šios veiklos padarinius; 3) Išnagrinėti teisinio reguliavimo, įskaitant teisinės atsakomybės, susijusios su tapatybės vagyste elektroninėje erdvėje, aspektus; 4) ištirti ir pateikti tapatybės vagystės elektroninėje erdvėje prevencijos priemones ir būdus.

[3] Tai, kad kyla problemų dėl tapatybės vagystės elektroninėje erdvėje tyrimo, nurodė 5 autorių apklausti ekspertai.

Šio metodo taikymo *tikslas* – ištirti tiriamojo reiškinio teisinį reguliavimą, nustatytą įvairiose teisės normose, tokio reguliavimo atsiradimą ir kitimą laike. Ištyrę teisinius dokumentus autoriai duomenis naudoja ir kitiems tyrimams (pvz., lyginamajai analizei ir kt.). Šio metodo privalumu laikytina jo suteikiama galimybė tirti atitinkamų valstybių ir laikotarpių dokumentus analizuojant ne tik dokumentų, bet ir teisinio reguliavimo atsiradimą ir kitimą.

Mokslinės literatūros analizės metodas leido atskleisti, įvertinti ir panaudoti tyrimams kituose mokslinės literatūros šaltiniuose sukauptas naujausias mokslo žinias apie tapatybės vagystę elektroninėje erdvėje ir su tuo susijusių santykių teisinį reguliavimą. Šiuo metodu siekta teoriškai pagrįsti atskirus teiginius. Mokslinės literatūros šaltiniais vadovaujamasi daugelyje monografijos dalių pateikiant tikslias nuorodas į cituojamus šaltinius.

Kontentinės analizės metodas[4] taikytas analizuojant straipsnių Lietuvos elektroninėje žiniasklaidoje privatumo turinį. *Tyrimo tikslas* ir *uždaviniai* atskleisti 5.1. dalyje. Šio metodo esmė –atrasti informaciniame masyve tyrimui įdomius prasminius vienetus. Tirta dvidešimties elektroninės žiniasklaidos šaltinių 2009–2010 metų publikacijos privatumo apsaugos aspektu.

Antrinė duomenų analizė. Autoriai tyrimams naudoja ir kitų institucijų ar atskirų asmenų surinktus duomenis, juos analizuoja ir vertina atsižvelgdami į kitą turimą informaciją. Pasitelkiant kitų asmenų surinktus duomenis labai svarbu atskirti, kur pateikiami tikri duomenys, koks jų patikimumo lygis, ir gebėti atskirti juos nuo atskirų asmenų nuomonės arba surinktų duomenų interpretavimo. Autoriai naudojo platų spektrą pirminių šaltinių – nuo žiniasklaidos iki rimtų gerai vertinamų duomenų šaltinių. Žiniasklaidos (spausdintinės ir elektroninės) šaltinius autoriai naudojo tikslingai, siekdami surinkti kuo daugiau faktinės informacijos apie santykinai naują tiriamąjį reiškinį. Autoriai atsiribojo nuo žurnalistinių interpretacijų, svarbiomis aplinkybėmis laikydami pačius tiriamojo reiškinio faktus, jo pasireiškimo būdus, dažnumą, naudotas priemones ir kt., o tokiomis aplinkybėmis žiniasklaidos priemonės yra vienas iš operatyviausių šaltinių. Autoriai įvertino, kad žiniasklaidoje atskleisti faktai gali būti netiksliai perteikti. Žiniasklaidoje pateiktą informaciją autoriai tyrė ir ankščiau nurodytu kontentinės analizės metodu, tačiau tokio tyrimo tikslas buvo specifinis – informacijos sklaidos vertinimas.

Siekiant nustatyti visuomenės dalies, besinaudojančios internetu, požiūrį į tiriamąjį reiškinį, ištirti šio reiškinio pavojingumo sampratą, papli-

[4] Tidikis, R. 2003. *Socialinių mokslų tyrimų metodologija.* Vilnius: Lietuvos teisės universitetas, p. 498–504.

timą, priemonių ir lėšų skyrimą jo prevencijai ir sužinoti atsakymus į kitus monografijai svarbius klausimus, atlikti keli vienas kitą papildantys *anketiniai tyrimai*, kurių *tikslai* ir taikytų metodų specifika pateikta monografijos 5.2.1 dalyje. Buvo atliktos vartotojų, viešojo sektoriaus darbuotojų, Valstybinio socialinio draudimo fondo administravimo įstaigų (toliau – Sodros) darbuotojų ir verslo sektoriaus darbuotojų apklausos.

Nors toks internetinis anketavimo metodas turi trūkumų ir jo rezultatai negali būti interpretuojami atskirai nuo bendro konteksto ir kitų tyrimų rezultatų analizės, tačiau jo privalumais laikytina tai, kad asmenys, pildydami anketas visiškai anonimiškai, niekieno netrukdomi sau priimtinoje aplinkoje, neribojami laiko, gali laisvai pasirinkti, ar atsakyti į pateiktą klausimą, todėl jos pildomos savarankiškai ir atvirai. Šiuo anketiniu metodu pašalinami arba gerokai sumažinami tyrimų metodologijoje pabrėžiami anketinio tyrimo metodo trūkumai (apklausos vedėjo įtaka respondentams, laiko atsakymams ribotumas, į anketos klausimus atsakančiam asmeniui nepriimtina aplinkos įtaka, respondento baimė dėl galimo jo asmenybės nustatymo)[5]. Dėl internetinės apklausos trūkumų (pavyzdžiui, atsakyti galima kelis kartus tam pačiam asmeniui, visiško anonimiškumo jausmas leidžia anketą pildyti ne itin kruopščiai ir atsakingai ir pan.) šių rezultatų nereikia suabsoliutinti, dera vertinti tik bendriausias tendencijas. Autorių atliktų tyrimų gana didelis respondentų skaičius eliminuoja pavienių asmenų galimą netinkamą elgesį ir neabejotinai atskleidžia bendrąsias tendencijas. Mažiau patikimi yra viešojo sektoriaus ir verslo darbuotojų apklausų rezultatai, nes autoriams pavyko apklausti santykinai nedaug šių respondentų grupių asmenų, tačiau galima pastebėti, kad atskirais klausimais lyginant minėtas mažiau patikimas apklausas ir didelės imties apklausas gaunami labai panašūs rezultatai.

Ekspertų apklausos metodas. Jam taikomas anketinės apklausos būdas, t. y. atrinkti ekspertai turėjo atsakyti į anketose pateiktus atviro pobūdžio klausimus. Detaliau tyrimo tikslai ir specifika nurodyta monografijos 5.2.1 dalyje. Metodas buvo pasitelktas siekiant nustatyti svarbius klausimus, kurių negali atskleisti kiti tyrimai (pvz., vartotojų apklausa ir kt.), nes dėl reiškinio sąlygiško naujumo ir sudėtingumo, norint ištirti specifinius reiškinio aspektus, reikalingos specifinės žinios ir patirtis.

Neabejotinai būtina įvertinti tai, kad kiekvienas ekspertas turi savo nuomonę, vertybių skalę, pasaulėžiūrą, jausmus ir kt., o tai lemia subjek-

[5] *Ibid*., p. 488.

tyvų požiūrį į vieną ar kitą problemą, tačiau ekspertai buvo pasirinkti atsižvelgiant į jų žinias ir patirtį.

Kaip visų minėtų metodų pagalbinė arba savarankiška priemonė, taikomas dar vienas empirinis metodas: *profesinės patirties apibendrinimo metodas.* Jis pagal apibendrinamą informaciją dar skirstomas į tris atskirus:

Pirmasis iš jų yra *asmeninės profesinės patirties apibendrinimo metodas*. Kadangi autorių mokslinis tiriamasis, pedagoginis, taip pat praktinis darbas yra susijęs su nagrinėjamojo reiškinio tyrimais ir dėstymu, todėl jie gali vertinti informaciją remdamiesi savo žiniomis ir patirtimi.

Antrasis yra *geriausios praktikos apibendrinimo metodas.* Šis metodas labai svarbus tiriant reiškinio plitimo ateities tendencijas, galimą geriausią sprendimą, prevencijos priemones ir kt. Atskirose monografijos dalyse jis taikomas kaip savarankiškas tyrimo metodas.

Trečiasis metodas, itin svarbus ir dažnai susipinantis su kitais (pvz., dokumentinės analizės), yra *teisinių precedentų apibendrinimo metodas.* Jis taikytas tiriant atskirų valstybių teisinio reguliavimo patirtį.

Šie metodai itin padeda, kai reikia įvertinti atskirus kokybinius parametrus arba apibendrinti atliktus tyrimus ar kitų autorių nuomonę. Vertinant visų šių metodų pritaikomumą konkrečiam tyrimui, rezultatų patikimumą, būtina atžvelgti į jų specifiką.

Asmeninės profesinės patirties apibendrinimo metodas turi ir esminių *trūkumų*, nes yra pagrįstas konkretaus asmens patirtimi ir pastabomis, galimomis subjektyvumo apraiškomis ir įsitikinimais. Visi profesinės patirties apibendrinimo metodai turi būti vertinami atsargiai, o išvados daromos tik patikslinus kitais arba pasitelkiant tirti kartu ir kitus metodus, kadangi profesinės patirties apibendrinimas yra tik tikimybinio pobūdžio.

Iš esmės profesinės patirties ir jos apibendrinimo metodų svarbą ir objektyvumą reikia vertinti labai atsargiai. Anot profesoriaus Rimanto Tidikio, „svarstant ir aiškinantis profesionalizmo sampratą, dažnai vyksta teoretikų ir praktikų konfrontacija. Grynieji praktikai dažnai ignoruoja teoriją, laiko ją per daug abstrakčia, mažai pritaikoma veikloje ir tinkama tik ginčams akademinėse srityse. Priešingai, mokslininkai teoretikai dažnai praktiką traktuoja tik kaip individualią, elementarią, empirinę patirtį, įgytą per ieškojimus ir klydimus. Tokie priešingi požiūriai dėl to paties reiškinio analizės, skeptiški jo vertinimai daro didžiulę žalą ir praktikai, ir teorijai, tiek teoretikų, tiek praktikų profesionaliam tobulėjimui“[6].

[6] *Ibid*., p. 557.

Profesinės patirties apibendrinimo metodai nėra dažnai taikomi Lietuvoje rengiamose disertacijose, tačiau šių metodų svarba socialiniams mokslams pabrėžiama mokslinių tyrimų metodikų literatūroje[7].

Monografijoje neapsiribojama išskirtinai vienu ar kitu tyrimo metodu, bet analizuojami jau esami tyrimai, trūkstama informacija renkama atlikus kelis vienas kitą papildančius tyrimus, nuosekliai siekiant iškeltų uždavinių bei užsibrėžto tikslo.

Atliekant tyrimus taikyti šie **teoriniai metodai**:

Istorinis lyginamasis ir genezės metodai. Jie taikyti siekiant atskleisti reiškinio genezę, evoliucinę seką, kitimą ir raidą bei tai lėmusias priežastis. Šie metodai leidžia atsakyti, kaip ir kodėl atsirado tiriamasis reiškinys, kokie yra jo reguliavimo būdai ir ar toks reguliavimas reikalingas.

Be to, monografijoje plačiai taikomas (pvz., 3.3.2; 3.4.1 dalys) *lyginamasis metodas*, t. y. lyginami skirtingi tų pačių reiškinių aspektai, kitų valstybių ar regionų patirtis nagrinėjamais klausimais, kylančios problemos, sprendimo būdai, taip pat skirtingi reiškinio reguliavimo būdai. Lyginamasis metodas padeda autoriams nustatyti tiriamųjų reiškinių panašumus ir skirtumus, padeda atlikti analitines tyrimo funkcijas, išgryninti atskirus reiškinius ir jų tendencijas.

Analitinis kritinis metodas taikomas, siekiant pažvelgti į teisinio reguliavimo trūkumus ir jo įgyvendinimo disfunkcionalumą.

Atskiriems klausimams tirti autoriai taiko ir kitus teorinius tyrimo metodus (alternatyvų, analogijos, apibendrinimo, dedukcijos, indukcijos).

Monografijos autorių kolektyvas už pagalbą rengiant leidinį dėkoja ekspertams, sutikusiems pasitelkiant ekspertines žinias įvertinti tapatybės vagystę elektroninėje erdvėje: dr. Algirdui Kunčinui, Vitalijui Kirvaičiui, dr. Irmantui Rotomskiui, Ryčiui Rainiui, dr. Rolandui Krikščiūnui, Renatai Marcinauskaitei, dr. Skirmantui Bikeliui, dr. Alfredui Kiškiui bei Žydrūnui Paškauskui. Dėkojame Žmogaus teisių institutui ir jo direktoriui Henrikui Mickevičiui už sutikimą tyrimo tikslais naudoti šio instituto darbuotojų surinktas elektroninės žiniasklaidos publikacijas apie privatumą. Taip pat dėkojame monografijos recenzentams doc. dr. Irmantui Rotomskiui ir doc. dr. Antanui Kerui.

[7] *Ibid.,* p. 563.

TURINYS

Lentelių sąrašas

Paveikslų sąrašas

„Dar nėra sukurta sistemos, kuri užkirstų kelią ryžtingam ir profesionaliam nusikaltėliui pavogti ir panaudoti tapatybę“.

„Experian“[8]

„Pavogta tapatybė – galinga anonimiškumo skraistė nusikaltėliams, kelianti grėsmę ne tik piliečiams, bet ir nacionaliniam saugumui“.

FTB[9]

1. Tapatybės vagystė elektroninėje erdvėje kaip socialinis teisinis reiškinys

1.1. Asmens tapatybė ir asmens tapatybės nustatymas

1.1.1. Asmens tapatybė

Turint tikslą išnagrinėti tapatybės vagystę elektroninėje erdvėje kaip socialinį teisinį reiškinį, pirmiausia reikia aptarti asmens tapatybę, jos svarbą ir tapatybės nustatymo procesą.

Tarptautinių žodžių žodyne identitetas (tapatybė) aiškinama: ko nors apibrėžtumas, individualumas. Dabartiniame Lietuvių kalbos žodyne tapatybė reiškia objekto lygybę pačiam sau arba kitam objektui, tolygumą, vienodumą[10].

Vienas iš garsiausių tapatybės vagystės ekspertų Jungtinėse Amerikos Valstijose John D. Sileo[11] 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

[8] "Experian" yra pasaulyje pirmaujanti informacinių technologijų paslaugų įmonė, dirbanti duomenų teikimo ir analizės įrankių kūrimo srityje daugiau nei 80 šalių. Experian [interaktyvus, žiūrėta 2011-09-15]. <http://www.experianplc.com/about-experian.aspx>.

[9] FBI [interaktyvus, žiūrėta 2011-09-15]. <http://www.fbi.gov/about-us/investigate/cyber/identity_theft>.

[10] „Tapatybė“. 2005. *Lietuvių kalbos žodynas*. Vilnius: Lietuvių kalbos institutas.

[11] Informacija apie John D. Sileo: The Sileo Group [interaktyvus, žiūrėta 2011-09-15] <http://www.thinklikeaspy.com/about-john-sileo.php>.

privatumą ir tapatybės vagystę, dėmesys turi būti sutelktas į tapatybę, susijusią su asmens duomenimis – tai, pagal ką mus atpažįsta įvairios įmonės, organizacijos ar valdžios institucijos. Autoriaus teigimu, tapatybę sudaro bet koks vardas, numeris ar kitas požymis, kuris suteikia informacijos apie mus arba kuriuo pasinaudojus galima prieiga prie kitų asmens duomenų[12]. Autorių nuomone, vardas, numeris ar kitas požymis nėra asmens tapatybė kaip tokia, o tiktai priemonė asmeniui nustatyti.

Tapatybę galima suvokti skirtingais lygiais: tautiniu, regioniniu, profesiniu, asmeniniu. Tokia tapatybė apima asmens suvokimą, savęs sąsają su kita grupe ar grupėmis. Tokią tapatybę galima pavadinti socialine. Socialinė tapatybė apima identifikavimą kolektyve ar grupėje, priklausymą tautai, klasei, nusako priklausomumą etninei, religinei grupėms, tokiai tapatybei taip pat priskiriamas ir kultūrinis identitetas[13].

Kitas moksliniuose šaltiniuose išskiriamas svarbus asmens tapatybės bruožas – tapatybė medicininiu aspektu. Tai pati tiksliausia su asmeniu vienareikšmiškai susieta tapatybė. Ją galima apibūdinti kaip asmens duomenis ir informaciją, kuri naudojama asmens tapatybei nustatyti – tai asmens atvaizdas, pirštų atspaudai, išsamus aprašymas (kūno, veido), DNR duomenys, kiti ypatingi kūno bruožai (apgamai, fiziniai požymiai)[14] (kaip papildomi identifikatoriai).

Visuomeniniams santykiams labai svarbi tokia tapatybė, kurios nustatymo priemones asmeniui patvirtina valstybė. Tokią tapatybę nustatantys duomenys nurodomi atitinkamuose registruose. Valstybės registruose sukaupta ir saugoma informacija apie asmenį gali būti vadinama teisinės asmens tapatybės prielaida, nes tokiu atveju tapatybė nustatoma vadovaujantis konkrečiai teisės normose įtvirtinta tvarka, t. y. suteikiant asmeniui skaitinius kodus (asmens kodai, socialinio draudimo numeriai, asmens identifikavimo kodai ir kt.), valstybės registruose darant įrašus, tiesiogiai susietus su asmeniu (vardas, pavardė, gimimo

[12] Sileo, J. D. *Stolen lives: identity theft prevention made simple.* 2005, p. 31.

[13] Alcoff, L.; Hames-Carcia, M.; Moya, P. M. L. 2006. *Identity Politics Reconsidered*. Palgrave Macmillan, Basingstoke.

[14] "Medical ID". John M. Last. 2007. *A Dictionary of Public Health*. Oxford University Press, Inc.

data ir kt.)[15]. Galima teigti, kad tokius tapatybės nustatymo duomenis ir priemones kuria tik valstybė. Dabar valstybė asmens tapatybei nustatyti taiko ne tik aptartą įrašų metodą, bet ir modernų medicininį biometrinį, kuris leidžia išvengti klaidų ir klastočių, nes pasisavinti asmens medicininės tapatybės faktiškai neįmanoma. Gali egzistuoti ir egzistuoja tapatybės nustatymo priemonės, kurių valstybė nekuria, tačiau pripažįsta (pvz., saugus identifikavimas per bankinę sistemą, naudojamas Valstybinės mokesčių inspekcijos paslaugoms gauti ir valdyti).

Taip pat galimas ir vadinamasis tapatybės nustatymas sutartiniu būdu, kai asmuo identifikuojamas ne remiantis valstybės patvirtintais metodais ir priemonėmis, o taikomi sutartiniai identifikavimo būdai ir priemonės. Kai toks tapatybės nustatymas nėra teisiškai sureguliuotas, jis gali būti nepatikimas, neretai tokie identifikavimo metodai tinka abiem šalims.

Detaliau nagrinėjant tapatybės sukūrimą ir nustatymą elektroninėje erdvėje, galima pastebėti, kad skirtingose valstybėse tai apibrėžiama nevienodai. JAV elektroninė tapatybė – unikalus individualaus asmens pavadinimas. Kadangi asmenų pavadinimai nebūtinai yra unikalūs, elektroninė asmens tapatybė turi apimti pakankamai papildomos informacijos, kad būtų sukurta visiškai unikali elektroninė tapatybė[16]. Kiek kitokį apibrėžimą pateikia Naujosios Zelandijos institucijos: elektroninė tapatybė – nustatyta grupė požymių ir / ar duomenų, susijusių su konkrečiu asmeniu[17]. Tačiau nenurodoma, ar tokia tapatybė gali būti prilyginama tai tapatybei, kurios nustatymo priemones asmeniui tvirtina valstybė (išskyrus, kai naudojamos atitinkamos elektroninio parašo technologijos ir sprendimai) ir kokie duomenys reikalingi, norint identifikuoti asmenį elektroninėje erdvėje.

---

[15] Cane, P.; Conaghan, J. 2006. *The New Oxford Companion to Law*. Oxford University Press Inc.

[16] Electronic Authentication Guideline. Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-63 Version 1.0.2., 16 p. [interaktyvus, [žiūrėta 2011-09-15]. <http://www.usda.gov/egov/egov_redesign/intranet/eauth/SP800-63V6.pdf>.

[17] Guide to Authentication Standards for Online Services. State Services Commission, June 2006, Version 1.0. ISBN 0–478–24461–4. Crown Copyright. 33 p. [interaktyvus, žiūrėta 2011-09-15]. <http://www.e.govt.nz/library/egif-guide-to-authentication-standards-june-2006.pdf >.

Kai kalbama apie asmens 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[18]. 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.

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 matoma iš tam tikrų dokumentų, pavyzdžiui, sudaromų rinkėjų sąrašų, išduodamų santuokos liudijimų, įgytą išsilavinimą ar specialią kvalifikaciją patvirtinančių dokumentų, darbo patirties istorijos.

Taigi, asmens tapatybė – individo atitikimo nustatymas, naudojant pakankamą duomenų ir priemonių asmeniui identifikuoti visumą.

---

[18] Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas. *Valstybės žinios*, 2008, Nr. 22-804, 2 str. 1 d.

[19] United Kingdom Cabinet Office, Economic and Domestic Secretariat. Identity Fraud: A Study [interaktyvus]. London, 2002 [žiūrėta 2011-09-14]. <http://www.statewatch.org/news/2004/may/id-fraud-report.pdf>.

1.1.2. Asmens identifikavimas fizinėje ir elektroninėje erdvėje

Identifikavimas literatūroje suprantamas kaip asmeninio identifikatoriaus susiejimas su asmeniu, pateikiančiu tam tikrus identifikavimo atributus[20]. 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, 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 tapatybei nustatyti verslo institucijų, bankų informacinėse sistemose, atliekant elektroninius pirkimus, mokėjimus, naudojantis elektroninėmis paslaugomis.

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, 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[21].

Asmens identifikavimas fizinėje erdvėje

Fizinėje erdvėje identifikuojama, naudojant vieną iš privalomų identifikavimo priemonių – tinkamą asmens dokumentą ir lyginant dokumente esančią nuotrauką su konkrečiu asmeniu. Toks identifikavimas, naudojant oficialius valstybės išduotus dokumentus, gali būti vadinamas oficialiuoju. Taip pat fizinėje erdvėje galimas ir kitoks identifikavimas –

[20] Camp, L. J. 2010. *Economics of Identity Theft*. Springer, p. 13.

[21] Sileo, J. D. 2005. *Stolen lives: identity theft prevention made simple.* p. 32.

naudojant ne valstybės, o kitų subjektų išduotus dokumentus (pvz., darbuotojo pažymėjimą), tačiau šis identifikavimas yra lokalus ir šioje monografijoje nagrinėjamas nebus.

Reikia paminėti, kad identifikavimas fizinėje erdvėje vyksta tam tikromis numatytomis aplinkybėmis (pvz., kai valstybės norminiai teisės aktai įsakmiai nurodo identifikavimo būtinybę arba tai svarbu tam tikriems šalių santykiams) ir santykinai daugeliu atvejų identifikavimas, kaip toks, nėra būtinas. Galima pateikti paprastą pavyzdį, kai perkant prekę parduotuvėje identifikuoti asmens nereikalaujama, kadangi vyksta momentinis sandoris ir atsiskaitoma iš karto, t. y. prekės pirkimo momentu.

Svarbiausi įstatymiškai pripažįstami dokumentai Lietuvoje, kurie patvirtina asmens tapatybę fizinėje erdvėje, yra: gimimo liudijimas, asmens tapatybės kortelė, pasas, naujo pavyzdžio vairuotojo pažymėjimas, valstybės tarnautojo pažymėjimas. Tokius dokumentus suteikia tik Valstybės įgaliotos institucijos ir jie yra vienintelė teisėta tapatybės nustatymo priemonė Lietuvoje. Kiekvienas iš šių dokumentų skirtas tam tikram specialiam tikslui, todėl šie dokumentai nesidubliuoja[22] ir juose nurodoma tiek asmens duomenų, kiek būtina konkrečiam teisiniam santykiui. Atlikus platesnę analizę (apžvelgus kitas valstybes – JAV ir Rusiją), nustatyta, kad pagrindiniai įstatymiškai pripažįstami tapatybės dokumentai Rusijos Federacijoje yra gimimo liudijimas, pasas (piliečio, diplomatinis pasas, tarnybinis pasas, užsienio pasas, jūrininkų pasas), karinis pažymėjimas. Tuo tarpu JAV dalį funkcijų, susietų su asmens tapatybės dokumentais, įgyvendinimo yra delegavusi savo valstijoms, todėl pripažįstamų asmens dokumentų įvairovė JAV yra labai didelė, o asmens šių dokumentų išdavimo tvarka – labai lanksti. Tačiau JAV vienintelė iš minėtų valstybių turi tokią didelę asmens dokumentų įvairovę, kuri savo ruožtu palengvina nusikaltėliams atlikti tapatybės vagystes.

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. Tačiau plati dokumentų įvairovė gali nusikaltėliams palengvinti tapatybės vagystę.

[22] Išskyrus pasą ir kortelę.

Asmens identifikavimas elektroninėje erdvėje

Plėtojant elektronines paslaugas, valstybėms iškilo poreikis identifikuoti asmenis ne tik fizinėje erdvėje, bet ir elektroninėje. Identifikuoti naudojamų duomenų turinys fizinėje erdvėje, nepriklausomai nuo naudojamo asmens tapatybę patvirtinančio dokumento, yra panašus. Tačiau elektroninėje erdvėje pateikti oficialų tradicinį asmens tapatybę nustatantį ne elektroninį dokumentą yra neįmanoma, nors asmenims labai dažnai prireikia patvirtinti savo tapatybę ir šioje terpėje.

Reikia paminėti, kad lyginant su fizine erdve, identifikavimo elektroninėje erdvėje skaičius santykinai yra didesnis. Taigi, elektroninėje erdvėje daug dažniau reikia naudoti asmeninę informaciją, ir vien tai lemia didesnį tapatybės vagysčių skaičių[23].

Elektroninė erdvė identifikavimo aspektu pasižymi tam tikra specifika, kai norint identifikuoti, nereikia fiziškai būti atitinkamoje geografinėje vietoje. Elektroninė erdvė asmenis įgalina atlikti reikiamus veiksmus per atstumą. Šie veiksmai gali būti elektroninės informacijos perdavimas, kaupimas, apdorojimas, naudojimas, dėl to asmenims nereikia būti konkrečioje vietoje, jei jie nori pasinaudoti tokia informacija arba atlikti reikiamą veiksmą.

Elektroninėje erdvėje asmens tapatybės nustatymo procedūra yra kur kas sudėtingesnė, nes tarp asmenų, kurie bendrauja pasinaudodami informacinėmis ir ryšio technologijomis, yra 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.

Tad kyla klausimas, kokios tapatybės patvirtinimo priemonės naudojamos elektroninėje erdvėje? Taip pat kokie yra oficialūs valstybės patvirtinti identifikavimo metodai?

Pažymėtina, kad elektroninės erdvės sritys, kuriose asmuo identifikuojamas, yra labai įvairios: komercinių paslaugų teikimas, adminis-

[23] Higgins H. E. 2010. *Cybercrime: An Introduction to an Emerging Phenomen*. McGraw-Hill, p. 74.

tracinių paslaugų teikimas ir kt. Asmuo elektroninėje erdvėje gali būti identifikuojamas naudojant elektroninio parašo technologiją, pagal kompiuterio tinklo plokštės MAC[24] adresą, kompiuterio IP adresą[25], *wireless*[26] stotelės adresą, domeno vardą ir pan. Didžioji dalis elektroninių paslaugų sistemų naudoja panašias asmens identifikavimo priemones.

Literatūroje pateikiama tokia asmens autentifikavimo schema:

1 pav. Asmens autentifikavimas, atliekamas informacinių technologijų sistemų (Leenes (ed.), FIDIS network, deliverable 5.2b, ID-related crime: towards a common ground for interdisciplinary research, May 2006[27]. p. 80.)

Apibendrinus ir sugrupavus bei pateikus pavyzdžius, galima išskirti šiuos svarbiausius asmens elektroninėje erdvėje identifikavimo elementus ir identifikavimo pavyzdžius (2 pav.)[28]:

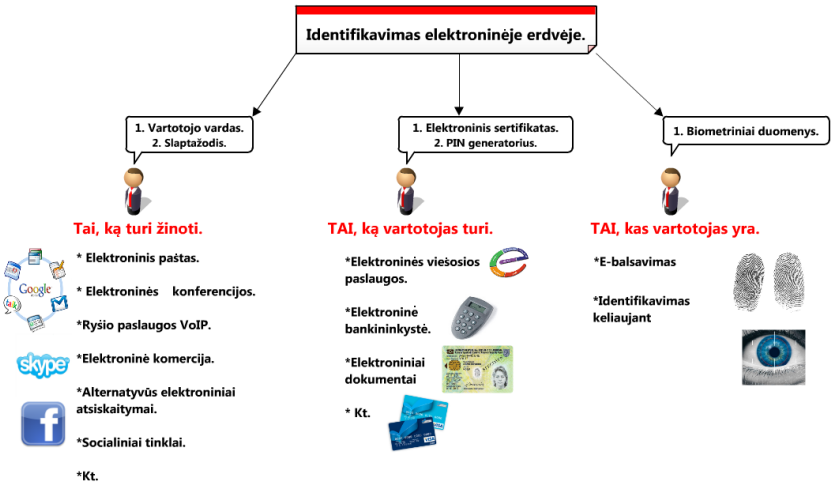
[24] MAC (angl. *Media Access Control*) adresas – tai tinklo plokštės identifikatorius.

[25] IP (*Internet Protocol*) adresas – kompiuterio identifikatorius tinkle, t. y. unikalus skaičius, naudojamas vienareikšmiškai identifikuoti duomenų paketo siuntėją ir gavėją.

[26] *Wireless* – bevielis ryšys.

[27] Leenes, R. Fidis, D5.2b: ID-related crime: towards a common ground for interdisciplinary research [interaktyvus]. 2006 [žiūrėta 2011-09-14], p. 80. <http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp5-del5.2b.ID-related_crime.pdf>.

[28] Electronic Authentication Guideline. Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-63 Version 1.0.2. [interaktyvus, žiūrėta 2011-09-18]. <http://www.usda.gov/egov/egov_redesign/intranet/eauth/SP800-63V6.pdf>.



2 pav. Identifikavimas elektroninėje erdvėje
(sudaryta autorių)

Identifikavimas pagal tai, ką vartotojas turi žinoti

Kaip nurodyta 1 pav., asmuo elektroninėje erdvėje gali būti identifikuojamas pagal unikalų pavadinimą (vardą) ir slaptažodį. Fizinėje erdvėje asmenų vardai gali kartotis, tačiau toje pačioje elektroninėje sistemoje asmens tapatybė turi būti nustatoma naudojant unikalų identifikatorių. Tai lemia pačių sistemų specifika, nes negali būti tokių pačių vardų, aprašančių skirtingus asmenis. Pasirinktas slaptažodis paprastai būna ženklų eilutės. Šio metodo patikimumas priklauso nuo informacinės sistemos apsaugos lygio. Trumpi slaptažodžiai yra nesaugūs, ilgus ir sudėtingus slaptažodžius sunku įsiminti. Tokių sistemų saugumas priklauso nuo pačių vartotojų. Jeigu vartotojai nesaugiai naudos savo identifikavimo elementus, jų tapatybes bus galima lengvai pasisavinti. Šiuo identifikavimo principu naudojasi didžiausioji dalis žinomų elektroninių paslaugų:

- Komunikacijos paslaugos – elektroninis paštas, elektroninės konferencijos, ryšio paslaugos *VoIP* ir kt.
- Elektroninė komercija – elektroninės parduotuvės, kiti subjektai, teikiantys elektronines paslaugas, alternatyvūs elektroniniai atsiskaitymai ir kt.
- Socialiniai tinklai, virtualios bendruomenės ir kt.

Jeigu tokius pačius socialinius santykius paanalizuotume fizinėje erdvėje, pastebėtume, kad identifikavimo fizinėje erdvėje panašiais atvejais gali iš viso nebūti. Jei paanalizuotume sandorius, tai fizinėje erdvėje yra daug momentinių sandorių, kur fizinio asmens tapatybė nereikšminga (svarbu, kad, pvz., tokio momentinio sandorio atveju būtų sumokamas atlygis. Tačiau elektroninėje erdvėje atlygintinų momentinių sandorių faktiškai nebūna, nes nėra galimybės betarpiškai atsiskaityti realiuoju laiku, tad netgi dėl menkiausios operacijos reikia asmenį identifikuoti. Kaip matome, dažnai toks identifikavimas būna sutartinis.

Paminėtina, kad šio identifikavimo būdo valstybė nereglamentuoja. Tai reiškia, kad toks identifikavimo mechanizmas yra paslaugos teikėjo ir kliento reikalas. Praktikoje dažnai asmenų pasirinkti unikalūs vardai neturi nieko bendro su tikruoju asmeniu. Vartotojai nėra įpareigoti patvirtinti savo tikrąją tapatybę registruodamiesi tokiose sistemose, bet tokia sukurta tapatybė tampa asmens duomenimis, kurių apsaugą užtikrina teisės aktai. Elektroninio pašto adresas neretai tampa vienu iš svarbiausių tapatybę identifikuojančių elementų elektroninėje erdvėje. Tačiau elektroninio pašto paslaugų teikėjai netikrina asmens tapatybių registravimosi momentu, taip sudarydami palankias sąlygas tapatybės klastotojams. Elektroninio pašto identifikavimo sistemų sąlygiškas paprastumas, galimybė pasisavinti vartotojų vardus ir slaptažodžius rodo rimtą problemą – elektroninės tapatybės praradimą[29].

Problemų taip pat kyla dėl sparčiai plintančių socialinių tinklų internete. Jie leidžia socialinius ryšius perkelti į elektroninę erdvę ir jiems identifikuoti naudoti elektronines priemones. Socialiniai tinklai tampa ne tik bendravimo priemone, bet ir verslo vykdymo, darbinių santykių plėtojimo terpe, kur kiekviena elektroninė tapatybė asocijuojasi su tikrąja asmens tapatybe – egzistuojančiu asmeniu. Asmenys registruojasi, į tokius tinklus perkelia savo asmens duomenis, tačiau neturi garantijų, kad jų tapatybės kas nors nepasisavins. Registracija į tokius socialinius tinklus pagrįsta elektroniniu paštu, todėl būtent elektroninis paštas ir pasirinktas slaptažodis tampa elektronine tapatybe. Tačiau patikimų identifikavimo priemonių netaikymas ir sąlygiškas paprastumas registruojantis didina riziką, kad socialiniai tinklai bus išnaudojami nusikalstamai veikai.

[29] *Google targeted in e-mail scam* [interaktyvus]. 2009-10-06 [žiūrėta 2011-09-18]. <http://news.bbc.co.uk/2/hi/technology/8292928.stm>.

2010 m. rugsėjo mėn. nusikaltėliai pasisavino Interpolo vadovo socialinio tinklo „Facebook“ tapatybę. Jo vardu buvo sukurti du netikri profiliai, nusikaltėliai juos naudojo siekdami gauti informacijos apie tarptautinės policijos agentūros vykdomas operacijas[30]. Socialinių tinklų saugumo spragos, registravimosi paprastumas tampa pasauline problema[31].

Aptariant asmens identifikavimą elektroninėje erdvėje, atskirai galima paminėti asmens kodo, kuris yra vienas iš pagrindinių asmens tapatybės identifikatorių, naudojimą. Asmens kodas – tai unikali skaitmenų seka[32]. Tokia asmens kodo struktūra atskleidžia asmeninę informaciją (lytį ir gimimo datą) ir yra unikali bei nekeičiama identifikavimo priemonė, skirta duomenims apie asmenį kaupti gyventojų registre. Taip pat pažymėtina, kad asmens kodas yra patogus požymis norint 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 naudojimas atviru pavidalu kelia grėsmę, kad asmens tapatybė elektroninėje erdvėje gali būti pasisavinta.

Identifikavimas pagal tai, ką vartotojas turi

Šiuo principu grindžiamas kliento atpažinimas pagal turimas priemones: laikmena su identifikavimo duomenimis (elektroninis parašas (patvirtintas elektroniniu sertifikatu), kodų generatoriai, kodų lentelės. Lyginant su fizine erdve, tai tos priemonės, kuriomis identifikavimą (atitinkamomis sąlygomis) reguliuoja (ar pripažįsta) valstybė. Tai santykinai patvirtina jų saugumą ir patikimumą.

Pirmiausia paminėtinas tapatybės nustatymas elektroninėmis priemonėmis, kurias valstybė imperatyviai reguliuoja. Įstatymiškai pripažįs-

[30] *Interpol chief has Facebook identity stolen* [interaktyvus]. 2010-09-19 [žiūrėta 2011-09-18]. <http://www.networkworld.com/news/2010/091910-interpol-chief-has-facebook-identity.html>.

[31] *First INTERPOL information security conference to provide global platform for preventing and detecting high-tech crimes* [interaktyvus]. 2010-09-15 [žiūrėta 2011-09-18]. <http://www.interpol.int/public/ICPO/PressReleases/PR2010/PR070.asp>.

[32] Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas, *Valstybės žinios*, 2008, Nr. 22-804, 7 str. 1 d.

tamas ir reguliuojamas asmens identifikavimo būdas elektroninėje erdvėje – elektroninis sertifikatas ir elektroninis parašas. Elektroninis sertifikatas – tai elektroninis liudijimas, kuris susieja parašo tikrinimo duomenis su pasirašančiu asmeniu ir patvirtina arba leidžia nustatyti pasirašančio asmens tapatybę.[33] Elektroninis parašas – tai duomenys, kurie įterpiami, prijungiami ar logiškai susiejami su kitais duomenimis pastarųjų autentiškumui patvirtinti ir (ar) pasirašančiam asmeniui identifikuoti[34]. Detaliau elektroninį sertifikatą, kaip asmens tapatybės patvirtinimo būdą elektroninėje erdvėje, apibrėžia LR Tapatybės kortelės įstatymas: „Asmens atpažinimo elektroninėje erdvėje sertifikatas – elektroninis liudijimas su įrašytais, nurodytais ir vidaus reikalų ministro nustatytais techniniais duomenimis ir patvirtinantis arba leidžiantis nustatyti asmens tapatybę elektroninėje erdvėje[35]. Aiškiai nurodoma paskirtis – nustatyti asmens tapatybę, ar asmens duomenys, kurie įrašomi į sertifikatą, atitinka tapatybės kortelės duomenis: vardas (vardai), pavardė, lytis, gimimo data, asmens kodas, pilietybė[36]. LR asmens tapatybės kortelė yra dokumentas, galintis patvirtinti jūsų tapatybę fizinėje erdvėje ir elektroninėje: „Asmens tapatybės kortelė gali būti naudojama asmens tapatybei elektroninėje erdvėje patvirtinti ar nustatyti ir elektroniniams duomenims pasirašyti (išduotos nuo 2009 m. sausio 1 d.)“[37].

Lietuvoje yra keli elektroninių sertifikatų ir kvalifikuotų elektroninių parašų paslaugų teikėjai[38]. Visi jie turi teisę sukurti galiojančias ir patvirtintas asmens tapatybės nustatymo elektroninėje erdvėje priemones[39], kuri teisiškai yra lygiavertė fizinei tapatybei, patvirtintai galiojančiais asmens dokumentais. Tačiau fizinėje erdvėje aptartus asmens

[33] Lietuvos Respublikos elektroninio parašo įstatymas. 2000. *Valstybės žinios*, Nr. 61-1827, 2 str. 14 d.

[34] Lietuvos Respublikos elektroninio parašo įstatymas. 2000. *Valstybės žinios*, Nr. 61-1827, 2 str. 4 d.

[35] Lietuvos Respublikos asmens tapatybės kortelės įstatymas. 2001. *Valstybės žinios*, Nr. 97-3417, 1 prim. str. 1 d.

[36] *Ibid*.

[37] *Ibid*.

[38] UAB „Skaitmeninio sertifikavimo centras“, VĮ „Registrų centras“, Gyventojų registro tarnyba prie Lietuvos Respublikos vidaus reikalų ministerijos.

[39] Paminėtina, kad elektroninį parašą galima turėti ne vieną (paremtą skirtingomis sistemomis), skirtingai nei fizinėje erdvėje, teisėtai niekada negalima turėti tokio paties dokumento dviejų originalų.

dokumentus turi teisę išduoti tik valstybinės institucijos, kurios garantuoja tokių dokumentų autentiškumą ir tikrumą. Tuo tarpu elektroninės asmens tapatybės nustatymo priemones gali kurti ir ne valstybinės įstaigos.

Elektroninis asmens sertifikatas sukurtas remiantis matematiniais algoritmais, jo patikimumas yra garantuojamas patvirtintų standartų. Toks sertifikatas teoriškai yra saugesnis už įprastinį asmens dokumentą. Tačiau jo saugumas priklauso ir nuo asmens, kuriam jis priklauso, nes pats sertifikatas yra apsaugotas slaptažodžiu, o jį praradus kyla rizika, kad kažkas gali pasinaudoti elektroniniu sertifikatu, identifikuodamas save kaip kitą asmenį. Rizika dar labiau padidėja dėl fizinio kontakto nebuvimo, galimybės pamesti sertifikato laikmeną.

Aptartas identifikavimas elektroninėmis priemonėmis, paremtas sertifikatais, šiuo metu plačiai naudojamas asmenų, siekiančių gauti dalį valstybės institucijų teikiamų elektroninių paslaugų. Institucijos identifikuoja asmenis pagal jų elektroninius sertifikatus, ir ne tik. Viešojo administravimo institucijų informacinių sistemų interoperabilumo sistemos funkcionavimo taisyklėse nurodyta, kad jungiantis prie viešojo administravimo institucijų informacinių sistemų, asmens tapatybė gali būti nustatoma naudojant elektroninį parašą, patvirtintą kvalifikuotu sertifikatu, bei elektroninės bankininkystės sistemas[40].

Paminėtina, kad kaip ir Lietuvoje, Rusijos Federacijoje taip pat yra elektroninio parašo įstatymas[41], nustatantis elektroninio sertifikato teisinę galią, kuriame nurodoma, kad kvalifikuotas sertifikatas yra tos pačios teisinės galios kaip ir raštiškas parašas bei gali identifikuoti pasirašantį asmenį. Tačiau Rusijos Federacijos teisės aktuose nenumatoma jokių kitų priemonių, kuriomis būtų galima nustatyti asmens tapatybę elektroninėje erdvėje, bet nuo 2010 m. vykdomas projektas, kurį rengiamasi visiškai įgyvendinti iki 2014 m., – tai elektroninės tapatybės kortelės. Tokioje kortelėje bus ir asmens elektroniniai sertifikatai, patvirtinantys tapatybę

[40] Informacinės visuomenės plėtros komiteto prie Lietuvos Respublikos Vyriausybės direktoriaus 2008 m. gruodžio 1 d. įsakymas „Dėl viešojo administravimo institucijų informacinių sistemų interoperabilumo sistemos funkcionavimo taisyklių patvirtinimo“ Nr. T-228. *Valstybės žinios*. 2008, Nr. 145-5850, IV dalis. 13.1 p.

[41] Ob elektronnoj cifrovoj podpisi [interaktyvus, žiūrėta 2011-09-18]. <http://www.obki.ru/DOCS/zakonECP.rtf>.

elektroninėje erdvėje[42]. Taip pat elektroninį parašą traktuoja ir JAV Elektroninių parašų globalioje ir nacionalinėje komercijoje aktas[43], kuriame nustata elektroninio sertifikato teisinė galia. Šiame įstatyme nurodoma, kad viena iš elektroninio parašo funkcijų yra pasirašančio asmens identifikavimas. Tačiau didžioji dalis elektroninių paslaugų sistemų JAV naudoja ankščiau monografijoje minėtas asmens identifikavimo priemones (tai, ką vartotojas turi žinoti).

Taip pat galimos ir valstybės pripažįstamos elektroninės tapatybės nustatymo priemonės. Elektroninės bankininkystės paslaugos naudoja savo identifikavimo sistemą, kuri sujungia du identifikavimo elektroninėje erdvėje elementus: „Tai, ką žino" ir „Tai, ką turi" ir kurią pripažįsta valstybė. Toks tapatybės nustatymas turi teisinę galią, nes remiasi Lietuvos Respublikos elektroninio parašo įstatymo 8 straipsnio 3 dalies nuostata: "Elektroninis parašas visais atvejais turi šio straipsnio 1 dalyje įtvirtintą teisinę galią, jeigu parašų naudotojai tarpusavyje dėl to susitaria"[44]. Banko ir kliento susitarimas, kad tam tikra banko sistema atitinka saugios sistemos požymius, minėtoji įstatymo teisės norma ir identifikavimas remiantis šia sistema ir suponuoja tą faktą, kad ši identifikavimo sistema yra pripažįstama valstybės.

Banko naudojamos apsaugos priemonės identifikuoti klientus:[45]

- Atpažinimo kodas – tai unikali ženklų seka, kuri naudojama asmens tapatybei nustatyti registruojantis sistemoje.
- Slaptažodis – tai unikali ženklų seka, kuri naudojama asmens tapatybei patvirtinti registruojantis sistemoje; slaptažodį bankas rekomenduoja sudaryti iš raidžių, skaičių ir simbolių bei reguliariai jį keisti.

Banko naudojamos atpažinimo priemonės identifikuoti klientus:

- Slaptažodžių kortelė, kurioje nurodyti sunumeruoti slaptažodžiai, įvedami į sistemą ryšio seanso pradžioje arba patvirtinant operacijas.

[42] Medvedev poruchil do 1 maja izdat akty dlja vypuska i premenenija UehK [interaktyvus]. 2011-03-16 [žiūrėta 2011-09-18]. <http://www.rian.ru/economy/20110316/354390288.html>.

[43] Electronic signatures in global and national commerce act [interaktyvus, žiūrėta 2011-09-18]. <http://www.ftc.gov/os/2001/06/esign7.htm>.

[44] Lietuvos Respublikos elektroninio parašo įstatymas. 2000. *Valstybės žinios*, Nr. 61-1827, 8 str. 3 d.

[45] Parengta vadovaujantis Lietuvoje veikiančių komercinių bankų paslaugų teikimo sutartimis.

- Slaptažodžių generatorius, kuris pagal specialų algoritmą kiekvieną kartą registruojantis sistemoje sudaro unikalų slaptažodį – skaitmenų seką.

Klientas pasirenka naudotojui teikiamą atpažinimo priemonę savo nuožiūra. Vartotojas privalo žinoti savo unikalų numerį sistemoje, slaptažodį, kurį jis turi nuolat keisti, bei turėti vieną iš atpažinimo priemonių. Pasirinkus slaptažodžių generatorių, jo gaunamos skaitinės išraiškos niekada nepasikartoja, priešingai nei slaptažodžių kortelėje.

Naudotojo autentiškumas laikomas patvirtintu, jei naudotojas ryšio seanso pradžioje teisingai panaudojo banko suteiktas atpažinimo ir apsaugos priemones ir jei bankas gavo naudotojo informaciją apie jo registravimąsi sistemoje. Bankas pripažįsta ir laiko naudotojo pasirašytais ir patvirtintais banko sistema gautus pranešimus apie kliento sąskaitose esančių lėšų panaudojimą, sutarčių sudarymą, sutarties sąlygų pakeitimą, sutarties papildymą, termino pratęsimą arba sutarties nutraukimą ir kitą informaciją, jei ryšio seanso pradžioje buvo nurodytos teisingos atpažinimo ir apsaugos priemonės, kitaip tariant, bankas pripažįsta šią identifikavimo sistemą kaip elektroninį sertifikatą ir visus patvirtintus dokumentus jis laiko ekvivalentiškais rašytiniams. Kaip minėta, tokią galimybę bankams suteikia Lietuvos Respublikos elektroninio parašo įstatymas, dėl to bankų naudojamos klientų elektroninių duomenų identifikavimo sistemos turi tokią pat teisinę galią kaip ir parašas rašytiniuose dokumentuose ir yra leistinas kaip įrodinėjimo priemonė teisme visais atvejais, nes klientas ir bankas dėl to tarpusavyje susitarė[46].

Šiuo metodu vykdomas identifikavimas atitinka tikrąją – formalią asmens tapatybę, tai užtikrina institucijos, išduodamos elektroninius sertifikatus, ir bankai, vadovaudamiesi svarbiausiu principu – tinkamu kliento identifikavimu.

Identifikavimas pagal tai, kas vartotojas yra

Šiuo atveju naudojami biometriniai tapatybės elementai, kurie leidžia identifikuoti asmenį pagal asmens specifines fiziologines arba elgesio charakteristikas. Naudojamos nekintančios asmeninės charakteristikos reikalauja specialios įrangos. Dažniausiai naudojami: pirštų antspaudai,

[46] Lietuvos Respublikos elektroninio parašo įstatymas. 2000. *Valstybės žinios*, Nr. 61-1827, 8 str.

akies tinklainės skenavimas, akies rainelės skenavimas. Mažiau patikimi metodai – veido atvaizdavimas, rankos geometrija, parašo ir balso atpažinimas. Tokios technologijos turi daug privalumų:[47]

- Biometrinės charakteristikos negali būti perduodamos kitam žmogui.
- Biometrinės technikos neleidžia atsirasti klaidoms, susijusioms su klaidingu įvertinimu, kylančiu iš išankstinės nuomonės, išsiblaškymo ar nuovargio.
- Žmogui nereikia nešiotis jokių papildomų daiktų (paso, mokėjimo kortelės), nereikia prisiminti įvairių slaptažodžių ir kodų.

Nors ši technologija saugiausia iš aptartų, tačiau jos integravimo sudėtingumas verčia rinktis kitas pigesnes asmens identifikavimo priemones. Iš principo teisės aktai šio identifikavimo būdo nereglamentuoja, išskyrus tik biometrinių duomenų, saugomų tapatybės kortelėje, reguliavimą.

Reikia paminėti, kad 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, kad pseudonimas priklauso būtent jam. Kai naudojamas pseudonimas, visada turi būti užtikrinama, kad jis naudojamas būtent to asmens, kuriam priklauso. Technologijos turėtų garantuoti, 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.

Pažymėtina, kad pagal autorių atliktą verslo atstovų apklausą, net 37,2 proc. respondentų mano, kad verslo sektoriaus taikomos priemonės, kuriomis siekiama apsaugoti nuo tapatybės vagystės elektroninėje erdvėje, yra nepakankamos. Tad verslo taikomų apsaugos priemonių plėtojimas taip pat turėtų būti vienas iš prioritetų.

Apibendrinančios išvados:

• Asmens tapatybe laikytinas individo atitiktis jam pačiam, naudojant pakankamą asmens identifikavimo duomenų ir priemonių visumą. Nepai-

[47] Stan Z. Li, Anil K. Jain. 2009. *Encyclopedia of Biometrics*. Springer Science Business Media, LLC, 2–5 p.

sant identifikavimo tiek fizinėje, tiek elektroninėje erdvėje priemonių ir būdų, kiekvienu konkrečiu atveju galima nustatyti tik vieną asmenį.

• Tapatybės nustatymas fizinėje erdvėje dažniausiai siejamas su valstybės patvirtinta identifikavimo priemone, t. y. su atitinkamu oficialiu valstybės išleistu dokumentu. Šių dokumentų identifikavimo informacijos turinys skiriasi, priklausomai nuo dokumento paskirties.

• Identifikavimo priemonės ir būdai fizinėje ir elektroninėje erdvėje nėra tie patys. Asmens identifikavimo informacija fizinėje ir elektroninėje erdvėje gali skirtis pagal jai keliamus reikalavimus. Identifikavimas elektroninėje erdvėje, ypač dėl šios erdvės specifikos (elektroninėje erdvėje identifikavimas vyksta asmeniui tiesiogiai fiziškai nedalyvaujant) vykdomas daug dažniau.

• Elektroninėje erdvėje identifikavimas, naudojant kvalifikuotu sertifikatu patvirtintą elektroninį parašą (kaip valstybės sureguliuota saugi identifikavimo priemonė), arba asmens identifikavimas naudojant bankines sistemas (valstybės pripažįstama tapatybė[48]) saugaus identifikavimo aspektu atitinka valstybės reguliuojamus tapatybės nustatymo būdus fizinėje erdvėje (kai tapatybė nustatoma naudojant dokumentus).

• Apibendrinant technologinį tapatybės patvirtinimo elektroninėje erdvėje aspektą, pabrėžtina, kad informacinių technologijų sistemos asmenis sugeba atpažinti pagal tam tikrus identifikatorius: pagal tai, kas asmuo yra (taikant 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).

1.2. Elektroninė erdvė ir tapatybės vagystė kaip visuomenei pavojinga veika, šios veikos padariniai (pasekmės)

1.2.1. Elektroninė erdvė ir tapatybės vagystė kaip visuomenei pavojinga veika

Šiuolaikinė informacinė visuomenė jau neįsivaizduoja savo gyvenimo be informacinių ir ryšio technologijų. Informacinė visuomenė, kuriai stebėtinai didelį poveikį daro informacinės ir ryšio technologijos, nuolat

[48] Jei naudojamasi sutartiniu elektroniniu parašu.

vartoja „interneto“ ir „elektroninės erdvės“ sąvokas, kurios, atrodo, niekuo nesiskiria, todėl vartojamos kartu kaip sinonimai. Tačiau elektroninės erdvės nereikėtų tapatinti su internetu. Elektroninė erdvė – tai nepriklausoma, neturinti fizinių ir teisinių sienų komunikacijos aplinka, neturinti centralizuoto valdymo ar centralizuotų kontrolės mechanizmų, o internetas turėtų būti suprantamas tik kaip vienas iš elektroninės erdvės elementų. Vis dėlto šios dvi sąvokos labai dažnai vartojamos kaip sinonimai ir globali elektroninė erdvė (kompiuterių tinklai ir internetas) tapatinama su internetu, kuris dar vadinamas tinklų tinklu. Manoma, kad vienas tinklas – internetas neegzistuoja, jį sudaro grupės privačių ir viešų tarpusavyje sujungtų tinklų. Todėl, pavyzdžiui, vietinis kompiuterių tinklas, neprijungtas prie interneto, taip pat sudaro elektroninę erdvę[49]. Toliau 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 paslaugų. Ši 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, jį naudojant 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.

Be to, išaugo verslo teikiamų elektroninių paslaugų vartotojams mastas: daugelis verslo subjektų perkėlė savo veiklą (visą arba dalį jos) į elektroninę erdvę, bankai savo klientams siūlo elektroninės bankininkystės paslaugas, vartotojai įgyja vis daugiau patirties pirkdami prekes ar paslaugas internetu. Pavyzdžiui, 2009–2010 metais elektroninėje erdvėje perkančių žmonių skaičius Lietuvoje padidėjo beveik dvigubai – 73 proc., kaip rodo „TNS LT“ tyrimas[50].

Numatydama galimą interneto reikšmės didėjimą, Ekonominio bendradarbiavimo ir plėtros organizacija (angl. *Organization for Economic Cooperation and Development, toliau – OECD*) dar 1998 m. pabrėžė elektroni-

[49] Štitilis, D. 2003. Prekių ženklų naudojimas elektroninėje erdvėje: teisiniai aspektai, *Jurisprudencija* 41(33): 141.

[50] Apsiperkančių internete padvigubėjo. Delfi.lt [interaktyvus]. 2011-05-18 [žiūrėta 2011-09-14]. <http://mokslas.delfi.lt/archive/print.php?id=45640243>.

nių transakcijų svarbą pasaulinei ekonomikai ir pačiai visuomenei. Tačiau OECD taip pat įspėjo savo nares apie tokių tamsiųjų pokyčių, kaip naujų grėsmių, galinčių padaryti žalos klientams ir vartotojams elektroninėje erdvėje, atsiradimą. Elektroninėje erdvėje santykiai „akis į akį" neegzistuoja, todėl gana sudėtinga nustatyti tikrąją asmens tapatybę atliekant elektronines transakcijas, o sukčiauti tokioje aplinkoje yra kur kas lengviau nei fizinėje erdvėje[51]. Taip yra todėl, kad tapatybės nustatymas fizinėje erdvėje yra visiškai kitoks nei elektroninėje erdvėje. Fizinėje erdvėje savo tapatybę asmuo patvirtina vienu iš privalomų elementų – asmens dokumentu. Elektroninėje erdvėje tapatybę gali atstoti vardas ir slaptažodis: vardas – kokio nors objekto sutartinis tą objektą vienareikšmiškai identifikuojantis pavadinimas, kuris sistemoje turi būti unikalus; slaptažodis – ženklų seka, žinoma tik paslaugos teikėjui ir jos vartotojui, pagal kurią paslaugos teikėjas patikrina į jį besikreipiančiojo tapatybę. Iš sąvokų matyti, kad elektroninėje erdvėje tapatybė sutapatinama su prisijungimo vardu ir slaptažodžiu ir visos saugumo užtikrinimo priemonės, pavyzdžiui, skaitmeniniai sertifikatai ir kt., iš esmės atitinka asmens tapatybę elektroninėje erdvėje[52].

Elektroninė erdvė – tai ne kas kita, kaip mūsų visuomenės atspindys; tai puiki terpė ne tik teisėtiems tikslams siekti, bet ir pavojingoms, priešingoms teisės normų veikoms atlikti bei jas atliekančių subjektų išradingumui parodyti: efektyvūs veiksmai (informacijos siuntimas, gavimas, saugojimas, apdorojimas – visi veiksmai, atliekami elektroninėje terpėje (įskaitant per atstumą), naudojantis informacinėmis technologijomis pačiais įvairiausiais, paprastam elektroninės erdvės naudotojui dažniausiai ne visada suprantamais ir (ar) pastebimais būdais.

Naudojantis elektroninėmis paslaugomis, vienas iš didžiausių pavojų, su kuriuo dažnai susiduria vartotojai, yra tapatybės vagystė elektroninėje erdvėje. Tapatybės vagystės elektroninėje erdvėje plitimą skatina vis didesnis elektroninių tapatybių naudojimo mastas[53]. Pastaruoju metu tai tampa vis didesne problema, su kuria elektroninėje erdvėje susiduria šiuolaikinė informacinė visuomenė. Tai pažymima ir 2010 m. Europos

[51] Online Identity Theft [interaktyvus]. OECD, 2009 [žiūrėta 2011-09-14], p. 15. <http://browse.oecdbookshop.org/oecd/pdfs/browseit/9309021E.PDF >.

[52] Štitilis, D.; Laurinaitis, M. 2009. Tapatybės vagystė elektroninėje erdvėje, *Informacijos mokslai* 50: 241.

[53] Rannenberg, K.; Royer, D.; Deuker, A. 2009. *The Future of Identity in the Information Society*. Springer-Verlag, p. 316.

skaitmeninėje darbotvarkėje, kur nurodyta, kad dėl tapatybės vagysčių ir sukčiavimo internete kyla vis daugiau problemų[54].

Šis socialinis teisinis reiškinys sparčiai plinta ir bent jau kol kas atrodo sunkiai sustabdomas: tiesiog stulbinamai daugėja nukentėjusiųjų nuo tapatybės vagystės skaičius, jos sukeliama žala, 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 tobulėjančios 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 gana saugioje aplinkoje, nukreipti savo veiksmus bet kuria linkme ir į bet kurią vietą. Taip pat sudaromos puikios sąlygos pažeidėjams išlikti anonimiškiems, per trumpesnį laiką padaryti gerokai daugiau žalos didesniam vartotojų skaičiui, nei veikiant fizinėje erdvėje. Be to, vienu metu galima atlikti keletą neteisėtų ir pavojingų veikų, o tokių veikų subjektas gali būti bet kas – netgi asmenys, nesulaukę reikiamo amžiaus, kad pagal teisės aktus galėtų kiltų atsakomybė. 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 tobulinti. Dėl veikų, įvykdomų elektroninėje erdvėje, globalaus pobūdžio, slaptumo ir savitumo, valstybės yra bejėgės kovoti su šiuo reiškiniu būdamos izoliuotos vienos nuo kitų, todėl vien tik nacionalinio mechanizmo, siekiant užkirsti kelią tokioms veikoms, nepakanka. Tačiau dėl minėtų priežasčių ir skirtingo veikų pobūdžio 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.

[54] *Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui „Europos skaitmeninė darbotvarkė“ KOM.* (2010) 245 galutinis [interaktyvus, žiūrėta 2011-09-14], p. 17. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:LT:PDF>.

Globalus elektroninės erdvės pobūdis ir specifinės jos savybės sudaro prielaidas pažeidėjams veikti gana saugioje aplinkoje, veiksmus nukreipti 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 veiksmingiau 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 ką galima asmenį patraukti baudžiamojon atsakomybėn. O kitos valstybės laikosi nuomonės, kad tokios veikos yra specifinės, todėl tapatybės vagystės kriminalizavimas yra naudinga priemonė siekiant užkirsti kelią tapatybės vagystės keliamoms grėsmėms. Dažnai teisinio reguliavimo, kaip ir tapatybės vagystės elektroninėje erdvėje, nespėjama adaptuoti naujų technologijų keliamiems iššūkiams, ir tai yra viena iš didžiausių problemų.

Tapatybės vagystė – viena iš pavojingiausių veikų, kurios gali būti atliekamos elektroninėje erdvėje, nes jų pavojingumas dažnai yra kur kas didesnis nei analogiškų veikų fizinėje erdvėje. Tapatybės vagystė tapo vienu iš pelningiausių nusikaltimų iš visų nusikaltimų rūšių[55]. Didžiausia problema, siekiant efektyviai kovoti su šia veika, yra ta, kad didžiuliu greičiu didėjant šio socialinio teisinio reiškinio mastams, vis dar vyksta diskusijos, kas turėtų būti vadinama tapatybės vagyste, ir ar ši veika turėtų būti kriminalizuota. Sąvokos, apibrėžimai, dažniausiai naudojami statistiniais tikslais, skirtingose valstybėse skiriasi, be to, daugeliu atvejų terminai „tapatybės vagystė“ ir „tapatybės klastotė“ vartojamos kaip sinonimai. Todėl pirmiausia valstybės, siekdamos efektyviai kovoti su neigiamų padarinių visuomenei turinčiais reiškiniais, turėtų juos tiksliai įvardyti ir visapusiškai įvertinti, o po to sukurti veiksmų planą ir plėtoti tarptautinį bendradarbiavimą.

Pažymėtina, kad pirmieji tapatybės vagystės atvejai buvo žinomi dar gerokai anksčiau, nei atsirado internetas. Paprastai tradicinė tapatybės vagystė buvo – ir vis dar yra – atliekama taikant tokius metodus kaip „šiukšlių rinkimas“, mokėjimo kortelės vagystė, dingsties ieškojimas, „žiūrėjimas per petį“, apgaulės būdu duomenų nuskaitymas nuo kortelių arba kompiuterio vagystė. Tačiau per pastaruosius kelerius metus minė-

[55] Higgins, G. E. 2010. *Cybercrime: An Introduction to an Emerging Phenomenon*. McGraw-Hill, p. 67.

tieji metodai gerokai patobulėjo dėl sparčios interneto, informacinių bei ryšio technologijų plėtros, kuri, pavyzdžiui, suteikia galimybę tapatybės vagystės subjektams naudoti duomenų vagystės metodą kenkėjiškų programų[56] ar nepageidaujamų elektroninio pašto žinučių forma.

Pabrėžtina ir tai, kad patys asmenys dažnai nesuvokia, kokie svarbūs ir vertingi yra jų asmens duomenys, ir tokiais duomenimis disponuoja nesilaikydami elementarių saugumo taisyklių. Naujausia Eurobarometro apklausa parodė, kad Lietuvos gyventojai socialiniuose tinkluose drąsiai skelbia savo asmens duomenis ir kitą informaciją. Interneto socialiniais tinklais 2011 m. rugpjūčio mėn. naudojosi 56 proc. lietuvių – tai šiek tiek daugiau nei ES vidurkis. Pavyzdžiui, net pusė socialinių tinklų vartotojų Lietuvoje į internetą deda savo nuotraukas, apie trečdalis skelbia s namų adresą, beveik penktadalis yra nurodę mobiliojo telefono numerį, kas dešimtas viešina ir darbo istoriją. Tapatybės kortelių ir paso numerius internete skelbia 6 proc. lietuvių. Beje, kitose valstybėse paso numeris socialiniuose tinkluose skelbiamas daug dažniau: pavyzdžiui, tai skelbia net 43 proc. švedų ir 37 proc. estų[57].

Asmens duomenys reikalingi kiekviename gyvenimo žingsnyje: savo tapatybę reikia įrodyti norint atidaryti banko sąskaitą, gauti mokėjimo korteles, pajamas, paskolas, įkeisti turtą, gauti prekių ar paslaugų, 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 neturėjo, įvykdymo; gauna pranešimą apie išnaudotą kredito limitą; susiduria su nesėkmėmis ieškodamas darbo, norėdamas išsinuomoti būstą,

[56] Kenkėjiška programa monografijoje 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.).

[57] Žurnalas „Veidas“, 2011-08-08, p. 7.

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, kad tai yra visuomenei itin pavojinga veika, kuri gali būti įvairi – 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, kita 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 pavyzdžiai gali būti asmens reputacijos sumenkinimas, duomenų apie teistumą įrašymas asmens byloje ir pan.

Literatūroje nurodoma, kad tapatybės vagystė sudaro galimybę atlikti kitus nusikaltimus, tokius kaip prieiga prie socialinio draudimo informacijos, naujų kredito kortelių ar paskolų kito asmens vardu gavimas ir kt. Dažniausiai tapatybės vagystė būna susijusi su kreditinės kortelės panaudojimu ar piktnaudžiavimu socialinio draudimo informacija[58].

Pabrėžtina ir dar viena esminė problema – **latentiškumas**. Būtent 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 neparodo visų tapatybės vagysčių atvejų, nes dažniausiai apie juos net nesužinoma. Tokį šių veikų latentiškumą lemia kelios svarbiausios 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 latentiš-

[58] Higgins, G. E. 2010. *Cybercrime: An Introduction to an Emerging Phenomenon*. McGraw-Hill, p. 68.

kumas), nes nenori atskleisti informacijos apie savo darbą, bijodamos viešumo arba prarasti gerą vardą, investuotojus, visuomenės pasitikėjimą (pvz., bankai);
– trečia, aukos gali nepranešti dėl įsitikinimo, kad teisėsaugos institucijos tokios veikos atveju paprasčiausiai yra bejėgės.

Latentiškumo priežasčių gali būti ir kitų, pavyzdžiui, organizacijoje nėra saugumo politikos[59] ir neaišku, kokią veiką elektroninėje erdvėje laikyti tapatybės vagyste; tapatybės vagystė dažnai aptinkama po ilgo laiko.

Autorių atlikti kiekybiniai ir kokybiniai tyrimai patvirtina, kad prielaidų Lietuvoje tapatybės vagystės elektroninėje erdvėje latentiškumui yra. Pavyzdžiui, atlikus vartotojų apklausą, 27 proc. respondentų teigė, kad iki tyrimo apie tapatybės vagystę elektroninėje erdvėje šie vartotojai iš viso nieko nežinojo. Autorių nuomone, jei vartotojas net nėra girdėjęs apie tapatybės vagystę elektroninėje erdvėje, kyla didelė rizika, kad jis gali nė nepastebėti šio pavojingo reiškinio arba nesugebėti jo įvertinti. Be to, net 46 proc. vartotojų mano, kad tapatybės vagystė elektroninėje erdvėje nėra paplitusi Lietuvoje. Tuo tarpu publikacijos spaudoje, atliekami tyrimai liudija, kad toks reiškinys Lietuvoje nėra retas. Dar viena iš latentiškumo prielaidų – pagal autorių atliktą tapatybės vagystės elektroninėje erdvėje apklausą, net 35,4 proc. apklaustų vartotojų nežino, kur kreiptis įvykus tapatybės vagystei elektroninėje erdvėje. Jei vartotojas nežino, kur kreiptis pažeidimo atveju, tokia veika į oficialią statistiką gali būti neįtraukta. Taip pat, įvertinus ekspertų apklausos rezultatus, paminėtina, kad 2-as ekspertas teigė, jog tapatybės vagystės paplitimas priklauso nuo identifikavimo taikymo elektroninėje erdvėje. Kadangi identifikavimo atvejai elektroninėje erdvėje Lietuvoje plačiai paplitę, tapatybės vagystės atvejų taip pat turėtų būti nemažai, nors oficiali statistika to nerodo[60]. Trys ekspertai – 4-as, 5-as ir 7-as – taip pat paminėjo, kad tikruosius šio reiškinio mastus dėl latentiškumo yra sunku nustatyti. Detalesni autorių atliktų tyrimų rezultatai pateikiami monografijos 5.2.6 dalyje.

Atsižvelgiant į tapatybės vagystės elektroninėje erdvėje prielaidas ir priežastis, autorių nuomone, Lietuvoje, kaip ir visame pasaulyje, gali būti nežinoma tikroji padėtis, susijusi su šiuo pavojingu reiškiniu. Todėl ne-

[59] Ghosh, S. ; Turrini, E. 2010. *Cybercrimes: A Multidisciplinary Analysis*. Springer-Verlag, p. 121.

[60] Kol kas dėl tapatybės vagystės elektroninėje erdvėje statistikos nėra iš viso.

mažos dalies neteisėtų / pavojingų veikų gali nebūti oficialiojoje statistikoje ir reiškinio pavojingumo vertinimas dėl to gali būti per žemas. Tokia situacija, kai neįvertinama pavojingos veikos grėsmė, gali daryti neigiamą įtaką kovai su šiuo pavojingu reiškiniu. Todėl, autorių nuomone, tapatybės vagystei elektroninėje erdvėje ir kovai su šiuo reiškiniu reikėtų skirti daugiau dėmesio, ypač Lietuvoje. Be to, tapatybės vagystės elektroninėje erdvėje latentiškumo mažinimas, autorių nuomone, turėtų būti vienas iš prioritetų kovojant su šiuo pavojingu reiškiniu. Tai padėtų įvertinti tikrąją būklę ir planuoti reikiamas prevencijos priemones. Dėl latentiškumo mažinimo pasisako ir autorių apklaustas 5-as ekspertas.

Tapatybės vagystės elektroninėje erdvėje pavojingumą patvirtino autorių atlikta šios srities ekspertų apklausa. Ekspertai vieningai teigė, kad reiškinys pavojingas. Detalesnė informacija pateikiama šios monografijos 5.2.6 dalyje.

Tapatybės vagystės elektroninėje erdvėje pavojingumą liudija įvykiai praktikoje. Paminėtinas Lietuvoje įvykęs incidentas: 2009 m. spalio 13 d. visuomenės informavimo priemonėse mirgėjo antraštės, kad 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 nedelsdami 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[61].

[61] Lietuvos bankai masiškai blokuoja mokėjimo korteles dėl galimos duomenų vagystės. *Lietuvos rytas* [interaktyvus]. Vilnius, 2009-10-13 [žiūrėta 2011-09-14]. <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>.

Dėl galimos duomenų vagystės bankai blokuoja korteles. *15 min* [interaktyvus]. 2009-10-13 [žiūrėta 2011-09-14]. <http://www.15min.lt/naujiena/aktualu/pinigai/58/59976/>.

Bankų atstovai dar kartą priminė, kad siekiant visiško duomenų saugumo mokėjimo kortele turi naudotis tik tas asmuo, kurio vardu ji išduota, ir PIN[62] kodas turi būti žinomas tik pačiam klientui (t. y. mokėjimo kortelės PIN kodą reikia saugoti atskirai nuo mokėjimo kortelės, ant mokėjimo kortelės ar 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 turi būti dėmesingi naudodamiesi mokėjimo kortele, ypač atsiskaitydami nežinomoje ar neįprastoje vietoje – užsienyje, internetu ar telefonu, o būdami užsienyje turėtų naudotis tik patikimų ir žinomų bankų bankomatais, pavyzdžiui, įrengtais bankų padaliniuose – tokiu atveju, kilus neaiškumams besinaudojant bankomatu, iš karto yra galimybė kreiptis į banko padalinio darbuotoją pagalbos.

Prieštaringų visuomenės, politikų ir teisėsaugos institucijų vertinimų susilaukė ir dar vienas precedento Lietuvoje kol kas neturintis incidentas: 2010 m. sausio 19 d. paaiškėjo, kad už Seime nesantį kolegą Liną Karalių posėdžio metu net keturis kartus balsavo naujasis „Vienos Lietuvos“ frakcijos seniūnas Aleksandras Sacharukas, kuris vėliau tikino, kad tai darė tik norėdamas įsitikinti, ar įmanoma iš kitos vietos balsuoti už nesantį kolegą. Seimo sudaryta laikinoji Specialioji tyrimo komisija dėl Seimo narių pateiktų siūlymų pradėti apkaltos procesą Seimo nariui Aleksandrui Sacharukui (toliau – Specialioji tyrimo komisija) 2010 m. gegužės 13 d. nutarė, kad A. Sacharukas gali būti vertas apkaltos dėl to, kad galėjo nesilaikyti Konstitucijos ir sulaužyti Seimo nario priesaiką, kai sausio mėnesį sąmoningai daug kartų balsavo už frakcijos kolegą L. Karalių (sausio 14 ir 19 d. plenariniuose posėdžiuose už L. Karalių jo kortele balsavo 11 kartų). Panašus sprendimas priimtas ir dėl Lino Karaliaus. Tyrimo metu paaiškėjo, jog politikas A. Sacharukas daug kartų sąmoningai balsavo už L. Karalių, melavo nežinojęs apie balsavimo sistemos veikimą (aiškino, kad vienais atvejais supainiojo savo ir kolegos kortelę, kitais – kad už L. Karalių iš savo darbo vietos balsavo norėdamas įsitikinti, ar apskritai egzistuoja tokia techninė galimybė, nes esą anksčiau buvo informuotas, kad tai nėra įmanoma; Komisija nustatė, kad nuo 2009 m. rugsėjo mėn. iki 2010 m. sausio mėn. A. Sacharukas už save ne

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

iš savo darbo vietos balsavo 55 kartus, vadinasi, negalėjo nežinoti, kad Seimo narys tikrai gali išreikšti valią aktyvaveęs balsavimo kortelę ne savo darbo vietoje), klastojo dokumentus, galbūt neteisėtai įgijo, laikė ir naudojo kolegai priklausiusį dokumentą. Už dokumentų ir balsavimo klastojimą parlamentaras gali būti traukiamas baudžiamojon atsakomybėn, todėl apkaltos komisija dėl to nutarė kreiptis į Generalinę prokuratūrą. 2010 m. gegužės 14 d. Seimo specialioji tyrimo komisija kreipėsi į Generalinę prokuratūrą dėl galimo Seimo nario A. Sacharuko veiksmų tyrimo pagal Baudžiamojo kodekso 300 (numato baudžiamąją atsakomybę už dokumento suklastojimą ar disponavimą suklastotu dokumentu) ir 302 (numato baudžiamąją atsakomybę už antspaudo, spaudo ar dokumento pagrobimą arba pagrobtojo panaudojimą) straipsniuose numatytas nusikalstamas veikas. 2010 m. gegužės 25 d. Seimas nutarė kreiptis į Konstitucinį Teismą dėl apkaltų opozicinės Krikščionių partijos frakcijos nariams A. Sacharukui ir L. Karaliui pagrįstumo, prašydamas išvados, ar konkretūs A. Sacharuko ir L. Karaliaus veiksmai, nurodyti Seimo specialiųjų tyrimų komisijų medžiagose, prieštarauja Lietuvos Konstitucijai, ir Konstitucinis Teismas 2010 m. rugsėjo 29 d. pradėjo nagrinėti parlamento kreipimąsi dėl apkaltų Seimo Krikščionių partijos frakcijos nariams A. Sacharukui ir L. Karaliui[63]. 2010 m. spalio 27 d. Konstitucinis Teismas konstatavo, kad Seimo nariai A. Sacharukas ir L. Karalius šiurkščiai pažeidė Konstituciją ir sulaužė priesaiką. Slapto balsavimo Seime metu buvo nuspręsta pašalinti iš parlamento opozicinės Krikščionių partijos frakcijos narį L. Karalių, o A. Sacharukas mandatą Seime išsaugojo[64].

Be to, 2010 m. sausio 28 d. JAV ir Lietuvoje paskelbta, kad lietuviai tuštino JAV bankus neiškeldami kojos iš namų: įsilaužę į JAV gyventojų sąskaitas du broliai iš Vilkaviškio rajono su dar keliais bendrininkais per pusmetį į draugų sąskaitas Lietuvos bankuose sugebėjo pervesti daugiau

[63] Oficialus Lietuvos Respublikos Seimo tinklalapis [interaktyvus, žiūrėta 2011-09-14]. <http://www3.lrs.lt/pls/inter/w5_show?p_r=618&p_k=1&p_d=98673>. <http://www3.lrs.lt/pls/inter/w5_show?p_r=618&p_d=98800&p_k=1>.

Oficialus Lietuvos Respublikos Konstitucinio Teismo tinklalapis [interaktyvus, žiūrėta 2011-09-14].<http://www.lrkt.lt/Pranesimai/txt_2010/L20100929c.htm>.

[64] A. Sacharukas išsaugojo Seimo nario mandatą, L.Karalius neteko. *Lietuvos rytas* [interaktyvus]. 2010-11-11 [žiūrėta 2011-09-14]. <http://www.lrytas.lt/-12894613511288584418-a-sacharukas-i%C5%A1saugojo-seimo-nario-mandat%C4%85-l-karalius-neteko-nuotraukos-3-video.htm>.

kaip 400 tūkst. dolerių, apie 2 mln. dolerių grupuotės nariai pervedė į įvairių neapmokestinamų kompanijų sąskaitas Latvijos bankuose. Aferistai planavo pagrobti dar apie 5 mln. dolerių, tačiau jų planus sužlugdė Finansinių nusikaltimų tyrimo tarnybos ir Marijampolės apylinkės prokuratūros pareigūnų operacija. Pirmieji sukčių bandymai 2008 m. nebuvo sėkmingi, nes JAV bankai blokavo pervedimus į Lietuvą, tačiau sukčiai sugalvojo naują būdą: naudodamiesi kompiuteriais kitame JAV banke savo aukos vardu atidarydavo naują sąskaitą ir į ją pervesdavo pinigus, kurie toliau keliaudavo į Latviją ir Lietuvą; tais atvejais, kai nepavykdavo atidaryti naujos sąskaitos, sukčiai atidarydavo sąskaitas benamių JAV ir Kanados piliečių vardu Kanadoje: tada svetimi pinigai keliaudavo benamiui, o iš ten – į Lietuvą[65].

1.2.2. Tapatybės vagystės elektroninėje erdvėje padariniai

Tapatybės vagystės išteklių centras (angl. *Identity Theft Resource Center*) tapatybės vagystę / klastotę skirsto į penkias kategorijas[66]:

1) Verslo, komercinės tapatybės vagystės (juridinių asmenų klastotės).
2) Kriminalinės tapatybės vagystės (sulaikymo metu sukuriama kita tapatybė).
3) Finansinės tapatybės vagystės (tapatybe pasinaudojama prekėms, paslaugoms gauti).
4) Tapatybės klonavimas (naudojant kitą informaciją, siekiama tapatybe naudotis kiekvieną dieną).
5) Medicininės tapatybės vagystės (siekiant gauti medicininę priežiūrą arba narkotinių ir (ar) psichotropinių medžiagų).

Pavojingiausios ir didžiausią finansinę žalą darančios yra finansinės tapatybės vagystės. Būtent į finansų sektorių nukreiptas didžiausias tapatybės vagystės subjektų dėmesys. Taip pat tapatybės vagystė / klastotė dažniausiai naudojama siekiant palengvinti nusikaltimų, tokių kaip nelegali imigracija, terorizmas, šnipinėjimas, šantažas, finansiniai nusikaltimai, įvykdymą. Dėl minėtų veikų grėsmę patiria tiek privatus sektorius, tiek valstybės saugumo ir finansinių interesų užtikrinimo institucijos. Kalbant

[65] Lietuviai tuštino JAV bankus neiškeldami kojos iš namų. *Lietuvos rytas* [interaktyvus]. 2010-01-28 [žiūrėta 2011-09-14]. <http://m.lrytas.lt/?data=20100128&id=akt28_a4100128&view=2>.

[66] Identity Theft Resource Center [interaktyvus, žiūrėta 2011-09-14]. <http://www.idtheftcenter.org/>.

apie pavojingumą ir mastą, ne visais atvejais motyvas yra finansinės priežastys, tai gali būti asmens persekiojimas, troškimas apsimesti kitu asmeniu. Tačiau jau vien tapatybės klastojimas pats savaime yra nusikalstama veika. Nusikaltimas gali prasidėti suklastojus tapatybę, kuri tampa būsimų nusikaltimų pradžia. Tapatybės vagystė / klastotė neapsiriboja tik apsimetimu kitu asmeniu. Ji apima ir melagingos dokumentacijos naudojimą, apgaulingą neegzistuojantį ryšį su teisėtomis kompanijomis, neegzistuojančiomis korporacijomis ar pasinaudojimą kitomis organizacijomis.

Taip pat būtina pabrėžti, kad tapatybė fizinėje erdvėje yra visiškai kitokia nei elektroninėje. Fizinėje erdvėje tapatybė nustatoma pagal dokumentą, kuriame nurodyti asmens duomenys, asmens atvaizdas ir kt. Asmens tapatybės nustatymas skirstomas į kategorijas:

- identifikatorius (vienareikšmiškai nurodo asmenį).
- kitus duomenis.

Fizinėje erdvėje pats asmuo, savo tapatybę gali patvirtinti vienu iš privalomų elementų – asmens dokumentu. O elektroninėje erdvėje dažniausi tapatybės nustatymo būdai yra šie:

- slaptažodžio valdymas vartotojų kompiuteryje.
- tapatybės nustatymas interneto paslaugų *proxy* serveryje.
- tapatybę nustato trečioji šalis (naudojami specialūs protokolai).
- tapatybę nustato šalis, kuri yra viena iš pasitikėjimo grupės narių (pavyzdžiui, Elektroninio deklaravimo sistema (EDS) Lietuvoje, kurios pasitikėjimo šalis – bankas, identifikuojantis vartotoją elektroninėje erdvėje).

Norint tinkamai suprasti pavojingumo mastą ir galimus padarinius, susijusius su tapatybės vagyste, reikia suvokti tapatybės nustatymo metodologiją elektroninėje erdvėje, nes būtent ji ir sudaro galimybę klastoti tapatybę.

Su tapatybės vagyste susiję asmenys nuolat reaguoja į besikeičiančią aplinką ir sugalvoja vis naujų būdų pasipriešinti visiems, bandantiems šį reiškinį paveikti. Daugelis bando sustabdyti šią grėsmę, bet jų veiksmai kol kas yra mažai veiksmingi. Per pastaruosius 35 metus tapatybės vagysčių skaičius išaugo, pasikeitė jos įvykdymo būdai ir pasireiškimo formos, o pati tapatybės vagystė tapo sparčiausiai plintanti elektroninių nusikaltimų rūšis visame pasaulyje. Prieš kelerius metus „CBS News“ pranešė, kad kieno nors tapatybė būna pavagiama kas 79 sekundes. Federalinės JAV prekybos komisijos (toliau – FPK) atlikta apklausa 2006 m. parodė,

kad 8,3 milijono suaugusių amerikiečių tapo tapatybės vagystės aukomis. Tyrimo metu buvo apskaičiuota, kad tapatybės vagystės nuostoliai iš viso siekė 1,56 milijardo JAV dolerių. Nors nuostoliai, lyginant su ankstesniais tyrimais, gerokai sumažėjo (panašūs FPK tyrimai atlikti 2003 m.; tada bendra nuostolių suma buvo 4,76 milijardo JAV dolerių), tapatybės vagystės didėjimo tempai stulbinantys. Pagal 2008 metų FPK atliktą tyrimą, 2008 metais tapatybės vagystės aukomis tapo jau 10 mln. amerikiečių[67], o 2009 metais šis skaičius padidėjo iki 11,1 mln. asmenų[68].

Žurnalas „Kiplinger's asmeniniai finansai" 1995 m. pranešė, kad ataskaitų apie kreditines operacijas biuras „Experian" kiekvieną dieną gaudavo 600–700 tapatybės vagystės skundų. „MasterCard International" pranešė, kad tapatybės vagystės sudarė 96 % valstybių narių bankų sukčiavimo nuostolių 1997 m. tapatybės vagystės nuostoliai padidėjo nuo 450 milijonų 1996 m. iki daugiau nei 2 mlrd. JAV dolerių 1999 m. Pasak FPK, nesąžiningas naudojimasis kreditinėmis kortelėmis sudarė 50 % visų tapatybės vagystės skundų 2000 m. Tapatybės vagystės skundai, susiję su socialiniu piktnaudžiavimu, asmens identifikavimo numeriais, šoktelėjo nuo 27 tūkstančių 1998 m. Iki 73 tūkstančių 2002 m. JAV Socialinės apsaugos administracija pranešė apie daugiau nei 500 tokių incidentų. 2005 m. ir 2007 m. pirmąjį pusmetį buvo pasisavinta daugiau nei 155 milijonai asmenų įrašų. Duomenys pasisavinti iš nešiojamųjų kompiuterių, pasinaudojant vartotojų nerūpestingumu ir duomenų apsaugos principų nepaisymu. Tapatybės vagystės turėjo įtakos įstaigų veiklai, ligoninėms, finansines paslaugas teikiančioms įmonėms ir kt.

Kaip viena iš stambiausių tapatybės vagysčių JAV istorijoje įvardijamas precedentas, kai Philip Cummings, dirbantis firmai, tiekiančiai programinę įrangą finansinėms institucijoms ir bankams, neteisėtai prisijungdavo ir pasisavindavo finansinę ir kreditinę informaciją apie konkrečius asmenis. Šią informaciją minėtasis asmuo pardavinėdavo nusikaltėliams iš Nigerijos, kurie savo ruožtu, pasinaudodami pagrobta asmenine informacija, iš aukų pasisavindavo finansines lėšas. Iš viso aukų

[67] Kshetri, N. 2010. *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives*. Springer-Verlag, p. 5.

[68] Javelin Study Finds Identity Fraud Reached New High in 2009, but Consumers are Fighting Back [interaktyvus, žiūrėta 2011-09-14]. <http://www.prnewswire.com/news-releases/javelin-study-finds-identity-fraud-reached-new-high-in-2009-but-consumers-are-fighting-back-83987287.html>.

skaičius viršijo 30 000 JAV, Kanadoje ir kitose valstybėse, o žala –milijonus JAV dolerių.

Tapatybės vagystė kaip finansiškai naudinga sulaukia didelio nusikaltėlių dėmesio visame pasaulyje[69]. Akivaizdu, kad anksčiau ar vėliau pasaulinio lygio ekonominius nusikaltimus vykdančios organizuotos grupės nusitaikys į šią silpnai apsaugotą nusikaltimų nišą. Nors tapatybės vagystė per pastaruosius 30 metų stipriausiai paveikė JAV, tačiau šiuo metu nusikaltėliai visame pasaulyje telkia dėmesį į tapatybės vagystę ir su ją susijusius nusikaltimus. Per pastaruosius kelerius metus JAV teisėsaugos institucijos pastebėjo didėjantį užsienio organizuotų nusikalstamų grupuočių, pasitelkiančių nusikaltimams atlikti kompiuterius, internetą ir draudžiamas kompiuterines programas, aktyvumą.

Azijoje ir Rytų Europoje organizuoto nusikalstamumo grupės taiko sudėtingesnius tapatybės vagystės metodus, naudoja sudėtingas programas, kurios registruoja kiekvieną klavišo paspaudimą, kai interneto vartotojas prisijungia savo kompiuteryje prie banko sąskaitos interneto svetainėje. Jos taip pat siekia suklaidinti interneto vartotojus, bandydamos atskleisti asmens duomenis naudodamos šnipinėjimo programas (programinė įranga, kuri slaptai renka vartotojo informaciją ir ją perduoda per vartotojo interneto ryšį be vartotojo žinios), „zombius“, kompiuterinius „kirminus“ bei stengiasi perimti duomenų kontrolę kitais tikslais, platina elektroninio pašto šiukšles, vykdo išpuolius kituose kompiuteriuose[70].

Beveik kiekvienoje pasaulio šalyje pastebimas tapatybės vagystės aktyvumo didėjimas. Tos šalys, kurios iki šiol neturėjo tokios patirties, susiduria su nauja problema. Deja, daugelis valstybių nesimoko iš kitų valstybių, neanalizuoja JAV patirties, nesigilina, kaip ši nauja nusikalstamumo rūšis didėjo ir plito.

Tapatybės vagystės elektroninėje erdvėje padariniai Australijoje

Tapatybės nusikaltimas – taip tapatybės vagystė vadinama Australijoje. Tai viena iš svarbiausių problemų šiuo metu, o prognozuojamos nusikalstamumo tendencijos šioje šalyje kalba apie naują nusikaltimo rūšį. Kaip ir daugelyje kitų šalių, Australijoje yra daug nuo tapatybės vagysčių

[69] *No Ordinary Case of Identity Theft*. 2004 [interaktyvus]. October 18, [žiūrėta 2011-09-14]. <http://www.fbi.gov/news/stories/2004/october/uncoveridt_101504>.

[70] *The President's Identity Theft Task Force, Combating Identity Theft: A Strategic Plan.* [interaktyvus] April 2007, 13. [žiūrėta 2011-09-14]. <www.idtheft.gov/reports/StrategicPlan.pdf>.

nukentėjusių asmenų ir tokių incidentų toliau tik daugės[71]. Tapatybės vagysčių skaičius didėjo kelerius metus iš eilės ir dabar tai yra pagrindinė daugelio organizuoto nusikalstamumo grupių veikla. Nors ir dedamos pastangos siekiant užkirsti kelią tapatybės vagystėms ir sumažinti jų skaičių, organizuoto nusikalstamumo grupės ir toliau sėkmingai tęsia nusikalstamą veiklą. 2004 m. Naujojo Pietų Velso Parlamentas patvirtino ataskaitą, kurioje nurodė, kad tapatybės vagysčių nuostoliai Australijoje siekė 3,5 milijardo dolerių. Kita statistika rodo, kad kasmetiniai tapatybės vagystės nuostoliai svyruoja tarp 1,1 ir 3,5 milijardo dolerių[72]. 2006 m. atlikus tyrimą paaiškėjo, kad 8 % apklaustų respondentų nurodė, jog jie buvo tapę tapatybės vagystės nusikaltimų aukomis[73].

Tapatybės vagystės elektroninėje erdvėje padariniai Japonijoje

Japonijoje paplitę duomenų pažeidimai, susiję su asmenine informacija, įskaitant konfidencialią finansinę informaciją ir asmenų sveikatos duomenis. Japonijos verslo lyderiai paprastai perima patirtį iš Vakarų partnerių, paplitę vieši atsiprašymai, skirti visiems klientams, kurie tapo tapatybės vagysčių aukomis. Tai daroma tiek raštu, tiek per spaudos konferencijas. Nors Japonijos kultūra išskirtinė, atsiprašymų procesas negali sustabdyti tapatybės vagystės didėjimo. Japonijoje visuomenė labai pritaria naujoms elektroninėms finansinėms paslaugoms, tačiau būtent šios paslaugos ir sukelia tapatybės vagystės problemas[74]. 2000 m. nusikaltėlių taikomi metodai vogti kredito kortelių duomenis leido pasisavinti apie 80 tūkst. klientų finansinių paslaugų duomenų. Kadangi vis daugiau vartotojų ir įmonių naudojasi tokiomis elektroninių atsiskaitymų paslaugomis, tapatybės vagysčių skaičius ir toliau didės. Japonijoje tapatybės vagys kėsinasi ir į juridinių asmenų tapatybes. Organizuoto nusikalstamumo grupės nariai melagingai teigė, kad jie buvo susiję su Japonijos NEC korporacija, dešimtys bendrovių iš Kinijos ir Taivano gamino produktus pagal fiktyvios NEC korporacijos užsakymus, naudodami jiems nepriklausantį prekės ženklą. Nusikaltėliai pasisavino NEC korporacijos vardą

[71] Biegelman, M. T. 2009. *Identity Theft Handbook – Detection, Prevention, and Security*.

[72] *Ibid*.

[73] *Ibid*.

[74] Blass, E. NEC falls victim to sophisticated "corporate identity theft" [interaktyvus]. 2006-04-27 [žiūrėta 2011-09-14]. <http://www.engadget.com/2006/04/27/nec-falls-victim-to-sophisticated-corporate-identity-theft/>.

ir galėjo išnaudoti jo teikiamus pranašumus. Tokia schema veikė beveik dvejus metus. NEC korporacija sužinojo apie tokį sukčiavimo metodą, bendrovė vėliau atliko savo tyrimą pasitelkdama privačius tyrėjus. Tyrimo metu buvo suimti šio nusikaltimo organizatoriai. Japonija tobulina standartus ir imasi apsaugos priemonių, skirtų asmeninei informacijai apsaugoti finansų, medicinos, telekomunikacijų srityse. Priimtos priemonės užtikrina galimybę plačiai naudotis asmens duomenimis, ypač skaitmenine forma. Iš daugelio reikalavimų vienas svarbiausių – įmonės privalo užtikrinti, kad duomenys būtų apsaugoti nuo praradimo, neleistino naudojimo ir atskleidimo.

Tapatybės vagystės elektroninėje erdvėje padariniai Jungtinėje Karalystėje

Manoma, kad tapatybės vagystės žala kiekvienais metais siekia 3,4 milijardo dolerių. 2007 m. tapatybės vagystė buvo pavadinta vienu iš sparčiausiai plintančių nusikaltimų šalyje. 2008 m. tapatybės vagystės sąrašus papildė vagystės iš mobiliųjų telefonų. Nors tapatybės vagystės yra seniai teisiškai apibrėžtos Jungtinėse Amerikos Valstijose, tai yra santykinai naujas reiškinys Jungtinėje Karalystėje[75]. Daugelis piliečių nežino, kaip geriausiai apsisaugoti nuo tapatybės vagystės ar net kaip reaguoti, jei taptų tokio nusikaltimo auka. Atlikto tyrimo metu nustatyta, kad 25 % visuomenės nepraneštų, jei dingtų jų pasai, o 80 % nežinojo, ką daryti, jeigu prarastų savo gimimo liudijimą. Tapatybės vagys pavogtą informaciją naudoja kredito kortelių sąskaitoms gauti, apeliuojant į paskolas, prekes internetu. Vidutiniškai vienos tapatybės vagystės nuostoliai Jungtinėje Karalystėje siekia 16 tūkstančių dolerių[76]. Sukčiavimo aktas ir 2006 m. priimtas Asmens tapatybės kortelės įstatymas[77] skirti sureguliuoti tapatybės naudojimą Jungtinėje Karalystėje. Vyriausybė taip pat įkūrė Pagrindinį biurą – Tapatybės vagystės iniciatyvinį komitetą, kuris nuolat bendradarbiauja su finansų įstaigomis, vyriausybe.

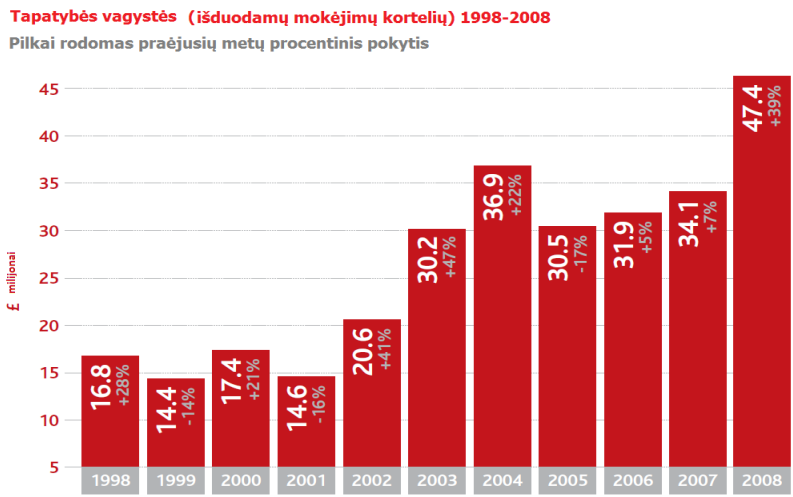
[75] Heath, N. Brits living in fear of identity fraud [interaktyvus]. 2008-05-20 [žiūrėta 2011-09-15]. <http://www.silicon.com/legacy/research/specialreports/fulldisclosure/0,3800014102,39225528,00.htm>.

[76] ID burglary risk ignored [interaktyvus]. 2008-04-22 [žiūrėta 2011-09-15]. <http://www.myfinances.co.uk/savings/news//bank-account-fraud/id-burglary-risk-ignored-$1219804.htm>.

[77] Biegelman, M. T. 2009. *Identity Theft Handbook– Detection, Prevention, and Security*.

2008 m. balandžio mėn. iš bankų buvo pavogta daugiau nei 27 tūkstančiai klientų sąskaitų[78]. Nepaisant padidėjusio visuomenės informavimo apie tapatybės vagystės poveikį, daugelis įmonių neatsižvelgia į šią riziką. Ištirti 56 atvejai parodė, kad 2007 m. buvo pasisavinami klientų duomenys iš finansinių paslaugų įmonių, dar blogiau – sukčiavimo schemos išimtinai buvo nukreiptos į finansines institucijas.

Tapatybės vagystės naudojant mokėjimų korteles 2008 m. atnešė daugiau nei 47 milijonus svarų sterlingų nuostolių (3 pav.). Tapatybės vagystės vykdomos pasisavinant kortelės duomenis – asmeninę informaciją, siekiant perimti kortelės sąskaitą kito asmens vardu. Apskritai tapatybės vagysčių skaičius naudojant korteles 2008 m. padidėjo 39 %, o tai sudaro 8 % visų rūšių sukčiavimų naudojant mokėjimų korteles.

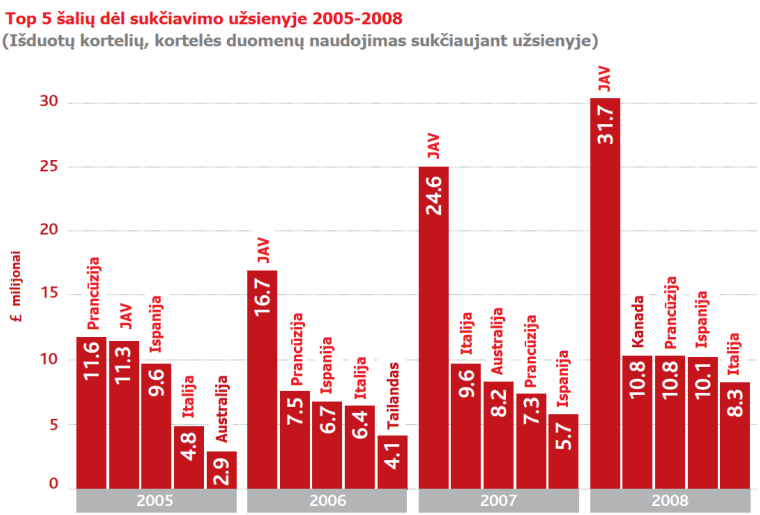


3 pav. Tapatybės vagystės naudojant mokėjimų korteles
(sudaryta remiantis „APACS - the UK payments association in conjunction" ir „The UK Cards Association" duomenimis)

Sėkmingai įgyvendinus PIN kodo reikalavimą Jungtinėje Karalystėje, sukčiai vis dažniau išvyksta į užsienį, kur nėra tokių reikalavimų. Nusikaltėliai pavagia duomenis, esančius magnetinėje juostelėje, padaro

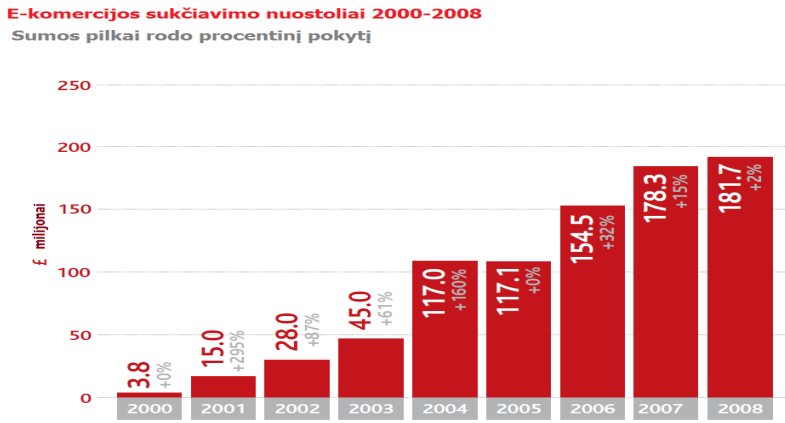
[78] APACS - the UK payments association in conjunction. Fraud The Facts 2009 [interaktyvus, žiūrėta 2011-09-15]. <http://www.eastscotlandfraudforum.org.uk/documents/Fraud%20the%20Facts%202009.pdf>.

netikrą kortelę ir ją realizuoja užsienio šalyse, kurios dar nenustatė PIN kodo reikalavimo. Sukčiavimo užsienyje atvejai, kai naudojami Jungtinėje Karalystėje pavogti kortelių duomenys, sudaro daugiau nei trečdalį (38 proc.) visų kortelių sukčiavimo nuostolių. Šalių, kuriose išduodamų kortelių sąlygos pasikeitė, per pastaruosius ketverius metus sukčiavimo atvejų sumažėjo. Nustatyta, kad Prancūzijoje gerokai sumažėjo sukčiavimų, naudojant Jungtinėje Karalystėje pavogtų kortelių duomenis (4 pav.). Nusikaltėliai orientuojasi į tas valstybes, kuriose PIN kodo reikalavimas vis dar nėra privalomas.



4 pav. Šalys, kuriose realizuojami Jungtinėje Karalystėje pavogtų mokėjimų kortelių duomenys
(sudarytas remiantis „APACS - the UK payments association in conjunction“ ir „The UK Cards Association“ dumenimis)

Tapatybės vagys taip pat išnaudoja e. komerciją. Dėl sukčiavimo kortelėmis internete per 2008 m. padaryta 181,7 milijono svarų sterlingų nuostolių (5 pav.). Dauguma šios rūšies sukčiavimo atvejų susiję su kortelės duomenų naudojimu, taikant tam tikrus apgaulės būdus, pavyzdžiui, įsilaužimą į duomenis, taip pat nepageidaujamais elektroniniais laiškais, telefono skambučiais. Kortelės duomenys vėliau naudojami atliekant apgaulingas finansines operacijas internete.



5 pav. Tapatybės vagystės nuostoliai naudojant elektroninę komerciją
(sudarytas remiantis „APACS - the UK payments association in conjunction" ir „The UK Cards Association" dumenimis)

Tapatybės vagysčių, atliktų naudojantis elektronine bankininkyste, 2008 m. bendra nuostolių suma buvo 52,5 milijono svarų sterlingų, o tai 132 % daugiau nei ankstesniais metais (6 pav.). Šį padidėjimą lėmė tokie veiksniai, kaip vis dažnesnės kenkėjiškų programų atakos, masinis vartotojų skaičius.

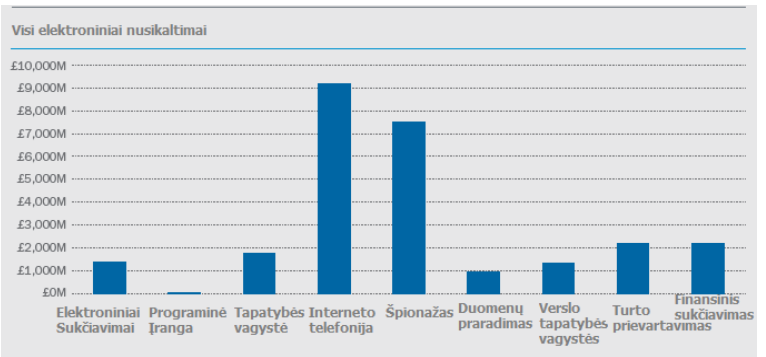
6 pav. Tapatybės vagystės nuostoliai naudojant elektroninę bankininkystę
(sudarytas remiantis „APACS - the UK payments association in conjunction" ir „The UK Cards Association" duomenimis)

Tapatybės vagys daug dėmesio skiria elektroninės bankininkystės paslaugoms klastoti (7 pav.).

Mėnesiai	I	II	III	IV	V	VI	VII	VIII	IX	X	XI	XII	VISO
2008	3,144	3,243	3,848	3,719	3,091	3,637	3,584	3,716	4,121	4,536	3,896	3,456	43,991
2007	1,290	974	1,130	1,188	1,274	1,368	3,066	3,268	2,597	3,170	3,277	3,195	25,797
2006	606	669	1,074	947	919	872	970	1,484	1,513	1,596	1,993	1,513	14,156
2005	18	29	27	54	72	122	153	160	190	267	255	353	1,700

7 pav. Suklastotų elektroninės bankininkystės tinklalapių skaičius JK
(sudarytas remiantis „APACS - the UK payments association in conjunction" ir „The UK Cards Association" duomenimis)

Toliau pateiktoje diagramoje vaizduojami 2010 m. padaryti nuostoliai, susiję su tapatybės vagyste Jungtinėje Karalystėje, lyginant su kitais elektroniniais nusikaltimais (8 pav.).



8 pav. Elektroninių nusikaltimų žala Jungtinės Karalystės ekonomikai
(sudarytas remiantis The Cost of Cybercime, A Detica Report[79])

Tapatybės vagystės elektroninėje erdvėje padariniai Brazilijoje

Sparčiai auganti ekonomika tokiose šalyse, kaip Brazilija, Rusija, Indija ir Kinija, ne tik traukia pasaulio verslo dėmesį, bet ir pritraukia tapatybės vagystes. Brazilijoje elektroniniai nusikaltimai yra dar klastingesni nei Šiaurės Amerikoje. Elektroninis sukčiavimas yra viena iš pagrindinių

[79] The Cost of Cybercime, A Detica Report [interaktyvus]. 2011 [žiūrėta 2011-09-15], p. 3. <http://www.detica.com/uploads/resources/THE_COST_OF_CYBER_CRIME_SUMMARY_FINAL_14_February_2011.pdf>.

problemų, su kuriomis susiduria finansinės institucijos. 2005 m. rugpjūčio mėn. Brazilijos policija suėmė 85 žmones, kurie tariamai pavogė daugiau nei 33 milijonus JAV dolerių iš banko sąskaitų internete, aukoms net neįtariant. 2006 m. vasario mėn. 55 tapatybės vagys buvo suimti už 4,7 milijono JAV dolerių vagystę iš daugiau nei 200 banko sąskaitų, pasinaudojant pavogtais sąskaitos numeriais ir slaptažodžiais, kurie buvo gauti platinant kompiuterinius virusus[80]. Per pirmąjį 2008 m. ketvirtį Brazilijos nacionalinio elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimų padalinys (CERT) pranešė apie 30 tūkstančių įvykdytų elektroninių nusikaltimų. Daugelis organizuotų nusikalstamų grupuočių gauna didelę finansinę naudą iš tapatybės vagysčių internete dėl lengvai prieinamų technologijų, taip pat egzistuoja teisėsaugos personalo atrankos problema.

Tapatybės vagystės elektroninėje erdvėje padariniai Rusijoje

Rusijoje naudojimosi kredito kortelėmis mastas gana didelis. Tapatybės vagystės yra tipiškos sukčiavimo kredito kortelėmis schemos, tačiau jų įvairovė stebina. Tapatybės vagys, naudodamiesi pavogtais asmens duomenimis, atidaro trijų skirtingų kredito linijų sąskaitas, taip pat mobiliųjų telefonų sąskaitas aukos vardu. Manoma, kad dėl tapatybės vagysčių Rusijos bankai praranda daugiau nei 4 milijardus eurų per metus[81]. Taip pat įtariama, kad daugelį tapatybės vagystės schemų organizuoja ir realizuoja bankų tarnautojų grupė. Pasauliniai technologijų ir finansų verslo lyderiai kartu su teisėsaugos institucijomis, orientuotomis į tapatybės vagystes, 2007 m. gruodį Rusiją pripažino viena iš trijų pasaulio šalių, kuriose tapatybės vagysčių išpuolių internete daugiausia. Taip pat Rusija buvo tarp šešių pasaulio valstybių, kuriose tapatybės vagysčių, naudojant kenkėjiškas programas, duomenų rinkimą ir kompiuterinius virusus interneto svetainėse, skaičius buvo didžiausias[82]. Beje, skelbiama, kad sukčiavimo internete atvejų Rusijoje 2011 metais (lyginant su 2010 metų duomenimis) padidėjo net 95,5 proc.[83].

[80] Biegelman, M. T. 2009. *Identity Theft Handbook– Detection, Prevention, and Security*.

[81] *Ibid*.

[82] *Ibid*.

[83] MVD RF soobshhaet o kiberprestupnosti. [interaktyvus}. 2011-07-01 [žiūrėta 2011-09-15]. <http://www.crime-research.ru/news/01.07.2011/7251/>.

Tapatybės vagystės elektroninėje erdvėje padariniai Indijoje

Tapatybės vagystės verslui gali turėti tiek finansinį, tiek socialinį poveikį. Pastaruoju metu paplito viešieji tapatybės sukčiavimai. 2005 m. skambučių centras Pune, Indijoje, dirbdamas pagal JAV banko sutartį, įsivėlė į tapatybės vagystes – buvo vagiami JAV banko klientų sąskaitų duomenys. Skambučių centrai yra sparčiausiai auganti Indijos pramonė. Tyrimai parodė, kad duomenų vagystės ir netinkamas naudojimasis asmenine informacija Indijoje nėra didesnis nei kitose šalyse, įskaitant JAV, bet kyla klausimų dėl duomenų saugumo procedūrų. Akcentuojamas didėjantis tapatybės vagysčių iš Indijos pavojus. Vienos iš Indijos užsakomųjų paslaugų įmonių, dirbusių skambučių centre „Citibank“, darbuotojai buvo kaltinami keturių „Citibank“ klientų tapatybių klastotėmis, pasisavinus klientų socialinės apsaugos numerius, asmens identifikavimo numerius, ir kitus svarbius duomenis, kuriuos naudojant vėliau buvo pavogta pinigų iš sąskaitų. Darbuotojai ir jų bendrininkai pavogė 350 tūkstančių JAV dolerių[84]. Šis epizodas parodė galimą duomenų saugumo spragą, dėl kurios gali daugėti duomenų saugos pažeidimų ir tapatybės vagysčių atvejų. Prie šios problemos prisideda ir darbuotojų kaita, nes besikeičiančius darbuotojus sunku išmokyti dirbti bei stebėti ir atrinkti tinkamus kandidatus[85].

Tapatybės vagystės elektroninėje erdvėje padariniai Kinijoje

Kinijoje yra 220 milijonai interneto vartotojų – ši šalis pirmauja pasaulyje pagal interneto vartojimą. Akivaizdu, kad dalis asmenų naudojasi technologijomis iš blogų paskatų. 2007 m. gruodžio mėn. Kinija buvo pirmoji pasaulyje pagal interneto svetaines, kuriose pasitaikydavo kenksmingas programinis kodas, pagrįstas raktiniais kaupikliais. Taip pat ji buvo antroje vietoje tarp pasaulio šalių, kuriose sukčiavimo būdu apsimetama tikromis svetainėmis. 2008 m. sausio mėn. buvo suimta 18 narių, užsiėmusių interneto tapatybės vagystėmis, grupė, kurios padaryti nuostoliai Kinijoje siekė beveik 13,7 milijono JAV dolerių. Sukčiai naudodavo apgaulingas įmones, kurios teikdavo paskolas be palūkanų ir greitai pa-

[84] Rai, S. Indian outsourcers move to fix security. *The New York Times* [interaktyvus]. 2005-06-17. [žiūrėta 2011-09-15]. <http://www.nytimes.com/2005/06/16/technology/16iht-security.html?_r=1>.

[85] McCue, A. $350,000 Citibank theft victims 'gullible and careless [interaktyvus]. 2005-04-12. [žiūrėta 2011-09-15]. <http://www.silicon.com/legacy/research/specialreports/offshoring/0,3800003026,39129475,00.htm>.

tvirtindavo paskolų išdavimą. Kinijos organizuotos nusikalstamos grupės veikia pasauliniu mastu, palaikydamos ryšį su kitų regionų tapatybės vagystėmis užsiimančiomis grupuotėmis[86].

Kitas svarbus aspektas – tai terorizmas ir tapatybės vagystės. Teroristai taip pat naudoja pavogtas tapatybes ir suklastotus identifikavimo dokumentus. Tapatybės vagystes, naudojami kaip priedangą, įgytas finansines priemones jie skiria teroristinei veiklai finansuoti. Pavogtų tapatybių naudojimas teroristiniais tikslais kelia susirūpinimą, nes po 2001 m. rugsėjo mėn. išpuolių tapatybės vagystė tapo neatsiejama teroristų veikla. Dennis M. Lormel, buvęs Federalinių tyrimų biuro direktorius, finansinio terorizmo vertinimo grupės narys, 2002 m. vykusiame kongrese apie šią grėsmę kalbėjo: „Nerimą kelia tai, kad teroristai užsiima tapatybės vagystėmis – prisidengdami pavogta asmens tapatybe jie tampa anonimiški, o tai padeda atlikti nusikaltimus. Jie naudojasi pašto laiškais, pašto dėžutėmis, butų nuoma, biuro patalpomis, transporto priemonių nuomos, saugojimo paslaugomis, taip pat ryšio ir įvairiomis komunalinėmis paslaugomis. Grėsmė kyla dėl to, kad teroristai jau seniai užsiima tapatybės vagyste, pasisavindami socialinio draudimo numerius, kad galėtų pridengti savo darbą ir prieigą prie saugomų vietų[87]. Šios ir panašios priemonės gali būti panaudotos teroristams siekiant gauti vairuotojų pažymėjimus, banko ir kredito kortelių sąskaitas, per kurias terorizmą finansuoti yra lengviau. Teroristai ir teroristų grupės gauna finansavimą, užtikrinantį veiklos tęstinumą, o tapatybės vagystės tai tik palengvina. Metodai, naudojami terorizmui finansuoti, yra sudėtingi ir faktiškai nėra tokio finansavimo metodo, kuris būtų įmanomas be tapatybės vagystės. Tapatybės vagystė yra pagrindinis katalizatorius, kad teroristinio tinklas sėkmingai veiktų“[88]. Taikydami pavogtas kredito korteles, fiktyvias pardavimo sutartis, sukčiavimą ir daugelį kitų metodų, jie užsitikrina ryšių su Pakistanu, Afganistanu, Libanu ir t. t. palaikymu. Daug suklastotų pasų ir kelionės dokumentų buvo naudojama

[86] Wu Nanlan. Police crack down on Internet identity theft [interaktyvus. 2008-01-11 [žiūrėta 2011-09-15]. <http://www.china.org.cn/english/China/239068.htm>.

[87] Testimony of Dennis Lormel, Chief, Terrorist Financing Operations Section, Counterterrorism Division, FBI Before the Senate Judiciary Committee, Subcommittee on Technology, Terrorism, and Government Information interaktyvus]. 2002 [žiūrėta 2011-09-15]. <http://www.investigativeproject.org/documents/testimony/234.pdf>.

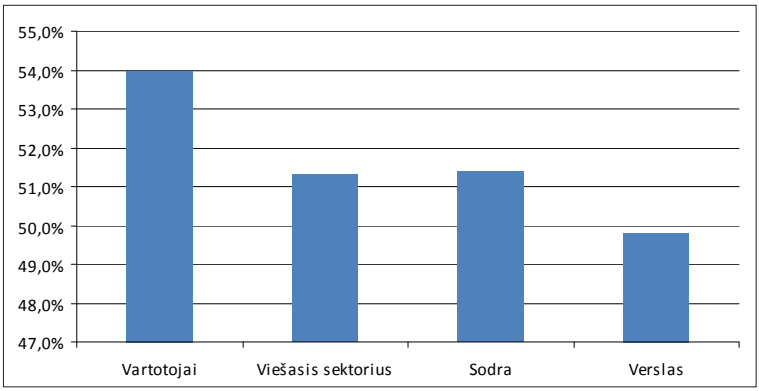
[88] Biegelman, M. T. 2009. *Identity Theft Handbook– Detection, Prevention, and Security.*

banko sąskaitoms atidaryti, siekiant paslėpti pinigų judėjimą iš tokių šalių, kaip Pakistanas ir Afganistanas. Teroristų tinklai akcentuoja tapatybės vagystės svarbą, jie pateikia supaprastintas suklastotos tapatybės naudojimosi instrukcijas, mokymo vadovus, kuriuose galima rasti tikrus skirsnius ir nuorodas į suklastotus dokumentus, asmens tapatybės duomenų vagystes ir kontrolės išvengimo būdus. Be menamo „šventojo karo“, nukreipto prieš kiekvieną, kuris nėra radikalus fanatikas, kur kas pavojingesnis tampa teroristų „ekonominis karas“. Teroristinės organizacijos pasiryžusios bet kokiu įmanomu būdu kenkti finansinei JAV infrastruktūrai. Teroristai siekia perimti technologijas, leidžiančias elektroninėmis informavimo priemonėmis sukurti ekonominę griūtį ir chaosą. Naudojami programišių metodai, siekiant organizuoti tapatybės vagystes, kuriami netikri tinklai. Sėkmingas tokių tinklų darbas, šimtai tūkstančių išpuolių mažina vartotojų pasitikėjimą elektroninės komercijos priemonėmis, o tai atneša milžiniškų ekonominių nuostolių. Šio ekonominio karo strateginis pajėgumas yra problemiškas, tačiau viena aišku – bus panaudotos visos įmanomos priemonės siekiant užsibrėžtų tikslų. Pabrėžiama, kad teroristams kelionės dokumentai yra tokie pat svarbūs kaip ir ginklai: jie leidžia slaptai susitikti, planuoti ir gauti prieigą prie reikiamos informacijos. Kelionės, įvairūs išsisukinėjimo būdai, pakeisti ir padirbti pasai – be tapatybės vagystės tai nebūtų įmanoma.

Be terorizmo grėsmės valstybių ekonominei ir socialinei gerovei, tapatybės vagystės plačiai naudojamos, siekiant nusikalstamu būdu legalizuoti įgytas lėšas – pinigų plovimui. Tapatybės vagystė greitai tapo globalia problema, o prie šio fakto prisidėjo technologijų plėtra. „Baltųjų apykaklių“ nusikaltimai dažnai klaidingai suvokiami, teigiant, kad smurtiniai nusikaltimai su jais nesusiję, tačiau tapatybės vagystės susijusios su narkotikų prekyba, prekyba žmonėmis, pinigų plovimu, netgi žmogžudystėmis. Organizuotų nusikalstamų grupių, veikiančių JAV, sudarytų iš asmenų, atvykusių iš Vakarų Afrikos šalių, pagrindinė veikla susijusi su nelegalia heroino kontrabanda ir platinimu, sukčiavimais, naudojant kredito korteles, mokėjimo schemomis, banko ir kredito kortelių, sąskaitų perėmimu ir pinigų plovimu. Visos minėtos nusikalstamos veiklos rūšys glaudžiai susijusios su tapatybės vagystėmis.

Šiame kontekste svarbu, kaip, autorių atliktais tyrimais, tapatybės vagystę elektroninėje erdvėje vertinama Lietuvos respondentai. Tam tik-

roms respondentų grupėms buvo užduotas klausimas, ar jų manymu, tapatybės vagystė elektroninėje erdvėje yra paplitęs reiškinys. Gautus atsakymus galima pavaizduoti taip:



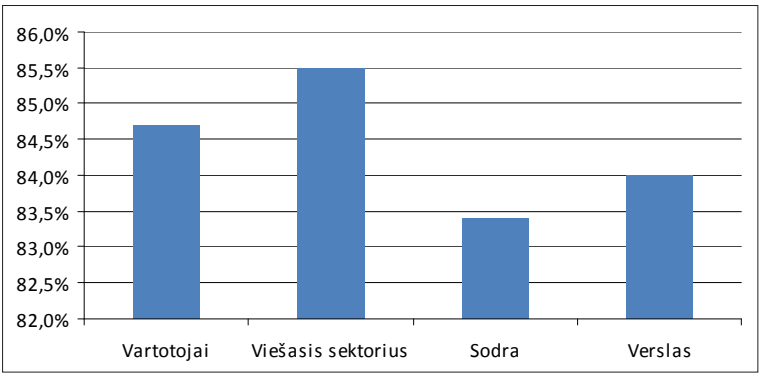
9 pav. Tapatybės vagystės elektroninėje erdvėje paplitimas Lietuvoje

Rezultatai rodo, kad vidutiniškai šiek tiek daugiau nei pusė respondentų mano, kad tapatybės vagystė elektroninėje erdvėje Lietuvoje yra paplitusi.

Ekspertai taip pat vertino tapatybės vagystės elektroninėje erdvėje paplitimą. Atkreiptinas dėmesys, kad nors šio klausimo Lietuvoje nebuvo keliama, vertinant tapatybės vagystės elektroninėje erdvėje paplitimą ekspertų nuomonės pasidalijo taip: 4 ekspertai (1-as, 5-as, 6-as ir 8-as) mano, kad Lietuvoje tai nėra paplitęs reiškinys, 3 ekspertai (2-as, 3-as, 9-as) mano, kad tai santykinai dažnas reiškinys, 2 ekspertai (4-as, 7-as) atsakė, kad tai slapta veika, todėl nėra galimybės jos įvertinti. Paminėtina ekspertų nuomonė, kokį pavojų tapatybės vagystė kelia elektroninėje erdvėje. Dauguma ekspertų neapsiribojo siauru požiūriu, kad pavojus kyla tik konkrečiam asmeniui, kurio duomenys gauti ar panaudoti ne pagal jo norą, bet nurodo ir daugiau neigiamų pasekmių atvejų: pvz.: 1-asis ekspertas labai argumentuotai išdėstė, kad šis reiškinys kenkia verslui, vartotojams ir valstybei, 6-asis ekspertas teigė, kad nukenčia asmuo, kurio duomenys panaudojami, taip pat verslo subjektai ir visuomeninė tvarka, 9-asis ekspertas mano panašiai ir atskleidžia platesnį požiūrį argumentuodamas, kad nukenčia vartotojas ir elektroninės komercijos vykdytojas, panašiai samprotauja ir dalis kitų ekspertų (pvz.: 5-as ekspertas mano, kad nukenčia finansinės institu-

cijos ir piliečiai), kiti ekspertai pavojų apibrėžė kiek siauriau (pvz.: nurodė, kad nukenčia tik asmuo, kurio duomenys pavogti (8-as ekspertas).

Taip pat paminėtini autorių atliktų tyrimų rezultatai apie tapatybės vagystės elektroninėje erdvėje pavojingumą. Atitinkamoms respondentų grupėms buvo užduotas klausimas, ar jų manymu, tapatybės vagystė elektroninėje erdvėje yra pavojingas reiškinys. Gautus atsakymus galima pavaizduoti taip:



10 pav. Tapatybės vagystės elektroninėje erdvėje pavojingumas

Ekspertams buvo užduotas platesnis klausimas: „Kaip vertinate šį reiškinį?“, todėl tiesiogiai lyginti ekspertų atsakymus pavojingumo aspektu būtų netikslu. Tačiau paminėtina, kad visi ekspertai tapatybės vagystę elektroninėje erdvėje vertino neigiamai.

Vertinant tapatybės vagystės elektroninėje erdvėje įtaką veiklai, apskritai viešojo sektoriaus darbuotojų – respondentų nuomonė apie neigiamą šio reiškinio įtaką beveik identiška Sodros darbuotojų apklausos rezultatams: atsakiusiųjų, kad reiškinys apskritai nedaro įtakos, viešojo sektoriaus respondentų buvo 26,3 proc., Sodros darbuotojų – 25,9 proc., manančiųjų, kad daro tiesioginę neigiamą įtaką, bendrai viešojo sektoriaus buvo 39,5 proc., Sodros – 39,9 proc., o manančiųjų, kad daro netiesioginę neigiamą įtaką: viešojo sektoriaus buvo 34,2 proc., o Sodros – 34,2 proc. 32,6 proc. verslo respondentų nemano, kad tapatybės vagystė elektroninėje erdvėje daro neigiamą įtaką jų įmonės veiklai. Manančiųjų, kad reiškinys daro tiesioginę neigiamą įtaką buvo daugiausia – 39,5 proc., o kartu su asmenimis, galvojančiais, kad reiškinys daro netiesioginę įtaką (27,9 proc.)

jų įmonės veiklai, buvo 67,4 proc. Taigi, tiek versle, tiek viešajame sektoriuje manančiųjų, kad tapatybės vagystė elektroninėje erdvėje daro tiesioginę neigiamą įtaką įmonės ar organizacijos veiklai yra beveik 40 proc.

Atsakant į klausimą, kokius padarinius gali sukelti tapatybės vagystė elektroninėje erdvėje jūsų organizacijos veiklai, dažniausias Sodros bei viešojo sektoriaus darbuotojų atsakymas buvo „gali", „duomenų saugumui", o verslo darbuotojai atsakė, kad dažniausiai tai gali turėti finansinių pasekmių (pavyzdžiui, nuostoliai, negautos pajamos). Tai reiškia, kad verslo sektorius neigiamus padarinius labiausiai suvokia kaip finansinius.

Detaliau autorių atliktų atitinkamų tyrimų duomenis žr. monografijos 5.2 dalyje.

1.2.3. Tapatybės vagystės elektroninėje erdvėje padarinių (pasekmių) klasifikacija

Kiekviena klasifikacija reikšminga tuo, kad sudėtingus reiškinius išskaidžius į atskirus elementus, kiekviena reiškinio sudedamoji dalis gali būti nagrinėjama atskirai nuo visumos, be to, klasifikacijos yra vertingos mokymo procese. Atsižvelgiant į tai, kad visos reiškinių klasifikacijos yra santykinės, toliau pateiktas tapatybės vagystės elektroninėje erdvėje padarinių grupavimas parodys ne visus šios pavojingos veikos aspektus.

Siekiant susisteminti tapatybės vagystės padarinius, bus vertinami ne tik tapatybės vagystės kaip pavojingos veikos, bet ir kitų nusikalstamų veikų, kurios buvo įvykdytos naudojant tapatybės vagystę kaip priemonę, padariniai. Tapatybės vagystė elektroninėje erdvėje yra sudėtingas ir kompleksinis socialinis reiškinys, galintis turėti įvairių padarinių, kurie gali būti klasifikuojami remiantis įvairiais kriterijais.

Taip pat paminėtina, kad į daugelį toliau pateiktų klasifikacijų gali būti įtraukti ir mišrūs padariniai. Nors kai kuriose klasifikacijose mišrūs padariniai į atskiras kategorijas nėra išskirti, praktikoje, šių padarinių gali būti ne vienas, o keli. Pavyzdžiui, tapatybės vagystės elektroninėje erdvėje padariniai pagal tai, kokioje srityje jie kyla ir kokiems santykiams padaroma žala, gali būti teisinio, ekonominio ir netgi techninio pobūdžio.

Tapatybės vagystės elektroninėje erdvėje padariniai pagal tai, kokioje srityje jie kyla ir kokiems santykiams padaroma žala, gali būti skirstomi į:

1) teisinius;

2) ekonominius;
3) techninius;
4) kitus.

Tapatybės vagystės elektroninėje erdvėje gali sukelti teisinių padarinių, nors pažymėtina, kad asmuo, kurio duomenys buvo pasisavinti, dažnai net nesuvokia, kad nukentėjo nuo neteisėtos veikos, ir tik vertinant veiką pagal teisės normas galima konstatuoti, kad padarytas teisės pažeidimas. Tačiau dėl tapatybės vagystės gali kilti ir kitokio pobūdžio padarinių, pavyzdžiui, techninių (sugadinta programinė įranga ir kt.); ekonominių (kito asmens vardu prisiimta įsipareigojimų, pasisavintos materialinės vertybės ir pan.) ir kt.

Tapatybės vagystės elektroninėje erdvėje padariniai pagal vertybių, į kurias kėsinamasi, pobūdį / materialumą:

1) materialūs (daiktų, lėšų praradimas, piniginiai nuostoliai, negautos pajamos ir kt.);
2) nematerialūs (moralinis nepasitenkinimas, pažeminimas, šmeižtas, garbės ir orumo, privatumo pažeidimai ir pan.).

Tapatybės vagystė tiek realioje erdvėje, tiek elektroninėje erdvėje dažnai susijusi su neigiamomis pasekmėmis, kurios gali kilti dėl materialių įvairią vertę turinčių vertybių praradimo, be to, gali kilti ir nematerialių pasekmių (psichologinis diskomfortas, baimė ir kt.), kurios taip pat turi būti rimtai vertinamos, nes šios pasekmės fiziniam asmeniui gali sukelti stresą, psichologinę įtampą ar net norą nusižudyti. Be abejo, dažnai pasekmės būna mišrios, nes praradus materialines vertybes, neišvengiamai atsiranda ir neigiamų nematerialių pasekmių. Rečiau pasitaiko tapatybės vagystės elektroninėje erdvėje atvejų, kai nukentėjusiajam siekiama sukelti tik nematerialaus pobūdžio pasekmių (pavyzdžiui, apšmeižti, pažeminti, pagąsdinti ir pan.).

Tapatybės vagystės elektroninėje erdvėje padariniai pagal pasikėsinimo objektą:

1) grėsmė asmens garbei ir orumui;
2) finansiniai;
3) turtiniai;
4) sveikatai (sveikatos priežiūros srityje);
5) valstybės mastu;

6) privatumui;
7) duomenų saugumui;
8) vartotojų teisėms.

Dažniausiai tapatybės vagystės elektroninėje erdvėje padariniai pagal pasikėsinimo objektą būna finansiniai, tačiau galimi ir kitokie. Pavyzdžiui, naudojant kito asmens slaptažodžius, neteisėtai prisijungus šio asmens vardu prie socialinio tinklo profilio, platinama asmens garbę ir orumą žeminanti informacija.

Tapatybės vagystės elektroninėje erdvėje padariniai pagal tai, kokios socialinės normos pažeidžiamos:

1) pažeidžiantys baudžiamosios teisės normas ir užtraukiantys baudžiamąją atsakomybę;
2) pažeidžiantys administracinės teisės normas ir užtraukiantys administracinę atsakomybę;
3) pažeidžiantys civilinės teisės normas ir užtraukiantys civilinę atsakomybę;
4) pažeidžiantys moralės ar (ir) papročių normas ir užtraukiantys moralinę atsakomybę / visuomenės pasmerkimą;
5) kiti.

Tapatybės vagystės elektroninėje erdvėje padariniai taip pat gali būti skirstomi ir pagal sritis, kuriose jie kyla arba į kurias yra orientuoti:

1) bankų / finansinių paslaugų srityje;
2) sveikatos apsaugos srityje;
3) draudimo srityje;
4) asmeninių santykių srityje;
5) valstybės sektoriuje;
6) kt.

Tapatybės vagystė elektroninėje erdvėje dažniausiai susijusi su bankų / finansinių paslaugų sritimi. Literatūroje pateikiamas pavyzdys, kaip neteisėtai gali būti panaudojamos mokėjimo priemonės: pavogtos elektroninio mokėjimo kortelės buvo panaudotos vaikų pornografijai įsigyti[89].

[89] Camp, L. J. 2010. *Economics of Identity Theft*. Springer, p. 17.

Tapatybės vagystės elektroninėje erdvėje padariniai pagal tai, kokiame sektoriuje jie kyla:

1) viešajame sektoriuje;
2) privačiame sektoriuje.

Pasisavintą tapatybę galima panaudoti kaip priemonę kitoms nusikalstamoms veikoms įvykdyti, gali būti pasikėsinta į įvairias įstatymo saugomas vertybes ir sukelta pavojingų padarinių.

Tapatybės vagystės elektroninėje erdvėje padariniai pagal nukentėjusiųjų skaičių:

1) vienas konkretus asmuo;
2) apibrėžta asmenų grupė;
3) neapibrėžta asmenų grupė.

Tapatybės vagystės elektroninėje erdvėje subjektas (-ai) gali siekti šia pavojinga veika sukelti pasekmes vienam asmeniui arba apibrėžtai asmenų grupei, tačiau gali būti (o elektroninė erdvė tai leidžia atlikti gana nesudėtingai), kad tapatybės vagystės elektroninėje erdvėje subjektas (-ai) nesitaiko į konkrečius asmenis ir jį (-uos) tenkina bet kokios pavojingos neteisėtos veikos, dėl kurių nukentės daugelis (pavyzdžiui, naudojant programinę įrangą renkami milijonų tarpusavyje nesusijusių asmenų tapatybės duomenys).

Pagal jurisdikciją tapatybės vagystės elektroninėje erdvėje padariniai gali būti skirstomi į:

1) kilusius vienos valstybės (ar jurisdikcijos) ribose;
2) kilusius keleto valstybių (ar jurisdikcijų) ribose.

Kartais nusikalstamos veikos subjektai, darydami nusikaltimą net nežino, kokiose valstybėse gali kilti pavojingų pasekmių, tačiau tiriant nusikalstamą veiką ir jos pasekmes, svarbu identifikuoti ne tik nusikalstamos veikos įvykdymo vietą, bet ir vietą (-as), kurioje (-ose) kilo pavojingi padariniai.

Pažymėtina, kad jurisdikcijos problema tapatybės vagystės elektroninėje erdvėje atveju yra viena iš aktualesnių problemų. Šioje monografijoje jurisdikcijos problemų nenagrinėjama, tačiau tai galėtų būti tolesnių mokslinių tyrimų objektas.

Tapatybės vagystės elektroninėje erdvėje padariniai pagal mastą:

1) lokalių pasekmių;
2) pavojingi daugeliui.

Neteisėtos veikos, padarytos elektroninėje erdvėje, yra specifinės tuo, kad gali be didelių nusikalstamos veikos subjekto pastangų sukelti neigiamas pasekmes ne tik vienam asmeniui, o būti pavojingos dideliam kartais net neapibrėžtam asmenų ratui. Pavyzdžiui, įsilaužus į banko informacinę sistemą, gali būti pasisavinta daugelio asmenų prisijungimo prie elektroninės bankininkystės kodai ir kita svarbi informacija.

Tapatybės vagystės elektroninėje erdvėje padariniai pagal nusikalstamą ketinimą:

1) kai asmuo, vykdydamas tapatybės vagystę elektroninėje erdvėje, neturėjo nusikalstamų ketinimų;
2) kai asmuo, vykdydamas tapatybės vagystę elektroninėje erdvėje, siekė padaryti kitas nusikalstamas veikas.

Dažnai asmens tapatybė pasisavinama siekiant kito pavojingo tikslo, kuris dažniausiai yra nusikalstamas.

Tapatybės vagystės elektroninėje erdvėje padariniai pagal tai, prieš ką bus nukreipta pasisavinta tapatybė:

1) siekiant paveikti asmenį (jo turtą, teises ir interesus), kurio tapatybė pasisavinama;
2) siekiant paveikti kitus asmenis pasinaudojant pasisavinta tapatybe.

Pirmuoju atveju, pasinaudojant asmenį identifikuojančiais duomenimis ir (ar) asmenine informacija, asmuo gali būti šantažuojamas, reikalaujama jam priklausančio turto ar daromas kitoks poveikis (konkrečiam asmeniui arba tam tikrai grupei asmenų). Antruoju atveju tampa svarbus pats apsimetimas kitu asmeniu, siekiant nuslėpti tikrąją nusikaltėlio (-ių) tapatybę (-es) ir atlikti nusikalstamą veiką (pvz., teroro aktą, naudojant nepriekaištingos reputacijos piliečio tapatybę, siekiant suklaidinti teisėsaugos institucijas ir apsunkinti nusikalstamos veikos atskleidimą).

Tapatybės vagystės elektroninėje erdvėje padariniai pagal tai, kas nukenčia nuo šios veikos:

1) padariniai, kilę fiziniam asmeniui ar jų grupei;

2) padariniai, kilę juridiniam asmeniui;
3) padariniai, kilę valstybei;
4) padariniai, kilę tarptautinei bendruomenei.

Pasisavinant tapatybę gali nukentėti fiziniai, juridiniai asmenys (tiek privatūs, tiek viešieji), o jei atskirai išskiriama valstybė, įvairūs valstybių junginiai ir sąjungos, tai gali nukentėti ir šie dariniai (turintys arba neturintys juridinio asmens teises). Kitas svarbus aspektas yra tas, kad nusikaltimus gali padaryti tiek fizinis asmuo arba jų grupė, tiek juridinis asmuo (pvz., pramoninio šnipinėjimo atveju), tiek valstybės (numanoma 2007 m. balandžio pabaigos – gegužės pradžios Rusijos ataka prieš Estiją).

Kaip pavyzdį, kai pasisavinama juridinio asmens tapatybė, galima paminėti atvejį, kai Lietuvos pilietis P. S., įsilaužęs į JAV įmonių duomenų bazes, pasisavino elektroninius duomenis ir įkūręs svetaines labai panašiu pavadinimu, pardavinėjo neteisėtai pasisavintus elektroninius duomenis už nedidelę kainą. Skelbiama, kad JAV įmonėms padaryta žala siekia 10 milijonų litų[90].

Išvados

• Elektroninėje erdvėje atliekant įvairias transakcijas gana sudėtinga nustatyti tikrąją asmens tapatybę, kadangi joje santykiai „akis į akį“ neegzistuoja. Tačiau sukčiauti tokioje aplinkoje yra kur kas lengviau nei fizinėje erdvėje.

• Tapatybės nustatymas fizinėje erdvėje yra visiškai kitoks nei elektroninėje erdvėje. Fizinėje erdvėje savo tapatybę asmuo patvirtina vienu iš privalomų elementų – asmens dokumentu. Elektroninėje erdvėje tapatybę gali atstoti vardas ir slaptažodis. Joje tapatybė sutapatinama su prisijungimo vardu ir slaptažodžiu ir visos saugumo užtikrinimo priemonės, pavyzdžiui, skaitmeniniai sertifikatai ir kt., iš esmės atitinka asmens tapatybę elektroninėje erdvėje.

• Vartotojai dažnai nesuvokia, kokie svarbūs ir vertingi yra jų asmens duomenys. Disponavimas asmens duomenimis nesilaikant elementarių saugumo taisyklių, socialiniuose tinkluose viešinant asmens duomenis ir (ar) informaciją apie privatų gyvenimą, sudaro prielaidas tapatybės vagystei elektroninėje erdvėje įvykdyti ir didina riziką tapti šios pavojingos

[90] Įsilaužėlis pralobti nespėjo. *Lietuvos rytas*, 2011-08-25.

veikos, kurios padariniai gali būti labai įvairūs ir gali kilti įvairiose gyvenimo srityse, auka.

• Tapatybės vagystė elektroninėje erdvėje pasižymi latentiškumu. Atlikti kokybiniai ir kiekybiniai tyrimai patvirtino, kad Lietuvoje yra prielaidų tapatybės vagystės elektroninėje erdvėje latentiškumui. Dėl latentiškumo šios pavojingos veikos atveju teisėsaugos institucijoms sunku identifikuoti ir patraukti atsakomybėn tokias veikas įvykdžiusius asmenis, todėl tapatybės vagystės elektroninėje erdvėje latentiškumo mažinimas, turėtų būti vienas iš prioritetų kovojant su šiuo pavojingu reiškiniu. Tai padėtų įvertinti tikrąją būklę ir planuoti reikiamas prevencijos priemones.

• Beveik kiekvienoje pasaulio šalyje pastebimas tapatybės vagystės aktyvumo padidėjimas, tačiau tos šalys, kurios iki šiol neturėjo tokios patirties kovojant su tapatybės vagystėmis elektroninėje erdvėje, susiduria su nauja problema ir daugelis jų nesinaudoja kitų valstybių sukaupta patirtimi, netaiko gerosios praktikos pavyzdžių imdamosi prevencijos priemonių, nesigilina, kaip ši nauja nusikalstamumo rūšis augo ir vystėsi.

1.3. Socialinis teisinis tapatybės vagystės elektroninėje erdvėje aspektas

Kad socialiniai santykiai būtų laikomi teisiniais santykiais, būtinos tam tikros sąlygos. Santykiai turi būti visuotinai pripažinti ir dėl jų reguliavimo svarbumo konkrečiai sutarta. Ne visi socialiniai santykiai teisiškai reguliuojami, reguliavimo objektas yra socialiniai santykiai, kai atsiranda būtinybė juos teisiškai sunorminti[91]. Būtinybė teisiškai sunorminti reikšmingiausius santykius reiškia, kad teisinis reguliavimas negali apimti visų santykių, negali būti per platus, privalu nustatyti orientacinę ribą, kuri neleistų teisiniam reguliavimui plėstis tose srityse, kuriose jis nėra būtinas[92]. Socialinių santykių, kurie formavosi kartu su elektroninės erdvės, konkrečiai su interneto plėtra, dalis buvo pradėta plėtoti naujoje erdvėje. Kai kurie iš tų santykių buvo visiškai nauji ir teisiškai nereguliuojami dėl jau minėto santykių reikšmingumo būtinumo, nes tie nauji santykiai, kurie buvo plėtojami elektroninėje erdvėje, nebuvo reikšmingi daugumai.

[91] Vaišvila, A. 2009. *Teisės teorija*. Vilnius: Mykolo Romerio universitetas, 3-asis leid., p. 194.
[92] *Ibid*., p. 195.

Funkcinio ekvivalentiškumo principas numato, kad tokie patys socialiniai santykiai turi būti reguliuojami taip pat, nepriklausomai, ar jie atsiranda ir plinta elektroninėje erdvėje, ar fizinėje. Svarbu pažymėti, kad esantys tam tikri socialiniai santykiai fizinėje erdvėje teisiškai nereguliuojami tik dėl to, kad nėra tam būtinumo. Pavyzdžiui, asmenų tarpusavio bendravimas, draugystės – visa tai paremta pasitikėjimu ir vienas kito pažinojimu, tad teisiškai nėra būtina reguliuoti tokių asmenų bendravimo, bet kaip vertinti tokį asmenų bendravimą elektroninėje erdvėje? Fizinėje erdvėje pažįstamas asmuo neturi įrodyti, kas jis toks yra, draugas jis jums ar ne, tačiau elektroninėje erdvėje tokiu asmeniu gali tapti bet kas. Būtent dėl elektroninės erdvės specifikos, dėl galimos rizikos ir potencialios žalos iki šiol teisiškai nereguliuoti socialiniai santykiai privalo būti reguliuojami. Vis daugiau socialinių santykių pradedami ir tęsiami išimtinai tik elektroninėje erdvėje.

Elektroninėje erdvėje atsirandančios naujos elektroninio verslo formos skatina rimčiau pažvelgti į tokių santykių teisinį reguliavimą (elektroninės komercijos teisinis reguliavimas, asmens duomenų naudojimo elektroninėje erdvėje reguliavimas). Neretai toks teisinis reguliavimas atsilieka nuo realių socialinių santykių elektroninėje erdvėje, nors ir bandoma tokį atotrūkį mažinti pasitelkiant savireguliaciją, bet to nepakanka dėl nuolatos tobulėjančių technologijų ir atsirandančių naujų galimybių išnaudoti elektroninę erdvę asmenų socialinėje veikloje. Į elektroninę erdvę persikėlė dauguma mums įprastos tiek komercinės, tiek privačios veiklos. Atsirado iki tol nebuvusių ir negalėjusių būti socialinių santykių, kurie jau pateko į esamą teisinio reguliavimo objektą – turtinius žmonių santykius. Tapatybės vagystės atveju santykiai, kurie plėtojosi elektroninėje erdvėje, buvo nereguliuojami: identifikacija elektroninėje erdvėje, finansinių paslaugų teikimas ir kontrolė ir t. t., būtent šie nauji socialiniai santykiai tiesiogiai liečia asmens turtinius interesus, nes pati tapatybės vagystė pradžioje buvo orientuota į finansinės naudos gavimą. Tačiau turtiniai santykiai yra tik vienas iš teisinio reguliavimo objektų, į kurį patenka ir tapatybės vagystė. Tapatybės vagystė taip pat gali būti nukreipta į kitus elektroninėje erdvėje plėtojamus asmens socialinius santykius, kurie iki šiol nėra teisiškai reguliuojami. Būtina paminėti, kad socialiniai santykiai patenka į teisinio reguliavimo sritį, jei atitinka šias sąlygas[93]:

[93] *Ibid*., p. 199.

1) Socialinius santykius galima teisiškai formuluoti;
2) Socialinius santykius galima kontroliuoti valstybės priemonėmis;
3) Socialiniai santykiai kartojasi, yra visuotiniai ir tipiški visuomenei.

Teisiškai formuluoti naujus socialinius santykius elektroninėje erdvėje, o konkrečiai tapatybės vagystę, parenkant tinkamą teisinio reguliavimo metodą, jau imtasi daugelyje šios monografijos nagrinėjamų šalių. Tapatybės vagystė įgavo santykių reikšmingumo būtinumą, tapo daugeliui asmenų opia problema, galinčia sukelti negatyvių pasekmių. Taip pat atsirado galimybė tam tikrus minėtų naujų socialinių santykių elementus elektroninėje erdvėje kontroliuoti valstybės priemonėmis, t. y. užkirsti kelią teisės pažeidimams. Buvo įsteigtos naujos valstybinės institucijos ar struktūriniai padaliniai, kurių pagrindinis uždavinys – teisės pažeidimų elektroninėje erdvėje tyrimas, kontrolė ir prevencija[94]. Kaip minima kitose šios monografijos dalyse, tapatybės vagystė tampa viena iš rimčiausių problemų elektroninėje erdvėje, ji nuolatos kartojasi, jos mastai didėja ir vis daugiau asmenų su tuo susiduria. Tačiau tapatybės vagystės kaip tik ir atspindi tą socialinių santykių dalį, kuri iki šiol yra mažai teisiškai reguliuojama. Elektroninė erdvė sudarė tinkamas sąlygas išnaudoti šią nesureguliuotą sritį, todėl tapatybės vagystės ir tapo viena iš pavojingiausių nusikalstamų veikų. Dažnai tapatybės vagystės grėsmė yra siejama su galima finansine žala, neretai ir teisinis reguliavimas būna orientuotas tik į finansinio pobūdžio nusikaltimus, tačiau tapatybės vagystės padariniai gali būti labai įvairūs ir dėl to svarbu tinkamai teisiškai sureguliuoti tokius santykius. Kita svarbi detalė – tarptautinio reguliavimo būtinumas. Asmenys išnaudoja elektroninės erdvės siūlomas galimybes ir plėtoja socialinius santykius už savo valstybės ribų, tikėdamiesi, kad teisinis reguliavimas tinkamai apsaugos jų interesus, bet ne visos valstybės yra pripažinusios naujų socialinių santykių elektroninėje erdvėje reikšmingumą.

Negalima siekti visiško visų socialinių santykių elektroninėje erdvėje reguliavimo. Galimos grėsmės ir pavojai turi būti numanomi. Teisiškai svarbu formuluoti ne gatavus konfliktų sprendimus, o tik jų sprendimo priemones[95]. Jei bus bandoma teisiškai formuluoti visus naujus socialinius santykius elektroninėje erdvėje, susidursime su problema – atsiras

[94] Lietuvoje buvo įsteigta „Lietuvos kriminalinės policijos biuro Nusikaltimų elektroninėje erdvėje tyrimo valdyba“.

[95] Vaišvila, A. *Teisės teorija*. 2009. Vilnius: Mykolo Romerio universitetas, 3-asis leid., p. 205.

vis naujų socialinių santykių, kurie nebus reguliuojami teisinėmis priemonėmis. Šioje situacijoje, kai plėtojami nauji socialiniai santykiai elektroninėje erdvėje, svarbūs tampa teismai, o teismų praktika yra tokia pat gausi kazusų, kaip ir pats gyvenimas[96].

Plečiantis asmenų laisvėms elektroninėje erdvėje kyla daug nesutarimų ir konfliktų, todėl valstybė, kurdama teisės normas, negali ir neturi nustatyti visų galimų konfliktų šalinimo priemonių[97]. Tokių nesutarimų ir prieštaravimų sprendimas paliekamas patiems asmenims. Kaip jau minėta ankščiau, savireguliacija gali padėti išspręsti daugumą nesutarimų elektroninėje erdvėje, tačiau tapatybės vagystės kontekste, kai patiems asmenims nepavyksta šito padaryti tarpusavio sutarimais, būtinas teisinis reguliavimas.

Apibendrinančios išvados

• Tokie patys socialiniai santykiai turi būti reguliuojami taip pat, nepriklausomai nuo to, ar jie atsiranda ir plėtojasi elektroninėje erdvėje, ar fizinėje (funkcinio ekvivalentiškumo principas). Tačiau dėl elektroninės erdvės specifikos, dėl galimos rizikos ir potencialios žalos neteisėtos / pavojingos veikos (taigi, ir tapatybės vagystės elektroninėje erdvėje) atveju, iki šiol teisiškai nereguliuoti socialiniai santykiai elektroninėje erdvėje privalo būti reguliuojami.

• Elektroninėje erdvėje atsirandančios naujos elektroninio verslo formos skatina persvarstyti esamą tokių santykių teisinį reguliavimą, kadangi dėl nuolatinės technologijų pažangos ir atsirandančių naujų galimybių išnaudoti elektroninę erdvę asmenų socialinėje veikloje, teisinis reguliavimas atsilieka nuo realių socialinių santykių elektroninėje erdvėje. Šį atotrūkį bandoma mažinti pasitelkiant savireguliaciją.

• Tapatybės vagystė elektroninėje erdvėje atspindi socialinių santykių dalį, kuri iki šiol yra menkai teisiškai reguliuojama. Elektroninė erdvė sudarė tinkamas sąlygas išnaudoti šią nesureguliuotą sritį ir tapatybės vagystė elektroninėje erdvėje tapo viena iš pavojingiausių nusikalstamų veikų. Įvertinant tai, kad šios pavojingos veikos padariniai gali būti labai įvairūs, svarbu tinkamai teisiškai sureguliuoti santykius, susijusius su tapatybės vagyste elektroninėje erdvėje.

[96] *Ibid.*

[97] *Ibid.*

1.4. Tapatybės vagystės elektroninėje erdvėje samprata

Terminas „tapatybės vagystė“ bene kiekvieną dieną minimas užsienio valstybėse, pabrėžiant, kad šis reiškinys yra itin pavojingas ir galintis sukelti pačių įvairiausių neigiamų padarinių kiekvienam – tiek fiziniams asmenims, paprastiems vartotojams, finansų institucijoms ir galiausiai visai ekonomikai. Tuo tarpu Lietuvoje tapatybės vagystė yra mistifikuojama: kartkartėmis, dažniausiai finansinių institucijų tinklalapiuose, pasirodo pavieniai pranešimai, įspėjantys, kad 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.

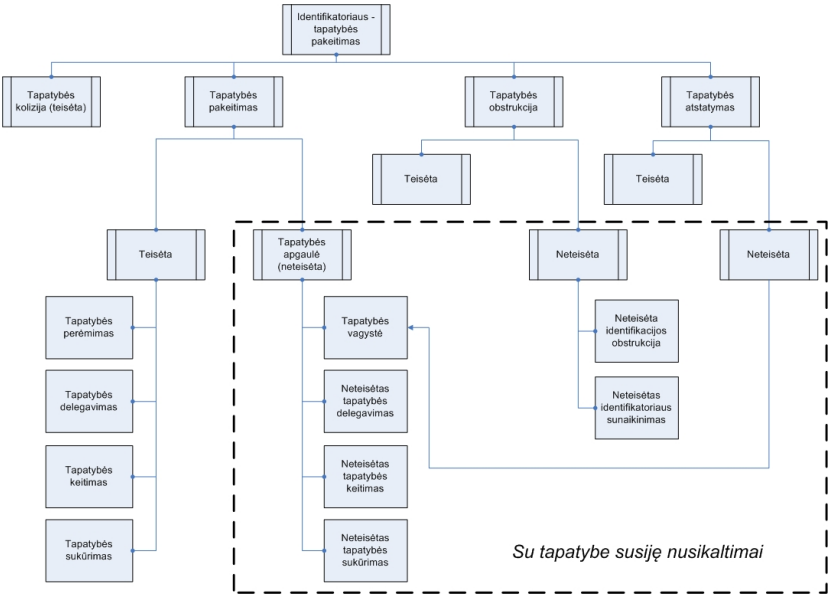
Tačiau problema yra kur kas didesnė ir keleto atidumą skatinančių pranešimų per metus nepakanka efektyviam visuomenės švietimui apie vieną iš pavojingiausių reiškinių, susijusių su asmens duomenų ir privatumo apsauga. Todėl pirmiausia teisėsaugos, finansų sektoriaus ir kitos institucijos privalo tinkamai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

Vertėtų atsisakyti požiūrio, kad 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.

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, keičiant vieną ar daugiau tapatybės nustatymo elementų, pavyzdžiui, gali būti kitas vardas, gimimo data, adresas ir pan.); *tapatybės vagystę* (apsimetimas kitu asmeniu, kuris vėliau gali sudaryti sąlygas neteisėtiems veiksmams atlikti)[98].

Tapatybės vagystės vietą tarp kitų su tapatybe susijusių neteisėtų veikų grafiškai galima pavaizduoti taip:

[98] *Standardisation of defi nitions of identity crime terms: A step towards consistency.* Australasian Centre for Policing Research, 2006, p. 7.



11 pav. Tapatybės vagystės vieta tarp kitų su tapatybe susijusių veikų
(Šaltinis: Rannenberg, K.; Royer, D.; Deuker. A. *The Future of Identity in the Information Society: Challenges and Opportunities*. 320 p.)

Akcentuotina tai, kad nors tapatybės vagystė yra tarptautinio pobūdžio problema, nei tarptautiniu, nei regioniniu lygiu privalomojo 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 sąvokos iš viso nepateikiama. Kai kurios valstybės pasirinko tapatybės vagystę traktuoti plačiąja prasme, t. y. apimant tapatybės vagystės atvejus ir elektroninėje, ir fizinėje erdvėje. Tačiau tik nedaugelis valstybių tapatybės vagystę laiko specifiniu teisės pažeidimu. Dėl tokio požiūrių skirtumo skiriasi ir tapatybės vagystės teisinis pobūdis, 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 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.

Ekonominio bendradarbiavimo ir plėtros organizacija (EBPO) 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 sukčiauti arba įvykdyti kitus nusikaltimus[99].

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 sunkus nusikaltimas pagal galiojančius Valstijos ar vietinius teisės aktus[100]. Iš šios teisės 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 įstatyme įtvirtintu nusikaltimu, kuris apima ir apgaulę, įvykdytą elektroninėje erdvėje. Šiame teisės akte numatoma, 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[101].

Taip pat įtvirtinti nauji nusikaltimai, tokie kaip nesąžiningas paslaugų teikimas, jei už jas atliekami mokėjimai, pavyzdžiui, elektroninėje erdvėje apgaulės būdu pasinaudojant mokėjimo kortele; priemonių, įskaitant bet kokių laikomų elektronine forma programų ar asmens duomenų, skirtų

[99] Online Identity Theft [interaktyvus]. OECD, 2009 [žiūrėta 2011-09-15], p. 16. <http://browse.oecdbookshop.org/oecd/pdfs/browseit/9309021E.PDF>.

[100] United States Code („U. S. C“), Title 18, Part I, Chapter 47, Section 1028 (a) (7). [interaktyvus, žiūrėta 2011-09-15] . < http://www.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00001028----000-.html>.

[101] Fraud Act 2006 [interaktyvus, žiūrėta 2011-09-15]. <http://www.legislation.gov.uk/ukpga/2006/35/contents>.

apgaulei įvykdyti, kurios yra susijusios su tapatybės klastote, turėjimas; taip pat tokių priemonių gaminimas ir siūlymas, žinant, kad jos sukurtos ar pritaikytos atlikti apgavikiškiems veiksmams[102]. 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 asmeniu ar klastojimas, dispozicijos. Tačiau pasiruošimo įvykdyti nusikaltimą, pavyzdžiui, informacijos, padedančios nustatyti asmens tapatybę, rinkimas, turėjimas ir perdavimas paprastai nepatenka į patvirtintų nusikaltimų sudėtį[103].

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*** būna tada, kai turima pakankamai informacijos apie tapatybę tam, kad būtų lengviau įvykdyti tapatybės klastotę, nepriklausomai nuo to, ar auka yra gyva ar mirusi;
- ***tapatybės klastotė*** būna 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 (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

[102] Phishing kits banned by new Fraud Act. *Out-Law news* [interaktyvus]. 2006-11-13 [žiūrėta 2011-09-15]. <www.out-law.com/page-7469>.

[103] Kanados teisingumo departamento oficialus tinklalapis [interaktyvus, žiūrėta 2011-09-15]. <http://www.justice.gc.ca/>.
Ibid., [interaktyvus, žiūrėta 2011 09 15]. <http://www.justice.gc.ca/eng/news-nouv/nr-cp/2007/doc_32178.html>.
Ibid., [interaktyvus, žiūrėta 2011 09 15]. <http://www.justice.gc.ca/eng/news-nouv/nr-cp/2009/doc_32348.html>.
Ibid., [interaktyvus, žiūrėta 2011 09 15]. <http://www.justice.gc.ca/eng/news-nouv/nr-cp/2009/doc_32347.html>.

įrangos ar paslaugų (banko sąskaitos atidarymas, paskolos prašymas arba prašymas išduoti mokėjimo kortelę)[104].

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 naudojimas nusikalstamai veikai padaryti, siekiant apgaulės būdu gauti prekes ir paslaugas. Paprastai tokia veika apima pavogtų ar suklastotų tapatybės dokumentų, tokių kaip pasas ar vairuotojo pažymėjimas, panaudojimą[105].

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. O tapatybės klastotės atveju duomenys ir informacija apie kitą asmenį yra renkami tam, kad jais pasinaudojus būtų galima gauti kokios nors apčiuopiamos, dažniausiai finansinės, naudos, – 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, kad tapatybės vagystė yra priemonė tapatybės klastotei įvykdyti.

Toks terminų „tapatybės vagystė“ ir „tapatybės klastotė“ alternatyvus vartojimas kritikuotinas, nes remiantis anksčiau pateikta sąvokų turinio

[104] Tapatybės vagystė; netapk auka [interaktyvus, žiūrėta 2011 09 15]. <http://www.identitytheft.org.uk/identity-crime-definitions.asp>.

[105] CIFAS [interaktyvus, žiūrėta 2011 09 15]. <http://www.cifas.org.uk/default.asp?edit_id=561-56>.

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 materialią 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. Apibrėžiant klastojimo rūšis sutinkamas „tikro dokumento“ terminas turėtų būti suprantamas kaip dokumentas, surašytas ar kitaip pagamintas asmens, turinčio teisę tai daryti, 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 asmuo 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 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, kurį identifikuojančios priemonės buvo gautos, tačiau *neturint tikslo įvykdyti nusikalstamą veiką*. „Piktnaudžiavimo“ terminas pabrėžia veiksmų neleistinumo aspektą: net jei tokiais veiksmais realiai jokios žalos ar nuostolių nesukeliama, pats veiksmų atlikimo faktas yra priešingas teisei ir dažniausiai patenka į neteisėto asmens duomenų tvarkymo, už kurį paprastai numatoma administracinė atsakomybė, kategoriją. Tokios veikos pavyzdžiai galėtų būti prisijungimas prie socialinio tinklalapio, 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, kurį identifikuojančios priemonės buvo gautos, 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[106] gavimą pasinaudojant įvairiais slaptais metodais[107]. 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 klastoti, tačiau nusikalstamos veikos gali būti kaip alternatyvūs tikslai[108].

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[109].

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, reikalinga suklastoti tapatybei arba apsimesti kitu asmeniu užgrobiant pastarojo tapatybę, turint tikslą įvykdyti vagystę, klastotę ar kitus piktavališkus veiksmus[110]. Reikia atkreipti dėmesį, kad šie autoriai, pateikdami tapatybės vagystės apibrėžimą, iš esmės apibūdina 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,

[106] Tokie duomenys gali ne visada identifikuoti asmenį, pavyzdžiui, kas jūs esate; jie gali autentifikuoti, tarkim, ar jūs esate tikrasis vartotojas, ar autorizuoti, ką jūs galite padaryti, nebūtinai nustatant konkretaus individo tapatybę.

[107] Autorių nuomone, asmeninė informacija gali būti gaunama ir neslaptais metodais.

[108] Reed, C.; Angel, J. 2007. *Computer Law: the law and regulation of information technology*. 558 p.

[109] Sullivan, B. 2004. *Your evil twin: behind the identity theft epidemic.*, p. 10.

[110] Duquenoy, P., *et al.* 2008. *Ethical, legal and professional issues in computing*, p. 39.

pagal kuriuos atribojamos dvi tapatybės vagystės rūšys: tapatybės vagystė fizinėje erdvėje ir tapatybės vagystė elektroninėje erdvėje.

Bob Sullivan tapatybės vagystę traktuoja kaip nusikaltimą, kuris kyla iš informacinės politikos struktūros – tai paaiškina, kodėl šį nusikaltimą taip lengva įvykdyti ir taip sunku kaltą asmenį patraukti atsakomybėn[111].

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

[111] *Ibid*., p. 12.

kalbant apie šios rūšies tapatybės vagystę 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) elektroninėje terpėje (įskaitant per atstumą), pasinaudojant informacinėmis technologijomis.

Per pastaruosius dešimt metų smarkiai padidėjo verslo teikiamų elektroninių paslaugų vartotojams mastas. Tai lėmė kelios priežastys: daugelis verslo subjektų savo veiklą (visą arba dalį jos) perkėlė 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, kad nei teisės aktuose ar teismų praktikoje nėra įtvirtinta tapatybės vagystės ar tapatybės vagystės elektroninėje erdvėje sąvokų. Kaip išimtis paminėtina teisės doktrina, kai 2009 m. Darius Štitilis ir Marius Laurinaitis suformulavo tapatybės vagystės elektroninėje erdvėje galimą sampratą[112]. Tapatybės vagystę galima bandyti aiškinti remiantis atskirų šios sąvokos elementų lingvistine analize. Pavyzdžiui, Dabartinės lietuvių kalbos žodynas[113] „tapatybę“ apibrėžia kaip tapatumą, t. y. identiškumą, tolygumą. Lietuvių kalbos žodyne[114] turinio prasme įtvirtinta iš esmės 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. O tapatybės vagystė elektroninėje erdvėje galėtų būti aiškinama kaip tapatybės

[112] Štitilis, D.; Laurinaitis, M. 2009. Tapatybės vagystė elektroninėje erdvėje, *Informacijos mokslai* 50: 240–247.

[113] Dabartinės lietuvių kalbos žodynas [interaktyvus, žiūrėta 2011-09-15]. <http://www.lki.lt/dlkz/>.

[114] Lietuvių kalbos žodynas [interaktyvus, žiūrėta 2011-09-15]. <http://lkz.mch.mii.lt/Zodynas/Visas.asp>.

vagystės atlikimas elektroninėje terpėje (įskaitant 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.

Apibendrinančios išvados

• 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 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 fizinėje erdvėje. Mokslinėje literatūroje tapatybės vagystės sąvoka taip pat nepateikiama: išskiriami tik kai kurie sampratos fragmentai, be to, pasirinktas tapatybės vagystės traktavimas plačiąja prasme.

• Dažniausiai akcentuojama, kad tapatybės vagystė yra teisės pažeidimų ir nusikaltimų 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.

• 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, kurį identifikuojančios priemonės buvo gautos, tam, kad būtų galima atlikti teisės pažeidimus ir (ar) nusikalstamas veikas.* O

tapatybės vagystė elektroninėje erdvėje galėtų būti suprantama kaip *tapatybės vagystės rūšis, kai tapatybės vagystė atliekama elektroninėje erdvėje, t. y. pasinaudojant informacinėmis ir ryšio technologijomis.*

• Tikslinga išskirti dvi tapatybės vagystės rūšis pagal šios veikos padarymo metu turimą tikslą:

1) piktnaudžiavimas tapatybe*,* kai atliekami įvairūs veiksmai su kito asmens duomenimis ir (ar) asmenine informacija, siekiant apsimesti tuo asmeniu, kurį identifikuojančios priemonės buvo gautos, tačiau *neturint tikslo įvykdyti nusikalstamos veikos.*

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

1.5. Tapatybės vagystės 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. Tapatybės vagystės formos taip pat bus aptariamos vadovaujantis tapatybės vagystės plačiąja prasme samprata, nes, kaip jau 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 neatskleidžia šio pavojingo reiškinio sudėtingumo, nes tapatybės vagystė gali pasireikšti įvairiomis formomis, kurių išskyrimas ir analizė yra svarbūs minėto reiškinio

kompleksiškumui, sudėtingumui ir toms sritims, kuriose tapatybės vagystė gali pasireikšti, atskleisti ir tinkamai įvertinti.

Jungtinių Amerikos Valstijų Federalinė prekybos komisija išskiria šias tapatybės vagystės formas (jas dar galima įvardyti kaip pavogtos tapatybės panaudojimo būdus)[115]:

1) sukčiavimas, susijęs su kreditinėmis kortelėmis:

- kreditinių kortelių sąskaitų atidarymas nukentėjusiojo asmens vardu: kai pasinaudojama kreditine kortele, nukentėjusiojo nuo tapatybės vagystės skolos ataskaitoje atsiranda įrašų apie neapmokėtas sąskaitas;
- gali būti pakeistas adresas, kuriuo asmuo gauna sąskaitas, siekiant, kad jam daugiau neapmokėtos sąskaitos nebūtų siunčiamos, o kaltininkas galėtų apmokėti mokesčius naudodamasis nukentėjusiojo sąskaita. Kai sąskaitos siunčiamos kitu adresu, kartais gali būti sunku greitai nustatyti 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 naudojant 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;

[115] Federalinės prekybos komisijos tinklalapis, skirtas kovai su tapatybės vagyste [interaktyvus, žiūrėta 2011-09-15]. <http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html>.

- 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;
- pasinaudojant nukentėjusiojo asmens duomenimis gali būti išsinuomojamas namas arba gaunamos medicininės paslaugos;
- nukentėjusiojo asmeninė informacija gali būti perduodama policijai arešto metu. Jei kaltininkas nepasirodo teisme ir neprisipažįsta, arešto orderis išduodamas nukentėjusiojo vardu ir kt.

Atkreiptinas dėmesys, kad informacinės visuomenės nariai dažnai naudojasi elektroninėmis paslaugomis, kurios galėtų būti apibrėžiamos kaip teisės aktuose 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 ir kitomis telekomunikacijų priemonėmis. Naudojantis elektroninėmis paslaugomis galima ne tik prisijungti prie elektroninės bankininkystės sistemos, bet ir deklaruoti pajamas, pateikti prašymus dokumentams išduoti ar net įregistruoti juridinį asmenį. Todėl asmenys, išmanantys informacines ir ryšio technologijas, turintys specialių įgūdžių ir priešingų teisei ketinimų, elektroninę erdvę laiko santykinai 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 teikiamomis 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[116]:

[116] Teisės profesoriaus David E. Sorkin sukurtas tinklalapis. <http://www.spamlaws.com/passport-identity-theft.html>. [žiūrėta 2011-09-15].

1) medicininė tapatybės vagystė (angl. *Medical Identity Theft*): tai viena iš greitai plintančių apgaulės formų, kurią įgyvendinti 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 tinklalapiais arba elektroniniu paštu: naudodamiesi šiomis priemonėmis jie apsimeta esantys, pavyzdžiui, mokesčių rinkimo 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 nereikalingą 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 išmanančio asmens gali būti nesunkiai atkurta ir taip atskleistos, pavyzdžiui, elektroninio pašto žinutės, aukos vardas, pavardė, gimimo data ir kita svarbi 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*): susijusi ne tik su neatsakingu kreditinių kortelių naudojimu ir pirkimo išsimokėtinai galimybe – tokios tapatybės vagystės auka gali tapti bet kas.

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 dokumentams klastoti. Tuo tarpu tapatybės vagystė elektroninėje erdvėje gali likti iš viso nepastebėta, t. y. aukos gali net nežinoti, kad jų asmeninė informacija buvo pavogta, o kai sužino, dažniausiai jau būna per vėlu. Pradedantysis interneto vartotojas dažnai nežino, kad kompiuterio kietajame diske kaupiama ir saugoma daugybė 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 padaro finansinių nuostolių. Šiuo atveju tapatybės vagystė įvykdoma apgaulės būdu atidarant naują kreditinės kortelės ar banko sąskaitą. Kai išnaudojamas kredito limitas, aukai lieka neapmokėtos sąskaitos ir skolos. Taip pat pažeidėjas gali perimti asmens tapatybę, kuri leidžia 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 apie auką, gauti daugiau asmeninės informacijos, ir panaudoti tai, pavyzdžiui, paskolai gauti. Asmuo, tapęs auka, apie tokio tipo tapatybės vagystę dažniausiai sužino tada, kai sulaukia kreditorių reikalavimų dėl piniginių sandorių, kurių jis nesudarė, apmokėjimo.

8) banko operacijų tapatybės vagystė (angl. *Banking Identity Theft*): šiuo atveju banko klientai dažniausiai informuojami elektroniniu paštu, kad

buvo kėsintasi 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 tinklalapį, 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 neigiamų pasekmių 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 nukentėjusįjį, pavyzdžiui, sužinoti gimimo vietą, gatvę, kurioje jis užaugo, lankytą mokyklą, santykius su kitais moksleiviais, informaciją, susijusią su tėvais ir kitais šeimos nariais, nuolatinę gyvenamąją vietą, socialinio draudimo numerį ir t. t. Trumpiau tariant, „tapatybės klonai" stengiasi sužinoti kiek galima daugiau informacijos, 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 as-

mens 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 įvykdoma ir tada, kai apgavikams pakanka pasinaudoti savo draugų ar giminių vardais ir adresais, tačiau nereikia parodyti 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, bet nustatytu laiku teisme nepasirodo, teisėjas priima sprendimą atvesdinti kaltinamąjį. Vietoj jo atvesdinamas nieko neįtariantis ir nekaltas kitas asmuo. Taip pat įmanoma, kad apsimetėlis gali atvykti į teismo posėdį be aukos žinios. Tokiu atveju įrašas apie teistumą įtraukiamas į duomenų bazėse esančią aukos asmens bylą.

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 nedaroma skirtumo tarp sąvokų „forma“ ir „rūšis“. Rūšis turėtų būti suprantama kaip skirstymo pakopa, vienetas, 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, atliekamą 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, kurį identifikuojančios priemonės buvo gautos.

Trumpai apžvelgus tapatybės vagystės formas, būtų klaidinga teigti, kad viena tapatybės vagystės forma yra pavojingesnė už kitą. Jau pats tapatybės vagystės reiškinys yra kompleksiškas ir pavojingas, nepriklausomai nuo jo pasireiškimo formos, nes kėsinimosi objektas yra asmens duomenys ir (ar) asmeninė informacija, pagal kurią 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.

Apibendrinančios išvados

• Klaidinga manyti, kad viena tapatybės vagystės forma yra pavojingesnė už kitą. Pats tapatybės vagystės reiškinys yra kompleksiškas ir pavojingas, nepriklausomai nuo jo pasireiškimo formos.

• Nors tapatybės vagystė pasižymi formų įvairove, nepriklausomai nuo to, kokia forma ši pavojinga veika pasireiškia, rezultatas kiekvienu atveju bus tas pats – kitas asmuo, neturėdamas tam teisės, turi galimybę pasinaudoti nukentėjusiojo asmens duomenimis ir (ar) informacija apie šį asmenį, o pačiam nukentėjusiajam iškyla potencialus pavojus susidurti su neigiamomis tapatybės vagystės pasekmėmis įvairiose gyvenimo srityse.

1.6. Tapatybės vagystės elektroninėje erdvėje plitimo tendencijos

Tapatybės vagystė elektroninėje erdvėje yra daug platesnis ir daug sudėtingesnis nusikaltimas (nei galima įsivaizduoti) ir gali daryti įtaką įvairioms visuomenės sritims, įskaitant ekonomiką ir nacionalinį saugumą[117]. Dėl to tapatybės vagystės elektroninėje erdvėje tendencijos gali pasireikšti labai plačiai.

Elektroninės erdvės panaudojimo plitimas ir elektroninė asmens tapatybė

Kaip jau minėta šioje monografijoje, internetas iš esmės pagerina verslo galimybes. Dideliais tempais didėja elektroninės komercijos apimtys. Pavyzdžiui, elektroninės komercijos pardavimai JAV, lyginant 2009 m. ir 2010 m. duomenis, padidėjo 14,8 procento ir pasiekė 165 mlrd. JAV dolerių sumą[118]. Taip pat internetas yra kaip priemonė gyventojams ir įmonėms teikti viešąsias paslaugas. Taigi, internetas iš principo pakeitė tiek globalią ekonomiką, tiek visuomenę ir jo poveikis artimiausiu metu vis stiprės[119].

[117] Hoffman, S. K.; Mccinley T., G. 2010. *Identity theft*. Greenwood publishing group, p. 4.

[118] E-commerce sales rise 14.8% in 2010 [interaktyvus]. 2011-02-17 [žiūrėta 2011-09-24]. <http://www.internetretailer.com/2011/02/17/e-commerce-sales-rise-148-2010 >.

[119] Online Identity Theft [interaktyvus]. OECD, 2009 [žiūrėta 2011-09-15], p. 15. <http://browse.oecdbookshop.org/oecd/pdfs/browseit/9309021E.PDF>.

Visa minėta veikla elektroninėje erdvėje vykdoma asmens tapatybę nustatant pagal elektroninius duomenis. Tokiu būdu didžiuliais tempais plinta elektroninės asmens tapatybės naudojimas, kuris pakeičia tradicinius metodus. Pavyzdžiui, prieš gerą dešimtmetį, daugelis žmonių, norėdami atlikti vieną ar kitą bankinę operaciją, turėdavo fiziškai apsilankyti banke ir pateikę asmens tapatybę patvirtinantį dokumentą, atlikti atitinkamą operaciją. Tuo tarpu dabar nemaža dalis banko vartotojų visas reikiamas bankines operacijas atlieka elektroniniu būdu, prisijungę prie elektroninės bankininkystės sistemos. Tapatybės prasme – tai yra esminis skirtumas, nes naudojamos specialios identifikavimo priemonės. Asmuo identifikuojamas ne pagal asmens dokumentus, o pagal gautus elektroninius kodus ir paties susigalvotus slaptažodžius.

Galima išskirti saugų asmens tapatybės elektroninėje erdvėje nustatymą ir kitus tapatybės nustatymo būdus (iš kurių dalis yra mažiau saugūs). Kaip nurodyta Lietuvos informacinės visuomenės plėtros 2010–2015 metais strategijos projekte, „šiuo metu gyventojai plačiai naudojasi vienu iš asmens tapatybės elektroninėje erdvėje nustatymo būdų – elektroninės bankininkystės identifikavimo sistemomis. Lietuvoje jau yra galimybė asmens tapatybę nustatyti naudojant elektroninį parašą, patvirtintą kvalifikuotu sertifikatu. Šiuo metu jau išduota daugiau kaip 300 tūkstančių asmens tapatybės kortelių su integruotu sertifikatu asmens tapatybei nustatyti, veikia trys kvalifikuotų sertifikatų išdavimo paslaugų teikėjai“[120]. Deja, kol kas tai yra tik galimybės, kadangi, pavyzdžiui, kortelių nuskaitymo infrastruktūros naudojimas Lietuvoje nėra plačiai paplitęs, tačiau saugios bankininkystės sistemų naudojimas yra pakankamai didelis. Elektroninės bankininkystės vartotojų didėjimą lemia interneto skvarba ir technologijų plėtra. Lietuvos Respublikos statistikos departamento duomenimis, 2010 metais Lietuvoje internetu naudojosi 60,5 % Lietuvos gyventojų.[121] Nuolat (ne rečiau kaip kartą per savaitę) internetu naudojosi 58 proc. gyventojų. 2009 metų duomenimis, nuolat naudojan-

[120] Lietuvos informacinės visuomenės plėtros 2010–2015 m. strategijos projektas. [interaktyvus, žiūrėta 2011-09-15], 33 p. <http://www.transp.lt>.

[121] LR Statistikos departamentas. 16–74 m. amžiaus asmenys, kurie naudojosi kompiuteriu, internetu [interaktyvus, žiūrėta 2011-09-15]. <http://db1.stat.gov.lt/statbank/selectvarval/saveselections.asp?MainTable=M9020201&PLanguage=0&TableStyle=&Buttons=&PXSId=9492&IQY=&TC=&ST=ST&rvar0=&rvar1=&rvar2=&rvar3=&rvar4=&rvar5=&rvar6=&rvar7=&rvar8=&rvar9=&rvar10=&rvar11=&rvar12=&rvar13=&rvar14=>.

čių internetą buvo 55 %. Lietuvos rodikliai atsilieka nuo Europos Sąjungos vidurkio – 70 %.[122] Lietuvos Respublikos statistikos departamento duomenimis, 2010 metais internetine bankininkyste naudojosi 37 % Lietuvos gyventojų, o tai 5 % daugiau negu 2009 metais[123].

Gana aukštas ir vis didėjantis interneto naudojamumo rodiklis nulemia vis didesnį asmeninės informacijos pateikimą elektroninėje erdvėje. Kadangi kol kas nėra pakankamai taikomos saugios tapatybės nustatymo platformos, daugėja nesaugios elektroninės tapatybės naudojimo atvejų.

Asmeninės elektroninės informacijos kiekiai pasiekė tokį lygį, kad atsiranda terminas „e. reputacija". E. reputacija – tai asmeninės informacijos visuma, nusakanti asmens savybes ir kitą su asmens veiksmais praeityje susijusią informaciją. Atsiranda netgi naujo tipo verslo kryptis – kuriasi bendrovės, siūlančios asmeninės informacijos paieškos elektroninėje erdvėje ir tokios informacijos koregavimo paslaugas. Elektroninės reputacijos apsaugos paslaugos, dar vadinamos „į reputaciją orientuotos paslaugos" (angl. *reputation-oriented service*) nėra pigios[124], tokios reputacijos apsaugos paslaugos gali kainuoti iki 10 tūkstančių JAV dolerių per mėnesį[125].

Taigi, elektroninis tapatybės duomenų naudojimas tampa masiniu reiškiniu, keliančiu vis didesnę grėsmę tiems patiems asmenims, kurie naudojasi elektroninės erdvės teikiamomis galimybėmis. Tačiau elektroninė erdvė ne tik sudaro neįtikėtinas galimybes plėtoti verslą, naudotis paslaugomis ir pan., bet taip pat sukuria daug rizikos rūšių, iš kurių viena grėsmingiausių –tapatybės vagystė elektroninėje erdvėje. Paminėtina ir tai, kad, be asmeninės informacijos elektroninėje erdvėje plitimo, daugėja ir išgalvotos arba nepatikimos asmeninės informacijos. Šis procesas vyksta ir dėl tos priežasties, kad internete nėra informacijos tikrinimo

[122] Internet usage in 2010 – Households and Individuals [interaktyvus, žiūrėta 2011-09-15]. <http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/KS-QA-10-050/EN/KS-QA-10-050-EN.PDF >

[123] Informacinių technologijų naudojimas namų ūkiuose [interaktyvus,žiūrėta 2011-09-15] <http://www.stat.gov.lt/lt/news/view/?id=7963 >.

[124] Viena iš daugelio „Švarios reputacijos saugotojų" kompanijų internete pateikia savo kainas. BrandsEye. [interaktyvus, žiūrėta 2011-09-15]. <http://www.brandseye.com/pricing-plans>

[125] How to clean up your online reputation. IT Business.ca. [interaktyvus, žiūrėta 201-09-15]. <http://www.itbusiness.ca/it/client/en/home/News.asp?id=60843&PageMem=2>.

mechanizmų. Kaip pavyzdį galima pateikti registravimosi į socialinį tinklalapį procesą. Registruojantis nereikalaujama patikimos identifikacijos ir besiregistruojantis asmuo gali įvesti bet kurio kito asmens asmeninius duomenis.

Visuotinis asmeninės informacijos prieinamumas ir interneto socialiniai tinklai

Gigantės „Google" kompanijos atstovas Eric Schmidt[126], kalbėdamas apie elektroninės reputacijos valdymą, akcentavo: „Aš netikiu, kad visuomenė supranta, kas atsitinka, kai visa informacija internete tampa prieinama ir lengvai pažįstama, kai visą laiką registruojamas kiekvienas veiksmas, žingsnis. Greitai kiekvienas jaunas žmogus turės teisę automatiškai pakeisti savo vardą, kad taptų saugus, siekiant išsižadėti jaunatviško neapdairumo, savo gyvenimą atiduodant socialiniams tinklams". „Google" kompanijos atstovas neatsitiktinai akcentavo pernelyg laisvą informacijos sklaidą ir dėjimą į internetą, juk jaunas žmogus nepagalvoja, kad visa jo sudėta informacija (garso, vaizdo, nuotraukos) liks ilgam, kad jo tapatybė bus randama kitų asmenų ir kuo daugiau apie save jis atskleis, tuo tapatybės vagystės rizika didės.

Tapatybės vagystės kaip socialinio-teisinio reiškinio plitimo tendencijas visų pirma identifikuoja „informacijos prieinamumo" kategorija. Pastaruoju metu internete prieinamos su asmens tapatybe susijusios informacijos vis daugėja. Atsiranda ištisa elektroninės tapatybės kultūra, kurią skatina tokie interneto bendruomenės portalai, kaip „Facebook"[127], „Twitter"[128], „MySpace"[129] ir kiti. Galima netgi teigti, kad atsiranda ištisi elektroniniai gyvenimai[130], kuriuos žmonės „gyvena" elektroninėje erdvėje.

Šiuo metu didžiausias pasaulyje socialinis tinklas yra **Facebook**. Šis tinklas turi daugiau kaip 500 mln. aktyvių vartotojų. Pagal skelbiamą sta-

[126] Eric Schmidt's Name Game Doesn't Make Sense. [interaktyvus, žiūrėta 2011-09-15]. <http://techcrunch.com/2010/08/16/eric-schmidt-change-name/ >.

[127] <www.facebook.com>.

[128] <www.twitter.com>.

[129] <www.myspace.com>.

[130] Hoikkanen A.; Bacigalupo, M.; etc. 2010. New Challenges and Possible Policy Options for the Regulation of Electronic Identity, *Journal of International Commercial Law and Technology* 5(1): 1. [interaktyvus, žiūrėta 2011-09-15]. <http://www.jiclt.com/index.php/jiclt/index>.

tistinę informaciją, 50 procentų vartotojų prie šio tinklo jungiasi kiekvieną dieną. Vidutiniškai vienas vartotojas turi 130 draugų. 150 mln. vartotojų „Facebook“ pasiekia mobiliuoju telefonu[131]. Kokie yra „Facebook“ plėtros tempai, liudija tokie faktiniai duomenys ir prognozės:

- „Facebook“ savo veiklą pradėjo 2004 metais, kaip Harwardo universiteto studentams skirtas bendravimo elektroninėje erdvėje įrankis;
- nuo 2006 metų „Facebook“ pasidarė prieinamas užsienio studentams;
- visai netolimoje ateityje planuojama, kad „Facebook“ apims 750 mln. ar net milijardą vartotojų[132], kadangi kuo didesnis „Facebook“ narių skaičius, tuo didesnis plėtimasis.

Minimo socialinio tinklo veikimas paremtas asmeninės informacijos pateikimu ir socialiniais ryšiais su kitais „Facebook“ vartotojais. „Facebook“ (angl. *face* – „veidas“, *book* – „knyga“; pažodžiui „Facebook“ – „veidaknygė“) – interneto platforma, interneto bendruomenė. „Facebook“ užsiregistravę nariai gali sukurti savo profilį (asmens aprašą), įkelti nuotraukų, paveikslėlių, vaizdo failų ir nurodyti ryšius su draugais, pažįstamais asmenimis ir kt. Bendruomenėje gali būti kuriami fotoalbumai, vidinės grupės (pagal interesus, pomėgius ir kt. kriterijus), keičiamasi žiniomis tarp grupės narių ir bendraujama kitomis formomis.

„Facebook“ pačių vartotojų dedama labai įvairi asmeninė informacija – nuo vardo ir pavardės, biografinių duomenų iki asmeninių pomėgių. Dažnai asmeninės informacijos būna tiek daug, kad asmenį labai lengva identifikuoti, nustatyti jo socialinius ryšius, susisteminti kitą asmeninę informaciją.

Kiti socialiniai tinklai veikia panašiu principu kaip ir „Facebook“. Toliau paminėt duomenys, susiję su pasauliniu mastu populiariausiais socialiniais tinklais.

Socialinis tinklas **Twitter** šiuo metu pagal vartotojų skaičių pasaulyje yra antroje vietoje. „Twitter“ – nemokama socialinių tinklų paslauga, leidžianti jos vartotojams siųsti ir skaityti trumpąsias žinutes (angl. *tweets*).

[131] <http://www.facebook.com/press/info.php?statistics>.

[132] *Facebook banga šluoja konkurentus* [interaktyvus]. 2010-07-22 [žiūrėta2011-09-18]. <http://www.lrytas.lt/-12797981811279127001-facebook-banga-%C5%A1luoja-konkurentus-jonari%C5%B3-skai%C4%8Dius-pasiek%C4%97-500-milijon%C5%B3-video.htm >.

„Tweet“ – tekstinė iki 140 simbolių žinutė, parodoma autoriaus puslapyje ir nusiunčiama jo prenumeratoriams, dar žinomiems kaip sekėjai (angl. *followers*). Autoriai gali apriboti žinučių matomumą iki savo draugų rato arba leisti žinutes matyti visiems. Vartotojai gali siųsti ir gauti žinutes per „Twitter“ svetainę, SMS arba išorines programas. Nors pati paslauga nemokama, žinučių gavimas per SMS yra mokamas – kainos nustatytos paslaugų tiekėjų. Tvirtinama, kad šiuo metu socialinis tinklas Twitter turi daugiau kaip 100 mln. vartotojų[133].

MySpace (liet. *mano erdvė*) – interneto platforma, interneto bendruomenė. 2006 metų birželio mėn. „MySpace“ tapo populiariausiu Jungtinėse Valstijose interneto bendruomenės tinklalapiu. 2008 metų balandžio mėn. „MySpace“ tarptautiniu mastu buvo aplenkta pagrindinės konkurentės internetinės bendruomenės puslapio „Facebook”.

Paminėtina, kad atskirose valstybėse veikia nacionaliniai socialiniai tinklalapiai. Pavyzdžiui, Lietuvoje vienas iš populiariausių socialinių nacionalinio masto socialinių tinkllapių – *www.klase.lt*. Šiame socialiniame tinkllapyje socialiniai ryšiai paremti esamų ir buvusių klasės draugų įsiregistravimu.

Tokie portalai asmens duomenims grėsmę kelia ne tik dėl to, kad juose viešai skelbiama daugybė asmens duomenų, tačiau dar ir dėlto, jog tokie portalai gali tapti (neretai ir tampa) elektroninių nusikaltėlių objektais. Pavyzdžiui, 2010 metais buvo paskelbta, kad pagrobta ir viešai publikuota 100 mln. „Facebook“ vartotojų asmens ir prisijungimo duomenų[134].

Vis daugiau elektroninės erdvės naudojama nusikaltimams daryti ir didėja falsifikuotos elektroninės tapatybės poreikis.

Plintant internetui, nusikaltėliai suprato, kad daug lengviau apiplėšti internetinį banką, nei tikrą banką, kurį saugo sargybiniai, įrengtos signalizacijos ir pan. Elektroninė erdvė suteikia nusikaltėliams unikalias galimybes paslėpti nusikaltimo pėdsakus, prisidengti kito asmens elektronine tapatybe ir likti nenubaustiems.

Prieš dešimtmetį ir daugiau, kai elektroninė erdvė nusikaltimams vykdyti buvo naudojama dar labai mažai, būdavo labai lengva paslėpti nusikaltimų, padarytų naudojantis internetu, pėdsakus. Be to, kad elekt-

[133] Twitter lankomumas per metus išaugo 109 proc. [interaktyvus]. 2010-08-18 22 [žiūrėta2011-09-18]. <http://www.elektronika.lt/news/computers/24804/>.

[134] Detaliau žr. <http://www.bbc.co.uk/news/technology-10796584>.

roninė informacija apskritai gali būti lengvai pakeičiama, ir ištrinama, tai lemdavo ir kitos priežastys:

- tyrimo institucijos dėl žinių stokos nesugebėdavo tinkamai surinkti elektroninių įrodymų;
- patys nukentėjusieji menkai išmanydavo, ką reikia daryti, kad elektroniniai įrodymai būtų kuo greičiau užfiksuojami;
- atsižvelgiant į tai, kad elektroniniai nusikaltimai būdavo globalūs, nebuvo tinkamų tarptautiniu mastu nustatytų teisėsaugos institucijų bendradarbiavimo mechanizmų.

Tačiau pastaruoju metu tiek tarptautiniu mastu, tiek atskirose valstybėse buvo imtasi tam tikrų žingsnių tam, kad būtų galima greičiau ir tinkamiau surinkti elektroninius įrodymus. 2001 m. buvo priimta Konvencija dėl elektroninių nusikaltimų[135], kuri, be materialinės ir procesinės teisės normų, buvo skirta tarptautinio bendradarbiavimo tiriant elektroninius nusikaltimus mechanizmui Nustatyti. Be to, 2006 metais Europos Sąjungoje buvo priimta duomenų saugojimo direktyva[136] – 2006 m. kovo 15 d. direktyva dėl duomenų, generuojamų arba tvarkomų teikiant viešai prieinamas elektroninių ryšių paslaugas arba viešuosius ryšių tinklus, saugojimo, iš dalies keičianti direktyvą 2002/58/EB. Ši direktyva nustatė reikalavimus srauto duomenims[137] išsaugoti. Šie duomenys teisėsaugos institucijoms padeda nustatyti, iš kur (elektroninio nusikaltimo atveju) buvo prisijungta, kas konkrečiai buvo prisijungęs ir pan.

Dėl minėtų priemonių nusikaltėliai pradėjo suprasti, kad atsirado daug daugiau galimybių nustatyti nusikaltimą padariusį asmenį. Dėl to pradėta galvoti apie tai, kad darant nusikaltimą galima pasinaudoti kito

[135] Convention on Cybercrime CETS No.: 185 [interaktyvus, žiūrėta 2011-09-18]. <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm >.

[136] Directive 2006/24/EC of the European parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communication services or of public communications networks and amending Directive 2002/58/EC [interaktyvus, žiūrėta 2011-09-18]. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF>.

[137] Pagal Lietuvos Respublikos elektroninių ryšių įstatymą, srauto duomenimis laikytini „duomenys, tvarkomi siekiant perduoti informaciją elektroninių ryšių tinklu ir (arba) tokio perdavimo apskaitai“. Tradicinės telefonijos atveju srauto duomenų pavyzdžiu yra informacija apie sujungimo laiką, trukmę ir skambinančiojo telefono numerį, o elektroninio pašto atveju – siuntėjo IP adresas, elektroninio pašto adresas, elektroninio pašto žinutės dydis, elektroninio pašto žinutės pavadinimas, elektroninio pašto žinutės priedų dydis ir tipas.

asmens tapatybe. Tokiu atveju nusikaltėliui nereikia slėpti nusikaltimų pėdsakų, kitaip maskuoti savo veiklos: užtenka tik pasisavinti kito asmens tapatybę ir imtis priemonių, kad nebūtų nustatytas prisijungimo vietos adresas. Dėl šios priežasties labai padidėjo suklastotos elektroninės tapatybės poreikis. Literatūroje suklastota elektroninė tapatybė skirstoma į:

1) sufalsifikuotą elektroninę tapatybę (angl. *False identity*): neegzistuojančio asmens sukūrimas kartais yra sudėtingesnis procesas ir brangiau kainuojantis, nes norint, kad tokia tapatybė būtų priimta, reikia garantuoti jos tikrumą įrašais duomenų bazėse. Nusikaltimai, kuriems atlikti reikia tokių tapatybių, dažniausiai nėra nukreipti į finansinį sektorių (dauguma tapatybės vagysčių įvyksta turint tikslą pasisavinti finansines lėšas, todėl vagiamos egzistuojančių asmenų tapatybės), falsifikuotos tapatybės naudojamos kriminaliniame pasaulyje, kai kalbama apie prekybą žmonėmis, ginklais, terorizmo rėmimą ir teroro aktų organizavimą.
2) pakeistą egzistuojančią tapatybę (angl. *Identity manipulation*)[138].

Tapatybės vagystės elektroninėje erdvėje įtakos ekonomikai didėjimas

Tapatybės vagystės elektroninėje erdvėje įtaka ekonomikai[139] vis labiau didėja. Taip pat svarbu akcentuoti tokių nusikaltimų atskleidimo ir tyrimo kainą valstybei. JAV, kur minėtų nusikaltimų skaičius nuolatos didėja, tyrimo išlaidos vidutiniškai sudaro nuo 15 iki 20 tūkstančių dolerių vienai bylai[140].

Pagal Javelin Strategy & Research atliktą tyrimą[141], JAV didėja tiek tapatybės vagystės elektroninėje erdvėje aukų, tiek šio pavojingo reiškinio žala. Detali 2003–2009 metų informacija pateikta 12 pav.

[138] Clough, J. 2010. *Principles of Cybercrime*. Cambridge University Press, p. 209.

[139] Kshetri, N. 2010. *The Global Cybercrime Industry: Economical, Institutional and Strategic Perpectives*. Springer-Verlag Berlin Heidelberg, p. 5.

[140] How Does Identity Theft Impact Human Society? *eHow.com* [interaktyvus, žiūrėta 2011-07-14] <http://www.ehow.com/about_6293396_identity-theft-impact-human-society_.html>.

[141] Identity Theft on the Rise: Survey [interaktyvus, žiūrėta 2011-09-18]. <http://gigaom.com/2010/02/10/identity-theft-on-the-rise-survey/>.

Vis daugiau vartotojų JAV susiduria su sukčiavimu.

Bendras Poveikis:

	Tyrimo ataskaita							
	Lygis	2009	2008	2007	2006	2005	2004	2003
Tapatybės vagystės aukos (>18 metų)		11.1 mln.	9.9 mln.	8.1 mln.	8.4 mln.	8.9 mln.	9.3 mln.	10.1 mln
Procentinis auku skaičius (lyginant su populiacija)		4.8%	4.3%	3.6%	3.7%	4.0%	4.3%	4.7%
Bendra tapatybės vagysčių žala (mlrd.)		$54	$48	$45	$50	$57	$60	$58

12 pav. Vis daugiau vartotojų JAV susiduria su sukčiavimu

Tapatybės vagystės tampa prielaida elektroniniam terorizmui

Tapatybės vagystė elektroninėje erdvėje kaip pavojingas reiškinys tampa vis dažniau susijusi su vadinamuoju elektroniniu terorizmu ir organizuotu elektroniniu nusikalstamumu. Tai parodė ir 2007 m. Estijos įvykiai, kai botnetas[142], kurį sudarė apie 1 milijonas kompiuterių, buvo panaudotas Estijos kompiuteriams ir kompiuterių tinklams atakuoti, dėl to buvo sutrikdytas šalies valstybinių institucijų, parlamento bei daugumos bankų darbas[143]. Dėl tokių neteisėtų veiksmų kilo grėsmė daugeliui Estijos valstybės institucijų interneto svetainių (daugelis jų patyrė vienokio ar kitokio pobūdžio sutrikimų). Nusikalstami veiksmai elektroninėje erdvėje prieš Estiją buvo organizuojami slepiant nusikaltėlių tapatybes. Beje, tokie veiksmai gali būti vertinami ir kaip elektroninis terorizmas[144].

Didėjantys tapatybės vagystės elektroninėje erdvėje mastai daro įtaką elektroniniam verslui ir elektroninėms viešosioms paslaugoms

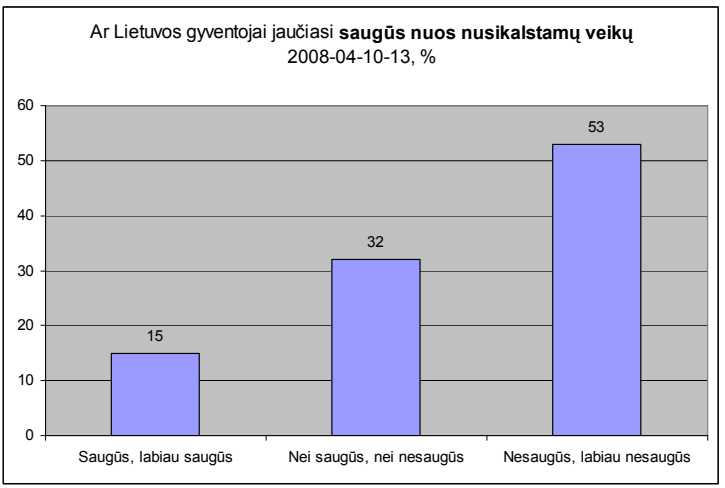
Pagal autorių atliktą tyrimą į klausimą, „ar vengiate naudotis viešosiomis elektroninėmis paslaugomis dėl tapatybės vagystės elektroninėje erdvėje grėsmės“, 43,2 proc. vartotojų atsakė „taip“. Taip pat pažymėtina,

[142] Sujungtų į bendrą tinklą ir trečiosios šalies valdomų kompiuterių tinklas (angl. *botnet*) – turbūt yra viena didžiausių tinklų ir informacijos saugumo problemų. Botas (nuo žodžio robotas) – tai apkrėstas kenksmingu programiniu kodu kompiuteris, kuris specialiomis komandomis gali būti valdomas nuotoliniu būdu. Keletas tokių kompiuterių sudaro vadinamąjį botų tinklą. Toks kompiuterių „zombių” tinklas gali būti valdomas bendromis komandomis ir atlikinėti didelio masto atakas, kokios buvo aprašytos ankstesniuose skyriuose.

[143] Kshetri N. 2010. *The Global Cybercrime Industry: Economic, Institutional and Strategic Perpective*. Springer-Verlag, p. 7.

[144] Russia accused of unleashing cyberwar to disable Estonia. *Guardian.co.uk*. [interaktyvus]. 2007-05-17 [žiūrėta 2011-09-18]. <http://www.guardian.co.uk/world/2007/may/17/topstories3.russia>.

kad net 50 proc. vartotojų atsakė, jog dėl tos pačios priežasties vengia naudotis elektroninio verslo paslaugomis. Be to, respondentai vartotojai, kurie naudojasi elektroninio verslo paslaugomis, baimę nukentėti nuo tapatybės vagystės dešimties balų sistemoje įvertino vidutiniškai 7,24 proc. Dažniausiai pasitaikantis atsakymas buvo 10 balų. Autorių atliktas vartotojų tyrimas taip pat parodė, kad 85,8 proc. apklaustųjų nesijaučia saugūs atskleisdami savo duomenis internete (detalesni autorių atliktų tyrimų duomenys pateikti monografijos 5.2.2 dalyje). Nors tiesiogiai rodiklių lyginti negalima, paminėtina, kad tik 53 proc. Lietuvos gyventojų jaučiasi nesaugūs dėl nusikalstamų veikų apskritai. Gauti tyrimo duomenys pavaizduotini diagramoje[145]:



13 pav. Lietuvos gyventojų saugumo pojūtis nusikalstamų veikų atžvilgiu

Tai reiškia, kad tapatybės vagystės rizikos atveju nesaugumas yra daug didesnis nei apskritai kitų nusikalstamų veikų atveju.

Taigi, elektroninėje erdvėje tapatybės vagystės galimybė naudojantis viešosiomis elektroninėmis ir elektroninio verslo paslaugomis yra labai didelė ir ateityje plintant elektroninės erdvės naudojimui (ir nesiimant veiksmingų prevencijos priemonių), matyt, tik didės.

[145] Starkus S., Kiškis A. 2008. Kam reikalingos prevencinės programos ir projektai? Kodėl prevencija, kodėl turime rengti prevencines programas ir/ar projektus? *Kriminologijos paskaitų konspektas*, p. 2.

Apibendrinančios išvados:

• Gana aukštas ir vis didėjantis interneto naudojimo rodiklis lemia vis didesnį asmeninės informacijos naudojimą elektroninėje erdvėje. Šiuo metu nepakankamai naudojama saugios tapatybės nustatymo platformų, todėl elektroninės tapatybės naudojimo nesaugumo lygis didėja.

• Elektroninis tapatybės duomenų naudojimas tampa masiniu reiškiniu, keliančiu vis daugiau grėsmės asmenims, kurie naudojasi elektroninės erdvės teikiamomis galimybėmis. Viena iš pavojingiausių grėsmių elektroninėje erdvėje yra tapatybės vagystė.

• Elektroninėje erdvėje ne tik plinta asmeninė informacija ir daugėja prieinamos su asmens tapatybe susijusios informacijos, bet taip pat daugėja ir išgalvotos arba nepatikimos asmeninės informacijos – tai lemia aplinkybę, kad internete nėra nustatyta informacijos tikrinimo mechanizmų.

• Tapatybės vagystė elektroninėje erdvėje kaip pavojingas reiškinys vis dažniau siejama su vadinamuoju elektroniniu terorizmu ir organizuotu elektroniniu nusikalstamumu. Didėja neigiama įtaka elektroninėms viešosioms paslaugoms ir elektroniniam verslui. Nesaugumo jausmas tapatybės vagystės rizikos atveju yra daug didesnis nei apskritai nusikalstamų veikų atveju.

1.7. Tapatybės vagystės elektroninėje erdvėje subjektai ir aukos

1.7.1. Tapatybės vagystės elektroninėje erdvėje subjektai[146]

Kas yra tapatybės vagystės subjektai (asmenys, kurie atlieka arba gali atlikti šią veiką)? Tai klausimas, į kurį atsakymas svarbus siekiant tinkamai įvertinti ir pasiūlyti neigiamą poveikį darančios veikos prevencijos priemones. Atsakius į klausimą, kas gali būti tapatybės vagystės elektroninėje erdvėje subjektai, galima sudaryti atitinkamą šios veikos subjektų klasifikaciją, leidžiančią nustatyti pagrindinius nusikaltėlių bruožus ir jų veikimo specifiką, tikslus ir motyvus – visa tai tapatybės vagystės atveju nukreiptų tinkama linkme tiriant pavojingą veiką, ieškant ją atlikusio asmens ir svarbiausia pasirenkant veiksmingiausias prevencijos priemones, kad ateityje būtų dar labiau sumažinta tapatybės vagystės rizika.

[146] Tapatybės vagystės elektroninėje erdvėje subjektai bus nagrinėjami reiškinį vertinant tik baužiamosios teisės aspektu, t. y. traktuojant kaip nusikalstamą veiką.

Nors tapatybės vagystės elektroninėje erdvėje subjektus, kaip ir visus elektroninius nusikaltėlius, reikėtų vertinti kaip visumą, tačiau pagal tam tikrus požymius galima išskirti atskiras jų rūšis ir grupes. Dažniausiai elektroniniai nusikaltėliai yra studentai, mėgėjai, teroristai, nusikalstamų grupuočių nariai, tačiau skiriasi jų padarytų nusikaltimų pobūdis. Asmuo, kuris įsilaužia į kompiuterių sistemą neturėdamas nusikalstamų ketinimų, skiriasi nuo finansinės institucijos darbuotojo, kuris vagia pinigus iš klientų sąskaitų. Labai skiriasi elektroninių nusikaltėlių įgūdžių lygis. Be to, elektroniniai nusikaltėliai būna iš skirtingų visuomenės sluoksnių ir jų amžius vidutiniškai svyruoja nuo 10 iki 60 metų, įgūdžių lygis – nuo naujoko iki profesionalo[147].

Atsižvelgiant į tai, kad tapatybės vagystė elektroninėje erdvėje yra viena iš elektroninių nusikaltimų rūšių, galima išskirti tokią mokslinėje literatūroje dažniausiai taikomą elektroninių nusikaltimų subjektų klasifikaciją[148], remiantis tokio pobūdžio nusikaltimų įvykdymo motyvu:

1) programišiai (hakeriai): šie asmenys labai gerai išmano programas ir tinklų kūrimo procesus, todėl ieško kompiuterinės įrangos trūkumų ir dažniausiai nori tik patekti į sistemą ir pademonstruoti savo sugebėjimus, o ne padaryti žalą. Didžiausią dalį tokio tipo nusikaltėlių sudaro paaugliai, kurie nors ir pasižymi gerais protiniais gebėjimais, dažniausiai prastai mokosi arba visai nelanko mokyklos;

2) tipiniai nusikaltėliai: kai programišiai (hakeriai) suvokia, kad iš savo veiklos gali gauti finansinės naudos, jie pereina į kitą – tipinių nusikaltėlių grupę, kurios tikslas yra gauti finansinės naudos arba atitinkami politiniai, religiniai motyvai. Šią subjektų grupę dažniausiai sudaro suaugę žmonės, turintys nusikalstamų ketinimų, pasireiškiančių tokiomis pavojingomis veikomis, kaip sukčiavimas, šnipinėjimas, šantažas, pinigų plovimas ar net teroro aktai. Pasikėsinimo objektais dažniausiai tampa bankai ir kredito įstaigos, taip pat didelius asmens duomenų kiekius tvarkančios valstybės institucijos, strateginę reikšmę nacionaliniam saugumui arba didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinčios informacinės sistemos;

[147] Kiškis, M.; Petrauskas, R.; Rotomskis, I.; Štitilis, D. 2006. *Teisės informatika ir informatikos teisė*. Vilnius: Mykolo Romerio universitetas, p. 242.

[148] Tapatybės vagystės elektroninėje erdvėje subjektų neteisėtų veikų atlikimo būdai nurodomi monografijos 2.1 dalyje.

3) vandalai: šios kategorijos asmenys elektroninius nusikaltimus įvykdo iš kerštо, pykčio, nusivylimo, tačiau ne tam, kad pademonstruotų savo protinius gebėjimus ar būtų skatinami finansinių, politinių motyvų. Pagrindinis šių nusikaltėlių tikslas – savo aukai padaryti kuo daugiau žalos – tiek turtinės, tiek neturtinės.

Tapatybės vagystės elektroninėje erdvėje subjektai – dažniausiai yra asmenys, gerai išmanantys kompiuterio sąrangą ir programavimo subtilybes, galintys nesunkiai įsilaužti į vieną ar kitą kompiuterį ar apeiti duomenų apsaugos priemones ir gauti prieigą prie duomenų bazių ir (ar) informacinių sistemų. Atsižvelgiant į tai, kad tapatybės vagystė elektroninėje erdvėje gali būti įvykdyta pasinaudojant įvairiomis informacinėmis ir ryšio technologijomis, jos subjektus galima klasifikuoti, remiantis nusikalstamų veikų padarymo būdų kriterijumi:

1) įsilaužėliai (krakeriai) (angl. *cracker*) – tai asmenys, įsilaužiantys į informacines sistemas;

2) frekeriai (angl. *phreak*) – tai asmenys, kurie vykdo elektroninius nusikaltimus, pasinaudodami elektroniniais ryšiais ir specialiomis priemonėmis perima konfidencialią informaciją;

3) karderiai (angl. *carder*) – tai asmenys, vykdantys elektroninius nusikaltimus, susijusius su kreditinių kortelių apyvarta.

Reikėtų paminėti ir elektroninių nusikaltėlių klasifikaciją, paplitusią Rusijoje: elektroninių nusikaltimų subjektai skirstomi į tris grupes[149]:

1. Pirmajai grupei priklauso kompiuterių technikos profesionalai, programavimo žinovai. Jiems būdingas tam tikras fanatizmas ir išradingumas. Kai kurių autorių manymu, šie subjektai kompiuterių technikos priemones vertina kaip tam tikrą iššūkį siekiant parodyti profesionalias žinias. Būtent tai ir yra pagrindinis stimulas įvykdyti veikas, kurių didžioji dalis yra nusikalstamos. Reikia paminėti dar vieną šios grupės požymį – šie nusikaltėliai neturi jokių konkrečių tikslų pažeisti įstatymo. Faktiškai visus veiksmus jie atlieka norėdami pademonstruoti intelektualinius ir profesinius gebėjimus. Šios grupės atstovai yra gana žingeidūs, aukšto intelekto, taip pat pasižymi tam tikru „sportiniu azartu“. Jie bet kokiomis priemonėmis nori įrodyti, kad gali valdyti kompiuterius. Paprastai tai ir skatina padaryti nusikaltimą.

[149] Kiškis, M.; Petrauskas, R.; Rotomskis, I.; Štitilis, D. 2006. *Teisės informatika ir informatikos teisė*. Vilnius: Mykolo Romerio universitetas, p. 247.

Kartais bėgant laikui šios kategorijos žmonės ne tik įgyja patirties, bet keičiasi ir jų interesai. Iš savo veiklos jie pradeda ieškoti materialinės naudos. Tokiu būdu programuotojas mėgėjas virsta profesionaliu nusikaltėliu.

2. Šiai grupei artima ir kita nusikaltėlių grupė, serganti naujomis psichikos ligomis, t. y. informacinėmis ligomis ir kompiuterinėmis fobijomis.

Nurodyti susirgimai kyla žmogui, sistemingai pažeidžiančiam informacinį režimą: arba informacinio bado, arba informacinės perkrovos. Šių klausimų tyrimu užsiima gana nauja medicinos šaka – informacinė medicina. Vertinant iš šios šakos pozicijų, žmogus suprantamas kaip universali, save reguliuojanti informacinė sistema su nustatytu biologinės informacijos balansu. Balansą pažeidus dėl vidinių ar išorinių destabilizavimo veiksnių susergama įvairiomis informacinėmis ligomis, iš kurių labiausiai paplitusios informacinės neurozės. Kitais žodžiais tariant, žmogui reikia vienodos tiek fizinės, tiek informacinės apkrovos. Kai jos mažai, ateina informacinis badas, kai daug – žmogus kenčia nuo informacinės perkrovos (pasireiškia įvairūs stresai ir emociniai protrūkiai). Visa tai gali peraugti į informacinę ligą. Esant dabartiniam kompiuterizavimo lygiui, daugelis darbuotojų patenka į stresines situacijas, kurios kai kada baigiasi kompiuterine fobija. Tai ne kas kita, kaip profesinė liga. Jos simptomai tokie: greitas nuovargis, staigūs kraujospūdžio šuoliai, galvos svaigimas ir skausmas, galūnių drebėjimas ir t. t. Faktiškai atsiranda baimė prarasti savikontrolę.

Taigi elektroninius nusikaltimus gali vykdyti žmonės, sergantys minėtomis psichikos ligomis. Tiriant tokį elektroninį nusikaltimą, būtina skirti teismo psichiatrinę ekspertizę, kad būtų nustatyta kaltinamojo psichinė būklė nusikaltimo padarymo metu (ar tai nebuvo afekto būsena arba nepakaltinamumas).

Dažniausiai šios grupės nusikaltėliai, iš dalies arba visiškai praradę kontrolę, fiziškai naikina kompiuterius (be nusikalstamų ketinimų).

3. Trečiąją grupę sudaro profesionalūs elektroniniai nusikaltėliai. Į šią grupę įeina žmonės, turintys aiškių nusikalstamų ketinimų. Skirtingai nuo pirmųjų dviejų grupių, jų veikos nebūna vienkartinės. Dažniausiai savo nusikaltimus jie slepia. Paprastai šie žmonės būna gerai organizuotų grupių, aprūpintų specialia technika (neretai operatyvine), nariai. Tai kvalifikuoti specialistai, turintys techninį, aukštąjį juridinį ar ekonominį išsilavinimą. Būtent ši grupė visuomenei ir kelia didžiausią grėsmę.

Daugelis žmonių nerimauja, kad programišiai gali pasisavinti jų slaptažodžius arba nusikaltėliai, pasinaudodami „šiukšlių rinkimo“ metodu, pavogti jų finansinius dokumentus. Tačiau didžioji dalis tapatybės vagystės elektroninėje erdvėje atvejų yra įvykdoma aukai artimiausių ir brangiausių žmonių arba tų, kuriuos nukentėjęs asmuo tikrai pažįsta: tai gali būti giminės, draugai, bendradarbiai, kaimynai ar netgi šeimos nariai. Dažniausiai tapatybės vagystės aukos net nenutuokia, kokiu būdu buvo pasisavinti jų asmens duomenys ir (ar) asmeninė informacija, ir tik nedaugelis gali įvardyti arba įtarti nusikaltėlį, nuo kurio veikos nukentėjo.

Finansų ekspertė Liz Pulliam Weston teigia, kad tapatybės vagystė yra tokia paplitusi, kad būtina imtis priemonių savo finansinei informacijai apsaugoti ir visada akylai stebėti jūsų gyvenime esančius asmenis. Ji išskiria aštuonis įspėjamuosius požymius, kurie gali padėti atpažinti tapatybės vagystės subjektą (subjektų kategorijas):

1) asmuo, kenčiantis nuo priklausomybės, kuriam žūtbūt reikalingi pinigai, pavyzdžiui, narkomanas, lošėjas ar alkoholikas, kurie linkę įvykdyti tapatybės vagystę, kad tik patenkintų savo žalingą įprotį. Internete taip pat yra daugybė mokamų lošimo svetainių ir pornografijos tinklalapių, už kuriuos gali būti atsiskaitoma vogta arba pasinaudojant šeimos nario ar draugo kreditine kortele.

2) asmuo, viskam randantis pasiteisinimą: kad ir kas nutiktų, toks asmuo teigia, kad tai nutiko ne dėl jo kaltės ir viską randa racionalų paaiškinimą. Kai kurie savo elgesį netgi įvardija kaip „nusikaltimą be aukų“. Pavyzdžiui, tėvai, pasinaudoję savo vaiko socialinio draudimo numeriu, siekdami naudos, gauti kredito kortelę ar paskolą, gali kategoriškai neigti, kad jie padarė kažką blogo ir net gali bandyti nuteikti kitus šeimos narius prieš nepasitenkinimą reiškiantį vaiką.

3) pasiturintis dykaduonis, kuris, siekdamas gauti paskolą, „pasiskolina“ gerą kito asmens vardą: sukčiai, išeikvotojai, apsimetėliai, tapatybės vagys – visi jie gyvena geriau, nei leidžia jų finansinės galimybės.

4) asmuo, priskiriamas „turiu tai gauti“ kategorijai: tokiam asmeniui sunku kontroliuoti savo impulsus. Šiam tipui gali būti priskiriami tiek tie, kurie kenčia nuo vienokios ar kitokios priklausomybės, tiek tie, kurie randa savo veiksmams pateisinimą, bet dažniausiai tai yra išlaidūnai, kurie tai, ko nori, siekia gauti tada, kai tik užsimano. Tai, pavyzdžiui, gali būti paauglys, kuriam buvo pasakyta, kad tam tikro daikto jis negali

turėti, pasisavindamas vieno iš tėvų kreditinę kortelę, neįvertina visų pasekmių. Taip pat tai gali būti asmuo, manantis, kad „nusipelnė“ daugiau, nei gali sau teisėtai leisti.

5) smalsusis draugas: toks asmuo gali būti netikėtai užkluptas sėdintis prie jūsų kompiuterio ir (ar) naršantis po jūsų asmeninius dokumentus, be to, gali užduoti gana konkrečių klausimų apie jūsų finansus ar siekti sužinoti informaciją, kuri tikrai nėra jo reikalas. Toks asmuo gali būti tiesiog įkyrus, tačiau taip pat gali turėti ir piktų ketinimų.

6) pavyduolis: tai gali būti kerštingas buvęs sutuoktinis, buvęs mylimasis, buvęs draugas (*ex* kategorija), kuris per gana trumpą laiką gali jūsų gyvenime sukelti daug sumaišties, nes tikriausiai apie jus žino viską, ko, pavyzdžiui, reikia atidarant naują sąskaitą banke, ir turi motyvą paversti jūsų gyvenimą apgailėtinu.

7) recidyvistas: tapatybės vagystės subjektai žino, kad tikimybė, jog už tokio pobūdžio veiką jie bus patraukti atsakomybėn, yra gana maža, o tie, kurie savo aukomis pasirenka šeimos narius arba draugus, dar labiau sumažina tokią tikimybę, kadangi dauguma nukentėjusiųjų vengia pareikšti kaltinimus artimiems žmonėms.

8) nepažįstamasis, turintis prieigą: net ir labai malonūs žmonės savo gyvenime gali toleruoti tuos, kurie yra tikri niekšai. Pavyzdžiui, jūsų vertinama namų tvarkytoja gali būti ištekėjusi už sukčiaus, kuris gali pasinaudoti palankiomis sąlygomis tapatybės vagystei įvykdyti[150].

Pažymėtina, kad pateiktos tapatybės vagystės subjektų klasifikacijos yra gana sąlyginės, kadangi sudaryti tapatybės vagystės elektroninėje erdvėje baigtinį sąrašą, klasifikuojant subjektus pagal vieną kokį nors kriterijų, yra sudėtinga.

Apžvelgiant rezonansinius tapatybės vagystės elektroninėje erdvėje atvejus galima daryti prielaidą, kad tai pavienių sukčių, gerai išmanančių šiuolaikines kompiuterines technologijas, atliekamos veikos. Tačiau su tokia nuomone nesutinka Judith M. Collins, kuri monografijoje „Tapatybės vagystės tyrimas. Vadovas verslui, įstatymus įgyvendinančioms institucijoms ir nuo jos nukentėjusiems (angl. „*Investigating Indenty Theft. A Guide*

[150] 8 požymiai, padedantys atpažinti tapatybės vagystės subjektą. [interaktyvus, žiūrėta 2011-07-09]. <http://articles.moneycentral.msn.com/Banking/FinancialPrivacy/8SignsYouMayKnowAnIdentityThief.aspx>.

for Businesses, Law Enforcement, and Victims“)[151] pateikia savo poziciją, kad toks siauras problemos suvokimas ir trukdo matyti reiškinio sudėtingumą, kompleksiškumą ir tirti nusikaltimus. Judith M. Collins nuomone, tapatybės vagystė yra tinklinis nusikaltimas, nes didžioji dauguma tokio pobūdžio veikų atliekama itin gerai organizuotų grupių[152]. Judith M. Collins išsako kategorišką nuomonę, kad nei fizinio asmens tapatybės vagystė, nei verslo tapatybės vagystė neatliekama pavienio nusikaltėlio: tapatybės vagystės paprastai įtraukia visą tinklą asmenų, kurie yra daugiau arba mažiau organizuoti ir veikia grupelėmis, kurios atlieka skirtingas, bet susijusias funkcijas. Tokiu atveju tiriant nusikaltimus yra didelė klaida suimti pavienį, lengviausiai pastebimą asmenį, neištyrus veikos plačiau, nes taip sulaikomi tik žemiausio lygio nusikaltėliai, nusikaltėlių grupelės, atsakingos už, pavyzdžiui, pašto dėžučių atidarymą, sukčiavimo būdu gautų prekių paėmimą ar pan. Grupelių lyderiai ir kiti hierarchiškai organizuoto tinklo nariai lieka neatskleisti: priklausomai nuo tinklo dydžio, sulaikytieji asmenys dažnai nežino grupelės lyderių vardų ar asmenų, kurie vagia duomenis, ar net vietos, iš kurios jie pavogti. Tai tokia organizacinė struktūra, kai atskiros grupelės atlieka atskiras funkcijas, įgyvendina daugiasluoksnį nusikaltimą ir paslepia pavojingus nusikaltėlius. Asmenų, atliekančių nesudėtingas funkcijas, areštas duoda visiems įspėjimą, kuris greitai pasklinda per visą tinklą, grupių nariai pasislepia, taigi, tapatybės vagystės tinklas lieka neištirtas ir tapatybės vagystės tęsiasi. Judith M. Collins pateikia pavyzdį[153], kai vieno didmiesčio policija neskubėjo areštuoti žemiausios grandies vykdytojų ir ištyrė didelį tapatybės vagysčių tinklą. Kaip specifinį ir įdomų pavyzdį, autorė pateikia „al Qaeda“: ši organizacija, kurios tikslas yra ne tapatybės vagystės, o teroro aktų, panaudojant visas priemones, organizavimas, savo nariams pateikia žinyną, kaip vykdyti tapatybės vagystes ir pasinaudoti pavogta tapatybe.

Judith M. Collins išsakyta pozicija ir pateikti pavyzdžiai yra įdomūs, pagrindžiantys, kad organizuota tapatybės vagystė yra paplitusi, tačiau šios monografijos autoriai nemano, kad visos tapatybės vagystės atliekamos tik organizuotų nusikaltėlių grupuočių. Tokią poziciją patvirtina

[151] Collins, M. J. *Investigating Identity Theft: A Guide for Businesses, law Enforcement, and Victims*. John Wiley & Sons, Inc., 2006.

[152] *Ibid*., p. 18.

[153] *Ibid*., p. 19.

ir pavienių programišių didžiavimasis patekus į asmens duomenų tvarkymo bazes. Vienas iš pavyzdžių: Lietuvoje įdiegus SODRA elektroninio nuotolinio prisijungimo bazes EDAS ir EGAS, programišius Delfi portalo žurnalistams pademonstravo, kaip nesudėtinga jas pažeisti, pasiekti asmens duomenis ir sukelti kitokios žalos. Dėl to buvo laikinai uždrausti bet koks prisijungimas per elektroninių valdžios vartų portalą prie visų Registrų centro, „Sodros", Valstybinės mokesčių inspekcijos duomenų[154]. Tai rodo, kad įrangos trūkumai (programinės ar aparatinės) ir atskirų asmenų veiksmai, kylantys dėl skirtingų motyvų (pvz.: noro išgarsėti, pakelti „kvalifikaciją", įgyti autoritetą tarp kitų panašia veikla užsiimančių asmenų, reklamuoti savo paslaugas, žeminti jiems nepatinkančių institucijų reputaciją ir kt.) gali sudaryti sąlygas atskleisti ar pasisavinti asmens duomenis, sukelti nuostolius asmenims ir valstybės institucijoms ir (arba) sutrikdyti svarbių valstybės institucijų veiklą bei mažinti asmenų pasitikėjimą veikla (privačia ar viešąja), vykdoma elektronine forma.

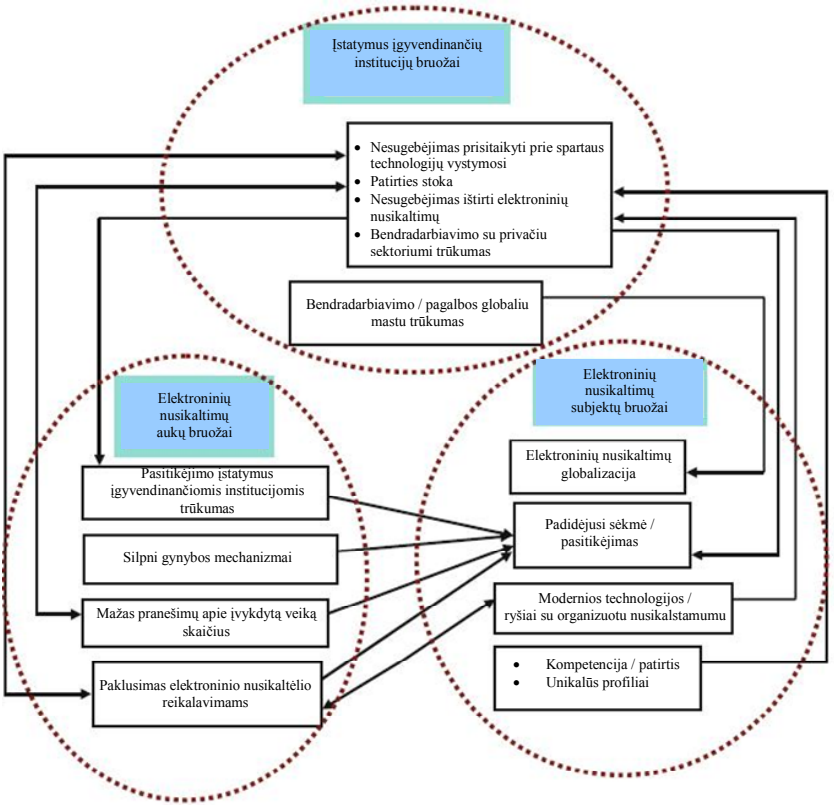
Atsižvelgiant į monografijos 2.1. dalyje aptartą tapatybės vagystės fizinėje ir elektroninėje erdvėje vykdymo būdų įvairovę, šios veikos pavojingumą, mastą ir latentiškumą, galima daryti išvadą, kad tapatybės vagystės subjektai gali būti ne tik kompiuterių genijai ar eiliniai elektroninės erdvės naudotojai kaip pavieniai asmenys, bet ir organizuotos elektroninių nusikaltimų grupės, taip pat įprasti kišenvagiai, įstaigos darbuotojai, turintys prieigą prie informacinių sistemų ir siekiantys pasipelnyti. Vienas požymis yra bendras – tapatybės vagystės elektroninėje erdvėje subjektai gerai moka naudotis kompiuteriais, internetu ir išmano tapatybės nustatymo mechanizmą[155]. Be to, įvertinant tai, kad tapatybės vagystė yra kompleksinis ir sudėtingas reiškinys, dažnai naudojamas kaip priemonė kitiems nusikaltimams įvykdyti, tapatybės vagystės subjektai taip pat gali būti asmenys, susiję su prekyba narkotikais, prekyba žmonėmis, pinigų plovimu, teroro išpuoliais, kurie naudojasi kitų asmenų tapatybėmis tam, kad nebūtų susekti ir patraukti atsakomybėn. Taigi tapatybės vagystės subjektu gali tapti bet kas: nuo kaimyno, kuris fiziškai negalėtų

[154] *Elektroninių valdžios vartų portalas dėl saugumo spragų sustabdė savo veiklą neribotam laikui* [interaktyvus]. 2010-07-12 [žiūrėta 2011-10-04]. <http://www.technologijos.lt/n/mtl/S-13875/straipsnis?name=S-13875&l=1&p=1>.

[155] *Understanding and Mitigating Identity Theft*. 2009. Thomson Reuters, p. 29.

nieko nuskriausti, ir kuris yra įsitikinęs, kad tapatybės vagystė – tai nusikaltimas be aukų, iki užkietėjusių nusikaltėlių, kuriems tapatybės vagystė yra priemonė kitiems nusikaltimams įvykdyti.

Pažymėtina, kad labiausiai tapatybės vagystės elektroninėje erdvėje subjektus veikti pažeidžiant teisės aktus skatina vartotojų technologinių ir saugaus elgesio elektroninėje erdvėje žinių trūkumas ir teisėsaugos institucijų patirties elektroninių nusikaltimų srityje trūkumas. Atsižvelgiant į tai, tarp vartotojų, tapatybės vagystės elektroninėje erdvėje subjektų ir teisėsaugos institucijų susidaro užburtas ratas, kurį grafiškai galima pavaizduoti taip:



14 pav. Elektroninių nusikaltimų struktūra: užburtas ratas
(Nir Kshetri. 2010. *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives*. Springer-Verlag, p. 39.

Nepaisant plataus tapatybės vagystės elektroninėje erdvėje subjektų rato, literatūroje pateikiama ir tokių minčių, kad dažniausiai motyvas atlikti tapatybės vagystę elektroninėje erdvėje kyla narkomanams, kurie neturi nuolatinio pajamų šaltinio. Užuot įsilaužę į automobilius ar būstus, tokie žmonės vykdo tapatybės vagystę ir kitus susijusius nusikaltimus[156]. Visgi tokia nuomonė gali remtis neišsamiomis žiniomis. Tapatybės vagystės elektroninėje erdvėje subjektus aprašyti labai sunku, nes nesant aiškiai apibrėžto reiškinio, sunku identifikuoti statistiką ir asmenis, vykdančius tokius nusikaltimus. Autorių nuomone, ateityje, aiškiau apibrėžus šį reiškinį, galimi detalūs ir patikimi tyrimai dėl šias pavojingas veikas vykdančių asmenų.

1.7.2. Tapatybės vagystės elektroninėje erdvėje aukos

Aptariant visuomenei pavojingas veikas, svarbu nustatyti asmenis, kurie gali tapti potencialiomis tokių veikų aukomis, kadangi galimas nukentėjusiųjų skaičius yra vienas iš kriterijų, kuriais remiantis vertinamas veikos pavojingumas.

Socialinis mokslas, nagrinėjantis nusikaltimų aukos aspektus, yra viktimologija. Tapę aukomis, žmonės patiria fizinę, emocinę, dvasinę, materialinę ir kitokią socialinę (pvz., moralinę) žalą. Viktimologija tyrinėja šios žalos mastą ir aukos bei skriaudėjo santykių ryšį. Taip pat ji tyrinėja visuomenės reakciją į aukos padėtį, baudžiamojo (ir socialinio) teisingumo vyksmą ir aukų problemų sprendimo kokybę, aukų pastangas kompensuoti patirtą įvairią žalą[157]. Šioje dalyje autoriai siekia atlikti nuodugnią nuo tapatybės vagystės elektroninėje erdvėje nukentėjusio asmens – aukos analizę ir išsamiai atskleisti viktimologijos aspektus. Tapatybės vagystės elektroninėje erdvėje viktimologijos aspektai – besivystanti mokslo sritis. Autoriai nori pabrėžti, kad ši sritis labai svarbi, suvokiant tapatybės vagystę elektroninėje erdvėje kaip aktualų reiškinį, ir siekia pateikti keletą reikšmingiausių viktimologijos aspektų.

Šiuo metu auka suprantama kaip asmuo, kuris patyrė žalą, finansinių nuostolių, neteisybę, sunkų išmėginimą, negatyvius moralinius išgyveni-

[156] *Understanding and Mitigating Identity Theft*. 2009. Thomson Reuters, p. 30.

[157] Ancelis, P. 2000. Dėmesingumas nusikaltimo aukai kaip prielaida kuriant atvirą visuomenę. Teisinės valstybės link. *Jurisprudencija* 15(7): 154.

mus ar psichologinį diskomfortą, t. y. asmuo, nukentėjęs nuo pavojingos ir (ar) priešingos teisei veikos ar nelaimingo įvykio. Nusikaltimų aukos gali būti asmenys (tiek fiziniai, tiek juridiniai), patyrę žalą dėl neteisėto veikimo arba neveikimo. Tiesioginės aukos pirmiausia susiduria su nusikalstamu elgesiu ir iš jo išplaukiančiomis pasekmėmis. Netiesioginės aukos (pvz., nusikaltimų aukų šeimos nariai) taip pat patiria neigiamus emocinius ir dvasinius išgyvenimus arba materialinę žalą. Įvairių rūšių žala gali būti padaroma skirtingoms socialinėms grupėms, socialiniams gyventojų sluoksniams ar net visiems gyventojams (pvz., karo metu), atskiroms valstybėms ar net ir visai žmonijai (pvz., biosferos naikinimas, kosminės katastrofos)[158].

Aukos ir jos elgesio analizė svarbi ir ieškant konkretaus nusikaltimo prevencijos būdų, nes neretai pati auka tiesiogiai arba netiesiogiai prisideda prie nusikaltimo padarymo. Vis dėlto, klaidinga manyti, kad dėl nusikaltimo visais atvejais kaltos aukos, nes dažnai pasitaiko situacijų, kai nukentėjusysis buvo ėmęsis visų atsargumo priemonių ir naudojosi asmens duomenimis, laikydamasis visų duomenų saugos reikalavimų, aukos veikoje nebuvo neatsargumo, skatinančio nusikaltėlį veikti, tačiau vis tiek nebuvo išvengta tapatybės vagystės elektroninėje erdvėje, kadangi nusikaltėlis, besidomintis informacinių technologijų naujovėmis ir puikiai išmanantis programinės įrangos kūrimo principus, šios srities žiniomis buvo pranašesnis už savo auką.

Mokslinių tyrimų statistika parodo, kiek procentų aukų išprovokavo žudikus (pvz., pirmieji pradėdami muštynes ir kt.), kiek yra iššaginimo aukų (kurios, pvz., išoriškai leido suprasti, kad sutinka seksualiai santykiauti, tačiau vėliau pakeitė nuomonę ir kt.), kiek apiplėšimų buvo paskatinta demonstruojant prabangius daiktus (pvz., juvelyriniai dirbiniai, didelės pinigų sumos ir kt.) tam netinkamoje aplinkoje (pvz., rajonuose, kur itin didelis nusikalstamumas, ir kt.). Atsižvelgiant į tai, kyla klausimas: kokias aplinkybes tapatybės vagystės elektroninėje erdvėje atveju reikėtų vertinti kaip nusikaltimo skatinimą ir ar jos priklauso tik nuo aukos ar nuo trečiojo asmens, t. y. „tarpininko“, skatinančio nusikaltėlio norą nusikalsti?

Apskritai elektroninėje erdvėje įvykdyti tapatybės vagystę skatina keli veiksniai. Vienas iš jų yra nepakankama asmens duomenų apsauga,

[158] Babachinaitė, G. 2003. *Nusikalstamumo ir kitų nepageidautinų socialinių procesų prevencijos problemos bei jų sprendimo būdai Europos valstybėse*. LTU, p. 202.

įskaitant ir neprotingus, kartais neadekvačius asmens veiksmus su asmens duomenimis. Labai svarbu įvertinti, ar asmuo suvokia, kad jis neapdairiai elgiasi su asmens duomenimis (pvz., pateikdamas juos į plačiai paplitusius socialinius tinklus asmuo nemano, kad atskleisti duomenys padarys žalos, nors nusikaltėliai įgunda juos panaudoti nusikaltimams daryti).

Atkreiptinas dėmesys, kad vartotojui sudėtinga rasti patikimos informacijos apie galimas grėsmes jo privatumui internete ar kitoje elektroninėje terpėje. Kaip nurodyta monografijos 4.3. dalyje, vartotojai labiausiai pasigenda viešos informacijos apie tapatybės vagystę elektroninėje erdvėje. Tačiau dažnai aukos elgesį nulemia ne nežinojimas, o tai, kad nusikaltėlis, gerai išmanantis psichologiją, neretai apsimeta kitu asmeniu (pvz., giminaičiu, banko tarnautoju, specialių valstybės tarnybų atstovu ir kt.) ir pasinaudojęs naivumu bei pasitikėjimu, prašo aukos atsiųsti svarbius duomenis, kurių jam pakanka nusikalstamai veikai įvykdyti, ar net pervesti pinigus į nusikaltėlio nurodytą banko sąskaitą arba perduoti kitu būdu.

Atsižvelgiant į tai, kad didelė dalis asmens duomenų ir asmeninės informacijos dedama į kitų asmenų sukurtas duomenų bazes ir informacines sistemas (fizinių, privačių juridinių, valstybės ir savivaldybės ar tarptautiniu mastu ir kt.) (pvz., asmuo atskleidžia savo asmens duomenis pildydamas anketas, pateikdamas privalomus valstybei pateikti duomenis ir kt.), didelę nusikaltimų elektroninėje erdvėje „skatintojų“ dalį ir sudaro šie tarpininkai. Pavyzdžių, kai tokie tarpininkai atskleidžia arba nesugeba apsaugoti duomenų, apstu, žiniasklaidoje pateikiama net tokių pavyzdžių, kai pasisavinamas didžiulis kiekis itin svarbių asmens duomenų (įskaitant informaciją apie asmenų turimas lėšas) iš valstybinių institucijų (pavyzdžiai pateikti monografijos 1.2.1. dalyje).

Taigi aukos pagal įsitraukimą į nusikaltimą gali būti suskirstytos į kelias grupes:

1) aukos, visiškai neprisidėjusios prie nusikaltimo;
2) aukos, pasielgusios nerūpestingai;
3) aukos, išprovokavusios nusikaltimą.

Analizuojant aukos elgesį galima pateikti apibendrintus tapatybės vagystės prevencijos patarimus asmeniui:

1) autorizuoti prieigą prie savo kompiuterio ar kito elektroninio prietaiso, per kurį galima pasiekti asmens duomenis,
2) bet kur nemėtyti nereikalingų kvitų ir bankomato išrašų;

3) patikimai naikinti dokumentus, iš kurių galima nustatyti asmens duomenis (pvz., įvairios ataskaitos ir kt.);
4) rinktis patikimus slaptažodžius;
5) nedalyti asmens kodo ir kitų asmens duomenų nežinomiems asmenims[159].

Tai tik pavyzdinis sąrašas. Detalesnė informacija apie tapatybės vagystės elektroninėje erdvėje prevenciją individualiu (konkretaus asmens) lygmeniu pateikta monografijos 4.1. dalyje.

Siekiant plačiau suvokti tiriamąjį reiškinį, tikslinga pasitelkti viktimologijos sukauptas žinias, tyrimo metodus ir apžvelgti šios kriminologijos šakos keliamus klausimus.

Aptariant pavojingas veikas dažnai susitelkiama prie labai svarbių klausimų: „Kas, kaip, kur, kada?“ Šie klausimai tiriami ir šioje monografijoje, tačiau būtina atsižvelgti ir į klausimus: „Kodėl?“ ir „Ką galima padaryti, kad to neatsitiktų?“ Šie klausimai rodo praeities (istoriniai, genezės aspektai) ir dabarties sąsajas, nes svarbus reiškinys nagrinėjamas ne tik šiandienos, bet ir ateities aspektu, kadangi žinant, kodėl vienokie ar kitokie reiškiniai kyla, galima imtis priemonių jiems kontroliuoti.

Viktimologija tiria aukos ir pažeidėjo, aukos ir platesnės visuomenės santykį. Šioje monografijos dalyje plati sąvoka „pažeidėjas“ bus vartojama tikslingai, t. y. socialinių normų pažeidėjas, o ne nusikaltėlis, todėl, kad daugelyje šalių tapatybės vagystė elektroninėje erdvėje nėra pripažįstama savarankišku nusikaltimu, nors pats reiškinys yra negatyvus ir sukelia aukoms neigiamų pasekmių, kurios gali būti ne tik finansinės (pvz., piniginiai nuostoliai, negautos pajamos, papildomos investicijos duomenų ir informacijos saugai užtikrinti), bet ir neturtinio ar moralinio pobūdžio (garbės ir orumo pažeidimai, juridinio asmens reputacijos sumenkinimas, kurio rezultatas – nusivylimas, nepasitikėjimas ir pan.).

Papildomai paminėtinas literatūroje nurodomas kritinis aspektas, susijęs su tapatybės vagystės elektroninėje erdvėje aukomis, yra tas, kaip greitai auka sužino apie problemą[160]. Pavyzdžiui, asmuo, kuris reguliariai tikrina savo sąskaitą banke ir atliktus mokėjimus, daug greičiau pastebės tapatybės vagystę. Viena iš specifinių tapatybės vagystės elektroninėje

[159] *OECD Policy Guidance on Online Indentity Theft*. OECD Ministerial Meeting on the Future of the Internet Economy. Seoul, Korea, 17–18 June 2008.

[160] *Understanding and Mitigating Identity Theft*. 2009. Thomson Reuters, p. 31.

erdvėje aplinkybių ir yra ta, kad aukos pačią tapatybės vagystę pastebi ne veikos atlikimo metu, o vėliau. Judith M. Collins pateikia pavyzdžių, kai viena moteris buvo atleista iš darbo, kita kredito kortelėje aptiko ne jos atliktus mokėjimus, trečioji – buvo areštuota už nusikaltimą, kurio ji nepadarė[161]. Tai tik keli pavyzdžiai, kaip žmonės susiduria su tapatybės vagyste ir jos pasekmėmis. Tačiau yra daug formų, kaip galima pastebėti, kad kiti asmenys pasinaudojo jūsų duomenimis galbūt ir nusikalstamai veikai. Minėti pavyzdžiai parodo, kad aukos visiškai nepastebėjo tapatybės vagystės, o apie šį nusikaltimą sužinojo tik tada, kai atsirado kitų neigiamų pasekmių panaudojus vogtus duomenis. Pateikti pavyzdžiai patvirtina, kad laiko tarpas tarp tapatybės vagystės ir sužinojimo apie įvykdytą pavojingą veiką gali būti gana ilgas. Ta pati autorė pateikia Amerikoje nutikusį pavyzdį, kai jauna pora tapatybės vagystę ir neigiamas jos pasekmes pastebėjo tik po beveik devynerių metų – visą tą laiką nusikaltėlis naudojosi šios poros vyro socialinio draudimo numeriu (angl. *Social Security number*) tam, kad gautų paskolas iš finansinių institucijų, esančių skirtingose valstijose. Nusikaltėlis gyveno iš šių paskolų, skolas apmokėdamas iš naujai paimtų paskolų, be to, paskolos buvo naudojamos ir naudotiems automobiliams perparduoti, siekiant užsidirbti papildomų pajamų. Tokia schema negalėjo tęstis visą laiką ir nusikaltėlis pradėjo negrąžinti eilinių paskolos mokėjimų, o asmens, kurio socialinio draudimo numeris buvo naudojamas, kreditingumas sumažėjo tiek, kad nusikaltėlis jau negalėjo paimti naujų paskolų[162].

Pateikti pavyzdžiai iliustruoja situacijas, kai asmenys pastebi tapatybės vagystes ir su jomis susijusias veikas ir jų pasekmes pavėluotai, tačiau pasitaiko ir kitokių atvejų, kai aukos gauna informacijos dar tik mėginant pasinaudoti asmens duomenims nusikalstamiems veiksmams, pavyzdžiui, bankui ar kitai finansinei institucijai susisiekus su asmeniu ir pasitikslinus, ar tikrai jis nori paimti paskolą ar atlikti kitą veiksmą, galintį turėti įtakos jo teisėms ir įsipareigojimams. Todėl viena iš galimų tapatybės vagystės elektroninėje erdvėje prevencijos priemonių – imtis riziką mažinančių veiksmų, pavyzdžiui, kai paskolos prašytojas informuoja apie jo adreso pasikeitimą arba pildydamas dokumentą nurodo kitą nei anks-

[161] Collins, M. J. 2006. *Investigating Identity Theft: A Guide for Businesses, law Enforcement, and Victims*. John Wiley & Sons, Inc., p. 68.

[162] *Ibid*.

tesniame buvusį adresą, nes naujas adresas gali būti nusikaltėlio adresas, kuriuo jis nori gauti informaciją, o auka lieka „senuoju adresu“.

Neretai aukos apie tapatybės vagystę sužino iš išieškojimo įmonių, kurios pareikalauja sumokėti už aukos vardu atliktus nusikaltėlio veiksmus. Kartais aukos gali sužinoti apie tapatybės vagystę atidžiau tyrinėdamos savo gaunamų paslaugų ataskaitas (pvz., bankų ataskaitas apie atliktus mokėjimus, elektroninių ryšių paslaugų teikėjų ataskaitas apie suteiktas paslaugas ir kt.). Tobulėjant technologijoms daugėja būdų ir pinga priemonės, leidžiančios nusikaltėliams paslėpti pėdsakus, pavyzdžiui, Lietuvoje labai nesudėtinga įsigyti daug išankstinio mokėjimo kortelių elektroninių ryšių paslaugoms ir jas nuolat keisti siekiant sutrukdyti susekti nusikaltėlį. Tą pripažindamas ir siekdamas sumažinti nusikaltėlių galimybes pasinaudoti tokiomis techninėmis ir organizacinėmis galimybėmis, 2011 m. gegužės 12 d. Lietuvos Respublikos Seimas priėmė LR Operatyvinės veiklos įstatymo Nr. XI-1374 3, 7, 9, 10, 11, 12, 13, 21, 23 straipsnių pakeitimo ir papildymo įstatymą[163], kuris leis teisėsaugos institucijoms klausytis ne konkretaus nurodyto telefono numerio, o visų su tam tikru asmeniu susijusių telefono numerių.

Atskira ir labai plati sritis yra debetinių ir (ar) kreditinių mokėjimo kortelių neteisėtas pasisavinimas, kai nusikaltėliai neteisėtai pasinaudoja asmens mokėjimo kortele. Ši sritis nėra naujiena ir Lietuvoje, todėl jau yra įdomios šios srities teisminės praktikos[164].

Minėtoji vėlyvo pavojingos veikos pastebėjimo aplinkybė sudaro galimybę veikos subjektui geriau paslėpti įvykdytos veikos pėdsakus (pvz., išsikelti iš ne savo vardu nuomojamo buto, kuriame naudojosi kompiuteriu pavojingai veikai atlikti, išvažiuoti iš veikos įvykdymo teritorijos siekiant pasislėpti ir kt.), o tai savo ruožtu apsunkina tokio pobūdžio veikų susekimą ir tyrimą nacionaliniu ir tarptautiniu lygiu. Todėl kuriant prevencijos priemones viena priemonių grupė turi būti orientuota į priemones, skirtas paankstinti aukų, teisėsaugos institucijų, finansinių institucijų ar kitų asmenų galimybę sužinoti apie tapatybės vagystę. Tokios priemo-

[163] Lietuvos Respublikos operatyvinės veiklos įstatymo Nr. XI-1374 3, 7, 9, 10, 11, 12, 13, 21, 23 straipsnių pakeitimo ir papildymo įstatymas. *Valstybės žinios*, 2011, Nr. 653047.

[164] Plačiau: Lietuvos Aukščiausiojo teismo 2002 m. vasario 20 d. nutartis civilinėje byloje Nr. 3K-3-390/2002; Lietuvos Aukščiausiojo Teismo Civilinių bylų skyriaus 2001 m. birželio mėn. 13 d. nutartis civilinėje byloje Nr. 3K-3-645.

nės būtų skirtos ne tik tapatybės vagystei elektroninėje erdvėje užkardyti ir prevencijai, bet ir kitų nusikalstamų veikų, kurioms įvykdyti gali būti naudojama pavogta tapatybė, prevencijai.

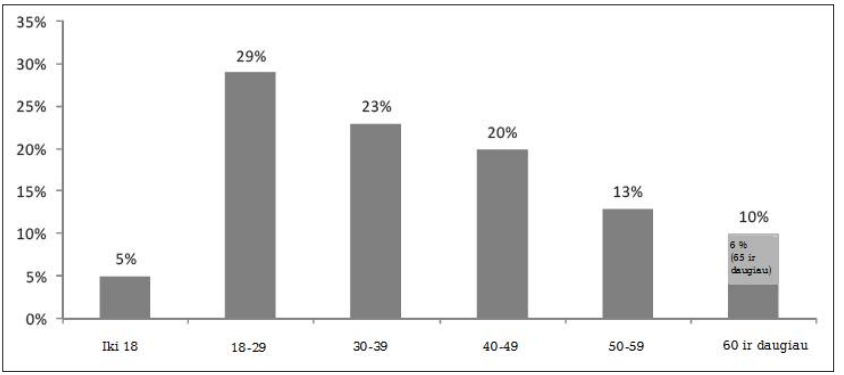
Tapatybės vagystės aukos sąvoka *a priori* gali būti apribota į ją įtraukiant tik tuos asmenis, kurių asmeninė informacija buvo pasisavinta kito asmens ir kurie dėl to patyrė finansinės ar kitokios žalos. Tačiau pateikiami statistiniai duomenys atspindi tik tuos tapatybės vagystės atvejus, apie kuriuos šios veikos aukos pranešė, ir neatskleidžia tikrosios situacijos apie nukentėjusiųjų dėl tapatybės vagystės skaičių. Tai tik patvirtina faktą, kad tapatybės vagystės aukos koncepcija yra kur kas sudėtingesnė. Pavyzdžiui, pats faktas, kad asmuo, nukentėjęs nuo tapatybės vagystės, apie tai pranešė atitinkamoms institucijoms, ne visada reiškia, kad verslo ar kitos institucijos taip pat tapo tapatybės vagystės aukomis. Tapatybės vagystės subjektai gali pasinaudoti vartotojo banko sąskaita neteisėtais tikslais arba pasinaudoti banko pavadinimu vykdydami duomenų vagystės ataką, kad galėtų pasisavinti banko vartotojo pinigus. Tokiu atveju bankas taip pat tampa tapatybės vagystės auka, kadangi jis turės grąžinti savo klientui prarastą pinigų sumą.

Galima teigti, kad jaunimas ir vidutinio amžiaus asmenys dažniau tampa tapatybės vagystės elektroninėje erdvėje aukomis, nes šios žmonių grupės dažniau naudojasi elektroninėmis paslaugomis, mėgsta išbandyti informacinių technologijų naujoves, pasinaudoti interneto teikiamais privalumais mažinančiais darbų atlikimo ir paslaugų suteikimo laiko sąnaudas ir pan., todėl aktyviai viešina asmeninio gyvenimo detales įvairiuose socialiniuose tinkluose. Tokie asmenys dažnai kreipiasi dėl paskolos, turi daug reikalų su finansinėmis institucijomis, keičia darbus ir pan.[165]. Tačiau vyresnio amžiaus asmenys gresia didesnė rizika nukentėti nuo tapatybės vagystės fizinėje erdvėje, kadangi šios grupės asmenys dažnai nepasitiki paslaugomis, teikiamomis elektroninėje erdvėje, nesiryžta išbandyti technologinių naujovių ir labiau pasitiki aukštas pareigas einančiais asmenimis, pavyzdžiui, banko ar valstybės institucijos atstovais (tuo dažniausiai pasinaudoja įvairaus pobūdžio sukčiai).

Pavyzdžiui, Jungtinių Valstijų Federacinės prekybos komisijos ataskaitoje pateikiami duomenys, kad 2006 m. daugiausia apie tapatybės va-

[165] *Understanding and Mitigating Identity Theft*. Thomson Reuters, 2009, p. 31.

gystės atvejus pranešė asmenys, kurių amžius buvo nuo 18 iki 29 metų (jie sudarė 29 % nukentėjusių nuo tapatybės vagystės asmenų, nurodžiusių savo amžių), o nukentėjusieji, pranešę apie tapatybės vagystę, kurių amžius buvo nuo 30 iki 39 metų, sudarė 23 %.



15 pav. Nukentėjusiųjų nuo tapatybės vagystės skaičius pagal amžiaus grupes (Šaltinis: US FTC (2007a), Report on Consumer Fraud and Identity Theft Complaint Data. P. 15[166])

Tačiau apie tapatybės vagystės elektroninėje erdvėje aukas atlikta užsienio valstybių ir tarptautinių organizacijų tyrimų ir ataskaitų analizė patvirtina, kad tapatybės vagystės elektroninėje erdvėje atveju nukentėjusiuoju gali tapti bet kas – tiek pavieniai fiziniai asmenys ir jų grupės, t. y. paprasti elektroninės erdvės naudotojai, tiek finansų institucijos ir kredito įstaigos, privataus ir viešojo sektoriaus institucijos, akademinės bendruomenės, taip pat valstybė ar net dalis tarptautinės bendruomenės ir net visa ekonomika apskritai. Pavyzdžiui, pasikėsinus į elektroninius duomenis ir (ar) informacines sistemas, turinčius didelę strateginę reikšmę nacionaliniam saugumui, valstybės valdymui, ūkiui ar finansų sistemai, gali būti padaryta žalos esminiams valstybės interesams – viešajam saugumui, valstybės valdymui, ekonominiams, finansiniams interesams ir kt.

Finansų srityje nuo tapatybės vagystės dažniausiai nukenčiančias aukas galima suskirstyti į 4 grupes: valdžios institucijos, privataus sektoriaus bendrovės, tvarkančios didelius asmens duomenų kiekius, finansinių paslaugų teikėjai ir vartotojai. Kiekviena iš minėtų grupių gali susi-

[166] US FTC (2007a), Report on Consumer Fraud and Identity Theft Complaint Data [interaktyvus, žiūrėta 2011-07-14] <http://www.ftc.gov/opa/2008/02/fraud.pdf>.

durti su įvairiais neigiamais tapatybės vagystės padariniais, kurie gali pasireikšti tiek tiesioginių nuostolių (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), tiek netiesioginių nuostolių (pavyzdžiui, asmens reputacijos sumenkinimas, duomenų apie teistumą įrašymas asmens byloje ir pan.) forma. Valdžios institucijos taip pat gali turėti tiek tiesioginių finansinių nuostolių (tapatybės vagystė gali būti nukreipta ir prieš viešuosius asmenis), tiek netiesioginių išlaidų, susijusių su prevencija ir teisės aktų įgyvendinimu. Bet kokiu atveju, jei valdžios institucijos patirtų tiesioginių nuostolių, jie būtų netiesiogiai užkrauti vartotojams, kaip mokesčių mokėtojams.

Tapatybės vagystės aukos taip pat patiria emocinę žalą (stresas, neigiama įtaka sveikatai), kuri neturėtų būti nuvertinama, nors ją ir sunku išmatuoti. Taip pat pažymėtina, kad gali būti labai didelė netiesioginė žala. Pavyzdžiui, valstybės institucijos, kurios išduoda tapatybę patvirtinančius dokumentus, nukentėjusios nuo tapatybės vagystės, gali prarasti valstybės piliečių ir kitų gyventojų pasitikėjimą išduodamais dokumentais ir pačia identifikavimo sistema. Finansų institucijos tapatybės vagystės atveju taip pat gali prarasti vartotojų pasitikėjimą jų teikiamomis paslaugomis elektroninėje erdvėje ir apskritai mokėjimais negrynaisiais pinigais. Be to, tapatybės vagystės atveju su neigiamais padariniais reputacijai gali susidurti asmens duomenų saugojimo paslaugų ir finansinių paslaugų teikėjai, o tai jau turi tiesioginės įtakos jų padėčiai rinkoje ir pačiam verslo modeliui.

Kadangi tapatybės vagystė skirtingose valstybėse vertinama nevienodai, apsunkinamas tokių veikų susekimas ir tyrimas, be to, ikiteisminio tyrimo institucijoms trūksta patirties ir atitinkamų priemonių tiriant tokio pobūdžio veikas, todėl asmenys, nukentėję nuo tapatybės vagystės, dažnai jaučia nusivylimą ir pasipiktinimą, bandydami įtikinti finansų ir teisėsaugos institucijas, kad tapo šios pavojingos veikos aukomis. Netgi jei nukentėjusieji gali tiksliai apibūdinti veiką, kurios aukomis tapo, dažnos situacijos, kai nepavyksta atstatyti kredito istorijos ir susigrąžinti gero vardo.

Tapatybės vagystė elektroninėje erdvėje, atsižvelgiant į jos įvykdymo būdų ir neigiamų padarinių įvairovę, galimą mastą ir latentiškumą, ne

veltui priskiriama vienai iš pavojingiausių ir labiausiai plintančių elektroninių nusikaltimų rūšių. Šios pavojingos veikos aukos gali susidurti su įvairiais tiek finansinio, tiek moralinio pobūdžio neigiamais padariniais, kadangi tapatybės vagystė elektroninėje erdvėje gali sukelti pačių įvairiausių neigiamų pasekmių, pradedant nuo to, kad asmenys kurį laiką negali naudotis savo kompiuteriais, internete netikėtai susiduria su rasistinio ar pornografinio turinio informacija, tampa sukčiavimo aukomis ir patiria finansinių nuostolių, iki to, kad įmonės ar organizacijos vidinis tinklas tam tikrą laiką tampa nepasiekiamas ar sužinoma informacija, kuri yra kaip komercinė paslaptis. Dar daugiau – gali būti užblokuoti valstybės valdžios institucijų internetinių tinklalapių adresai arba internete paviešinta valstybės ir (ar) tarnybos paslaptį sudaranti informacija. Todėl potenciali tapatybės vagystės elektroninėje erdvėje žala, pasikėsinimo objektas ir mastas, t. y. galimas nukentėjusiųjų skaičius, lemia jos pavojingumą – nuo grėsmės privatumui ir asmens duomenų apsaugai iki pavojaus valstybės interesams ir nacionaliniam saugumui. Plačiau apie šios veikos pavojingumą, neigiamus padarinius jos aukoms ir galimą prevenciją rašoma monografijos 1.2 ir 4 dalyse.

Pagal autorių atliktą kiekybinį tyrimą (vartotojų anketinę apklausą), 5,6 proc. tirtų Lietuvos vartotojų buvo susidūrę su tapatybės vagyste elektroninėje erdvėje[167] (daugiau apie autorių atliktus tyrimus nurodyta monografijos 5.2 dalyje). Pavyzdžiui, 2009 metais JAV 4,8 procento vartotojų susidūrė su tapatybės vagyste elektroninėje erdvėje[168]. Taigi, procentas labai panašus. Nepaisant 4,8 procento rodiklio, nuostoliai dėl tapatybės vagystės elektroninėje erdvėje JAV labai dideli – 54 mlrd. JAV dolerių[169].

[167] Paminėtina, kad pagal autorių atliktą viešojo sektoriaus tyrimą darbe su tapatybės vagyste elektroninėje erdvėje susidūrė net 15,8 proc. viešojo sektoriaus darbuotojų, o pagal verslo darbuotojų tyrimą – 14 proc. Tačiau Sodros darbuotojų rodiklis panašus kaip vartotojų – 4,9 proc. Kadangi viešojo ir verslo sektorių darbuotojų tyrimai mažiau patikimi dėl nepakankamos imties, detaliau šioje nuorodoje paminėti rodikliai nebus nagrinėjami.

[168] Javelin Study Finds Identity Fraud Reached New High in 2009, but Consumers are Fighting Back. [interaktyvus, žiūrėta 2011-09-18]. <http://www.prnewswire.com/news-releases/javelin-study-finds-identity-fraud-reached-new-high-in-2009-but-consumers-are-fighting-back-83987287.html>.

[169] *Ibid.*

Taip pat pagal 2009 metais atliktą Gallup tyrimą, 66 proc. JAV suaugusių gyventojų nurodė, kad yra susirūpinę dėl to, kad gali tapti tapatybės vagystės aukomis[170]. Tai galima paaiškinti tuo, kad Jungtinėse Valstijose santykių kūrimas elektroninėje erdvėje yra labai paplitęs, tačiau požiūris į asmens duomenų apsaugą grindžiamas sektoriniu reguliavimu ir savireguliacija, nėra vieno bendro pagrindinio asmens duomenų apsaugą reglamentuojančio teisės akto, o duomenų tvarkymo atžvilgiu vadovaujamasi „saugaus uosto" sistema ir yra taikomi kitokie apsaugos standartai, kurie daugeliu požiūrių yra žemiau vertinami nei esantys Europos Sąjungoje. Be to, lyginant su Europos Sąjunga, JAV šiuo požiūriu yra gana silpnai reglamentuota asmens duomenų apsauga, ribotas įstatymų, reglamentuojančių asmens duomenų apsaugą, taikymas ir problemiškas jų įgyvendinimas. Kadangi yra didelė asmens dokumentų įvairovė, o asmens identifikavimo dokumentų išdavimo tvarka gana lanksti, tai sudaro prielaidas tapatybės vagystei elektroninėje erdvėje įvykdyti ir už šią veiką išvengti atsakomybės, o visa tai ir vilioja nusikalsti trečiojo pasaulio šalių gyventojus, kuriems atrodo, kad visi amerikiečiai yra labai turtingi.

Apibendrinančios išvados

• Pagrindinių tapatybės vagystės elektroninėje erdvėje subjektų bruožų, jų veikimo elektroninėje erdvėje specifikos, tikslų ir motyvų identifikavimas palengvintų šios pavojingos veikos tyrimą ir padėtų pasirinkti efektyviausias prevencijos priemones, kad ateityje būtų dar labiau sumažinta tapatybės vagystės elektroninėje erdvėje rizika.

• Tapatybės vagystės elektroninėje erdvėje subjektais gali tapti tiek kompiuterių genijai, tiek eiliniai elektroninės erdvės naudotojai kaip pavieniai asmenys, organizuotos elektroninių nusikaltimų grupės, įprasti kišenvagiai, įstaigos darbuotojai, turintys prieigą prie informacinių sistemų ir siekiantys pasipelnyti. Kadangi ši pavojinga veika dažnai naudojama kaip priemonė kitiems nusikaltimams įvykdyti, tapatybės vagystės subjektais taip pat gali būti asmenys, susiję su prekyba narkotikais, prekyba žmonėmis, pinigų plovimu, teroro išpuoliais, kurie naudojasi kitų asmenų tapatybėmis tam, kad nebūtų susekti ir patraukti atsakomybėn.

[170] Kshetri, N. 2010. *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives*. Springer-Verlag, p. 2.

• Labiausiai tapatybės vagystės elektroninėje erdvėje subjektus veikti pažeidžiant teisės aktus skatina vartotojų technologinių ir saugaus elgesio elektroninėje erdvėje žinių trūkumas bei teisėsaugos institucijų patirties elektroninių nusikaltimų srityje stoka.

• Tapatybės vagystės elektroninėje erdvėje atveju nukentėjusiuoju gali tapti bet kas – tiek pavieniai fiziniai asmenys ir jų grupės, kaip paprasti elektroninės erdvės naudotojai, tiek finansų institucijos ir kredito įstaigos, privataus ir viešojo sektoriaus institucijos, akademinės bendruomenės, valstybė ar net dalis tarptautinės bendruomenės arba visa ekonomika apskritai.

2. Tapatybės vagystės elektroninėje erdvėje įvykdymo būdai ir jų specifika

2.1. Tapatybės vagystės elektroninėje erdvėje įvykdymo 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 galima gauti kito asmens duomenis ir asmeninę informaciją, leidžiančią identifikuoti asmenį, ir vieta, kurioje tokia veika atliekama. Pirmuoju atveju naudojamos paprastos, ypatingų žinių nereikalaujančios priemonės (angl. *low-tech*), o veiksmai atliekami fizinėje erdvėje, turint tiesioginį kontaktą su nukentėjusiuoju. Antruoju atveju veikiama elektroninėje erdvėje naudojantis informacinėmis ir ryšio technologijomis (angl. *high-tech*), neteisėti veiksmai atliekami elektroninėje terpėje (įskaitant per atstumą), o tokios veikos įvykdymo būdai yra gana sudėtingi, reikalaujantys specifinių žinių ir dažniausiai nepastebimi paprastam elektroninės erdvės naudotojui.

Taigi praktikoje tapatybės vagystės būdai evoliucionavo į atskirą sukčiavimų sritį, kuri dažniausiai skirstoma į:

- tradicinius sukčiavimus, atliekamus fizinėje erdvėje.
- sukčiavimus, atliekamus elektroninėje erdvėje[171], pasinaudojant moderniosiomis technologijomis.

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, paliekant 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. Vienas iš drastiškiausių pokyčių tapatybės vagystės istorijoje sutapo su 1990 m. technologijų plėtra. Nuo 1992 m. iki 1995 m. technologijos suteikė galimybę finansų institucijoms teikti paslaugas elektroninėje erdvėje, o duomenų bazės tapo būtinybe

[171] Štitilis, D.; Laurinaitis, M. 2009. Tapatybės vagystė elektroninėje erdvėje. *Informacijos mokslai: mokslo darbai* 50: 242.

keičiantis didžiuliais kiekiais asmeninio pobūdžio informacijos. Tobulėjant technologijoms, nusikaltėliai surado naujų būdų, kaip pasinaudoti technologijų silpnosiomis pusėmis. Pažeidimai prasidėjo tuo pačiu metu, kai finansų institucijos bandė įtikinti klientus atlikti finansines operacijas elektroninėje erdvėje, kol vienas įvykis privertė vartotojus susimąstyti, kad elektroninė bankininkystė rizikinga. Tai susiję su tarptautine grupuote, kuri pasinaudojo technologijų silpnosiomis savybėmis ir įvykdė didžiausią istorijoje banko vagystę internetu.

Vladimiras Levinas gyveno ir dirbo Sankt Peterburge, Rusijoje. 1971 m. jis baigė Technologijų universitetą. Būdamas 23 m. jis atrado spragą „Citibank" elektroninės bankininkystės saugumo sistemoje, kuri leido jam pinigus iš šio banko klientų sąskaitų pervesti į savo asmeninę sąskaitą Suomijoje. Suvokdamas galimą finansinę naudą, Levinas į pagalbą pasikvietė keletą pagalbininkų, kad jie jam padėtų apiplėšti banką. 1994 m. liepos mėn., pasinaudodamas pavogtais vartotojų vardais ir slaptažodžiais, jis prisijungė prie „Citibank" elektroninės bankininkystės sistemos ir greitai milijonus dolerių pervedė į finansinių institucijų, esančių įvairiose pasaulio vietose, sąskaitas. Rugpjūčio mėnesį banko darbuotojai pastebėjo du įtartinus pervedimus, kurie sudarė 400 tūkst. dolerių, ir apie tai pranešė FTB. Bendradarbiaudama su Rusijos valdžios institucijomis, FTB nustatė Levino nusikalstamus veiksmus. 1995 m. kovo 3 d. Interpolo agentas areštavo Leviną, jam buvo pareikšti kaltinimai pavogus apie 12 mln. dolerių. Levinas teisinosi ir pripažino kaltę tik dėl mažiau nei 3,7 mln. dolerių, už tai jam buvo paskirta 3 metų laisvės atėmimo bausmė, be to, jis turėjo atlyginti 240 tūks. nuostolius, padarytus „Citibank"[172].

Paprastai tradicinė tapatybės vagystė buvo – ir vis dar yra – atliekama naudojant 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 ir ryšio technologijų plėtros, kuri suteikia galimybę tapatybės vagystės subjektams kompiuteriuose įdiegti kenkėjiškas programas ar pritaikyti duomenų vagystės metodą pasinaudojant šiomis programomis ar nepageidaujamomis elektroninio pašto žinutėmis. Dėl minėtų priežasčių dauguma

[172] Hoffman, S. K.; McGinley, T. G. 2010. *Identity Theft*. p. 12–13.

tapatybės vagysčių yra atliekama elektroninėje erdvėje pačiais įvairiausiais metodais, kurie kinta ir tobulėja kartu su technologijų pažanga.

Galima išskirti tokius tapatybės vagystės būdus, kurie dažniausiai naudojami fizinėje erdvėje:

1) žiūrėjimas per petį (angl. *shoulder surfing*): būnant netoli kito asmens stebima, kaip šis 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, pavyzdžiui, kreditinių kortelių sandorių kopijų, prašymų suteikti paskolą, klientų aptarnavimo paslaugų ataskaitų, tarnybos vadovų, telefonų knygų, lygiai taip pat kaip kreditinių kortelių ir socialinio draudimo numerių, gimimo datų ir adresų;

3) vagystė (angl. *stealing*): gali būti pavogtas 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, taip pat mobilusis telefonas ar kompiuteris, kurie yra asmeninės informacijos šaltiniai. Pavyzdžiui, Jungtinėje Karalystėje 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, kad 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 nustatyta, kad diskas, kuriame buvo saugomi valstybės tarnautojų duomenys, dingo dar prieš metus[173].

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

[173] Dingo kaip į vandenį. *Kauno diena*. [interaktyvus]. 2008-09-08 [žiūrėta 2011 09 18]. <http://kauno.diena.lt/dienrastis/pasaulis/dingo-kaip-i-vandeni-121179>.

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 pasisavinimas (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, kuriuo asmeninė informacija tampa lengvai prieinama.

Dėl elektroninės erdvės specifikos galima išskirti būdus, kuriais tapatybės vagystė 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, disponuodamas tam tikrais duomenimis, gautais apie kitą asmenį fizinėje erdvėje, gali stengtis gauti daugiau to asmens duomenų elektroninėje erdvėje, ir atvirkščiai.

Su tapatybės vagyste elektroninėje erdvėje dažniausiai susiduriama tada, kai elektroninės erdvės naudotojai dalyvauja autentifikavimo procese. Šiame procese vartotojai, norėdami gauti prieigą prie atitinkamų informacinių sistemų, turi patvirtinti savo tapatybę. Tada ir kyla grėsmė tapti tapatybės vagystės auka, nes ne visi asmenys laikosi būtinų asmens duomenų apsaugos principų ir taisyklių, dažnai elgiasi neapdairiai, neatidžiai ar nesuvokia, kokią žalą gali padaryti internetinis sukčius, pasinaudojęs vartotojo neatsargumu ir gavęs jo asmens duomenis ar kitą asmeninę informaciją. Be to, turi būti užtikrinamas atsiskaitymų, duomenų tvarkymo[174] (t. y. bet kokio veiksmo, atliekamo su duomenimis) ir ryšio kanalų saugumas. To-

[174] 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.

dėl, 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[175]:

I. Tapatybės vagystė:

1) tiesioginė ryšio, siejančio asmenį ir autentifikavimo duomenis, ataka atliekant vieną ar kelis tolesnius žingsnius:

• *naudojant kompiuterinius kirminus*, kurie įdiegia kenkėjiškas programas (pavyzdžiui, *key logger*[176]). Autentifikavimo duomenys yra tiesiogiai paimami iš asmens, manipuliuojant jo 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 įtikinamą priežastį atskleisti prašomus duomenis, tarkim, nurodant, kad tokie duomenys reikalingi įmonės informacinių technologijų departamento administraciniam personalui tikrinimo tikslais. Tokia ataka yra nukreipta prieš konkretų asmenį;

• *Trojos arkliai*[177] *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

[175] Leenes (ed.), FIDIS network, deliverable 5.2b, ID-related crime: towards a common ground for interdisciplinary research. [interaktyvus]. May 2006, p. 83. <http://www.fidis.net/resources/deliverables/forensic-implications/int-d52b000/doc/29/>.

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

[177] Trojos arklys (angl. *Trojan horse*) – tai slaptas specialių programų patekimas į svetimą programinę įrangą; naujos programos pradeda atlikti naujas teisėto savininko neplanuotas funkcijas. Programa įrašoma šalia kitos programos arba įdiegiama 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.

susieti, žinios. Pirmiausia iš asmens gaunami reikalingi biometriniai duomenys, 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 pateiktos nuorodos, kuri nukreipia į suklastotą internetinį tinklalapį, iš pirmo žvilgsnio atrodantį lygiai taip pat kaip originalus institucijos tinklalapis. Tokia ataka yra nukreipta prieš ryšį tarp informacinės sistemos ir autentifikavimo duomenų (žr. 2 schemą, Ryšys 3). Suklastotame tinklalapyje vartotojas apgaulės būdu įtikinamas įrašyti savo autentifikavimo duomenis.

II. „Žmogus – viduryje“ (angl. *man in the middle*) **atakos**: leidžia atlikti ir tiesiogines, ir netiesiogines atakas. Šios rūšies atakų metu perimami 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);

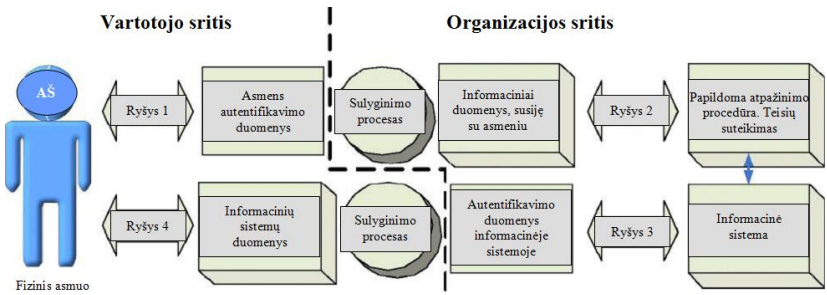
2) atsakomosios (angl. *replay*) ***atakos***: manipuliuojama interneto protokolo paketu, kuriame yra autentifikavimo duomenys su siuntėjo adresu. Toks protokolas persiunčiamas gaunančiajai sistemai. Ataka nukreipta prieš specialių įvesties įrenginių naudotoją (žr. 2 schemą, tiesioginė Ryšys 1 ataka);

3) tapatybės vagystė, atliekama peradresuojant pranešimą į suklastotą interneto tinklalapį (pavyzdžiui, naudojant apgaulės taktiką domenų vardų sistemos atžvilgiu (angl. *DNS-spoofing*): suklastotame interneto

tinklalapyje vartotojas apgaulės būdu įtikinamas įrašyti savo autentifikavimo duomenis (žr. 2 schemą, netiesioginė Ryšys 3 ataka).

III. Tapatybės perdavimas turint nesąžiningą tikslą arba apsikeitimas tapatybėmis nesąžiningu tikslu: šiuo atveju asmuo bendrininkauja su internetiniu sukčiumi, sąmoningai duoda jam savo autentifikavimo duomenis, suvokdamas, kad jie bus naudojami neteisėtai (žr. 2 schemą, ataka nukreipta prieš Ryšys 1).

IV. Tapatybės sukūrimas: internetinis sukčius paprastai pasinaudoja tam tikrais registracijos aspektais ir manipuliacinius veiksmus nukreipia prieš Ryšys 1 arba Ryšys 2 (žr. 2 schemą) tam, kad suardytų 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.



16 pav. Asmenų autentifikavimo procedūra informacinėse sistemose
(šaltinis: Report on Identity Theft/Fraud, 2007[178])

Elektroninėje erdvėje dėl įvairių sistemų ir programinės įrangos procesų prieiga prie informacinės sistemos ir autentifikavimo procesas yra sudėtingi, kadangi autentifikavimo procese dalyvauja keletas elementų ir įvairūs tarpininkai. Kiekvienas tarpininkas, pradedant nuo vartotojo ir baigiant institucija, teikiančia elektronines paslaugas ir turinčia informacinę sistemą, elektroninėje erdvėje vykstančio autentifikavimo proceso grandinėje pats savaime yra silpnoji grandis. Dėl šios

[178] *Report on Identity Theft/Fraud. Fraud Prevention Expert Group*. Brussels, 22 October 2007. [ineraktyvus, žiūrėta 2011-09-18]. <http://ec.europa.eu/internal_market/fpeg/docs/id-theft-report_en.pdf>.

priežasties yra nuolatinis pavojus, kad bus pasikėsinta į asmens duomenis ar asmeninę informaciją, perduodamą elektroninių ryšių tinklais ir būtiną efektyviai informacinės visuomenės narių tarpusavio komunikacijai. Todėl svarbu užtikrinti tapatybės nustatymo ir patvirtinimo proceso grandinės vientisumą.

Silpniausios grandinės dalys yra vartotojai, interneto paslaugų teikėjai, subjektai, atsakingi už duomenų tvarkymą ir veikiantys kaip trečioji šalis, lygiai taip pat ir 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 lygmeniu (darbo vieta, PDA[179], mobilieji telefonai, interneto kavinės ir pan.), pasinaudojant minėtų technologijų silpnosiomis vietomis (pavyzdžiui, naudojant kompiuterinius kirminus, virusus, kitas kenkėjiškas programas).

Interneto paslaugų teikėjai taip pat turi didelę reikšmę užtikrinant tapatybės nustatymo ir patvirtinimo proceso grandinės vientisumą: 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 apgavikai, atlikdami grobikiškus veiksmus spausdinimo klaidų (angl. *typographical error squatting*[180]) metodais. Verslo subjektai, vykdantys veiklą elektro-

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

[180] *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.

ninėje 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 taikant tokius metodus:

1) įsibrovimas (angl. *hacking*), kai sukčius apeidamas sistemos slaptažodžius, saugumo priemones, patenka į sistemą ar elektroninių ryšių tinklą. Ypač stengiamasi pasinaudoti saugumo spragomis, neapsaugotais bevieliais, intraneto tinklais, taip pat ieškoma sistemų, kuriose dauguma apsaugos funkcijų yra išjungtos. Pavyzdžiui, 2008 m. gegužės 8 d. Bostone buvo iškelta didžiausia tapatybės vagystės byla, kai 11 žmonių buvo pareikšti kaltinimai pavogus daugiau nei 40 mln. kreditinių kortelių numerių. Trys JAV piliečiai ir kiti asmenys iš Estijos, Ukrainos, Baltarusijos ir Kinijos įsilaužė į tokių smulkiųjų verslo atstovų, kaip *TJX Cos*., *BJ's Wholesale Club*, *OfficeMax*, *Boston Market*, *Barnes & Noble*, *Sports Authority*, *Forever 21* ir *DSW*, bevielius kompiuterinius tinklus ir įdiegė programas, kurios kaupė kortelių numerius, slaptažodžius ir informaciją apie sąskaitas. Jie naudojo sudėtingas kompiuterių įsilaužimo priemones, kurios leido apeiti saugumo sistemas ir įdiegti programas, kurios rinko milžiniškus kiekius asmeninių finansinių duomenų, kuriuos įsibrovėliai vėliau galėjo panaudoti patys arba parduoti tretiesiems asmenims. Dėl to nukentėjo bankai, smulkieji verslininkai ir vartotojai. Buvo naudojamasi *wardriving* metodu, kurio esmė – važinėti po skirtingas vietas kartu su nešiojamuoju kompiuteriu ir ieškoti pasiekiamų bevielio interneto signalų ir, suradus pažeidžiamą tinklą, įdiegti kenkėjiškas programas (*sniffer programs*), kurios renka kreditinių ir debetinių kortelių numerius, naudojamus smulkiųjų verslininkų tinkluose[181].

Taip pat paminėtina didžiausia tapatybės vagystės byla Majamyje, kai Albertas Gonzalezas, gimęs 1981 m., hakeris ir kompiuterinis nusikaltėlis, buvo apkaltintas kreditinių kortelių vagystės ir pavogtų korte-

[181] *Biggest Identity Theft Case Ever: 11 Indicted For Stealing And Selling Over 40 Million Credit Card Numbers.* [interaktyvus, žiūrėta 2011-09-18]. <http://www.huffingtonpost.com/2008/08/05/biggest-identity-theft-ca_n_117094.html>.

lių pardavimo organizavimu. Tai įvyko, kai 2005–2007 m. buvo pavogta daugiau nei 170 mln. kortelių ir bankomatų PIN kodų, naudojantis struktūrizuotos užklausų kalbos (angl. *SQL*) įterpimo būdu, surandančiu silpnąsias apsaugos vietas, kad būtų galima sukurti prieigą prie tam tikrų informacinių sistemų siekiant rinkti korporacijos tinklais keliaujančius elektroninius duomenis. 2010 m. kovo 25 d. A. Gonzalezas nuteistas 20 metų laisvės atėmimu, bausmę atliekant federaliniame kalėjime[182].

2010 m. vasario 17 d. kaimyninę šalį – Latviją – sukrėtęs įvykis buvo įvardytas amžiaus vagyste: 7,4 mln. (daugiau nei 120 GB) slaptų dokumentų, apimančių informaciją apie aukščiausių Latvijos politikų, valdininkų, privačių įmonių finansus, buvo pavogta iš šalies Valstybės pajamų tarnybos (Lietuvoje tokias funkcijas atitinka Valstybinė mokesčių inspekcija) elektroninės saugyklos. Už slaptų Latvijos politikų, valdininkų ir privačių įmonių finansinių dokumentų saugojimą atsakingos Valstybės pajamų tarnybos negalėjo atsakyti, kas pasisavino konfidencialią informaciją. „Ketvirtojo prabudimo liaudies armijos[183]“ atstovų teigimu, buvo bendrauta su žmogumi, kūrusiu Valstybės pajamų tarnybos (toliau – VPT) elektroninę deklaravimo sistemą. Jis esą pasakė, kad VPT vadovybė 10 metų žinojo apie silpnąsias sistemos vietas, tačiau liepė klaidų netaisyti. Latvijos valdžios atstovai dokumentų vagystės skandalą vadino šokiruojančiu ir baiminosi, kad teismus užplūs skundai dėl piliečių duomenų, kurių saugumą garantavo valstybė, vagysčių, o nukentėjusiems asmenims iš šalies iždo teks sumokėti dideles kompensacijas. Latvijos vidaus reikalų ministrės Lindos Murniecės teigimu, tokio didelio dokumentų kiekio vagystė yra nesuvokiamas dalykas ir šalies istorijoje tai atsitiko pirmą kartą, todėl svarbu ne tik surasti kaltininkus, bet ir užkirsti kelią galimybei pasikartoti panašiems atvejams. Gynybos ministro Imanto Liegio nuomone, incidentas parodė, kad elektroninėse sistemose kaupiama slapta informacija Latvijoje nėra deramai saugoma: į programišių rankas iš VPT pateko itin konfidenciali informacija apie Latvijos gynybos ministeriją, valstybės vadovą Valdį Zatlerą, didžiausias šalyje veikiančias įmones. Saugumo po-

[182] *Hack Pack The biggest identity theft case ever. Right here in Miami.* [interaktyvus, žiūrėta 2011-09-18]. <http://www.miaminewtimes.com/content/printVersion/2270696/>.

[183] Latvių įkurta organizacija arba judėjimu save vadinanti internetinė bendruomenė, kuri skelbiasi kovojanti už skaidrią Latviją, kurioje nebūtų korumpuotų pareigūnų, tačiau kova vyksta ne politinėmis priemonėmis, o visuomeninėmis iniciatyvomis, pvz., informacijos apie šalies pareigūnų neskaidrią veiklą skleidimas.

licijos atstovai tvirtino, kad pavogta informacija gali bandyti pasinaudoti nusikaltėliai ir šantažuoti verslininkus, politikus[184].

Vienas iš naujausių įvykių – įsilaužimas į „Citibank" kompiuterius. „Citibank" patvirtino, kad įsilaužėliai pagrobė asmeninius tūkstančio bankų klientų duomenis jungtinėse Valstijose ir Kanadoje. Įsilaužus į kompiuterius buvo pasisavintos klientų pavardės, jų sąskaitų numeriai ir kontaktinė informacija[185].

2) *duomenų vagystė* arba *slaptažodžio žvejyba* (angl. *phishing* terminas kilęs iš žodžių junginio *fishing for your password* – slaptažodžio žvejyba)[186]: tai vis dažniau pasitaikantis reiškinys, nuo kurio gali nukentėti bet kuris interneto vartotojas. Duomenų vagystė – tai tokia sukčiavimo forma, nukreipta prieš organizacijas ar privačius asmenis, kai pasinaudojant nepageidaujamomis elektroninio pašto žinutėmis ar falsifikuotais internetiniais tinklalapiais siekiama išgauti prisijungimo prie informacinių sistemų slaptažodžius ar kitus konfidencialius duomenis. Dažniausiai tokio sukčiavimo aukos būna banko klientai, sužinojus jų prisijungimo prie elektroninės bankininkystės sistemų slaptažodžius ar kreditinių kortelių duomenis. Gauta informacija gali būti panaudota pasipelnymo tikslais vykdant nusikalstamas veikas, neteisėtą prisijungimą prie informacinių sistemų, vagystes iš sąskaitų ar elektroninėje erdvėje atsiskaitant už prekes svetimomis mokėjimo kortelėmis. Taip pat egzistuoja trumpųjų žinučių sukčiavimai (angl. *SMiShing*), internetinės balso telefonijos sukčiavimai (angl. *vishing*), kurie yra duomenų vagystės atmainos.

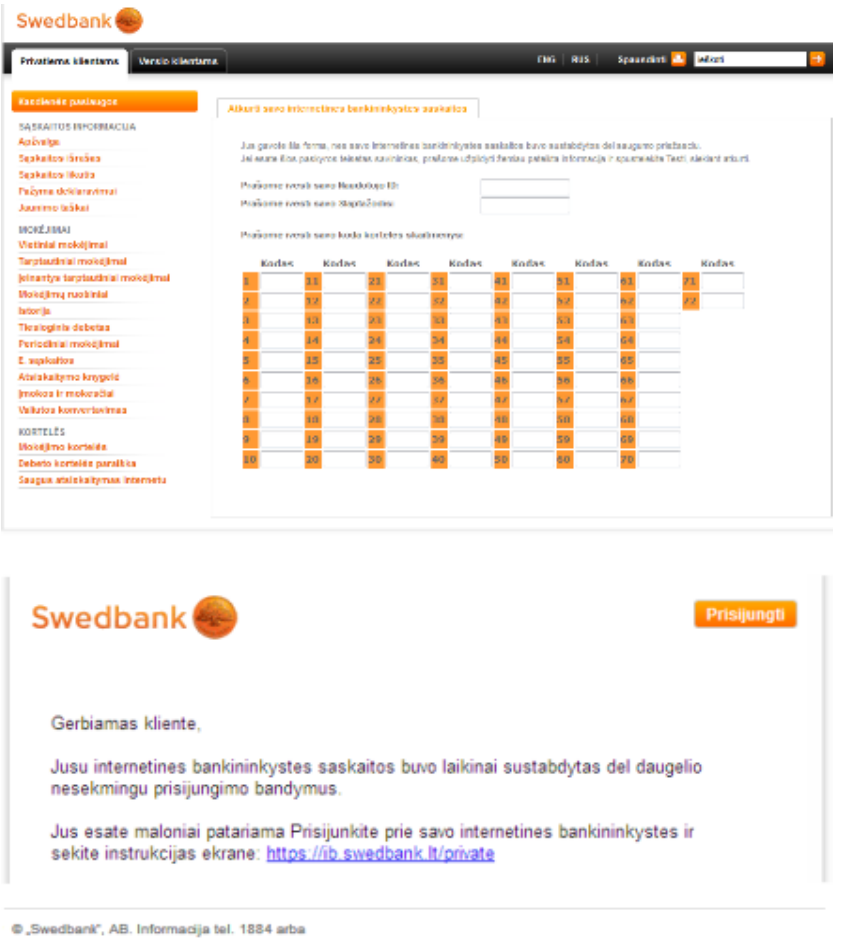
Kaip duomenų vagystės pavyzdį galima pateikti Lietuvos CERT 2011 m. liepos 18 d. įspėjimą vartotojams, kad platinami elektroniniai pranešimai neva iš „Swedbank", AB, kuriuose informuojama, kad e. bankininkystės sąskaita laikinai sustabdyta, ir prašoma klientų pateikti savo prisijungimo prie sistemos duomenis. Elektroniniuose pranešimuose, kurie atrodo identiški banko puslapiui, pranešama apie laikinai sustabdytą vartotojo sąskaitą. Interneto vartotojas, spustelėjęs ant paveikslėlio, esan-

[184] Latviją supurtė amžiaus vagystė. *Respublika* [interaktyvus]. 2010-02-17 [žiūrėta 2011-09-18]. <http://www.respublika.lt/lt/naujienos/pasaulis/nusikaltimai_ir_nelaimes/latvija_supurte_amziaus_vagyste/>.

[185] *Įsilaužėliai pavogė „Citibank" klientų duomenis. Delfi.lt* [interaktyvus]. 2011-06-09 [žiūrėta: 2011-09-18]. <http://verslas.delfi.lt/archive/print.php?id=46440885>.

[186] Daugiau informacijos apie *phishing* galima rasti čia: <http://www.esaugumas.lt/index.php?701248550>.

čio elektroniniame laiške, automatiškai nukreipiamas į duomenų vagysčių (angl. *phishing*) puslapius. Tokie paveikslėliai vartotojams siuntinėjami kaip elektroniniai laiškai[187]. Paveikslėlio pavyzdys pateikiamas toliau.



17 pav. Elektroninio laiško pavyzdys

3) falsifikuoti internetiniai tinklalapiai (angl. *scam*): tai atakos, pagrįstos padirbtu kokios nors institucijos (pvz., banko) tinklalapiu. Tink-

[187] *Internetu plinta pavojingi pranešimai* [interaktyvus]. 2011-07-18 [žiūrėta: 2011-09-18]. <http://www.rrt.lt/lt/pranesimai-spaudai/internetu-plinta-pavojingi-pranesimai.html>.

lalapis būna tiksliai nukopijuotas arba gali būti pavogtas ir atrodo bei funkcionuoja visiškai taip pat kaip ir reali svetainė. Tokių tinklalapių gaminimu ir naudojimu užsiima įsilaužėliai, norintys gauti priėjimą, pavyzdžiui, prie bankų informacinių sistemų. Galimas atvejis, kai sukuriami elektroninės komercijos paslaugas teikiantys tinklalapiai ir paslaugos ar prekės siūlomos neįprastai maža kaina[188]. Pavyzdžiui, Lietuvoje 2010 m. gruodžio 8–10 dienomis sukčiai iš patiklių pirkėjų išviliojo apie pusę milijono litų, internete įkūrę buitinės technikos parduotuvę, adresu *www.beribu.lt*, ir pasiūlę net 50 procentų dydžio kalėdines nuolaidas. Nurodyta realiai veikianti bendrovė, sąskaitos numeris banke, telefono numeris pasiteirauti, prekes pristatanti žinoma siuntų bendrovė, todėl pirkimo procedūra iš pradžių niekam nesukėlė įtarimų – pirkėjai netgi automatiškai gaudavo sąskaitas faktūras. Svetainėje buvo galima stebėti statistiką, kiek yra lankytojų, už kiek jie įsigijo prekių. Apgaulė pradėjo aiškėti tada, kai pirkėjai niekaip negalėjo prisiskambinti nurodytu informacijos telefonu, be to, kelis kartus pasikeitė sąskaita. Vėliau, pasipylus vartotojų skundams, svetainė buvo užblokuota. Pažymėtina tai, kad panašiu pavadinimu veikia didmeninės prekybos bendrovės „Sanitex“ interneto parduotuvė (*www.neriba.lt*)[189].

4) 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;

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

6) 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, naudojantis banko sąskaito-

[188] Higgins, G. E. 2010. *Cybercrime: An Introduction to an Emerging Phenomenon*. McGraw-Hill, p. 69.

[189] Sukčiai pakišo jauką – kalėdines nuolaidas. *Lietuvos rytas* [inetraktyvus]. 2010-12-10 [žiūrėta 2011 09 18]. <http://m.lrytas.lt/?data=20101210&id=akt10_a1101210&view=2>.

mis, ir siunčia šiuos duomenis tretiesiems asmenims – programų gamintojams ar kitiems suinteresuotiems asmenims – be vartotojo leidimo ir netgi be jo žinios (pvz., *key logging*);

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

8) Trojos arklys (angl. *trojans*) – tai klaidinanti programa, kuri, dėdamasi, kad sprendžia kokį nors naudingą uždavinį, iš tikrųjų, naikina ir gadina kompiuteryje esančius duomenis ir programas. Dažniausiai Trojos arkliai skirstomi į kirminams artimas programas, kurios platina savo kopijas kompiuterių tinkluose, ir nuotolinio valdymo programas, kurios naudojamos nuotoliniam sistemų administravimui. Pavojingiausios programos pasisavina informaciją ir ją persiunčia tretiesiems asmenims, dažnai net paprastu elektroniniu paštu ar internetinėmis svetainėmis. Naudojant trojos arklį, galimas ir elektroninių komunikacijų perėmimas[190].

9) apgaulinga IP taktika (angl. *pharming*): siekiama nukreipti vienos svetainės srautą į kitą. Tai gali būti atliekama pakeitus pagrindinio kompiuterio nustatymus arba pasinaudojus sričių vardų serverių (DNS) naudojimo pažeidimais. Pažeisti sričių vardų serveriai vadinami užnuodytais (angl. *DNS cache poisoning*).

10) 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;

11) elektroninių šiukšlių rinkimas (angl. *dumster diving*). Kaip fizinėje erdvėje galimas fizinių šiukšlių rinkimas, siekiant surinkti asmeninę informaciją, taip elektroninėje erdvėje įmanomas elektroninių šiukšlių rinkimas. Pavyzdžiui, ištrintų dokumentų ir informacijos peržiūrėjimas. Toks būdas literatūroje įvardijamas kaip dažniausias, siekiant pasisavinti kreditinių kortelių numerius arba banko sąskaitos numerius[191].

[190] Higgins, G. E. 2010. *Cybercrime: An Introduction to an Emerging Phenomenon*. McGraw-Hill, p. 69.

[191] *Ibid.,* p. 68.

12) netikro profilio socialiniame tinkle sukūrimas: kito asmens vardu užpildoma ir socialiniame tinkle užregistruojama anketa. Pavyzdžiui, 2010 m. rugsėjo 21 d. Interpolo generalinis sekretorius Ronald K. Noble pareiškė, kad elektroniniai nusikaltimai – didžiausia kriminalinė grėsmė, po to, kai kompiuterių įsilaužėliai pavogė Interpolo vadovo „Facebook" tapatybę: interneto nusikaltėliai sukūrė du netikrus profilius jo vardu ir juos naudojo siekdami gauti informacijos apie tarptautinės policijos agentūros – Interpolo – vykdomą operaciją, per kurią buvo suburta tyrėjų iš 29 Interpolo valstybių narių komanda, kuri ieškojo nuo teisėsaugininkų besislapstančių nusikaltėlių, įtariamų tokiomis veikomis, kaip nužudymai, pedofilija, prekyba narkotikais ir pinigų plovimas[192].

Tapatybės vagystės elektroninėje erdvėje įvykdymo būdai nuolat keičiasi, nes atsiranda vis naujų, todėl baigtinio ir išsamaus sąrašo pateikti neįmanoma. Ankščiau pateiktas sąrašas yra pavyzdinis, parodantis dažniausius tapatybės vagystės elektroninėje erdvėje būdus.

Taigi, nusikaltėliai yra labai išradingi, siekdami gauti informacijos apie aukas. Todėl atsižvelgiant į tapatybės vagystės elektroninėje erdvėje būdus, turi būti tobulinami ir tokio pavojingo reiškinio prevencijos būdai. Jų žinojimas padeda geriau tokias pavojingas veikas tirti ir kvalifikuočiau vertinti jas iš baudžiamosios, civilinės ar administracinės teisės pozicijų.

Apibendrinančios išvados

• Pirmieji tapatybės vagystės atvejai pasitaikė gerokai anksčiau, nei atsirado internetas, kai ši veika buvo – ir vis dar yra – atliekama taikant tokius metodus kaip „šiukšlių rinkimas", mokėjimo kortelės vagystė, dingsties ieškojimas, „žiūrėjimas per petį", duomenų nuskaitymas nuo kortelių apgaulės būdu arba kompiuterio vagystė.

• Šiuo metu tapatybės vagystės metodai yra gerokai tobulesni dėl sparčios interneto, informacinių ir ryšio technologijų plėtros, kuri suteikia galimybę tapatybės vagystės subjektams kompiuteriuose įdiegti kenkėjiškas programas ar taikyti duomenų vagystės metodą naudojant kenkėjiškas programas ar nepageidaujamas elektroninio pašto žinutes.

[192] *Interpolo vadas: kibernetiniai nusikaltimai – didžiausia grėsmė.* [interaktyvus]. 2010-09-22 [žiūrėta 2011 09 18]. <http://www.elektronika.lt/naujienos/kompiuterija/25373/interpolo-vadas-kibernetiniai-nusikaltimai-didziausia-gresme>.

• Tapatybės vagystės elektroninėje erdvėje yra atliekamos įvairiais būdais, kurie kinta ir tobulėja kartu su technologijų pažanga. Šiuo metu dažniausiai taikomi 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 nuo kortelių nuskaitymas apgaulės būdu (angl. *skimming*), apgaulinga IP taktika (angl. *pharming*), pakartojimo ataka (angl. *replay attack*), elektroninių šiukšlių rinkimas (angl. *dumster diving*), netikro profilio socialiniame tinkle sukūrimas.

• Atsižvelgiant į tapatybės vagystės elektroninėje erdvėje būdus, turi būti tobulinama ir šio pavojingo reiškinio prevencija. Būdų žinojimas taip pat padeda geriau atlikti tokių pavojingų veikų tyrimą ir kvalifikuočiau vertinti veikas iš baudžiamosios, civilinės ar administracinės teisės pozicijų.

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 kelia potencialią riziką, kad tretieji asmenys, neturintys teisės susipažinti su tam tikra informacija, vis dėlto turės galimybę tai padaryti.

Elektroninėje erdvėje galima naudotis neišsenkančiu informacijos kiekiu, tačiau kompiuteris internetu tampa pasiekiamas iš bet kurio kito kompiuterio. Dėl šios priežasties kyla 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 be jūsų žinios panaudoti savo kėslams, pavyzdžiui, įdiegęs specialias programas, siųsti iš jūsų kompiuterio nepageidaujamas elekt-

roninio pašto žinutes, panaudoti jį atakoms prieš kitus kompiuterius ir pan.[193].

Pati elektroninė erdvė pasižymi vartotojų gausa, sparčiais struktūros ir formos pokyčiais, informacijos tvarkymo decentralizavimu, teritorinių apribojimų nepaisymu ir pan.[194]. Tokie įrankiai kaip paieškos sistemos, slapukai (angl. *cookies*), elektroninės parduotuvės, elektroniniai atsiskaitymai, žaidimai, sveikatos diagnozė *on-line*[195], 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, kuria pasinaudojant, kaip jau buvo minėta anksčiau, galima nustatyti asmens tapatybę.

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 ir pakankamai individualizuoti ir apibūdinti 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;

---

[193] Lietuvos Respublikos ryšių reguliavimo tarnybos Tinklų ir informacijos saugumo skyriaus interneto tinklalapis, skirtas informacijos saugai elektroninėje erdvėje [interaktyvus, žiūrėta 2011-09-18]. <http://www.esaugumas.lt/index.php?-229839978>.

[194] Reidenberg, J. R.; Schwartz., P. M. Data protection law and on-line services: regulatory responses. ARETE Study, p. 4, 5. [interaktyvus, žiūrėta 2011-09-18]. <http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/regul_en.pdf >.

[195] *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.

2) nematomos nuorodos į kitus tinklalapius (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 ir serverio santykiams, duomenims rinkti ir gali būti serverio vertinami dabartinio ir vėlesnio apsilankymo tinklalapyje metu. Slapukai gali būti efektyviai naudojami palengvinti naršymo duomenų ir savanoriškai atskleistos informacijos rinkimą ir naudojimą. Tai padaroma kiekvienam vartotojui suteikiant unikalų kodą ir saugant šį numerį slapuke. Šis kodas yra atkuriamas kiekvieną kartą aplankant tą konkretų tinklalapį. Vėliau apie vartotoją surinkta informacija gali būti susieta su šiuo unikaliu kodu[196].

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

Kai įeinama į tinklalapį, iš vartotojo kompiuterio į serverį 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 tinklalapį; vartotojo elektroninio pašto adresas, o jei buvo naudojama paieškos sistema, – ir visos užklausos. Lankymosi internete metu generuojami duomenys apie aplankytus tinklalapius, 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 pagal IP adresą gali nustatyti tik interneto

[196] Civilka, M. *Asmens duomenų teisinis reguliavimas interneto kontekste*, p. 4. [interaktyvus, žiūrėta 2011-09-18]. <http://media.search.lt/GetFile.php?OID=92932&FID=269994>.

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 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 identifikuotu kompiuteriu nebūtinai 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 daryti išvadą, kad informacija, surinkta naudojant slapukus, neturėtų būti laikoma asmenine informacija. Slapukai patys savaime neidentifikuoja konkretaus asmens, nes duomenys, surinkti slapukų, yra labiau susiję su konkretaus kompiuterio naudojimu 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[197]. 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.

[197] *DoubleClick* kompanijos tinklalapis. [interaktyvus, žiūrėta 2011-09-18]. <http://www.doubleclick.com/privacy>.

Pažymėtina, kad internetas buvo kuriamas kaip atviras tinklas. Jo veikimas pagrįstas TCP/IP protokolų[198] pagrindu, tačiau vien tik TCP/IP protokolai neužtikrina konfidencialumo ir sąžiningumo, autentiškumo ar prieinamumo. Duomenų paketai gali būti persiunčiami kaip paprastas tekstas, t. y. neužšifruoti, ir tokiu atveju užpuolikas 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 iki šiol nebuvo numatę ir nėra išsprendę TCP/IP protokolai.

Be to, paminėtina, kad pavojų asmeniui elektroninėje erdvėje gali kelti ir jo paties viešai skelbiama asmeninė informacija[199]. Kuo daugiau asmuo apie save skelbia asmeninės informacijos (ypač svarbios, tokios kaip gyvenamosios vietos adresas, paso numeris ir kt.), tuo didesnė tikimybė, kad šio asmens tapatybė bus pasisavinta.

Apibendrinant galima teigti, kad šiame poskyryje nurodomų pavojų, kylančių asmens duomenims elektroninėje erdvėje, sąrašas nėra baigtinis. Kiekvieną apie vartotoją, prisijungusį prie interneto, (dažniausiai jam net nežinant) surenkama daugybė informacijos, kurios rinkimo ir naudojimo tikslai nėra aiškūs, tad visada išlieka rizika tapti potencialia teisės į privatumą ir duomenų apsaugą pažeidimo auka.

Apibendrinančios išvados

• Tapatybės vagystės atvejų daugėja, o pats reiškinys dėl nuolatinės informacinių ir ryšio technologijų pažangos įgyja naujų formų, kurios iš fizinės erdvės vis didesniu mastu 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

[198] 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.

[199] Higgins, G. E. 2010. *Cybercrime: An Introduction to an Emerging Phenomenon*. McGraw-Hill, p. 69.

duomenų rinkimas ir tvarkymas (angl. *browsing chaterring*); nematomos nuorodos į kitus tinklalapius (angl. *invisible hyperlinks*) ir slapukai (angl. *cookies*). Visais šiais atvejais eiliniam interneto vartotojui nepastebimu būdu apie jį renkami ir kaupiami didžiuliai asmeninės informacijos kiekiai, kurių naudojimo 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 efektyviai informacinės visuomenės narių tarpusavio komunikacijai.

3. Teisinis reguliavimas, susijęs su tapatybės vagyste elektroninėje erdvėje

Apskritai socialiniai santykiai, susiję su informacinėmis technologijomis ir elektronine erdve, pastaraisiais dešimtmečiais labai stipriai kito: atsirado naujų iki tol neegzistavusių technologijų (pvz., internetinė telefonija, internetinė televizija ir kt.) ir dėl jų atsiradimo susiklostė nauji socialiniai santykiai. Šie santykiai sparčiai globalizuojasi ir šiuo metu daugelyje sričių analizuoti socialinius santykius, atsirandančius informacinių technologijų ir elektroninės erdvės srityje bei nacionalinėje plotmėje sudėtingiau, negu analizuoti tarptautinius ir regioninius procesus.

Kitas labai svarbus aspektas: iki šiol skirtingais laikyti socialiniai santykiai, reguliuojami skirtingų teisės normų (ir net pasitelkiant skirtingus principus), tampa (susilieja) vientisais (kartais naujais), sunkiai atribojamais (pvz., anksčiau labai skirtingas teisinis reguliavimas buvo taikomas duomenims perduoti (internetui ir kt.) ir televizijai bei radijui; šiuo metu ir televiziją, ir radiją galima matyti ir girdėti internetu), todėl kyla klausimas, kaip rasti tokių skirtingų santykių bendrus teisinio reguliavimo modelius.

Prie tokio spartaus socialinių santykių kitimo valstybės privalo pritaikyti savo teisėkūros procesą, kuris dėl demokratiškos pobūdžio yra gana sudėtingas ir ilgai trunkantis. Pradinis klausimas, kurį turi išspręsti valstybė, norėdama sunorminti socialinius santykius, – ko ji siekia vienokiu ar kitokiu teisiniu reguliavimu, kiek vieni ar kiti santykiai yra svarbūs? Atsižvelgiant į tai, kad tas pačias problemas atskiros valstybės dažnai sprendžia panašiais, bet nevienodais būdais, atsiranda teisinio reguliavimo skirtumų, kurie ne visada dera globaliame elektroninės erdvės kontekste, t. y. akivaizdžiai trūksta vienodo suvokimo, kokie yra atitinkamo teisinio reguliavimo tikslai, kokios socialinės vertybės elektroninėje erdvėje yra teisės reguliuojamas gėris (vertybė), koks teisinio reguliavimo modelis veiksmingas siekiant teisinio reguliavimo tikslų, o kas, deja, šiuo metu plačiai taikoma, bet yra brangu ir neatitinka tikslų, o gal net neveiksminga.

Sparčiai kintant, darantis globaliems ir vientisiems socialiniams santykiams valstybių teisėkūros procesas nespėja užtikrinti ir laiku vykdyti

teisinio reguliavimo pokyčių. Dabartinėje teisėkūroje ir moksle, norint pagrįsti vienokių ar kitokių socialinių santykių teisinį reguliavimą, dažniausiai vadovaujamasi tik ekonominiais sektoriaus reguliavimo argumentais. Ekonominiai argumentai neabejotinai labai svarbūs, tačiau neatlikus gilios sisteminės teisinio reguliavimo analizės sudėtinga tobulinti konkrečių visuomeninių santykių teisinį reguliavimo sritį. Todėl toliau bus nagrinėjamas su tapatybės vagyste elektroninėje erdvėje susijusių visuomeninių santykių teisinis reguliavimas.

3.1. Tarptautiniai bei regioniniai teisinio reguliavimo dokumentai ir tapatybės vagystė elektroninėje erdvėje

Labai svarbu visų pirma nustatyti, kiek tarptautinių dokumentų nuostatos reglamentuoja tapatybės vagystę elektroninėje erdvėje. Šie dokumentai gali būti skirstomi į privalomojo ir rekomendacinio pobūdžio.

3.1.1. Konvencija dėl elektroninių nusikaltimų

Konvencija dėl elektroninių nusikaltimų buvo pasirašyta 2001 metais, o įsigaliojo 2004 m. liepos 1 d. Šis teisės aktas mokslinėje literatūroje laikomas vienu iš sistemingiausių tarptautinių teisės aktų, reguliuojančių žalingas ir kriminalines veikas naudojant kompiuterį[200] (Konvencija dėl elektroninių nusikaltimų pridedama kaip 1 priedas). 2011 m. balandžio mėn. konvenciją buvo pasirašiusios 30 valstybės, ratifikavo 17. Kadangi iš viso yra 195 valstybės, konvencija labai minimaliai turi įtakos globaliai kovai su elektroniniais nusikaltimais[201]. Todėl konvencija gali būti svarbus, bet ne vienintelis teisinis dokumentas kovojant su elektroniniais nusikaltimais.

Visgi konvencija šiuo metu yra vienintelis privalomojo tarptautinio pobūdžio dokumentas, skirtas elektroniniams nusikaltimams. Kovojant su tapatybės vagyste, svarbi visa konvencija ir jos struktūrinių dalių nuostatos. Ypač svarbios yra konvencijos nuostatos dėl materialinės teisės, nes būtent šios nuostatos skirtos nusikaltimams kaip atitinkamoms veikoms,

[200] Williams, M. 2006. *Virtually criminal: Crime, deviance and regulation online*. New York: Routledge, p. 33.

[201] Brenner, S. W. 2010. *Cybercrime. Criminal Threats from Cyberspace*. Library of Congress Cataloging, p. 209.

susijusioms su tapatybės vagyste elektroninėje erdvėje, įvardyti. Labai svarbios ir konvencijos nuostatos dėl proceso teisės (numatomos galimybės geriau atlikti procesinius veiksmus) ir nuostatos dėl tarptautinio bendradarbiavimo. Turint omenyje, kad tapatybės vagystė elektroninėje erdvėje dažnai peržengia vienos valstybės sienas, nuostatos dėl tarptautinio bendradarbiavimo būtent ir skirtos tiems atvejams, kai šis pavojingas reiškinys tampa ne nacionaliniu. Nepaisant kompleksinio konvencijos poveikio tapatybės vagystei elektroninėje erdvėje, toliau kaip svarbiausios bus minimos tik Konvencijos materialinės teisės nuostatos.

Labai svarbus pirmasis konvencijos skirsnis „Materialioji baudžiamoji teisė", kuriame numatoma, kad už tam tikras pavojingas veikas, vykdomas elektroninėje erdvėje, turi būti nustatyta baudžiamoji atsakomybė. Šiame skirsnyje tiesiogiai nenurodoma nustatyti atsakomybės už tapatybės vagystę elektroninėje erdvėje, tačiau daugelis pavojingų veikų gali būti vienaip ar kitaip susijusios su tapatybės vagyste elektroninėje erdvėje.

Antrajame konvencijos straipsnyje nurodoma nustatyti baudžiamąją atsakomybę už neteisėtą prieigą: „Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti pagal jos vidaus teisę nustatyti baudžiamajai atsakomybei už sąmoningą ir neteisėtą prieigą prie visos kompiuterinės sistemos arba jos dalies. Šalis gali reikalauti, kad toks nusikaltimas būtų padarytas pažeidžiant apsaugos priemones, ketinant gauti kompiuterinius duomenis ar turint kitą nesąžiningą ketinimą, arba kad jis būtų susijęs su kompiuterine sistema, sujungta su kita kompiuterine sistema"[202]. Šia nuostata siekiama, kad būtų nustatyta baudžiamoji atsakomybė už veikas, keliančias pavojų kompiuterinių sistemų ir duomenų saugumui (konfidencialumui, integruotumui ir prieinamumui), t. y. už vadinamąsias angl. *Hacking*, *Cracking*, *Computer trespass*[203]. Praktikoje neteisėta prieiga gali būti naudojama siekiant neteisėtai pasisavinti atitinkamus asmens duomenis, kurie vėliau gali būti naudojami kitiems nusikaltimams (pvz., sukčiavimui) įvykdyti. Kitaip tariant, neteisėta prieiga gali būti pirmoji tapatybės vagystės elektroninėje erdvėje stadija.

Kita pavojinga veika – neteisėta perimtis. Konvencijos 3 straipsnyje nurodyta, kad „kiekviena Šalis priima tokius teisės aktus ir kitas prie-

[202] Konvencija dėl elektroninių nusikaltimų. *Valstybės žinios*. 2004, Nr. 36-1188, 2 str.

[203] Štitilis D. 2002. *Teisinės atsakomybės už neteisėtas veikas elektroninėje erdvėje nustatymo problemos*: daktaro disertacija, socialiniai mokslai, teisė 01 S, p. 78.

mones, kurių gali prireikti pagal jos vidaus teisę nustatyti baudžiamajai atsakomybei už sąmoningą ir neteisėtą neviešo kompiuterinių duomenų perdavimo į kompiuterinę sistemą, iš jos ir jos viduje perimtį techninėmis priemonėmis, taip pat už elektromagnetinės emisijos iš kompiuterinės sistemos, perduodančios tokius kompiuterinius duomenis, perimtį. Šalis gali reikalauti, kad toks nusikaltimas būtų padarytas turint nesąžiningą ketinimą arba susijęs su kompiuterine sistema, sujungta su kita kompiuterine sistema“[204]. Šia nuostata siekiama apsaugoti duomenų komunikacijų privatumą, kuris apsaugotas Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos[205] 8 straipsniu. Ši pavojinga veika taip pat gali būti vykdoma siekiant perimti asmeninę informaciją, turint tikslą vėliau pasinaudojant šia informacija vykdant kitus nusikaltimus (pvz., sukčiavimą).

Kai siekiama pakeisti asmeninius duomenis, turint tikslą suklastoti tapatybę, gali būti įvykdoma kita konvencijoje aprašyta pavojinga veika – poveikis duomenims. Pagal konvencijos 4 straipsnį: „Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti pagal jos vidaus teisę nustatyti baudžiamajai atsakomybei už sąmoningą ir neteisėtą kompiuterinių duomenų sugadinimą, sunaikinimą, apgadinimą, pakeitimą arba galimybės naudotis tokiais duomenimis panaikinimą. Šalis gali pasilikti teisę reikalauti, kad veika, apibūdinta šio straipsnio 1 dalyje, turi padaryti didelę žalą“[206]. Šios nuostatos tikslas yra apsaugoti tinkamą kompiuterinės informacijos (įskaitant ir asmeninės informacijos arba informacijos, apimančios tapatybės nustatymo elektroninėje erdvėje duomenis) apdorojimą ir tinkamą išsaugotos kompiuterinės informacijos ar kompiuterinių programų naudojimą.

Siekiant pasisavinti tapatybės informaciją, gali būti neteisėtai naudojamos atitinkamos priemonės (pvz., slaptažodžių nulaužimo programos), apie kurias nurodoma konvencijos 6 straipsnyje:

„1. Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti pagal jos vidaus teisę nustatyti baudžiamajai atsakomybei už sąmoningą ir neteisėtą:

[204] Konvencija dėl elektroninių nusikaltimų. *Valstybės žinios*. 2004, Nr. 36-1188, 3 str.

[205] Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija. *Valstybės žinios*. 1995, Nr. 40-987.

[206] Konvencija dėl elektroninių nusikaltimų. *Valstybės žinios*. 2004, Nr. 36-1188, 4 str.

a) gaminimą, pardavimą, įsigijimą naudoti, įvežimą, platinimą arba kitokį galimybės naudotis suteikimą:

i) įtaiso, įskaitant kompiuterinę programą, sukurto ar pritaikyto pirmiausia 2–5 straipsniuose apibūdintiems nusikaltimams daryti;

ii) kompiuterio slaptažodžio, prieigos kodo arba panašių duomenų, kuriais galima prieiti prie visos kompiuterinės sistemos arba jos dalies,

kai ketinama juos panaudoti 2–5 straipsniuose apibūdintiems nusikaltimams daryti, ir

b) a punkto i ir ii papunkčiuose minimo dalyko turėjimą ketinant jį panaudoti 2–5 straipsniuose apibūdintiems nusikaltimams daryti. Šalis, vadovaudamasi savo teise, gali reikalauti, kad baudžiamoji atsakomybė būtų užtraukiama tik turint keletą tokių dalykų.

2. Šis straipsnis negali būti aiškinamas kaip užtraukiantis baudžiamąją atsakomybę kai šio straipsnio 1 dalyje minimas gaminimas, pardavimas, įsigijimas naudoti, įvežimas, platinimas ir kitoks galimybės naudotis suteikimas arba turėjimas nėra skirtas daryti nusikaltimui, apibūdintam šios Konvencijos 2–5 straipsniuose, o tik sankcionuotam kompiuterinės sistemos tikrinimui arba jos apsaugai.

3. Kiekviena Šalis gali pasilikti teisę netaikyti šio straipsnio 1 dalies, jei ši išlyga nesiejama su pardavimu, platinimu arba kitokiu galimybės naudoti šio straipsnio 1 dalies a punkto ii papunktyje nurodytas priemones sudarymą“[207].

Dar nuodugniau su tapatybės vagyste elektroninėje erdvėje susijusios veikos aprašytos pirmojo Konvencijos skirsnio 2 dalyje, kurioje siūloma nustatyti baudžiamąją atsakomybę už tokias pavojingas veikas, kaip kompiuterinės klastotės ir kompiuterinis sukčiavimas.

Konvencijos 7 straipsnyje „Kompiuterinės klastotės“ numatyta: „Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti pagal jos vidaus teisę nustatyti baudžiamajai atsakomybei už sąmoningą ir neteisėtą kompiuterių duomenų įvedimą, pakeitimą, sunaikinimą arba galimybės naudotis tokia informacija panaikinimą, kurių pasekmė yra neautentiški duomenys, su tikslu, kad jie būtų laikomi autentiškais, ar jais būtų naudojamasi teisėtiems tikslams, nepriklausomai nuo to, ar šie duomenys yra tiesiogiai skaitomi ir suprantami. Šalis gali reikalauti, kad

[207] *Ibid.*, 6 str.

baudžiamoji atsakomybė užtraukiama tik esant ketinimui apgauti ar panašiam nesąžiningam ketinimui.“[208] Kompiuterinių klastočių tikslu taip pat gali būti suklastojama ir asmeninė informacija, ir tapatybė.

Pagrindinė veika, kuri dažniausiai vykdoma suklastojus asmens tapatybę – sukčiavimas. Konvencijos 8 straipsnyje numatyta: „Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti pagal jos vidaus teisę nustatyti baudžiamajai atsakomybei už sąmoningus ir neteisėtus veiksmus, sąlygojusius kito asmens nuosavybės praradimą:

a) įvedant, pakeičiant, sunaikinant kompiuterinius duomenis arba panaikinant galimybę naudotis tokiais duomenimis;

b) paveikiant kompiuterinės sistemos darbą,

nesąžiningai arba nedorai ketinant gauti neteisėtos ekonominės naudos sau arba kitam asmeniui.“[209]

Paminėtina, kad suklastojus ar pasisavinus elektroninę asmens tapatybę elektroninėje erdvėje galima įvykdyti ir kitas konvencijoje paminėtas pavojingas veikas – turinio nusikaltimus ar nusikaltimus, susijusius su autorių teisėmis ar gretutinėmis teisėmis (konvencijos 9–10 straipsniai).

3.1.2. Europos Sąjungos dokumentai dėl elektroninių nusikaltimų

2007 m. gegužės 22 d. Komisijos komunikatas Europos parlamentui, Tarybai ir Regionų komitetui „Bendros politikos kovojant su elektroniniais nusikaltimais link“ KOM(2007)267 galutinis[210]

Komunikato „Link bendrosios politikos kovojant su elektroniniais nusikaltimais“ COM(2007)267 *final* 1.2.2 punkte „Tradiciniai nusikaltimai elektroninių ryšių tinkluose“ nurodyta, kad dauguma nusikaltimų gali būti įvykdomi naudojant elektroninių ryšių tinklus. Tačiau tapatybės vagystė traktuojama kaip instrumentas: „Tokie instrumentai, kaip tapatybės vagystė, duomenų vagystė, nepageidaujamos elektroninio pašto žinutės ir piktybiniai kodai gali būti panaudojami siekiant įvykdyti plataus masto sukčiavimą.“

[208] *Ibid.*, 7 str.

[209] *Ibid.*, 8 str.

[210] 2007 m. gegužės 22 d. Komisijos komunikatas Europos parlamentui, Tarybai ir Regionų komitetui „Bendros politikos kovojant su elektroniniais nusikaltimais link“ COM(2007)267 [interaktyvus, žiūrėta 2011-09-19]. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:LT:PDF>.

Tačiau jau kitoje komunikato vietoje apie tapatybės vagystę rašoma, jog teisės aktai kovojant su elektroniniais nusikaltimais, vis dėlto turėtų būti persvarstomi. Atskiras klausimas, kurį gali reikėti reglamentuoti, yra susijęs su situacija, kai įvykdytas elektroninis nusikaltimas susijęs su tapatybės vagyste. Taigi tapatybės vagystė šiame komunikate nevertinama kaip savarankiškas elektroninis nusikaltimas, tačiau apibūdinama kaip reiškinys, galintis būti glaudžiai susijęs su elektroniniais nusikaltimais. 3.3. komunikato punkte nurodoma, kad „apskritai „tapatybės vagystė" yra suprantama kaip asmeninės informacijos (pvz., kreditinės kortelės numerio) kaip instrumento panaudojimas tam, kad būtų galima įvykdyti kitus nusikaltimus. Daugelyje Šalių Narių nusikaltėlis veikiausiai būtų persekiojamas kaip už sukčiavimą ar kitą potencialų nusikaltimą, bet ne už tapatybės vagystę. Tapatybės vagystė, kaip tokia, nėra kriminalizuota visose Šalyse Narėse. Dažnai yra lengviau įrodyti tapatybės nusikaltimą nei sukčiavimą, todėl kriminalizavus tapatybės vagystę, Europos Sąjungos teisėsaugos institucijų bendradarbiavimas būtų geresnis"[211].

Komunikate taip pat nurodoma, kad turėtų būti pradėti išsamesni tyrimai tam, kad būtų parengti pasiūlymai specialiam teisiniam reguliavimui kovojant su tapatybės vagyste.

2009 m. kovo 30 d. Komisijos komunikatas Europos Parlamentui, Tarybai ir Regionų komitetui dėl ypatingos svarbos informacinės infrastruktūros apsaugos „Europos apsauga nuo didelio masto kibernetinių antpuolių ir veiklos sutrukdymo – geresnė parengtis, didesnis saugumas ir atsparumas" COM(2009)149 galutinis[212]

Šiame komunikate daugiausia dėmesio skirta prevencijai, parengčiai bei informavimui ir sudarytas neatidėliotinų veiksmų planas, kaip didinti ypatingos svarbos informacinės infrastruktūros objektų saugumą ir atsparumą.

[211] Communication from the Commission to the Parliament, the Council and the Committee of Regions „Towards a general policy on the fight against cyber crime" COM(2007) 267 final, p.3.3 [interaktyvus, žiūrėta 2011-09-19]. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF>.

[212] 2009 m. kovo 30 d. Komisijos komunikatas Europos Parlamentui, Tarybai ir Regionų komitetui dėl ypatingos svarbos informacinės infrastruktūros apsaugos „Europos apsauga nuo didelio masto kibernetinių antpuolių ir veiklos sutrukdymo – geresnė parengtis, didesnis saugumas ir atsparumas" COM(2009)149 galutinis [interaktyvus, žiūrėta 2011-09-19]. < http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:LT:PDF>.

Komunikato 3.2 punkte teigiama: „Kibernetiniai antpuoliai tapo kaip niekad sudėtingi. Paprasti eksperimentai perauga į sudėtingus veiksmus, vykdomus siekiant pelno arba politinių tikslų. Neseniai įvykdyti didelio masto kibernetiniai Estijos, Lietuvos ir Gruzijos antpuoliai – tai plačiausiai nušviesti bendrosios tendencijos pavyzdžiai. Kokia sunki problema, galima įsitikinti iš to, kad yra daug virusų, „kirminų" (savaime plintančių kenksmingų kompiuterinių programų) ir kitos kenkėjiškos programinės įrangos, kad didėja kenksmingu programiniu kodu apkrėstų kompiuterių tinklai (angl. *botnet*) ir nuolat daugėja nepageidaujamų e. pašto laiškų."[213] Ir nors pačiame komunikate tiesiogiai nenurodoma į tapatybės vagystę, tyrimai ir praktika liudija, kad dažniausiai kibernetiniai išpuoliai atliekami maskuojant tikrąją tapatybę, t. y. pasinaudojant netikra ar suklastota elektronine tapatybe. Kitaip tariant, tapatybės vagystė yra neatsiejama plataus masto ir labai pavojingų kibernetinių išpuolių dalis.

2006 m. gegužės 31 d. Komisijos komunikatas Europos Parlamentui, Tarybai ir Regionų komitetui saugios informacinės visuomenės strategija – „Dialogas, partnerystė ir teisių suteikimas" COM(2006)0251 galutinis[214]

Komunikate nurodyta, kad Komisija kviečia privataus sektoriaus suinteresuotąsias šalis imtis iniciatyvos <...> skatinti įvairovę, atvirumą, sąveiką, naudojimą ir konkurenciją kaip pagrindinius saugumą užtikrinančius veiksnius bei saugumą didinančių produktų, procesų ir paslaugų naudojimą siekiant užkirsti kelią asmens tapatybės duomenų vagystėms ir kitokioms privatumą pažeidžiančiomis atakoms. Pagal komunikatą: „Duomenų vagystės – apgavystės internetu forma, kai siekiama pavogti vertingą informaciją, tokią kaip kreditinių kortelių, banko sąskaitų numerius, var-

[213] 2009 m. kovo 30 d. Komisijos komunikatas Europos Parlamentui, Tarybai ir Regionų komitetui dėl ypatingos svarbos informacinės infrastruktūros apsaugos „Europos apsauga nuo didelio masto kibernetinių antpuolių ir veiklos sutrukdymo – geresnė parengtis, didesnis saugumas ir atsparumas" COM(2009)149 galutinis, p.5 [interaktyvus, žiūrėta 2011-09-19]. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:LT:PDF>.

[214] 2006 m. gegužės 31 d. Komisijos komunikatas Europos Parlamentui, Tarybai ir Regionų komitetui saugios informacinės visuomenės strategija – „Dialogas, partnerystė ir teisių suteikimas" COM(2006)0251 galutinis [interaktyvus, žiūrėta 2011-09-19]. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0251:FIN:LT:HTML>.

totojo tapatybės numerius ir slaptažodžius“[215]. Taigi komunikate tapatybės numerių pasisavinimas siejamas su duomenų vagyste kaip pažeidimu.

Europos Parlamento ir Tarybos direktyva dėl atakų prieš informacines sistemas ir dėl tarybos pamatinio sprendimo 2005/222/TVR panaikinimo KOM(2010)517 galutinis (siūlymas)[216]

Pamatiniame sprendime nurodoma, kad kai atakos rengiamos slepiant tikrąją nusikaltėlio tapatybę ir daroma žala teisėtam tapatybės turėtojui, tokia veika turėtų būti vertinama kaip sunkinanti aplinkybė[217]. Šios taisyklės turėtų derėti su baudžiamųjų nusikaltimų ir bausmių teisėtumo ir proporcingumo principais bei galiojančiais asmens duomenų apsaugą reglamentuojančiais teisės aktais.

Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui „Europos skaitmeninė darbotvarkė“ KOM(2010) 245 galutinis[218]

Pristatytoje Europos skaitmeninėje darbotvarkėje, pirmojoje pagal strategiją „Europa 2020“ parengtoje pavyzdinėje iniciatyvoje, pripažinta, kad būtina Europos mastu kovoti su naujų formų nusikaltimų, visų pirma elektroninių nusikaltimų, plitimu. Į pasitikėjimą ir saugumą orientuotų veiksmų srityje Komisija yra pasiryžusi imtis priemonių, skirtų kovoti su kibernetinėmis atakomis, nukreiptomis prieš informacines sistemas. Komunikato dalyje dėl didėjančio elektroninio nusikalstamumo ir menko

[215] 2006 m. gegužės 31 d. Komisijos komunikatas Europos Parlamentui, Tarybai ir Regionų komitetui saugios informacinės visuomenės strategija – „Dialogas, partnerystė ir teisių suteikimas“ COM(2006)0251 galutinis. [interaktyvus, žiūrėta 2011-09-19]. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0251:FIN:LT:HTML>.

[216] Europos Parlamento ir Tarybos direktyva dėl atakų prieš informacines sistemas ir dėl tarybos pamatinio sprendimo 2005/222/TVR panaikinimo KOM(2010)517 galutinis (siūlymas) [interaktyvus, žiūrėta 2011-09-19]. <http://www.europarl.europa.eu/meetdocs/2009_2014/documents/com/com_com(2010)0517_/com_com(2010)0517_lt.pdf >.

[217] Europos Parlamento ir Tarybos direktyva dėl atakų prieš informacines sistemas ir dėl tarybos pamatinio sprendimo 2005/222/TVR panaikinimo KOM(2010)517 galutinis (siūlymas), 3 B [interaktyvus, žiūrėta 2011-09-19]. <http://www.europarl.europa.eu/meetdocs/2009_2014/documents/com/com_com(2010)0517_/com_com(2010)0517_lt.pdf>.

[218] Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui „Europos skaitmeninė darbotvarkė“ KOM(2010) 245 galutinis [interaktyvus, žiūrėta 2011-09-19]. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:LT:PDF>.

pasitikėjimo tinklais pavojaus rašoma, kad Europoje privalu spręsti problemas, susijusias su tuo, kad plinta naujos rūšies nusikalstamumas, t. y. elektroninis nusikalstamumas, įskaitant vaikų išnaudojimą, tapatybės vagystes ir kibernetines atakas, ir sukurti tinkamus reagavimo mechanizmus[219].

Apibendrinančios išvados

• Konvencija dėl elektroninių nusikaltimų šiuo metu yra vienintelis privalomojo tarptautinio pobūdžio dokumentas, skirtas kovai su elektroniniais nusikaltimais, taigi ir su tapatybės vagystėmis elektroninėje erdvėje.

• Tarptautiniuose teisės aktuose tapatybės vagystei elektroninėje erdvėje skiriama nedaug dėmesio. Dažniausiai tiesiogiai neminima tapatybės vagystės elektroninėje erdvėje, o tuose dokumentuose, kur ši pavojinga veika minima tiesiogiai, apsiribojama tik abstrakčiu paminėjimu, kad tai pavojinga veika, siekiant įvykdyti kitus nusikaltimus.

• Naujausiuose teisės aktuose jau siūloma imtis konkrečių priemonių, kovojant su tapatybės vagyste elektroninėje erdvėje; vienas iš siūlomų galimų kovos būdų – šios pavojingos veikos kriminalizavimas.

3.2. Specifinės teisinio reguliavimo sritys, kovojant su tapatybės vagyste elektroninėje erdvėje (pasirinktų užsienio valstybių ir Lietuvos analizė)

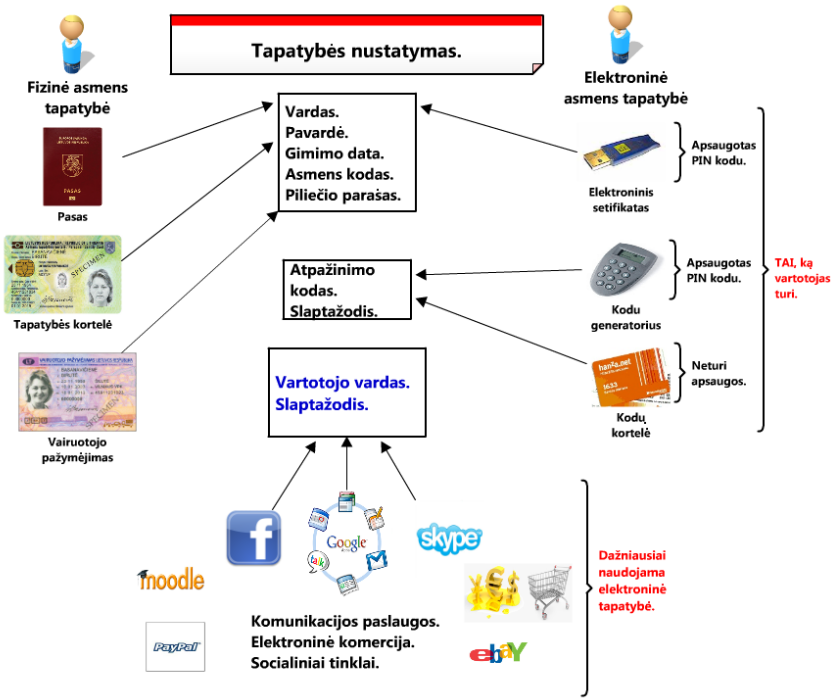
3.2.1. Asmens identifikavimo elektroninėje erdvėje teisinis reguliavimas

Vienas iš svarbiausių klausimų, susijusių su elektroninės tapatybės teisiniu reguliavimu, yra tokios tapatybės sukūrimas[220]. Kaip jau minėta, elektroninėje erdvėje tapatybė nustatoma dažniausiai pagal tai, ką vartotojas turi (patvirtinta tapatybė), tačiau per pastaruosius kelerius metus atsirado kitų, vartotojo pasirinktų tapatybių elektroninėje erdvėje, kurios skirstomos pagal profilius, sukuriamus oficialioje aplinkoje arba asmeninėje aplinkoje.

[219] Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui „Europos skaitmeninė darbotvarkė“ KOM(2010) 245 galutinis [interaktyvus, žiūrėta 2011-09-19], p. 6. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:LT:PDF>.

[220] Pirmoji iniciatyva ES šalyse vykdomas projektas STORK (angl. *Secure idenTity acrOss boRders linKed*). <www.eid-stork.eu>.

Elektroninių identifikavimo būdų ir priemonių naudojimą bei santykį su realiu asmeniu galima pavaizduoti grafiškai. 2 paveiksle pateikiama apibendrinta informacija dėl asmens tapatybės nustatymo tiek fizinėje, tiek elektroninėje erdvėje priemonių: kairėje pusėje pavaizduotos asmens tapatybės nustatymo fizinėje erdvėje priemonės, dešinėje – nurodytos patvirtintos elektroninės tapatybės priemonės, kai asmuo gali būti vienareikšmiškai nustatytas. O paveikslo apačioje nurodytos dažniausiai naudojamos nepatvirtintos tapatybės priemonės.



18 pav. Tapatybės nustatymas (sudaryta autorių)

Nepatvirtintos tapatybės atveju dažniausiai tapatybės nustatymo procese remiamasi vienu rodikliu, o jie lengviau suklastojami ir yra mažiau saugesni. Dažniausiai tapatybės vagystės pasitaiko būtent tokio tipo sistemose. Elektroninėje erdvėje daugiausia naudojama pačių vartotojų sukurta tapatybė, kurią pasisavinti nėra sudėtinga.

Siekiant identifikuoti asmenį asmeninėje aplinkoje, kyla daugiau problemų, susijusių su tapatumo nustatymu, nes vartotojai skirtingose sistemose naudoja įvairius tapatybės patvirtinimo būdus. Taigi, susidaro situacijos, kai vienas asmuo turi 20, 30 ir daugiau elektroninių identifikavimo priemonių. Jos dažnai pamirštamos, dėl to daugėja elektroninių tapatybių šiukšlių.

Gali kilti klausimas, ar reikia garantuoti teisę turėti teisingą, neiškreiptą elektroninę tapatybę. Ši teisė apima santykinai naujus teisinius santykius, kai subjektas pagrįstai tikisi, kad jis pagal elektroninę tapatybę bus tinkamai identifikuojamas ir niekas kitas tokios tapatybės turėti negalės. Ši teisė yra glaudžiai susijusi su kontekstinės vientisumo tapatybės idėja; ji apsaugo nuo neteisingų identifikavimų. Paminėtinas ir vartotojų teisių apsaugos aspektas, kuriuo remiantis, valstybė turėtų imtis tam tikrų priemonių pašalinti lengvai prieinamus būdus pasisavinti tam tikro vartotojo tapatybę (ir tikėtina, dėl to šiam vartotojui padaryti vienokią ar kitokią žalą).

Dažnai akcentuojama vartotojų pasirinkimo laisvė kuriant elektroninę tapatybę, bet tai kartais verčia rinktis pigesnes identifikavimo sistemas. Vartotojai susiduria su daugybe identifikavimo sistemų ir metodų, kurie jungia skirtingus tapatybės elementus, taiko skirtingus standartus ir techninius procesus. Sunku suprasti, kaip kiekviena sistema veikia, sunku jas naudoti. Reikia spręsti švietimo ir sąmoningumo problemas taip, kad vartotojai galėtų tinkamai valdyti savo elektronines tapatybes. Švietimas yra svarbus kuriant pasitikėjimą ir mažinant vartotojų susirūpinimą. Pagrindinis elementas didinant informatyvumą yra atskaitomybė ir aukštas skaidrumo lygis. Tačiau, klausimų, kylančių dėl didelio skaičiaus ir sudėtingumo sistemų atsiranda vis daugiau, atsižvelgiant į tai, turėtų būti parengtos priemonės, kuriomis bus siekiama didinti piliečių žinias, taip pat reikia apsvarstyti priemones, kurios reikalautų didesnio atskaitingumo iš elektroninės tapatybės paslaugų teikėjų.

Kitas klausimas, ar galima verslui privalomai nurodyti, kad būtų kuriamos saugios ir valstybės pripažįstamos tapatybės. Viena vertus, kištis į verslą ydinga praktika. Tačiau, kita vertus, siekiant užtikrinti vartotojų teisių apsaugą, tam tikri valstybės privalomi nurodymai netgi pageidautini.

Autorių nuomone, optimalus variantas – pati rinka turėtų nuspręsti, kokias konkrečiai priemones naudoti identifikavimui, tačiau valstybė turi paskatinti tai padaryti (naudodama teisinį reguliavimą). Valstybė turėtų

nustatyti minimalius identifikavimo elektroninėje erdvėje reikalavimus. Reikėtų nurodyti, kurie duomenys, tapatybės elementai turi būti vienodi skirtinguose sektoriuose, identifikuojant asmenį elektroninėje erdvėje. Derėtų sutarti ir perimti atitinkamą praktiką iš valstybės, kai tapatybei kurti elektroninėje erdvėje naudojami tie patys asmens duomenys kaip ir fizinėje erdvėje[221].

Pagal autorių atliktą ekspertų apklausą, pastarieji taip pat pritaria asmens identifikavimo elektroninėje erdvėje teisiniam reguliavimui. 2-as, 6-as, 7-as, 8-as ir 9-as ekspertai pritaria, kad tam tikros indentifikavimo teisinio reguliavimo priemonės turi būti, dalis jų nurodo, kad ne visas indentifikavimo priemones turi reguliuoti normos, pavyzdžiui: 2-as ekspertas teigia, kad indentifikavimo priemonės turi būti suskirstytos į lygmenis, iš kurių vieniems turėtų būti taikomos normos, kitiems – tik rekomendacijos, o rinkdamasis tam tikrą lygmenį asmuo turėtų nurodyti patikimumo lygį.

Paminėtina, kad pagal autorių atliktą verslo atstovų apklausą, didžioji dauguma respondentų pasisako už tai, kad elektroninio verslo sektoriaus naudojamos asmens identifikavimo priemonės būtų privalomai reguliuojamos teisės normose. Tik nedidelė dalis bijo, kad toks reguliavimas gali būti nelankstus ir apsunkintų veiklą. Atsižvelgiant į tai turi būti ieškoma lankstaus ir subalansuoto teisinio reguliavimo priemonių, nes neigiantieji papildomo teisinio asmens indentifikavimo priemonių reguliavimo poreikį dažniau abejoja ne tokiu poreikiu, o jo lankstumu, adekvatumu ir kt. Didelis respondentų, pritariančių, kad asmens indentifikavimo teisinio reguliavimo priemonės reikalingos, skaičius rodo, jog verslas turi tokio reguliavimo poreikį.

Autoriai taip pat siūlo teisės normose numatyti, kad jei naudojamos nepatikimos identifikavimo priemonės (nepripažįstamos valstybės), paslaugos teikėjas yra atsakingas[222] už neteisėtais veiksmais sukeltas pasekmes. Todėl, manytina, kad toks reguliavimas paskatintų rinką pradėti naudoti patikimas identifikavimo priemones (paremtas tuo, ką vartotojas turi). Ir rinka, remdamasi technologijų neutralumo principu, pati galėtų pasirinkti naudotiną technologiją.

[221] Štitilis, D.; Pakutinskas, P.; Dauparaitė, I.; Laurinaitis, M. 2011. Preconditions for Legal Regulation of Personal Identification in Cyberspace, *Jurisprudence* 18(2): 720.

[222] Prievolė atlyginti padarytus nuostolius

Taip pat paminėtina, kad esama problemų, užkertančių kelią elektroninės tapatybės plėtrai. Su elektronine asmens tapatybe susijusios sąvokos – visiškas, dalinis tapatumo identifikatorius, virtuali tapatybė, interneto vartotojų profiliai ir kt. – šiuo metu nėra teisiškai apibrėžtos. Nebuvimas aiškių ir bendrų sąvokų iškreipia traktavimą, trukdo pasiekti bendrą teisinį sutarimą šiuo klausimu. Be to, skirtinguose teisės šaltiniuose nėra bendros terminijos. Konkrečių apibrėžimų būtinumas atsiranda dėl santykių elektroninėje erdvėje paplitimo. Įvairių paslaugų teikimas elektroniniu būdu reikalauja nustatyti šalis, jų teises ir pareigas, numatyti būdus, kuriais subjektai identifikuojami (vardas, pavardė, numeris, organizacija, įstaiga), tokio identifikatoriaus atsekamumą, šalių autentifikaciją, be viso to, subjektas turi žinoti ir paslaugų teikėjo tapatybę.

3.2.2. Asmens duomenų teisinė apsauga (asmens duomenų teisinės apsaugos principų užtikrinimas įstatymo lygiu Lietuvoje, Rusijoje ir JAV)

Siekiant atlikti išsamią tapatybės vagystės ir tapatybės vagystės elektroninėje erdvėje kaip socialinio teisinio reiškinio analizę, neišvengiamai susiduriama su asmens duomenų sąvoka ir asmens duomenų apsauga, kadangi, kaip jau buvo minėta anksčiau, tapatybės vagystės objektas yra asmens duomenys ir (ar) asmeninė informacija, leidžianti identifikuoti kitą asmenį.

Šioje dalyje bus siekiama atskleisti, ar pasirinktose trijose valstybėse – Lietuvoje, Rusijoje ir Jungtinėse Amerikos Valstijose (toliau – JAV) – įstatymo lygiu yra užtikrinami pagrindiniai asmens duomenų apsaugos principai. Šių trijų ypač skirtingų valstybių pasirinkimą lėmė siekis atskleisti pagrindinius su asmens duomenų apsaugos principų teisiniu reguliavimu susijusius minėtų valstybių skirtumus, nustatyti, ar visose trijose valstybėse yra vienas pagrindinis įstatymas, reglamentuojantis asmens duomenų apsaugą, įtvirtinantis institucijos, atsakingos už tokio įstatymo priežiūrą ir kontrolę, kompetenciją, atsakomybę už asmens duomenų apsaugos reikalavimų nesilaikymą ir pan.

Trumpai pagrindžiant, dėl ko buvo pasirinktos minėtos valstybės, galima argumentuoti, kad Rusija pasirinkta todėl, kad šioje valstybėje klesti nusikaltimai elektroninėje erdvėje, JAV – jog ši valstybė užima pir-

maujančias pozicijas pagal nusikaltėlių, veikiančių elektroninėje erdvėje, skaičių, Lietuva – kaip viena iš Europos Sąjungos valstybių narių.

Asmens duomenų apsaugą reglamentuojantys teisės aktai gali būti skirstomi į privalomuosius ir rekomendacinio pobūdžio, tačiau atsižvelgiant į šio skyriaus tikslą, rekomendacinio pobūdžio teisės aktų nebus nagrinėjama. Siekiant išskirti asmens duomenų apsaugos principus ir atlikti jų perkėlimo į nacionalinius pasirinktų valstybių įstatymus analizę, plačiau bus nagrinėjami du pagrindiniai teisės aktai, reglamentuojantys asmens duomenų apsaugą tarptautiniu ir Europos Sąjungos (regioniniu) lygiu: 1981 m. Strasbūro konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu[223] ir 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva Nr. 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo[224]. Šiuose teisės aktuose įtvirtinti pagrindiniai asmens duomenų apsaugos principai ir jų perkėlimas į valstybių nacionalinius įstatymus.

1981 m. Strasbūro konvencijoje ir Europos Parlamento ir Tarybos direktyvoje Nr. 95/46/EB įtvirtinti pagrindiniai asmens duomenų teisinės apsaugos principai

1981 m. Strasbūro konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (toliau – Konvencija) yra pagrindinis privalomojo pobūdžio tarptautinės teisės aktas, reglamentuojantis asmens duomenų apsaugą. Lietuva Konvenciją pasirašė 2000 m. vasario 11 d., ratifikavo – 2001 m. birželio 1 d. Konvencija Lietuvoje įsigaliojo nuo 2001 m. spalio 1 d., Rusija Konvenciją pasirašė 2001 m. lapkričio 7 d., o JAV apskritai nėra Konvencijos narė.

Konvencijoje siekiama užtikrinti, kad tvarkant asmens duomenis automatizuotai visų šalių teritorijose bus gerbiamos kiekvieno asmens, nepaisant jo tautybės ir gyvenamosios vietos, teisės ir pagrindinės laisvės, o svarbiausia, jo teisė į privatų gyvenimą. Konvencija asmens duomenis apibrėžia kaip informaciją apie nustatytos tapatybės asmenį arba asmenį,

[223] Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu, ETS Nr. 108. *Valstybės žinios*, 2001, Nr. 32-1059.

[224] Europos Parlamento ir Tarybos direktyva Nr. 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo [interaktyvus, žiūrėta 2011-09-19]. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1995L0046:20031120:LT:PDF>.

kurio tapatybę galima nustatyti, ir įtvirtina tokius pagrindinius asmens duomenų apsaugos principus:

1) duomenų kokybės: automatizuotai tvarkomi asmens duomenys turi būti gauti ir tvarkomi sąžiningai ir teisėtai, saugomi konkrečiam ir teisėtam tikslui ir nenaudojami kitu šiam tikslui prieštaraujančiu būdu, tinkami, svarbūs ir ne pernelyg didelės apimties, kurie atitinka konkrečius tikslus, tikslūs, prireikus papildomi nauja informacija, laikomi tokio pavidalo, kad duomenų subjektų tapatybes būtų galima nustatyti ne ilgiau, nei tai yra reikalinga tam tikslui, dėl kurių duomenys buvo saugomi;

2) draudimo automatizuotai tvarkyti ypatingus asmens duomenis: asmens duomenys apie rasinę kilmę, politines pažiūras ir religinius bei kitus įsitikinimus ir asmens duomenys apie sveikatą bei intymų gyvenimą negali būti tvarkomi automatizuotai, jeigu nacionaliniuose teisės aktuose nėra numatyta atitinkamų apsaugos garantijų. Tokie pat reikalavimai taikomi ir asmens duomenims apie teistumą;

3) duomenų apsaugos: automatizuotai kaupiamiems asmens duomenims apsaugoti turi būti imtasi tinkamų apsaugos priemonių, kurios neleistų jų netyčia ar neteisėtai sunaikinti, netyčia prarasti, neleistinai palikti juos prieinamus, keisti ar platinti.

Kalbant apie regioninį asmens duomenų apsaugos reguliavimą, kaip pavyzdys bus nagrinėjamas Europos Sąjungos teisės aktas. Europos Sąjungos valstybėms narės priėmė įsipareigojimus pagal 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyvą Nr. 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo (toliau – Direktyva). Direktyva buvo priimta siekiant išvengti dėl pernelyg didelės nacionalinių įstatymų ir kitų teisės aktų įvairovės atsirandančių asmenų teisių ir laisvių, ypač jų privatumo teisės, apsaugos lygių tvarkant asmens duomenis skirtumų valstybėse narėse, kurie gali trukdyti perduoti tokius duomenis iš vienos valstybės narės į kitą, kliudyti užsiimti kai kuriomis ekonominės veiklos rūšimis Bendrijos lygiu, iškreipti konkurenciją ar trukdyti valdžios institucijoms vykdyti savo pareigas pagal Bendrijos teisę.

Direktyvos tikslas – saugoti fizinių asmenų pagrindines teises ir laisves, ypač privatumo teisę tvarkant asmens duomenis, tačiau nevaržyti ir nedrausti laisvo asmens duomenų judėjimo tarp valstybių narių dėl priežasčių, susijusių su asmens duomenų apsauga.

Asmens duomenys Direktyvoje apibrėžiami kaip bet kuri informacija, susijusi su asmeniu (duomenų subjektu), kurio tapatybė yra nustatyta arba gali būti nustatyta. Asmuo, kurio tapatybė gali būti nustatyta, yra tas asmuo, kurio tapatybė gali būti nustatyta tiesiogiai ar netiesiogiai, ypač pasinaudojus nurodytu asmens identifikavimo kodu arba vienu ar keliais to asmens fizinei, fiziologinei, protinei, ekonominei, kultūrinei ar socialinei tapatybei būdingais veiksniais.

Direktyvoje įtvirtinti tokie pagrindiniai asmens duomenų apsaugos principai:

1) duomenų kokybės, kuris reiškia, kad asmens duomenys turi būti:

– tvarkomi teisingai ir teisėtai;

– surinkti įvardytais, aiškiai apibrėžtais ir teisėtais tikslais, o po to tvarkomi su šiais tikslais suderintais būdais;

– adekvatūs, susiję ir savo apimtimi neviršijantys tikslų, kuriems jie renkami ir (arba) vėliau tvarkomi;

– tikslūs ir, jei būtina, nuolat atnaujinami; turi būti imtasi visų reikalingų priemonių, kad duomenys, kurie yra netikslūs ar neišsamūs, palyginti su tikslais, dėl kurių jie buvo surinkti ar po to tvarkomi, būtų ištrinti arba ištaisyti;

– laikomi tokio pavidalo, kad duomenų subjektų tapatybes būtų galima nustatyti ne ilgiau, nei tai yra reikalinga tais tikslais, dėl kurių duomenys buvo surinkti arba po to tvarkomi.

2) teisėto duomenų tvarkymo, kuris reiškia, kad asmens duomenis galima tvarkyti tik tuo atveju, jeigu:

– duomenų subjektas yra nedviprasmiškai davęs sutikimą;

– tvarkyti reikia vykdant sutartį, kurią duomenų subjektas yra sudaręs kaip viena iš šalių, arba duomenų subjekto reikalavimu norint imtis priemonių prieš sudarant sutartį;

– tvarkyti reikia vykdant teisinę prievolę, kuri privaloma duomenų valdytojui;

– tvarkyti reikia norint apsaugoti gyvybinius duomenų subjekto interesus;

– tvarkyti reikia vykdant užduotį, atliekamą visuomenės labui, arba įgyvendinant oficialius įgaliojimus, suteiktus duomenų valdytojui arba trečiajai šaliai, kuriai atskleidžiami duomenys;

– tvarkyti reikia dėl teisėtų interesų, kurių siekia duomenų valdytojas arba trečioji šalis (šalys), kurioms atskleidžiami duomenys, išsky-

rus atvejus, kai duomenų subjekto teisės ir laisvės yra viršesnės nei šie interesai.

3) draudimo tvarkyti ypatingus asmens duomenis: draudžiama tvarkyti asmens duomenis, kurie atskleidžia rasinę ar etninę kilmę, politines, religines ar filosofines pažiūras, priklausymą profesinėms sąjungoms, taip pat tvarkyti duomenis apie asmens sveikatą ar intymų gyvenimą, išskyrus tam tikrus atvejus.

4) tvarkymo konfidencialumo: bet kuriam asmeniui, veikiančiam pagal duomenų valdytojo ar duomenų tvarkytojo įgaliojimus, įskaitant ir patį duomenų tvarkytoją, galinčiam gauti asmens duomenų, draudžiama tvarkyti juos kitaip, kaip tiktai duomenų valdytojo nurodymu, nebent jo tai padaryti reikalautų įstatymas.

5) duomenų apsaugos: duomenų valdytojas privalo įgyvendinti tinkamas technines ir organizacines priemones, skirtas apsaugoti, kad asmens duomenys nebūtų netyčia ar neteisėtai sunaikinti ar netyčia prarasti, pakeisti, neleistinai atskleisti ar palikti prieinami, ypač kai tvarkomus duomenis tenka perduoti tinklu, taip pat apsaugoti nuo bet kokių kitų neteisėtų tvarkymo būdų.

6) asmens duomenų perdavimo į trečiąsias šalis: asmens duomenys, kurie yra tvarkomi arba kuriuos perdavus ketinama tvarkyti, gali būti perduodami į trečiąją šalį tik tuo atveju, jeigu nepažeidžiant nacionalinių nuostatų, priimtų pagal kitas Direktyvos nuostatas, ši trečioji šalis užtikrina adekvatų apsaugos lygį. Apsaugos, kurią suteikia trečioji šalis, lygio adekvatumas įvertinamas atsižvelgiant į duomenų perdavimo operacijos ar operacijų grupės aplinkybes; ypatingas dėmesys atkreipiamas į duomenų pobūdį, siūlomos tvarkymo operacijos ar operacijų tikslą ir trukmę, duomenų kilmės bei paskirties valstybę ar valstybes, bendrųjų ir atskiriems sektoriams taikomų įstatymų, galiojančių trečiojoje šalyje, nuostatas, taip pat profesines taisykles ir saugumo priemones, kurių laikomasi toje valstybėje.

Asmens duomenų teisinės apsaugos principai Lietuvoje

Lietuvoje Direktyvą įgyvendina Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas[225], kurio tikslas – ginti žmogaus privataus gyvenimo neliečiamumo teisę tvarkant asmens duomenis. Įstatymo

[225] Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas. *Valstybės žinios*, 2008, Nr. 22-804.

2 str. 1 p. įtvirtinama asmens duomenų sąvoka: **„asmens duomenys** – bet kuri informacija, susijusi 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“. Minėto straipsnio 8 p. pateikiama ypatingų asmens duomenų sąvoka: **„ypatingi asmens duomenys** – 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“.

Įstatyme įtvirtinami tokie pagrindiniai asmens duomenų tvarkymo reikalavimai (principai):

1) tikslo nustatymo: asmens duomenys turi būti renkami apibrėžtais ir teisėtais tikslais ir toliau nebūtų tvarkomi tikslais, nesuderinamais su nustatytaisiais prieš renkant asmens duomenis;

2) teisėtumo: asmens duomenys turi būti tvarkomi tiksliai, sąžiningai ir teisėtai;

3) asmens duomenų kokybės: asmens duomenys turi būti tikslūs ir, jei reikia dėl asmens duomenų tvarkymo, nuolat atnaujinami; netikslūs ar neišsamūs duomenys turi būti ištaisyti, papildyti, sunaikinti arba sustabdytas jų tvarkymas;

4) proporcingumo: asmens duomenys turi būti tapatūs, tinkami ir tik tokios apimties, kuri būtina jiems rinkti ir toliau tvarkyti;

5) saugumo užtikrinimo: asmens duomenys turi būti saugomi tokia forma, kad duomenų subjektų tapatybę būtų galima nustatyti ne ilgiau, negu to reikia tiems tikslams, dėl kurių šie duomenys buvo surinkti ir tvarkomi. Privalo būti įgyvendinamos tinkamos organizacinės ir techninės priemonės, skirtos apsaugoti asmens duomenims nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo;

6) panaudojimo apribojimo: asmens duomenys, surinkti kitais tikslais, gali būti tvarkomi statistikos, istoriniais ar mokslinio tyrimo tikslais tik įstatymų nustatytais atvejais, kai įstatymuose nustatytos tinkamos duomenų apsaugos priemonės;

7) draudimo tvarkyti ypatingus asmens duomenis: draudžiama tvarkyti ypatingus asmens duomenis, išskyrus tam tikras išimtis, kurias numato įstatymai;

8) individualaus dalyvavimo (duomenų subjekto teisių): duomenų subjektas Įstatymo nustatyta tvarka turi teisę žinoti (būti informuotas) apie savo asmens duomenų tvarkymą, susipažinti su savo asmens duomenimis ir kaip jie yra tvarkomi, reikalauti ištaisyti, sunaikinti savo asmens duomenis arba sustabdyti, išskyrus saugojimą, savo asmens duomenų tvarkymo veiksmus, kai duomenys tvarkomi nesilaikant šio ir kitų įstatymų nuostatų, nesutikti, kad būtų tvarkomi jo asmens duomenys;

9) atvirumo: duomenų subjektui, kurio asmens duomenys renkami tiesiogiai iš jo, turi būti pateikiama duomenų valdytojo kontaktinė informacija, kokiais tikslais ketinami tvarkyti duomenų subjekto asmens duomenys, kita papildoma informacija (kam ir kokiais tikslais teikiami duomenų subjekto asmens duomenys; kokius savo asmens duomenis duomenų subjektas privalo pateikti ir kokios yra duomenų nepateikimo pasekmės, apie duomenų subjekto teisę susipažinti su savo asmens duomenimis ir teisę reikalauti ištaisyti neteisingus, neišsamius, netikslius savo asmens duomenis), kiek jos reikia, kad būtų užtikrintas teisingas asmens duomenų tvarkymas nepažeidžiant duomenų subjekto teisių.

10) priežiūros ir sankcijų: kaip vykdomas Įstatymas, prižiūri ir kontroliuoja Valstybinė duomenų apsaugos inspekcija;

11) duomenų teikimas užsienio valstybėse esantiems duomenų gavėjams: asmens duomenys duomenų gavėjams, esantiems Europos Sąjungos valstybėse narėse ir kitose Europos ekonominės erdvės valstybėse, teikiami tomis pačiomis sąlygomis ir tvarka kaip ir duomenų gavėjams, esantiems Lietuvos Respublikoje. Asmens duomenys teikiami duomenų gavėjams trečiosiose valstybėse gavus Valstybinės duomenų apsaugos inspekcijos leidimą, išskyrus tam tikras Įstatymo numatytas išimtis. Be to, asmens duomenys teikiami duomenų gavėjams trečiosiose valstybėse, jeigu šiose valstybėse yra tinkamas asmens duomenų teisinės apsaugos lygis*.

Taigi, Lietuvoje požiūris į asmens duomenų apsaugą yra paremtas visapusišku teisiniu reguliavimu: Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas įtvirtina pagrindinius asmens duomenų apsaugos

* Asmens duomenų teisinės apsaugos lygis vertinamas atsižvelgiant į visas aplinkybes, susijusias su duomenų teikimu, ypač į trečiojoje valstybėje, į kurią ketinami teikti asmens duomenys, galiojančius įstatymus, kitus teisės aktus bei duomenų valdytojo parengtus dokumentus, užtikrinančius asmens duomenų teisinę apsaugą, į teikiamų duomenų pobūdį, duomenų tvarkymo būdus, tikslus, trukmę, saugumo priemones, kurių bus laikomasi toje valstybėje.

principus, įtvirtintus 1981 m. Strasbūro konvencijoje ir Europos Sąjungos direktyvoje Nr. 95/46/EB bei užtikrina minėtų principų apsaugą.

Asmens duomenų teisinės apsaugos principai Rusijoje

Konstitucija. Rusijos Federacijos Konstitucija[226] pripažįsta tokias teises kaip teisė į privatumą, teisė į duomenų apsaugą ir teisė į susižinojimo slaptumą. Konstitucijos 23 str. įtvirtinama, kad kiekvienas turi teisę į privatumą, asmeninio ir šeimos gyvenimo paslaptį ir garbės bei gero vardo apsaugą; taip pat teisę į korespondencijos, telefono pokalbių, pašto ir kitų ryšio priemonių privatumą, o bet koks minėtų teisių suvaržymas gali būti nustatytas tik įstatyme. 24 str. įtvirtinama, kad be asmens sutikimo draudžiama rinkti, saugoti, naudoti ir platinti informaciją apie jo asmeninį gyvenimą.

2006 m. Rusijos Respublikoje buvo priimtas *Asmens duomenų įstatymas*[227] *ir Informacijos, informacinių technologijų ir informacijos apsaugos įstatymas*[228], kurie pakeitė 1995 m. Informacijos, informatizacijos ir informacijos apsaugos įstatymą[229]. Asmens duomenų įstatymo priėmimas rodo, kad Rusija įvykdė savo įsipareigojimus perkelti 1981 m. Strasbūro konvencijos dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu nuostatas į nacionalinę teisę. Asmens duomenų įstatymo paskirtis – užtikrinti, kad asmens duomenys nebūtų neteisėtai ir be duomenų subjekto žinios renkami ir apdorojami. Tačiau pažymėtina, kad įstatymas vis dar yra nutolęs nuo tobulo (koks turėtų būti) asmens duomenų apsaugos reguliavimo modelio, kadangi jame įtvirtinta nemažai išimtinių nuostatų, kurios netaikomos valstybės valdžios institucijoms.

Rusijos įstatymai, reglamentuojantys duomenų apsaugą, iš esmės yra panašūs į tuos, kurie galioja Europos Sąjungoje. Vis dėlto Rusijos įstatymuose numatyti griežtesni ribojimai, taikomi asmens duomenims rinkti,

[226] The Constitution of the Russian Federation of 25.12.1993 [interaktyvus, žiūrėta 2011-10-01] <http://www.constitution.ru/en/10003000-01.htm>.

[227] Federal Act No. 152-FZ on Personal Data [interaktyvus]. 27 July, 2006 [žiūrėta 2011-09-19]. <http://www.mofo.com/docs/mofoprivacy/Federal%20Law%20of%2027%20July%202006%20N152-FZ%20on%20Personal%20Data%20%20(English).pdf>.

[228] Federal Act No. 149-FZ of the Russian Federation on Information, Information Technologies and Information Protection[interaktyvus]. 14 July, 2006 [žiūrėta 2011-09-19]. <http://www.medialaw.ru/e_pages/laws/russian/information-en.htm>.

[229] Federal Act No. 24-FZ of the Russian Federation on Information, Informatization and Protection of Information [interaktyvus]. 20 February, 1995 [žiūrėta 2011-09-19]. <http://www.medialaw.ru/e_pages/laws/russian/iipi-en.htm>.

naudoti, saugoti, perduoti ir apdoroti. Pavyzdžiui, verslo subjektai ilgai reiškė nepasitenkinimą, kad Asmens duomenų įstatyme numatyti tokie ribojimai duomenims tvarkyti, kurie yra nepraktiški, pavyzdžiui, įstatyme reikalaujama, kad tvarkant didžiąją dalį asmens duomenų būtų raštiškas duomenų subjekto sutikimas. Elektroninėje erdvėje tai reikštų, kad vartotojas privalo turėti elektroninį parašą, užuot, kaip įprastai, kontroliniame langelyje vartotojas, išreikšdamas savo sutikimą, uždėtų varnelę (tokia praktika priimtina Europos valstybėse)[230].

Asmens duomenų įstatymo 2 str. apibrėžiama įstatymo paskirtis ir įtvirtinama, kad šio įstatymo tikslas yra užtikrinti asmens ir piliečio teises ir laisves asmens duomenų tvarkymo srityje, įskaitant privataus gyvenimo neliečiamumo apsaugą, asmeninio ir šeimos gyvenimo privatumą.

Asmens duomenų įstatymo 3 str. 1 p. įtvirtinama asmens duomenų sąvoka: asmens duomenys – bet kuri informacija, susijusi su fizine esybe arba asmeniu, kurio tapatybė gali būti nustatyta remiantis tokia informacija (asmeninės informacijos subjektas), įskaitant pavardę, vardą, tėvavardį, gimimo datą ir vietą, gyvenamosios vietos adresą, šeimą, socialinę padėtį ir turimą nuosavybę, išsilavinimą, profesiją, pajamas ir kitokią informaciją.

Asmens duomenų įstatymas įtvirtina tokius pagrindinius asmens duomenų tvarkymo principus:

1) teisėtumo: asmens duomenų tvarkymo tikslai ir priemonės turi būti teisėti ir sąžiningi;

2) tikslo nustatymo: asmens duomenų tvarkymo tikslai negali prieštarauti tikslams, kurie iš anksto buvo apibrėžti ir nurodyti renkant asmens duomenis;

3) proporcingumo: tvarkomų asmens duomenų apimtis ir prigimtis, asmens duomenų tvarkymo metodai turi atitikti asmens duomenų tvarkymo tikslus;

4) atsakomybės ir panaudojimo apribojimo: atsakomybės už asmens duomenis, jų pakankamumą tvarkymo tikslais ir kad tvarkomi duomenys būtų tik tokios apimties, kuri yra būtina, o duomenys būtų tvarkomi tik tais tikslais, kuriais jie buvo renkami;

---

[230] Segalis, B. Russia Postpones Enforcement of Data Protection Law; Considers Revision [interaktyvus]. 2011-01-13 [žiūrėta 2011-09-19]. <http://www.infolawgroup.com/2011/01/articles/enforcement/russia-postpones-enforcement-of-data-protection-law-considers-revisions/>.

5) asmens duomenų informacinių sistemų duomenų bazių sujungimo nepriimtinumo, jei jos yra sukurtos tokiais tikslais, kurie yra vieni su kitais nesuderinami.

6) saugumo užtikrinimo: asmens duomenys turi būti saugomi tokia forma, kad duomenų subjektų tapatybę būtų galima nustatyti ne ilgiau, negu to reikia tiems tikslams, dėl kurių šie duomenys buvo surinkti ir tvarkomi, ir turi būti sunaikinti, kai tik tikslai yra pasiekti arba nebeliko poreikio tokių tikslų siekti. Privalo būti įgyvendinamos tinkamos organizacinės ir techninės priemonės, skirtos asmens duomenims apsaugoti nuo atsitiktinės ar neteisėtos prieigos, atsitiktinio ar neteisėto sunaikinimo, pakeitimo, blokavimo, kopijavimo, atskleidimo, taip pat nuo bet kokių kitų neteisėtų veiksmų;

7) draudimo tvarkyti ypatingus asmens duomenis: draudžiama tvarkyti ypatingus asmens duomenis, susijusius su rase ar etnine kilme, politinėmis pažiūromis, religiniais ar filosofiniais įsitikinimais, sveikata ar intymiu gyvenimu, išskyrus tam tikras išimtis, kurias numato įstatymai;

8) individualaus dalyvavimo (duomenų subjekto teisių): duomenų subjektas Įstatymo nustatyta tvarka turi teisę žinoti (būti informuotas) apie savo asmens duomenų tvarkymą, susipažinti su savo asmens duomenimis ir kaip jie yra tvarkomi, reikalauti ištaisyti, sunaikinti savo asmens duomenis arba sustabdyti savo asmens duomenų tvarkymo veiksmus, jei duomenys yra nepilni, neatnaujinti, neteisingi, gauti neteisėtomis priemonėmis arba tvarkomi ne tuo tikslu, kuriuo remiantis jie buvo gauti, imtis kitų teisės aktų numatytų priemonių, siekdamas apsaugoti savo teises;

9) duomenų perdavimas: prieš perduodant duomenis kitoje valstybėje esančiam duomenų gavėjui, turi būti įsitikinama, ar toje valstybėje yra garantuojamas tinkamas asmens duomenų teisinės apsaugos lygis.

10) atvirumo: duomenų subjektui, kurio asmens duomenys renkami tiesiogiai iš jo, turi būti pateikiama duomenų valdytojo kontaktinė informacija, kokiais tikslais ketinami tvarkyti duomenų subjekto asmens duomenys, kita papildoma informacija (kam ir kokiais tikslais teikiami duomenų subjekto asmens duomenys; kokius savo asmens duomenis duomenų subjektas privalo pateikti ir kokios yra duomenų nepateikimo pasekmės, apie duomenų subjekto teisę susipažinti su savo asmens duomenimis ir teisę reikalauti ištaisyti neteisingus, neišsamius, netikslius savo asmens duomenis), kiek jos reikia, kad būtų užtikrintas teisingas asmens duomenų tvarkymas nepažeidžiant duomenų subjekto teisių;

11) priežiūros ir sankcijų: už Įstatymo įgyvendinimo kontrolę ir priežiūrą atsakinga Federacijos vykdomosios valdžios institucija, atliekanti kontrolės ir priežiūros funkcijas informacinių technologijų ir ryšių srityje. Asmens duomenų įstatymo 24 str. numatoma atsakomybė už įstatymo nuostatų pažeidimą: asmenys, pažeidę šį Rusijos Federacijos įstatymą, gali būti patraukti civilinėn, baudžiamojon, administracinėn, drausminėn ir atsakomybėn ir kt., kurią numato Rusijos Federacijos įstatymai. Pažymėtina, kad Asmens duomenų įstatyme neįtvirtinama, kuri federalinė institucija yra atsakinga už jo įgyvendinimą, todėl iš pradžių daug painiavos kėlė tai, kad plačias ir besidubliuojančias galias turėjo įvairios institucijos ir sunku buvo nuspėti, kuri iš jų turi atlikti pagrindines funkcijas užtikrinant minėto įstatymo įgyvendinimą. Toks netikrumas buvo išspręstas 2008 m. gruodžio 3 d. įkuriant Federalinę ryšio, informacinių technologijų ir visuomenės informavimo priemonių (žiniasklaidos) priežiūros instituciją[231], kuri atsakinga už tai, kad nebūtų pažeisti Asmens duomenų įstatyme įtvirtinti reikalavimai, ir kuri yra atsakinga už asmens duomenų subjektų teisių apsaugą. Viena iš pagrindinių Institucijos veiklos sričių yra užtikrinti piliečių teises į privatumą, asmeninio ir šeimos gyvenimo konfidencialumą.

Taigi, Rusijoje požiūris į asmens duomenų apsaugą taip pat yra remiasi visapusišku teisiniu reguliavimu (galioja Rusijos asmens duomenų įstatymas), o įstatymai, reglamentuojantys duomenų apsaugą, iš esmės yra panašūs į tuos, kurie galioja Europos Sąjungoje (taip pat ir Lietuvoje), tačiau numato griežtesnius ribojimus asmens duomenų rinkimui, naudojimui, saugojimui, perdavimui ir apdorojimui.

Asmens duomenų teisinės apsaugos principai Lietuvoje ir Rusijoje. Saugaus uosto principai JAV

JAV asmens duomenų apsaugos teisinė sistema labai skiriasi nuo Europos Sąjungos ir Rusijos asmens duomenų reguliavimo modelio. JAV duomenų tvarkymo atžvilgiu yra taikomi kitokie apsaugos standartai, kurie daugeliu požiūrių yra žemesnio lygio nei Europos Sąjungoje. Jungtinės Valstijos per bendrąją teisę ir įstatymus pateikė skirtingus asmeninės infor-

[231] Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications (ROSKOMNADZOR) [interaktyvus, žiūrėta 2011-09-19]. <http://www.rsoc.ru/eng/>.

macijos apsaugos lygius. Panašiai ir federaliniu lygmeniu JAV privatumo apsauga plėtojosi sektorius po sektoriaus, kuriant daugybę įstatymų, numatančių skirtingus asmens duomenų apsaugos standartus, priklausomai nuo asmeninės informacijos rūšies ir pobūdžio, kai kurią informaciją, netgi labai svarbią, paliekant visai be jokios įstatyminės apsaugos[232].

Europos Sąjungoje 1998 m. įsigaliojusi Asmens duomenų apsaugos direktyva draudžia asmens duomenų perdavimą valstybėms ne Europos Sąjungos narėms, kurios neatitinka europinio privatumo apsaugos „pakankamumo" standarto. Pažymėtina, kad tiek Europos Sąjunga, tiek JAV turi bendrą tikslą – stiprinti piliečių privatumo apsaugą, tačiau JAV vyrauja kitoks požiūris į privatumą nei Europos Sąjungoje ar Rusijoje. JAV požiūris į asmens duomenų apsaugą remiasi sektoriniu reguliavimu ir savireguliacija, o Europos Sąjungoje ir Rusijoje – visapusišku teisiniu reguliavimu, pavyzdžiui, valstybės narės yra įsipareigojusios įkurti institucijas, atsakingas už asmens duomenų apsaugą, užtikrinti asmens duomenų valdytojų registraciją minėtų institucijų duomenų bazėse, išankstinio leidimo norint tvarkyti asmens duomenis gavimą. Būtent dėl šių pagrindinių požiūrio į privatumą skirtumų Direktyva gerokai apsunkino JAV organizacijų galimybes dalyvauti transatlantiniuose susitarimuose.

Siekdamas nutiesti tiltą tarp tokių skirtingų požiūrių į privatumą ir sukurti supaprastintas priemones JAV organizacijoms, kurios atitiktų Direktyvos reikalavimus, JAV Prekybos departamentas, pasitaręs su Europos Komisija, sukūrė „saugaus uosto" sistemą (Europoje patvirtinta 2000 m.), kuri svarbi tuo, kad JAV organizacijos gali išvengti trukdžių dėl verslo susitarimų su Europos valstybių organizacijomis ar Europos institucijų persekiojimo dėl Europos privatumo įstatymų reikalavimų pažeidimo. Saugaus uosto programa užtikrina, kad Europos organizacijos žino, kad JAV organizacija, kuri yra saugaus uosto narė, užtikrina *pakankamą* privatumo apsaugą, kaip tai apibrėžiama Direktyvoje.

Toliau pateikiami ir aptariami 7 pagrindiniai saugaus uosto principai[233]:

[232] Civilka M. Asmens duomenų apsaugos teisinis reguliavimas interneto kontekste [interaktyvus, žiūrėta 2011-10-01] <http://media.search.lt/GetFile.php?OID=92932&FID=269994>, p. 29.

[233] „Saugaus uosto" principai [interaktyvus, žiūrėta 2011-09-20]. <http://export.gov/safeharbor/eu/eg_main_018476.asp>.

1) pranešimo: organizacijos turi informuoti asmenis, kokiu tikslu jų asmeninė informacija bus renkama ir naudojama; jos turi pateikti informaciją, kaip asmenys gali pateikti klausimus ar skundus, nurodyti trečiuosius asmenis, kuriems tokio pobūdžio informacija gali būti atskleista, galimybes ir priemones, kurias organizacija siūlo, kad būtų apribotas asmeninės informacijos naudojimas ir viešinimas.

2) pasirinkimo: organizacijos privalo sudaryti galimybę asmeniui pasirinkti (*opt-out*), ar jo asmeninė informacija galės būti atskleista tretiesiems asmenims ar naudojama tikslais, nesuderinamais su tais, kuriais remiantis ta asmeninė informacija buvo surinkta, arba tais, kuriems asmuo davė sutikimą vėliau. Svarbios informacijos tvarkymo atveju privalo būti duotas aiškus (*opt-in*) sutikimas ar pritarimas, jei tokia informacija bus atskleista tretiesiems asmenims ar panaudota kitu tikslu, nei ji buvo renkama, arba tuo tikslu, kuriam asmuo davė sutikimą rinkti tokią informaciją vėliau.

3) perdavimo tretiesiems asmenims: organizacijos, norėdamos atskleisti informaciją trečiajai šaliai, turi laikytis pranešimo ir pasirinkimo principų. Jei organizacija nori perduoti informaciją trečiajai šaliai, kuri veikia kaip tarpininkas, informacija gali būti perduota, jei organizacija įsitikina, kad trečioji šalis pripažįsta saugaus uosto principus, ar yra subjektas, kuriam taikomos Direktyvos nuostatos ar kiti pakankamumo reikalavimai. Kaip alternatyva galimas rašytinis susitarimas su trečiąja šalimi, kuriuo ji įsipareigotų užtikrinti ne mažesnį privatumo apsaugos lygį, nei kad reikalauja tiesiogiai susiję principai.

4) prieigos: asmenims turi būti suteikta prieigos teisė prie jų asmens duomenų, kuriuos organizacija saugo, turi būti suteikta teisė jiems tokius duomenis taisyti, papildyti ar netikslius duomenis ištrinti, išskyrus atvejus, jei prievolė ar išlaidos, susijusios su tokios prieigos užtikrinimu, būtų neproporcingos asmens privatumui dėl rizikos arba jei būtų pažeidžiamos kito asmens teisės.

5) saugumo: organizacijos turi imtis pagrįstų atsargumo priemonių, kad apsaugotų asmeninę informaciją nuo praradimo, netinkamo naudojimo, neteisėtos prieigos, atskleidimo, pakeitimo ir sunaikinimo.

6) duomenų vientisumo: asmeninė informacija turi būti susijusi su tikslais, kuriais ji naudojama. Organizacija turi imtis tinkamų priemonių, kad būtų užtikrinta, jog duomenys yra patikimi, tikslūs, išsamūs ir aktualūs.

7) įgyvendinimo: tam, kad būtų užtikrintas saugaus uosto principų laikymasis, turi būti lengvai prieinami mechanizmai, užtikrinantys, kad kiekvieno asmens skundas ir ginčas bus ištirtas ir išspręstas bei patirta žala atlyginta; procedūros, kurios leistų patikrinti, ar organizacijos laikosi įsipareigojimų, susijusių su saugaus uosto principų įgyvendinimu; pareiga išspręsti problemas, kylančias dėl minėtų principų nesilaikymo. Sankcijos turi būti pakankamai griežtos. Tos organizacijos, kurios nesilaiko įsipareigojimo pateikti kasmetinę atestaciją, yra išbraukiamos iš dalyvių sąrašo ir joms daugiau nebeužtikrinamos saugaus uosto privilegijos.

Jungtinių Valstijų Prekybos departamento sukurta tarptautinių saugaus uosto privatumo principų pažymėjimų išdavimo programa yra kaip atsakas į 1995 m. Europos Komisijos direktyvos dėl asmenų apsaugos tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo Nr. 95/46/EB (Bendroji duomenų apsaugos direktyva) IV skyriaus (Asmens duomenų perdavimas į trečiąsias šalis) 25 straipsnį, kuriame įtvirtintas bendrasis reikalavimas, kad „asmens duomenys, kurie yra tvarkomi arba kuriuos juos perdavus ketinama tvarkyti, gali būti perduodami į trečiąją šalį tik tuo atveju, jeigu nepažeidžiant nacionalinių nuostatų, priimtų pagal kitas šios direktyvos nuostatas, ši trečioji šalis užtikrina adekvatų apsaugos lygį“. Jau daugelį metų Europos Sąjungoje privatumas yra griežtai reglamentuojamas. Europos Sąjungoje įsteigtos bendrovės negali perduoti asmens duomenų į trečiąsias šalis už Europos ekonominės erdvės ribų, jei jose nėra užtikrinamas adekvatus gaunamų asmens duomenų apsaugos lygis.

Saugaus uosto programa remiasi savanoriškumo principu: organizacijos, kurios nori tapti šios programos narėmis, turi užsiregistruoti; be to, jos turi atitikti daugelį standartų, kurie nustatyti, siekiant įvertinti jų atitiktį direktyvos 25 straipsnyje numatytam reikalavimui. 2000 m. liepos 26 d. Europos Komisija patvirtino, kad saugus uostas užtikrina adekvatų asmens duomenų apsaugos lygį, kaip tai numatyta direktyvos 25 str., saugaus uosto privatumo principai leidžia JAV bendrovėms registruoti savo pažymėjimus, jei jos atitinka Europos Sąjungos reikalavimus. Po to, kai bendrovė tampa programos nare, ji kas 12 metų turi gauti pažymėjimą. Bendrovė gali būti įvertinta arba pati įsivertinti, ir patvirtinti, kad atitinka saugaus uosto principus, arba gali pasamdyti trečiąją šalį, kuri atliktų įvertinimą.

3.2.3. Elektroninių duomenų saugumas (elektroninės informacijos saugos reguliavimas pasirinktose valstybėse)

Informacijos saugumas (sauga) suprantama kaip informacijos ir sistemos infrastruktūros apsauga nuo atsitiktinio ar tyčinio, natūralaus ar dirbtinio pobūdžio poveikio, galinčio sukelti žalą informacijos ar sistemos infrastruktūros savininkams bei vartotojams[234]. Praktikoje paprastai išskiriami trys pagrindiniai informacinių sistemų saugos aspektai:

- prieinamumas – galimybė tam tikrą laiką gauti reikalingą informaciją;
- vientisumas – informacijos svarbumas ir nepriekaištingumas bei apsauga nuo sunaikinimo ir neteisėto pakeitimo;
- slaptumas – apsauga nuo neteisėto nuskaitymo[235].

Autorių nuomone, viena iš tapatybės vagystės elektroninėje erdvėje pradinių stadijų yra susijusi su neteisėtu asmeninės informacijos pasisavinimu (gavimu), o tai dažnai įvyksta pažeidžiant informacinės sistemos saugumą. Dėl to labai svarbu, kaip užtikrinamas informacijos saugos lygis. Kuo informacinės sistemos saugesnės, tuo sunkiau nusikaltėliams ir pažeidėjams bus gauti asmens duomenis. Taigi, informacijos saugos lygis tam tikra prasme turėtų daryti įtaką ir tapatybės vagystės elektroninėje erdvėje paplitimui, ir tokių pažeidimų skaičiui.

Todėl, autorių nuomone, svarbu išnagrinėti informacijos saugos užtikrinimą pasirinktose užsienio valstybėse. Remiantis šio tyrimo rezultatais, bus daromos prielaidos dėl informacijos saugos įtakos tapatybės vagystei elektroninėje erdvėje.

Prieš atliekant pasirinktų užsienio valstybių analizę, svarbu paminėti, kad tapatybės vagystės elektroninėje erdvėje atveju svarbiausias yra trečiasis elementas, t. y. informacijos slaptumo užtikrinimas. Nepaisant to, kad tai tik vienas iš trijų informacijos saugos elementų, pasirinktose užsienio valstybėse bus nagrinėjama bendra informacijos saugos kategorija (daugiausia teisinis reguliavimas).

Analizuoti pasirinktos šios užsienio valstybės – JAV ir Rusija. JAV pasirinkta dėl to, kad šioje valstybėje daug dėmesio skiriama informa-

[234] Kiškis, M.; Petrauskas, R.; Rotomskis, I.; Štitilis, D. 2006. *Teisės informatika ir informatikos teisė*. Vilnius: Mykolo Romerio universitetas, p. 38.

[235] *Ibid*.

cijos saugai. JAV – tai valstybė, kuriai nuolat gresia terorizmo, įskaitant elektroninį terorizmą, grėsmė. Todėl ši valstybė privalo užtikrinti ir, tikėtina, kad užtikrina aukštą informacijos saugos lygį. Rusija pasirinkta dėl to, kad ši valstybė nepriklauso Europos Sąjungai, jai negalioja Europos Sąjungos teisinis reguliavimas ir informacijos saugą ji užtikrina savarankiškai. Be to, kadangi Rusijoje įvykdomas didelis skaičius elektroninių nusikaltimų, ši valstybė informacijos saugai taip pat turėtų skirti deramą dėmesį. Taip pat bus nagrinėjama Lietuva, kaip Europos Sąjungos narė.

Prieš atliekant informacijos saugos teisinio reguliavimo analizę, reikia paminėti ir tai, kad ši sritis tarptautiniu mastu nėra reguliuojama. Vienintelis dokumentas – tai 2002 m. Ekonominio bendradarbiavimo ir plėtros organizacijos patvirtintos Informacinių sistemų saugos gairės[236]. Tačiau tai rekomendacinis dokumentas, neturintis privalomos teisinės galios. Europos Sąjungoje informacijos sauga kol kas reguliuojama fragmentiškai.

Informacijos saugos reguliavimas JAV

Pagrindiniai teisės aktai, reguliuojantys informacijos saugą. Vienas iš svarbiausių teisės aktų JAV, reguliuojančių informacijos saugos sritį, yra Federalinis informacijos saugos valdymo įstatymas[237]. Šis įstatymas buvo priimtas 2002 metais, kaip e. valdžios įstatymo dalis. Įstatyme pabrėžiama informacijos saugos svarba ekonomikai ir nacionaliniam saugumui JAV.

Pagal šį įstatymą informacijos saugos terminas reiškia informacijos ir informacinių sistemų apsaugą nuo neteisėtos prieigos, naudojimo, atskleidimo, modifikavimo ar sunaikinimo, siekiant užtikrinti informacijos ir informacinių sistemų vientisumą, konfidencialumą bei prieinamumą.

Institucinė informacijos saugos priežiūros kontrolė. Federalinis informacijos saugos valdymo įstatymas specifines funkcijas informacijos saugos srityje numato federalinėms agentūroms, Nacionaliniam standartų ir technologijų institutui bei Valdymo ir biudžeto tarnybai (angl. *Office of Management and Budget*).

[236] *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* [interaktyvus, žiūrėta 2011-09-19]. <http://www.oecd.org/document/48/0,3746,en_2649_34255_15582250_1_1_1_1,00.html>.

[237] Federal Information Security Management Act, 2002. *US Code*, Title 44, Chapter 35, Subchapter III. [interaktyvus, žiūrėta 2011-09-19]. <http://www.law.cornell.edu/uscode/44/usc_sup_01_44_10_35_20_III.html>.

JAV informacijos saugos srityje daug pareigų ir teisių suteikiama Federalinėms agentūroms, kurios egzistuoja kiekvienoje valstijoje ir yra labai panašios. Federalinis informacijos saugos valdymo įstatymas iš kiekvienos agentūros vadovo reikalauja įgyvendinti reikiamą informacijos saugos politiką, taip pat vykdyti veiksmus, efektyviai ir priimtinomis sąnaudomis mažinti informacijos saugos riziką, siekiant priimtino rizikos lygio. Įstatymas taip pat reglamentuoja, kad kiekviena federalinė agentūra pagal savo veiklos apimtį plėtotų ir įgyvendintų informacijos ir informacinių sistemų aprūpinimo informacijos sauga programą. Įstatymas reikalauja, kad atsakingi už minėtas programas agentūrų vyriausieji informacijos pareigūnai (angl. *Chief Information Officers*) ir generaliniai inspektoriai (angl. *Inspectors general*) vykdytų kasmetes agentūros informacijos saugos programos apžvalgas ir apie rezultatus praneštų Valdymo ir biudžeto tarnybai. Ši tarnyba pagal gautą informaciją apie agentūros veiklos atitiktį įstatymui turi rengti metinę ataskaitą kongresui.

Pagal įstatymą Nacionalinis standartų ir technologijų institutas yra atsakingas už standartus, gaires ir metodikas, skirtas adekvačiai informacijos saugai federalinių agentūrų veikloje užtikrinti. Institutas glaudžiai bendradarbiauja su federalinėmis agentūromis, siekdamas gerinti įstatymo reikalavimų, užtikrinančių informacijos saugą, supratimą ir įgyvendinimą, ir skelbia standartus bei gaires, kurios šiose agentūrose sudaro pagrindą tinkamoms informacijos saugos programoms. Taip pat institutas naudoja testus ir atitikimo programas, kad būtų galima vertinti informacijos sistemų ir paslaugų saugą.

Pagrindiniai elektroninės informacijos saugos reikalavimai. Visos informacinės sistemos turi būti priskirtos tam tikroms kategorijoms. Šios kategorijos nustatomos pagal tikslus, kuriuos įgyvendinant siekiama užtikrinti atitinkamą informacijos saugos lygį, atsižvelgiant į rizikos lygį. Saugos kategorijas nustato pirmasis privalomas įstatyme reikalaujamas saugos standartas – Federalinės informacijos ir informacinių sistemų priskyrimo saugos kategorijoms standartas[238].

Federalinės informacinės sistemos turi atitikti minimalius saugos reikalavimus. Šie reikalavimai, nustatyti įstatymų įgyvendinamuosiuose

[238] Standards for Security Categorization of Federal Information and Information Systems [interaktyvus]. 2004 [žiūrėta 2011-09-19]. <http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf>.

aktuose, yra minimalūs saugos reikalavimai, taikomi Federalinei informacijai ir informacinėms sistemoms[239]. Atitikimas reikalavimų ir kontrolė turi būti reglamentuojama vidiniame organizacijos dokumente – sistemos saugos plane. Sistemos saugos planas dažnai vadinamas „gyvu dokumentu“, nes reikalauja nuolatinės peržiūros ir modifikavimo.

Rizikos analizei būdinga tai, kad identifikuojama potenciali rizika ir pažeidžiamos vietos bei nustatomos atsakomosios priemonės. Reikalaujama, kad atsakomosios priemonės sąnaudų prasme būtų veiksmingos. Kai įvertinama sistemos dokumentacija ir rizika, sistema turi būti peržiūrima ir sertifikuojama, kad funkcionuoja tinkamai. Remiantis peržiūros rezultatais, informacijos sistema akredituojama. Sertifikavimo ir akreditavimo procesas numatytas Federalinių informacinių sistemų sertifikavimo ir akreditavimo gairėse[240].

Pavyzdžiui, 2010 m. liepos mėn. pirmoji vyriausybinė nuotolinio paslaugų prisijungimo (angl. *cloud computing*) sistema gavo įstatymo numatytą sertifikatą. Šis patvirtinimas palengvino JAV valdžios įstaigoms ir agentūroms bei grupėms įvertinti ir savo veikloje pritaikyti *Google Apps*. Į *Google Apps* įeina tokie funkcijos, kaip *Gmail, Google Docs, Google calendar* ir kt.[241].

Saugumo konferencijose ši informacijos saugos reguliavimo rūšis kritikuojama. Teigiama, kad reguliavimo netaikoma daugeliui su kompiuteriais susijusių industrijos rūšių, pavyzdžiui, interneto paslaugų teikėjams ir programinės įrangos gamintojams. Taip pat kritikuojama, kad kai kuriuose reguliavimo aktuose nenustatyta, kokios konkrečiai elektroninio saugumo priemonės turi būti taikomos, o tik nurodoma, kad turi būti įgyvendintas racionalus saugos lygis[242].

---

[239] *Minimum Security Requirements for Federal Information and Information Systems* [interaktyvus]. 2006 [žiūrėta 2011-09-19]. <http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf>.

[240] *Guide for the Security Certification and Accreditation of Federal Information Systems* [interaktyvus]. 2008 [žiūrėta 2011-09-19]. <http://csrc.nist.gov/publications/nistpubs/800-53A/SP800-53A-final-sz.pdf>.

[241] Boulton, C. Google Apps for Government meets Federal Security Standart. eWeek.com [interaktyvus] 2010-07-06 [žiūrėta 2011-09-19]. <http://www.eweek.com/c/a/Cloud-Computing/Google-Apps-for-Government-Meets-Federal-Security-Standard-593503/>.

[242] Heiman, B. J. 2003. Cybersecurity regulation is here, *RSA security conference*. Washington, D. C. Retrieved October 17, 2005.

Visgi dėl informacijos saugos nuostatų taikymo privačiam sektoriui, paminėtina Kalifornijos valstijos praktika. 2003 metais Kalifornijoje buvo išleistas Pranešimo apie saugos pažeidimus įstatymas, kuriame numatoma, kad bet kokia įmonė, valdanti Kalifornijoje gyvenančių gyventojų asmens duomenis ir patyrusi saugos pažeidimą, turi atskleisti detalius duomenis apie šį įvykį[243]. Daugelis valstijų vėliau pasekė Kalifornijos valstijos praktika ir priėmė privalomus teisės aktus, reglamentuojančius privalomą pranešimo apie saugos incidentus procedūrą. Atkreiptinas dėmesys, kad toks reguliavimas skatina įmones savanoriškai investuoti į elektroninės informacijos apsaugą tam, kad būtų išvengta potencialios rizikos reputacijai (informacijos atskleidimo apie incidentą atveju, jei įsilaužimas į įmonės kompiuterių tinklą būtų sėkmingas).

Apibendrinant informacijos saugos reguliavimą JAV, paminėtina, kad federalinis teisinis reguliavimas nukreiptas į vyriausybės įstaigų ir informacinių sistemų darbą ir nenumatoma privalomų reikalavimų privačiam sektoriui. Tačiau naujausios reguliavimo tendencijos rodo tai, kad privačiam sektoriui informacijos saugos srityje taip pat gali būti nustatomi tam tikri įpareigojimai, ypač tokioje srityje, kaip viešųjų elektroninių ryšių tinklų ir informacijos sauga. Nepaisant to, JAV informacijos saugos reguliavimo sistema yra pakankamai išbaigta, nustatytos konkrečios kontroliuojančios ir vykdomosios institucijos, apibrėžta atsakomybė ir informacijos saugos procesai.

Informacijos saugos reguliavimas Rusijoje

Pagrindiniai teisės aktai, reguliuojantys informacijos saugą. Pagrindinis dokumentas informacijos saugos srityje Rusijoje yra Informacijos saugos Rusijos Federacijoje doktrina[244]. Tai bazinis konceptualus dokumentas, nustatantis pagrindines vienos iš svarbiausių valstybės saugumo sričių kryptis.

Doktrinoje pažymima, kad dabartiniam visuomenės raidos etapui būdingas stiprėjantis informacijos (į kurią įeina informacija, informacinė infrastruktūra, su tuo susiję subjektai ir kt.) vaidmuo.

[243] *California Data Security Breach Act Helps Protect Private Information*. Buzzle.com [interaktyvus, žiūrėta 2011-09-19]. <http://www.buzzle.com/articles/california-data-security-breach-act-helps-protect-private-information.html>.

[244] Doctrine of the Information Security of the Russian federation, 2000 [interaktyvus, žiūrėta 2011-09-19]. <http://www.medialaw.ru/e_pages/laws/project/d2-4.htm>.

Rusijos Federacijoje Informacijos saugos doktrina yra pagrindas:

- formuoti valstybės politiką informacijos saugos užtikrinimo srityje;
- rengti siūlymus tobulinant informacijos saugos teisinį reguliavimą;
- rengti tikslines informacijos saugos užtikrinimo programas[245].

Rusijos Federacijoje skiriami 4 informacijos saugos reguliavimo lygiai:

1) pirmąjį lygį sudaro tarptautiniai susitarimai dėl informacijos apsaugos ir valstybės paslapčių, taip pat valstybės informacijos apsaugos teisinio reguliavimo doktrina, į kurią įeina:
   - tarptautinės konvencijos dėl nuosavybės į informaciją apsaugos ir autorių teisių į informaciją apsaugos.
   - Rusijos Federacijos Konstitucija (23 str., nustatantis asmenų teises į susirašinėjimą ir kitus pranešimus).
   - Rusijos Federacijos civilinis kodeksas[246] (Kodekso 139 str. nustato teisę į nuostolių, atsiradusių dėl informacijos nutekėjimo, taikant neteisėtus metodus, atlyginimą).
   - Rusijos Federacijos baudžiamasis kodeksas[247] (nustatantis atsakomybę už elektroninius nusikaltimus).
   - Federalinis įstatymas „Dėl informacijos, informatizacijos ir informacijos apsaugos[248] (Įstatymo 10 str. nagrinėja informacijos išteklius pagal prieigos kategorijas: atvira informacija, valstybės paslaptis, konfidenciali informacija; 21 str. nustato informacijos apsaugos tvarką).
   - Federalinis įstatymas Dėl asmens duomenų[249].
2) antrąjį lygį sudaro įstatymų įgyvendinamieji teisės aktai: Prezidento nurodymai, Vyriausybės potvarkiai, Aukščiausiojo arbitražinio teismo nurodymai ir Rusijos Federacijos plenumų nurodymai.

[245] Doctrine of the Information Security of the Russian Federation. 2000 [interaktyvus, žiūrėta 2011-09-19]. <http://www.medialaw.ru/e_pages/laws/project/d2-4.htm>.

[246] Graždanskij kodeks Rosisjoj Federaciji. [interaktyvus, žiūrėta 2011-09-19]. Prieiga internetu: <http://base.garant.ru/10164072/>.

[247] Ugolovnij kodeks Rosiskoj Fdereaciji. [interaktyvus, žiūrėta 2011-09-19]. <http://www.interlaw.ru/law/docs/10008000/>.

[248] Federal Act No. 24-FZ of the Russian Federation on Information, Informatization and Protection of Information. 20 February, 1995 [interaktyvus, žiūrėta 2011-09-19]. <http://www.medialaw.ru/e_pages/laws/russian/iipi-en.htm>.

[249] Federal Act No. 152-FZ on Personal Data. 27 July, 2006 [interaktyvus, žiūrėta 2011-09-19]. <http://www.mofo.com/docs/mofoprivacy/Federal%20Law%20of%2027%20July%202006%20N152-FZ%20on%20Personal%20Data%20%20(English).pdf>.

3) trečiąjį lygį sudaro informacijos saugos standartai.
4) ketvirtąjį lygį sudaro lokalūs norminiai aktai, instrukcijos ir kt. dokumentai[250].

Institucinė informacijos saugos priežiūros kontrolė. Rusijos Federacijos informacijos saugos užtikrinimo sistema yra nacionalinio saugumo valstybėje užtikrinimo sistemos dalis. Pagrindiniai tokios sistemos elementai įvardijami Informacijos saugos doktrinoje: Rusijos Federacijos Prezidentas, Federalinės Asamblėjos Rūmai, Valstybės Dūma, Rusijos Federacijos Vyriausybė, Rusijos Federacijos saugos taryba, federalinės vykdomosios valdžios struktūros, valstybės komisijos, lokalios savireguliavimo struktūros, teisminė valdžia[251].

Rusijos Federacijos Prezidentas, vadovaudamasis konstitucijoje suteiktais įgaliojimais, prižiūri įvairias institucijas ir išteklius, kad būtų užtikrinta informacijos sauga Rusijos Federacijoje, taip pat sankcionuoja veiksmus, užtikrinančius informacijos saugą Rusijos Federacijoje. reorganizuoja ir panaikina tarnybas / įstaigas, atsakingas Prezidentui ir užsiimančias informacijos saugos užtikrinimu Rusijos Federacijoje. Identifikuoja valstybės prioritetus užtikrinant informacijos apsaugą Rusijos Federacijoje, taip pat Doktrinos įgyvendinimo priemones.

Rusijos Federacijos Federalinės Asamblėjos Rūmai, remdamiesi suteiktomis teisėmis, formuoja teisės aktų sistemą, užtikrinančią informacijos saugą Rusijos Federacijoje.

Rusijos Vyriausybė koordinuoja federalinių institucijų veiksmus informacijos saugos srityje, formuoja federalinį biudžetą ir numato informacijos saugos užtikrinimo finansavimą. Viena iš Rusijos Federacijos Vyriausybės sričių turėtų būti informacinių technologijų (toliau – IT) sektoriaus plėtra (įskaitant IT saugą), tačiau mokslinėje literatūroje nurodoma, kad IT sektoriaus plėtra nėra identifikuojama kaip viena iš pagrindinių Rusijos Federacijos Vyriausybės sričių[252].

Rusijos Federacijos saugos taryba identifikuoja ir vertina grėsmes informacijos saugumui Rusijos Federacijoje, rengia sprendimų projek-

[250] Doctrine of the Information Security of the Russian Federation, 2000 [interaktyvus, žiūrėta 2011-09-19]. <http://www.medialaw.ru/e_pages/laws/project/d2-4.htm>.

[251] *Ibid*.

[252] Graham, J. 2009. *Cyber Fraud: Tactics, Techniques and Procedures*. Taylor&Francis Group, p. 92.

tus prezidentui, skirtus tokių grėsmių prevencijai; rengia pasiūlymus dėl informacijos saugos gerinimo, taip pat pasiūlymus dėl doktrinos tobulinimo ir atnaujinimo; koordinuoja institucijų darbą užtikrinant informacijos saugą; kontroliuoja Rusijos Federacijos prezidento sprendimų įgyvendinimą informacijos saugos srityje.

Federalinės vykdomosios valdžios struktūros užtikrina Rusijos Federacijos įstatymų, Rusijos Federacijos Prezidento ir Rusijos Federacijos Vyriausybės sprendimų įgyvendinimą, kuria teisinio reguliavimo teisės aktus informacijos saugos srityje ir teikia jų projektus prezidentui bei vyriausybei.

Vykdomieji subjektai bendradarbiauja su federalinės vykdomosios valdžios struktūromis, siekdami užtikrinti teisinį reguliavimą informacijos saugos srityje; taip pat bendradarbiauja įgyvendinant įvairias federalines programas informacijos saugos srityje; kartu su vietine savivalda imasi priemonių skatinti bendradarbiavimą tarp piliečių ir organizacijų ir kt., taip pat užtikrinti informacijos saugumą; federalinės vykdomosios valdžios struktūroms teikia pasiūlymus dėl informacijos saugos gerinimo Rusijos Federacijoje.

Vietinės savivaldos struktūros užtikrina federalinių įstatymų atitikimą informacijos saugos srityje.

Teisminės valdžios institucijos užtikrina teisingumą ir teikia teisinę apsaugą piliečiams, kurių teisės informacijos saugos srityje buvo pažeistos.

Informacijos saugos užtikrinimo sistema gali turėti ir tam tikras subsistemas, galinčias padėti spręsti lokalias užduotis, garantuojant informacijos saugumą[253].

Pagrindiniai elektroninės informacijos saugos reikalavimai. Informacijos saugos Rusijos Federacijoje doktrinoje nurodoma, kad saugos priemonės turi būti įgyvendintos valstybės institucijose, įmonėse, organizacijose, nepriklausomai nuo šių subjektų nuosavybės. Doktrinoje, kuri priimta 2000 metais, rašoma, kad esama informacijos saugos būklė Rusijos Federacijoje reikalauja skubiai įgyvendinti šiuos veiksmus:

- sukurti valstybės politikos informacijos saugos gaires, taip pat priemones ir mechanizmus, skirtus įgyvendinti šioms gairėms;
- sukurti federalines tikslines programas informacijos saugos srityje;
- sukurti informacinių sistemų saugos užtikrinimo įvertinimo kriterijus ir metodus;

[253] Doctrine of the Information Security of the Russian Federation. 2000 [interaktyvus, žiūrėta 2011-09-19]. <http://www.medialaw.ru/e_pages/laws/project/d2-4.htm>.

- gerinti teisinę bazę, užtikrinančią informacijos saugą;
- nustatyti federalinių organų atitinkamų darbuotojų, lokalios savivaldos darbuotojų ir kt. atsakomybę informacijos saugos srityje;
- tobulinti mokslinius ir kitus metodus, kaip užtikrinti informacijos saugą;
- plėtoti metodus ir mechanizmus, įgyvendinančius nacionalinę informacijos politiką[254].

Informacijos saugos užtikrinimo Rusijos Federacijoje metodai skirstomi į tris grupes:

1) teisiniai;
2) organizaciniai-techniniai;
3) ekonominiai.

Teisiniams metodams priskiriamas teisės aktų informacijos saugos srityje rengimas. Svarbiausios sritys:

- atitinkamų įstatymų pakeitimai ir papildymai, siekiant tobulinti bendrąją informacijos saugos reguliavimo sistemą;
- teisės aktai, skirti atskirti atsakomybei tarp subjektų užtikrinant informacijos saugą;
- kūrimas teisės aktų, numatančių teisinę juridinių ir fizinių asmenų atsakomybę už neteisėtą prieigą prie kompiuterinės informacijos ir kitas neteisėtas veikas (elektroninius nusikaltimus);
- kūrimas teisės aktų, steigiančių regionines struktūras, užtikrinančias informacijos saugą Rusijos Federacijoje;
- ir kt. [255]

Taigi pagrindinės valstybės politikos nuostatos yra gairės, nustatančios federalinių ir kitų subjektų veiklą informacijos saugos srityje, įskaitant pareigas, atsakomybę ir kt.

Pagal Informacijos saugos Rusijos Federacijoje doktriną, valstybė, įgyvendindama atitinkamas funkcijas informacijos saugos srityje:

- vykdo grėsmių informacijos saugai analizę;
- organizuoja atitinkamų subjektų darbą, siekdama užkirsti kelią ir neutralizuoti grėsmes informacijos saugai;
- palaiko nevyriausybinių organizacijų veiklą, informuodama visuomenę apie aktualius aspektus, susijusius su informacijos sauga;

[254] *Ibid*.
[255] *Ibid*.

- organizuoja federalinių programų, užtikrinančių informacijos saugą, kūrimą;
- ir kt. [256]

Apibendrinant galima teigti, kad Rusijos Federacijoje formaliai informacijos saugai skiriama nemažai dėmesio, įskaitant ir teisės aktus. Tačiau nuostatos yra deklaratyvios, todėl jos labiau primena šūkius, o ne konkrečias informacijos saugos užtikrinimo priemones. Institucinė informacijos saugos kontrolė, nors atrodo aiški ir suprantama, tačiau, panagrinėjus detaliau, kyla abejonių dėl aiškaus institucijų funkcijų ir atsakomybės ribų atskyrimo.

Elektroninės informacijos saugos reguliavimas Lietuvoje

Pagrindiniai teisės aktai, reguliuojantys informacijos saugą. Iš teisės aktų paminėtinas Lietuvos Respublikos elektroninių ryšių įstatymas[257]. Šio įstatymo nuostatos dėl elektroninių ryšių informacijos saugos iš esmės buvo praplėstos įgyvendinant vieną iš Europos Sąjungos elektroninių ryšių paketo direktyvų – Direktyvą 2009/136/EB[258]. Direktyvos 2009/136/EB įgyvendinimas didele dalimi susijęs su elektroninių ryšių reglamentavimu elektroninės informacijos saugos srityje. Dėl to Lietuvos Respublikos elektroninių ryšių įstatyme (paskutiniai įstatymo pakeitimai priimti 2011 m. birželio 28 d.[259]) atsirado gana nemažai teisės normų dėl elektroninės informacijos saugos. Šis įstatymas taikomas ir privačiam sektoriui, t. y. elektroninių ryšių tinklų ir (ar) paslaugų teikėjams.

---

[256] *Ibid*.

[257] Lietuvos Respublikos elektroninių ryšių įstatymas. *Valstybės žinios*, 2004, Nr. 69-2382.

[258] 2009 m. lapkričio 25 d. Europos Parlamentas ir Taryba priėmė direktyvą 2009/136/EB, iš dalies keičiančią direktyvą 2002/22/EB dėl universaliųjų paslaugų ir paslaugų gavėjų teisių, susijusių su elektroninių ryšių tinklais ir paslaugomis, direktyvą 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje ir reglamentą (EB) Nr. 2006/2004 dėl nacionalinių institucijų, atsakingų už vartotojų apsaugos teisės aktų vykdymą, bendradarbiavimo bei direktyvą 2009/140/EB, iš dalies keičiančią direktyvą 2002/21/EB dėl elektroninių ryšių tinklų ir paslaugų bendrosios reguliavimo sistemos, direktyvą 2002/19/EB dėl elektroninių ryšių tinklų ir susijusių priemonių sujungimo ir prieigos prie jų ir direktyvą 2002/20/EB dėl elektroninių ryšių tinklų ir paslaugų leidimo.

[259] Elektroninių ryšių įstatymo 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 16, 17, 18, 21, 22, 23, 27, 28, 29, 30, 31, 32, 33, 34, 36, 37, 39, 40, 41, 48, 49, 50, 51, 52, 54, 56, 57, 58, 59, 61, 62, 63, 64, 66, 68, 69, 71, 72, 73, 74, 75, 77 straipsnių, antrojo skirsnio pavadinimo ir 2 priedo pakeitimo ir papildymo, Įstatymo papildymo 23(1), 23(2), 42(1) straipsniais ir 35 straipsnio pripažinimo netekusiu galios įstatymas. *Valstybės žinios*, 2011, Nr. 91-4327.

E. ryšių paslaugų saugumo ir vientisumo klausimu įstatyme nustatyta, kad viešųjų ryšių tinklų / paslaugų teikėjai privalo įgyvendinti tinkamas technines ir organizacines priemones savo teikiamų tinklų / paslaugų saugumo lygiui, atitinkančiam iškilusią grėsmę, užtikrinti ir užkirsti kelią saugumo incidentams arba sumažinti jų poveikį viešųjų ryšių tinklams ir viešųjų e. ryšių paslaugų gavėjams. Taip pat turi būti užtikrintas nepertraukiamas viešųjų e. ryšių paslaugų teikimas. Įstatyme taip pat nustatyta pareiga viešųjų ryšių tinklų / paslaugų teikėjui nedelsiant pranešti apie asmens duomenų saugumo pažeidimus Valstybinei duomenų apsaugos bei abonentui / registruotam naudotojui / kitam asmeniui, jei pažeidimas gali turėti neigiamą poveikį jo privačiam saugumui, išskyrus atvejus, kai jis Valstybinei duomenų apsaugos inspekcijai įrodo, kad įgyvendino tinkamas technines priemones, užtikrinančias, kad tam neįgalioti asmenys negalėtų susipažinti su asmens duomenimis. Toks teisinis reguliavimas, įpareigojantis pranešti apie asmens duomenų saugumo pažeidimus, ES direktyvoje siejamas su tapatybės vagystės prevencija. Direktyvos Nr. 2009/136/EB preambulėje nurodoma, kad dėl asmens duomenų saugumo pažeidimo, jei jis tinkamai ir laiku nenustatomas, susijęs abonentas arba asmuo gali patirti didelių ekonominių nuostolių arba socialinę žalą, įskaitant su tapatybe susijusį sukčiavimą[260].

Taip pat, svarbu paminėti Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymą[261]. Šio įstatymo nuostatos reglamentuoja valdomų ir tvarkomų asmens duomenų saugumą. Įstatymas taikomas tiek valstybiniam, tiek privačiam sektoriui, nesvarbu kokiam sektoriui priklauso asmens duomenų valdytojas.

Vis dėlto svarbu pažymėti, kad Lietuvoje buvo kilę iniciatyvų įstatymo lygmeniu reglamentuoti informacijos saugą. Kaip viena iš pagrindinių iniciatyvų paminėtinas pradėtas rengti Lietuvos Respublikos elekt-

[260] Europos Parlemento ir Tarybos direktyva 2009/136/EB iš dalies keičianti direktyvą 2002/22/EB dėl universaliųjų paslaugų ir paslaugų gavėjų teisių, susijusių su elektroninių ryšių tinklais ir paslaugomis, direktyvą 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje ir reglamentą (EB) Nr. 2006/2004 dėl nacionalinių institucijų, atsakingų už vartotojų apsaugos teisės aktų vykdymą, bendradarbiavimo. Preambulės 61 p. [interaktyvus, žiūrėta 2011-09-21]. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:LT:PDF>.

[261] Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas. *Valstybės žinios*, 2008, Nr. 22-804.

roninių ryšių tinklų ir informacijos saugumo įstatymo projektas. Šio projekto rengimo pradžią inicijavo Lietuvos Respublikos Vyriausybės nutarimu patvirtinta Elektroninių ryšių tinklų ir informacijos saugumo koncepcija. Teisinis šios koncepcijos parengimo pagrindas tas, kad koncepcija parengta įgyvendinant Lietuvos Respublikos Vyriausybės 2006–2008 metų programos įgyvendinimo priemonių, patvirtintų Lietuvos Respublikos Vyriausybės 2006 m. spalio 17 d. nutarimu Nr. 1020 (Žin., 2006, Nr. 112-4273), 157 punktą. Lietuvos informacinės visuomenės plėtros strategijoje, patvirtintoje Lietuvos Respublikos Vyriausybės 2005 m. birželio 8 d. nutarimu Nr. 625 (Žin., 2005, Nr. 73-2649), analizuojant informacinės visuomenės plėtros stiprybes, silpnybes, galimybes, grėsmes (SSGG), tarp informacinės visuomenės plėtros grėsmių nurodomos ir neišspręstos informacijos technologijų saugumo problemos. Taip pat pabrėžta, kad plėtojant naujas elektronines paslaugas ir taikomuosius sprendimus būtina užtikrinti informacijos technologijų saugumą. Minėtame nutarime yra įtvirtinti informacinės visuomenės plėtros prioritetai. Vienas iš jų – žinių ekonomika, kurį įgyvendinant siekiama tam tikrų tikslų, pvz., remti saugios, modernios informacinės infrastruktūros plėtrą[262].

Tačiau, nepaisant patvirtintos koncepcijos, minėtas Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymas taip ir nebuvo priimtas. Šis rengtas projektas taip ir nebuvo registruotas net Lietuvos Respublikos teisės aktų projektų registre.

Taigi šiuo metu Lietuvoje nėra įstatymo, kuris kompleksiškai reglamentuotų elektroninės informacijos saugos sritį. Keletu įstatymų reglamentuojami atitinkamų sektorių informacijos saugos klausimai.

Paminėtinas svarbus įstatymo įgyvendinamasis aktas šioje srityje. 2011 m. birželio 29 d. Lietuvos Respublikos Vyriausybė nutarimu Nr. 796 patvirtino Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programą[263]. Programa parengta atsižvelgiant į tai, kad valstybės ir visuomenės gyvenime vis didesnę reikšmę įgyja informacinėmis ir ryšių technologijomis tvarkoma ir perduodama

[262] Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymo koncepcija. *Valstybės žinios,* 2006, Nr. 134-5081, 1 str.

[263] Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011-2019 metais programa. *Valstybės žinios.* 2011, Nr. 83-4033.

elektroninė informacija, atsiradusios elektroninės informacijos tvarkymo galimybės paskatino nacionalinių ir globalių informacinių visuomenių atsiradimą ir sudarė sąlygas toliau modernizuoti šalių ūkius ir efektyviau valdyti valstybę, tačiau tuo pačiu metu į elektroninę erdvę perkeliama vis daugiau informacijos, sparčiai automatizuojami įvairūs šalies valdymo ir ūkio veiklos procesai, globali kibernetinė erdvė ir joje teikiamos viešosios paslaugos tapo patraukliu atskirų asmenų, nusikalstamų grupuočių, politinių jėgų ir kitų subjektų taikiniu[264]. Programos paskirtis – nustatyti elektroninės informacijos saugos (kibernetinio saugumo) plėtros tikslus ir uždavinius, kad būtų užtikrintas elektroninės informacijos ir kibernetinėje erdvėje teikiamų paslaugų konfidencialumas, vientisumas ir prieinamumas, elektroninių ryšių tinklų, informacinių sistemų ir ypatingos svarbos informacinės infrastruktūros apsauga nuo incidentų ir kibernetinių atakų, asmens duomenų ir privatumo apsauga, taip pat nustatyti uždavinius, kurių įgyvendinimas leistų užtikrinti bendrą kibernetinės erdvės ir joje veiklą vykdančių subjektų saugumą[265].

Institucinė informacijos saugos priežiūros kontrolė. Viena iš labiausiai savo veikla su elektroninės informacijos sauga susijusių institucijų yra Lietuvos Respublikos ryšių reguliavimo tarnyba (toliau – Tarnyba). Tarnybos nuostatuose nurodyta, kad:

- Tarnyba vykdo nacionalinio elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinio CERT (angl. *Computer Emergency Response Team*) veiklą;
- dalyvauja Europos tinklų ir informacijos saugumo agentūros, įkurtos 2004 m. kovo 10 d. Europos Parlamento ir Tarybos reglamentu Nr. 460/2004 dėl Europos tinklų ir informacijos saugumo agentūros įkūrimo, veikloje[266].

Nacionalinio elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinio CERT veikla pasireiškia vykdant pagrindinį padalinio tikslą – elektroninių ryšių tinklų ir informacijos saugumo stiprinimas

[264] Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programa. *Valstybės žinios.* 2011, Nr. 83-4033, 2 punktas.

[265] *Ibid*., 3 punktas.

[266] Lietuvos Respublikos ryšių reguliavimo tarnybos nuostatai. *Valstybės žinios.* 2004, Nr. 131-4743, p. 8.24, 8.43.

ir paslaugų gavėjų pasitikėjimo elektronine erdve didinimas[267]. Tarnybos svarbiausi uždaviniai, vykdant nacionalinio CERT padalinio veiklą, yra šie:

- koordinuoti CERT padalinių ir teikėjų veiksmus Lietuvos Respublikoje stabdant incidentų plitimą, šalinant incidentų padarinius viešuosiuose ryšių tinkluose ir informacinėse sistemose;
- pagal kompetenciją vykdyti incidentų tyrimus viešuosiuose ryšių tinkluose ir informacinėse sistemose;
- vykdyti incidentų prevenciją viešuosiuose ryšių tinkluose ir informacinėse sistemose;
- pagal kompetenciją atstovauti Lietuvos Respublikai palaikant santykius su užsienio valstybių incidentų tyrimo institucijomis ir CERT padaliniais[268].

Taigi padalinio veikla labiausiai susijusi su reagavimu į įvairius elektroninės erdvės incidentus ir tokių incidentų prevencija (siaurąja prasme). Šio padalinio veikla daro įtaką ir Lietuvos Respublikos ryšių reguliavimo tarnybos veiklai.

Kaip jau minėta, be CERT funkcijų, Tarnyba dar dalyvauja ENISA[269] veikloje. Tačiau ši veikla, išskyrus apsikeitimą informacija ir kitus susijusius aspektus, iš esmės nedaro įtakos Tarnybos funkcijoms informacijos saugos srityje, kurios kol kas lieka labiausiai susijusios su CERT veikla.

Kita paminėtina institucija – Valstybinė duomenų apsaugos inspekcija – atsakinga už asmens duomenų saugumą, įskaitant elektroniniais ryšiais valdomų asmens duomenų saugumą. Inspekcija atsakinga už Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo laikymosi priežiūrą (įstatymas reglamentuoja ir tvarkomų asmens duomenų saugumą).

Už elektroninės informacijos saugą Lietuvos valstybės institucijų sektoriuje atsakinga Lietuvos Respublikos vidaus reikalų ministerija. Jos nuostatuose įtvirtinta, kad ministerija <...> koordinuoja informacinių technologijų saugą valstybės institucijose ir įstaigose[270].

---

[267] Nacionalinio elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinio veiklos nuostatai, *Valstybės žinios*. 2009. Nr. 36-1419, 4 p.

[268] *Ibid*., 5 p.

[269] European Network and Information Security Agency [interaktyvus, žiūrėta: 2011-09-21] <http://www.enisa.europa.eu/>.

[270] Lietuvos Respublikos vidaus reikalų ministerijos nuostatai. *Valstybės žinios*. 2001, Nr. 27-794, 13, 2 p.

Pastebėtina, kad Lietuvoje nėra vienos už informacijos saugą atsakingos institucijos. Tačiau informacijos saugą valstybės sektoriuje koordinuojanti Lietuvos Respublikos vidaus reikalų ministerija neturi privalomų įgalinimų teisės kitoms institucijoms ir įstaigoms, t. y. kitos institucijos ir įstaigos nėra pavaldžios šiai ministerijai. Tai sukuria situaciją, kai nesant pavaldumo santykių ar kitokių įgalinimų, sunku sukontroliuoti informacijos saugą valstybės institucijose ir įstaigose.

Pagrindiniai elektroninės informacijos saugos reikalavimai. Lietuva ilgą laiką neturėjo net ilgalaikės informacinių technologijų plėtros strategijos. Lietuvoje taip pat ne kartą keitėsi institucijos, atsakingos už šios srities politikos įgyvendinimą mūsų valstybėje, dėl ko valstybės politika šioje srityje tapo išbalansuota ir silpnai koordinuojama. Galima sakyti, kad pirmą kartą šiuo klausimu rimtai buvo susidomėta tik 2000 m., kai buvo atliktas pirmasis valstybės informacinės infrastruktūros situacijos įvertinimas. Viena iš pagrindinių šio vertinimo sričių buvo informacijos saugos suvokimo lygis, šios srities politika ir tuometinis vyriausybinių įstaigų apsaugos laipsnis. Įvertinimas nurodė esamos informacinės infrastruktūros trūkumus, būtent tai, kad daugelyje vyriausybinių įstaigų apskritai informacijos apsauga yra nepakankama. Informacijos saugos kontrolė tuo metu buvo labai silpna. Beveik visose saugos srityse reikėjo gerinti situaciją, norint apsaugoti informacijos infrastruktūrą nuo išpuolių, kurie galėjo pakenkti Vyriausybės įstaigų veiklai. Viena svarbiausių silpnos apsaugos priežasčių buvo bendras nesuvokimas, kad rūpintis sauga yra būtina. Tarp kitų priežasčių galima paminėti nepatyrusius saugos srityje dirbančius specialistus bei finansavimo trūkumą – saugai užtikrinti reikalingos lėšos.

Būtina pabrėžti, kad išskirtinis valstybinio sektoriaus informacinių sistemų bruožas – būtinumas griežtai ir centralizuotai nustatyti tiesioginio valdymo ir kontrolės principus. Šiuo atveju būtinas saugos lygis turi būti nustatomas visų pirma atsižvelgiant į valstybės, nacionalinio saugumo interesus, o tik po to į galimas išlaidas. Todėl informacijos technologijų saugos svarba bene pirmą kartą valstybiniu mastu Lietuvos valstybės institucijose buvo nurodyta Informacijos technologijų saugos valstybinėje strategijoje, patvirtintoje 2001 m. gruodžio 22 d. Lietuvos Respublikos Vyriausybės nutarimu Nr. 1625[271].

[271] Informacijos technologijų saugos valstybinė strategija. *Valstybės žinios*, 2001, Nr. 110-4006.

Pastaruoju metu elektroninės informacijos saugos valstybės institucijų sektoriuje strategijos aspektai buvo įtvirtinti **Elektroninės informacijos saugos valstybės institucijų informacinėse sistemose valstybinėje strategijoje** iki 2008 metų[272]. Elektroninės informacijos saugos valstybės institucijų informacinėse sistemose valstybinė strategija iki 2008 metų nustatė pagrindinius elektroninės informacijos saugos užtikrinimo principus, tikslus, uždavinius ir jų įgyvendinimą Tačiau jau pačiame strategijos pavadinime nurodyta, iki kurių metų skirta minima strategija. Deja, po 2008 metų šios strategijos nepakeitė joks kitas strateginis dokumentas elektroninės informacijos saugos srityje, tad iš principo šiuo metu Lietuvoje nėra galiojančios elektroninės informacijos saugos valstybės informacinėse sistemose strategijos.

Nepaisant to, esminiai reikalavimai elektroninės informacijos saugai nurodyti daugelyje įstatymų įgyvendinamųjų teisės aktų. Pagrindiniai reikalavimai elektroninės informacijos saugai nurodyti **Bendruosiuose elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimuose**[273]**.** Reikalavimų 6 p. nustato, kad informacinės sistemos valdytojas privalo turėti pagal Vidaus reikalų ministerijos tvirtinamas Saugos dokumentų turinio gaires parengtus, su Vidaus reikalų ministerija suderintus ir patvirtintus šiuos saugos dokumentus:

- Nuostatus;
- Saugaus elektroninės informacijos tvarkymo taisykles;
- Informacinės sistemos veiklos tęstinumo valdymo planą;
- Informacinės sistemos naudotojų administravimo taisykles.

Bendrieji reikalavimai detaliai nurodo kiekvieno iš būtinų saugos dokumentų turinį. Tačiau detalūs reikalavimai numatyti Saugos dokumentų turinio gairėse[274].

Teisės aktu, kuriuo tvirtinami Nuostatai, skiriamas saugos įgaliotinis arba pavedama informacinės sistemos tvarkytojui paskirti saugos įgaliotinį ir nurodomi saugos politiką įgyvendinančių dokumentų rengėjai

[272] Elektroninės informacijos saugos valstybės institucijų informacinėse sistemose valstybinėje strategija iki 2008 metų. *Valstybės žinios.* 2006, Nr. 70-2575.

[273] Bendrieji elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimai. *Valstybės žinios.* 1997, Nr. 83-2075.

[274] Saugos dokumentų turinio gairės. *Valstybės žinios*. 2007, Nr. 53-2070.

bei saugos politiką įgyvendinančių dokumentų patvirtinimo terminai[275]. Bendruosiuose reikalavimuose nurodytos elektroninės informacijos saugos įgaliotinio funkcijos.

Be anksčiau paminėtų aspektų, Bendrieji reikalavimai taip pat nustato saugos incidentų valdymo taisykles, rizikos įvertinimo procedūras, informacinės sistemos funkcijų pokyčių valdymo tvarką, informacinių technologijų saugos atitikties vertinimą bei informacinės sistemos naudotojų atsakomybę.

Siekiant gerinti ir koordinuoti elektroninės informacijos saugą, Lietuvoje įsteigta Elektroninės informacijos saugos koordinavimo komisija. Personalinė komisijos sudėtis tvirtinama atskiru Lietuvos Respublikos Vyriausybės nutarimu. Komisijos uždaviniai yra šie:

- koordinuoti neįslaptintos elektroninės informacijos (toliau – elektroninė informacija) saugos įgyvendinimą;
- skatinti elektroninės informacijos saugos kultūros kėlimą;
- inicijuoti elektroninės informacijos saugos projektų rengimą.

Komisija, vykdydama jai paskirtus uždavinius, atlieka šias funkcijas:

- dalyvauja įgyvendinant valstybės politiką elektroninės informacijos saugos informacinių sistemų srityje;
- Lietuvos Respublikos Vyriausybės įstatymo ir Lietuvos Respublikos Vyriausybės darbo reglamento, patvirtinto Lietuvos Respublikos Vyriausybės 1994 m. rugpjūčio 11 d. nutarimu Nr. 728 (Žin., 1994, Nr. 63-1238; 2003, Nr. 27-1089), nustatyta tvarka rengia teisės aktų projektus, susijusius su elektroninės informacijos sauga;
- analizuoja elektroninės informacijos saugos tobulinimo tendencijas, stebi esminių pavojų esamoms ir būsimoms informacinėms vertybėms pokyčius informacinėse sistemose;
- teikia valstybės institucijoms rekomendacijas, kaip stiprinti elektroninės informacijos saugą;
- koordinuoja elektroninės informacijos saugos projektų įgyvendinimą;
- skatina valstybės institucijas bendradarbiauti elektroninės informacijos saugos srityje;

[275] Bendrieji elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimai. *Valstybės žinios*, 1997, Nr. 83-2075, 9 p.

- bendradarbiauja su privačiu sektoriumi elektroninės informacijos saugos srityje;
- atlieka kitas jai paskirtas funkcijas[276].

Valstybės institucijų ir įstaigų informacinės sistemos pagal tam tikrus kriterijus klasifikuojamos į keturias kategorijas: nuo pirmosios (aukščiausioji) iki ketvirtosios (žemiausioji kategorija). Ši klasifikacija numatyta Valstybės institucijų ir įstaigų informacinių sistemų klasifikavimo pagal jose tvarkomą elektroninę informaciją gairėse[277]. Pavyzdžiui, Valstybinio socialinio draudimo fondo funkcijų vykdymą užtikrinanti informacinė sistema priskiriama prie pirmosios, t. y. aukščiausios kategorijos informacinių sistemų. Konkretūs informacijos saugos reikalavimai minėtoms kategorijoms nustatyti Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos techniniuose saugos reikalavimuose[278]. Šiuo dokumentu nustatomi minimalūs elektroninės informacijos techniniai saugos reikalavimai Lietuvos respublikos Vyriausybei atskaitingų valstybės institucijų ir įstaigų informacinėms sistemoms. Pavyzdžiui, pirmosios kategorijos informacinių sistemų elektroninės informacijos papildomas saugos reikalavimas yra tas, kad institucija turi įgyvendinti Lietuvos standarte LST ISO-IEC 17799:2006 nurodytas technines saugos priemones[279].

Lietuvos Respublikos vidaus reikalų ministras įsakyme taip pat yra patvirtinęs Saugaus elektroninės informacijos teikimo sutartį[280]. Sutarties dalykas: sutartimi teikėjas įsipareigoja saugiai automatiniu būdu teikti sutarties priede nurodytą elektroninę informaciją gavėjui, o gavėjas įsipareigoja ją naudoti sutartyje nurodytu tikslu, sąlygomis ir tvarka[281].

Lietuvos Respublikos Vyriausybė taip pat yra patvirtinusi Valstybės informacinių sistemų steigimo ir įteisinimo taisykles[282]. Valstybės informaci-

[276] 2006 m. gruodžio 13 d. Lietuvos Respublikos Vyriausybės nutarimas Nr. 1266 „Dėl elektroninės informacijos saugos koordinavimo komisijos sudarymo“. *Valstybės žinios*. 2006, Nr. 137-5224.

[277] Valstybės institucijų ir įstaigų informacinių sistemų klasifikavimo pagal jose tvarkomą elektroninę informaciją gairės. *Valstybės žinios.* 2007, Nr. 78-3160.

[278] Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos techniniai saugos reikalavimai. *Valstybės žinios.* 2008, Nr. 127-4866.

[279] *Ibid*., 6.2 p.

[280] Saugaus elektroninės informacijos teikimo sutartis. *Valstybės žinios*. 2007, Nr. 75-2980.

[281] *Ibid*., 2 sk.

[282] Valstybės informacinių sistemų steigimo ir įteisinimo taisyklės. *Valstybės žinios.* 2004, Nr. 58-2061.

nių sistemų steigimo ir įteisinimo taisyklėse nustatytos valstybės informacinių sistemų (išskyrus valstybės ir žinybinius registrus) steigimo, kūrimo ir įteisinimo, modernizavimo ir likvidavimo procedūros[283].

Informacinių technologijų saugos atitiktis vertinama pagal Lietuvos Respublikos vidaus reikalų ministro patvirtintą Informacinių technologijų saugos atitikties vertinimo metodiką[284]. Pagal šią metodiką informacinių technologijų saugos atitiktis informacinėse sistemose vertinama dviem etapais: vertintojas parengia informacinių sistemų saugos atitikties vertinimo ataskaitą ir teikia ją įstaigos vadovui, kuris organizuoja trūkumų šalinimo priemonių plano rengimą. Kaip vykdomas trūkumų šalinimo priemonių planas, prižiūri įstaigos saugos įgaliotinis[285].

Taip pat reikia paminėti ir Lietuvos Respublikos vidaus reikalų ministro įsakymu patvirtintas Interneto tarnybinių stočių apsaugos rekomendacijas[286]. Šios rekomendacijos apibrėžia bendro pobūdžio priemonių tarnybinėms stotims valstybės institucijose ir įstaigose apsaugoti nuo išorinių ir vidinių grėsmių visumą ir yra skirtos kompiuterių tinklui, turinčiam ryšį su internetu, sukurti, siekiant užtikrinti interneto tarnybinių stočių saugą[287].

Taip pat kiekvienos organizacijos, užtikrinančios informacinių technologijų saugą, pagalbine knyga tapo 2002 m. liepos 1 d. įsigaliojęs Lietuvos standartas „Informacijos technologija. Praktiniai informacijos saugumo valdymo aspektai“, tapatus tarptautiniam standartui ISO/IEC 17799:2000, kuris 2004 m. buvo išverstas į lietuvių kalbą ir patvirtintas. Šiame standarte nurodoma geroji praktika, kuria vadovaujantis organizacijos turi kurti savo informacijos saugos politiką.

Taigi, Lietuvoje šiuo metu nėra galiojančios elektroninės informacijos saugos valstybės sektoriuje strategijos. Šioje srityje vis dar trūksta aiškios, koordinuotos valstybės politikos, informacinių technologijų, o informacijos saugą reglamentuojanti teisinė bazė nenustato vienodai taikomų ir aiškių reikalavimų informacinių sistemų valdytojams. Taip pat

[283] Valstybės informacinių sistemų steigimo ir įteisinimo taisyklės, *Valstybės žinios*. 2004, Nr. 58-2061, 1 p.

[284] Informacinių technologijų saugos atitikties vertinimo metodika. *Valstybės žinios*. 2004, Nr. 80-2855.

[285] *Ibid*., 6–7 p.

[286] Interneto tarnybinių stočių apsaugos rekomendacijos. *Valstybės žinios*. 2004, Nr. 85-3095.

[287] *Ibid*., 1 p.

vadovaujantis šiuo metu galiojančiomis teisinėmis nuostatomis, kuriama skirtinga praktika atskirose valstybės institucijose. Skirtingas teisės normų interpretavimas neleidžia sukurti bendros informacinių technologijų ir informacijos saugos politikos bei užtikrinti efektyvios informacinių sistemų valdytojų kontrolės.

Be to, nėra bendros metodologinės ir konsultacinės sistemos informacinių technologijų, sistemų ir informacijos saugos klausimais. Iš ne teisinių problemų taip pat paminėtina, kad šiuo metu situacija valstybės įstaigose tokia, kad tokios pareigybės arba iš viso nėra, arba ji yra tik formali, papildoma, pvz., informacinės sistemos administratoriaus funkcija. Nėra sukurta bendros tokių darbuotojų rengimo sistemos.

Autorių nuomone, šiuo metu šioje visuomeninių santykių srityje trūksta reguliavimo pamatinių teisės normų. Be siūlyto priimti Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymo projektą, kuriame turėtų būti įtvirtinti pagrindiniai tarptautinio koordinavimo dokumentuose atskleidžiami principai, Lietuvos Respublikai reikalinga nauja Elektroninės informacijos saugos valstybės institucijų informacinėse sistemose valstybinė strategija, kurioje atskirų priemonių forma būtų galima numatyti tarptautinio reguliavimo dokumentų nuostatų praktinį įgyvendinimą mūsų valstybėje. Ši strategija Lietuvos Respublikoje padėtų kurti saugią informacinę visuomenę. Strategija taip pat turėtų skatinti bendradarbiavimą informacinių technologijų saugos klausimais nacionaliniu ir tarptautiniu lygiu, prisidėti prie Lietuvos informacinių technologijų ir telekomunikacijų operatorių potencialo ir kompetencijos kėlimo; gerinti ir užtikrinti informacijos saugos rizikos valdymą ir pagrindinių piliečių teisių, laisvių, teisėtų interesų bei nacionalinio žinių potencialo apsaugą; plėtoti visuomenės informacinių technologijų, saugos klausimų supratimą. Vienas iš svarbesnių uždavinių – valstybės institucijų informacinių sistemų ir jose tvarkomos informacijos klasifikavimas priklausomai nuo kylančių ir esamų grėsmių faktoriaus bei sistemos ir joje tvarkomos informacijos svarbos asmenims, įstaigai, visai visuomenei ar valstybei. Todėl būtina spęsti klausimą dėl valstybės informacijos saugos sritis koordinuojančios institucijos paskyrimo, nustatyti konfidencialios informacijos prioritetus, išplėsti kontrolės tarnybos funkcijas bei spręsti klausimą dėl atsakomybės už neteisėtą duomenų tvarkymą ir nusikaltimus informacinėje erdvėje griežtinimo. Taip pat

tikslinga iš esmės apsvarstyti organizacijos informacijos saugos politiką sudarančių dokumentų rengimo tvarką, atsisakant šiuo metu galiojančių Tipinių duomenų saugos nuostatų. Atsižvelgiant į tai, reikėtų parengti ir kaip įstatymo įgyvendinamąjį aktą patvirtinti naujas „Informacijos saugos politiką sudarančių dokumentų rengimo gaires“. Jų pagrindu kiekviena valstybinė institucija turėtų parengti savo informacijos saugos politikos dokumentus.

Taip pat svarbi išvada ta, kad nepaisant minėtų įstatymų ir jų nuostatų, galima teigti, kad Lietuvoje pagrindinis informacijos saugos reguliavimas sutelktas įstatymų įgyvendinamuosiuose teisės aktuose, t. y. šio reguliavimo priemonės skirtos tik valstybės institucijų sektoriui, o privatus sektorius šioje srityje iš viso nereguliuojamas (išskyrus minėtus įstatymus).

Apibendrinančios išvados

• Elektroninėje erdvėje naudojamos papildomos identifikavimo priemonės ir būdai yra teisiškai nereguliuojami ir dėl to mažiau saugūs, tai sudaro daugiau galimybių vykdyti tapatybės vagystę.

• Valstybė turėtų nustatyti minimalius identifikavimo elektroninėje erdvėje reikalavimus. Reikėtų nurodyti, kurie duomenys, tapatybės elementai, identifikuojant asmenį elektroninėje, erdvėje turi būti vienodi visuose sektoriuose.

• Valstybė teisės normose turėtų reglamentuoti, kad nesaugių identifikavimo priemonių naudojimo atveju atsakingas verslininkas solidariai prisiimtų atsakomybę už dėl neteisėtos veiklos kilusias pasekmes (padarytą žalą). Tokiu būdu versle būtų skatinamas saugių (valstybės patvirtintų ar pripažįstamų) identifikavimo priemonių ir būdų naudojimas.

• JAV asmens duomenų apsaugos teisinė sistema labai skiriasi nuo Lietuvos (Europos Sąjungos) ir Rusijos asmens duomenų reguliavimo: JAV požiūris į asmens duomenų apsaugą yra paremtas sektoriniu reguliavimu ir savireguliacija, o Lietuvoje (Europos Sąjungoje) ir Rusijoje – visapusišku teisiniu reguliavimu.

• Rusijos įstatymai, reglamentuojantys duomenų apsaugą, iš esmės yra panašūs į tuos, kurie galioja Europos Sąjungoje (taip pat ir Lietuvoje). Vis dėlto Rusijos įstatymai numato griežtesnius ribojimus asmens duomenų rinkimui, naudojimui, saugojimui, perdavimui ir apdorojimui, tačiau JAV nėra vieno bendro pagrindinio asmens duomenų apsaugą reg-

lamentuojančio įstatymo, o duomenų tvarkymo atžvilgiu taikomi kitokie apsaugos standartai, kurie daugeliu požiūrių yra žemesnio lygio nei Europos Sąjungoje.

• Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas ir Rusijos asmens duomenų įstatymas įtvirtina pagrindinius asmens duomenų apsaugos principus, įtvirtintus 1981 m. Strasbūro konvencijoje ir Europos Sąjungos direktyvoje Nr. 95/46/EB bei užtikrina minėtų principų apsaugą. O JAV yra sukurta saugaus uosto sistema, kuri leidžia JAV organizacijoms išvengti trukdžių verslo susitarimuose su Europos valstybių organizacijomis ar Europos institucijų persekiojimo dėl Europos privatumo įstatymų reikalavimų pažeidimo, kadangi susitarta, jog JAV organizacija, kuri yra saugaus uosto narė, užtikrina „pakankamą" privatumo apsaugą, kaip tai apibrėžia Direktyva.

• Galima daryti prielaidą, kad savanoriškumo ir savireguliacijos principais pagrįsta asmens duomenų teisinės apsaugos sistema JAV daro tiesioginę įtaką sparčiam tapatybės vagystės elektroninėje erdvėje plitimui.

• Kaip geroji praktika informacijos saugos srityje vertintina aiškus funkcijų ir atsakomybės atskyrimas (pvz., JAV atveju). Tam tikra prasme tokio atskyrimo apraiškų yra ir Lietuvoje. Tačiau Lietuvoje pastebima problema institucinės informacijos saugos kontrolės srityje, kai aiškiai neatskirtos kontroliuojančių institucijų funkcijos, o viena iš pagrindinių kontroliuojančių institucijų (Vidaus reikalų ministerija) neturi pavaldumo įgalinimų kitoms institucijoms, be to, nėra pagrindinės už informacijos saugą Lietuvoje atsakingos institucijos.

• Lietuvoje kaip neigiama praktika vertintina tai, kad pagrindinės informacijos saugos taisyklės įtvirtintos ne įstatymo lygmeniu, o įstatymo įgyvendinamuosiuose teisės aktuose. Šios problemos nėra JAV, iš dalies – ir Rusijoje.

• Atsižvelgiant į šios dienos realijas, t. y. į tai, kad elektroninių ryšių tinklai dažnai priklauso privačiam sektoriui, tam tikri įpareigojimai užtikrinti informacijos saugą turėtų būti taikomi ir privačiam sektoriui. Ši problema aktuali ir Lietuvai.

• Tinkama informacijos saugos užtikrinimo praktika (įskaitant teisinį reguliavimą), užkerta kelią pasisavinti asmens duomenis, siekiant įvykdyti kitus nusikaltimus (t. y. tapatybės vagystę).

3.3. Kiti teisės aktai, reglamentuojantys visuomeninius santykius, susijusius su tapatybės vagyste elektroninėje erdvėje (specialūs teisės aktai)

3.3.1. JAV teisės aktai, reglamentuojantys visuomeninius santykius, susijusius su tapatybės vagyste elektroninėje erdvėje

Ankstesnėje dalyje minėta, kad Jungtinėse Amerikos Valstijose (toliau – Jungtinės Valstijos, JAV) nėra vieno pagrindinio teisės akto (pavyzdžiui, kaip Europos Sąjungos valstybėse narėse), išsamiai reglamentuojančio asmens duomenų teisinę apsaugą. Kadangi Jungtinėse Valstijose asmens privatumo ir asmens duomenų apsaugos sritis pagrįsta sektoriniu reguliavimu, šioje dalyje bus trumpai apžvelgiami pagrindiniai įstatymai, skirti užtikrinti minėtai vertybių apsaugai. Šio skyriaus tikslas – nustatyti, kokių visuomenės vertybių, be jau minėtų, apsaugą siekiama užtikrinti privatumo ir asmens duomenų apsaugos sritį reguliuojančiais įstatymais, kokia atsakomybė kyla už tokių vertybių pažeidimą bei tai, ar šiais įstatymais siekiama užkirsti kelią tapatybės vagystei.

JAV buvo priimta nemažai įstatymų, kurių tikslas yra apsaugoti vartotojų informacijos privatumą ir nustatyti tapatybės vagystę elektroninėje erdvėje[288]. Šie įstatymai aptariami toliau.

Sukčiavimo, susijusio su pašto paslaugomis, įstatymas (angl. *Mail Fraud Statute*[289]) (1872): skirtas apsaugoti visuomenei nuo bet kokios apgaulės ar sukčiavimo, įskaitant kreditinį sukčiavimą ir tapatybės vagystę. Sukčiavimas apibrėžiamas kaip bet koks bandymas suklaidinti ar gauti pinigų, įgyti kito turto, apgaulės būdu ar apsimetant kitu asmeniu. Įtvirtinti du būtini tokios nusikalstamos veikos elementai: sukčiavimas ir pasinaudojimas JAV paštu ar kitomis privačių ar komercinių valstijų pašto paslaugas teikiančių subjektų paslaugomis, turint tikslą įvykdyti sukčiavimą. Pagal šį įstatymą baudžiamoji atsakomybė kyla tam, kas pavagia asmeninę informaciją, suklastoja prašymus kreditinėms kortelėms gauti ir paštu išsiunčia bankams ir kitoms kreditines korteles išduodančioms institucijoms. Taip pat pagal šį įstatymą baudžiama ir už kitus su tapatybe

[288] Higgins, G. E. 2010. *Cybercrime: An Introduction to an Emerging Phenomenon*. McGraw-Hill, p. 69.

[289] Mail Fraud Statute, Title 18, United States Code, Section 1341 [interaktyvus, žiūrėta 2011-09-15]. <http://www.law.cornell.edu/uscode/usc_sup_01_18_10_I_20_63.html>.

susijusius nusikaltimus, kuriuose paštas yra būtinas sukčiavimo įvykdymo elementas. Už minėtą nusikaltimą baudžiama bauda arba laisvės atėmimu iki 20 metų arba ir bauda, ir laisvės atėmimu, o jei nuo to nukenčia ir finansų institucija, – bauda iki 1 000 000 dolerių arba laisvės atėmimu iki 30 metų arba ir bauda ir laisvės atėmimu.

Sukčiavimo, susijusio su ryšio priemonėmis, įstatymas (angl. *Wire Fraud Statute*[290]) (1952). Toks sukčiavimas apima valstijų telegrafo, radijo ir telefono ryšių panaudojimą siekiant apgauti, apgaulės būdu ar apsimetant kitu asmeniu įgyti pinigų ar kito turto. Už šį nusikaltimą baudžiama bauda arba laisvės atėmimu iki 20 metų arba ir bauda, ir laisvės atėmimu, o jei nuo to nukenčia ir finansų institucija, – bauda iki 1 000 000 dolerių arba laisvės atėmimu iki 30 metų arba ir bauda ir laisvės atėmimu.

Bankinio sukčiavimo įstatymas (angl. *Bank Fraud Statute*[291]) (1984). Nusikalstama veika įvykdoma tada, kai asmuo tyčia įvykdo arba pasikėsina įvykdyti sukčiavimą prieš finansų instituciją ir apgaulės būdu įgyti pinigų, lėšų, gauti paskolą, aktyvų, vertybinių popierių ar kito turto, kuris yra valdomas ar kontroliuojamas finansų institucijos. Už šį nusikaltimą baudžiama bauda iki 1 mln. dolerių arba laisvės atėmimu iki 30 metų arba ir bauda, ir laisvės atėmimu. Pagal šį įstatymą baudžiama už įvairius finansinius nusikaltimus, tokius, kaip paskolos gavimas apgaulės būdu, pinigų gavimas pagal suklastotus čekius, čekių klastojimas, kreditinį sukčiavimas ir kiti panašūs nusikaltimai.

Kreditinių kortelių sukčiavimo įstatymas (angl. *Credit Card Fraud Act*[292]) (1984): išplėtė kreditinių kortelių ir debetinių instrumentų sąvokas, į jas įtraukiant prieigos įrenginius, sąskaitų numerius, taip pat sugriežtino bausmes už tokio pobūdžio nusikaltimus. Iki 1984 m. kreditinių kortelių sukčiavimu buvo laikoma tokia veika, kai asmuo faktiškai panaudodavo kreditinę kortelę – fiziškai apčiuopiamą plastiko gabalėlį – tam, kad įvykdytų sukčiavimą. Tačiau priėmus minėtą įstatymą, daugiau nebereikėjo naudoti plastikinės kortelės, kad asmuo būtų apkaltintas kreditinių kor-

[290] Wire Fraud Statute, Title 18, United States Code, Section 1343 [interaktyvus, žiūrėta 2011-09-15]. < http://www.law.cornell.edu/uscode/usc_sup_01_18_10_I_20_63.html>.

[291] Bank Fraud Statute, Title 18, United States Code, Section 1344 [interaktyvus, žiūrėta 2011-09-15]. < http://www.law.cornell.edu/uscode/usc_sup_01_18_10_I_20_63.html>.

[292] Access Device Fraud, Title 18, United States Code, Section 1029 [interaktyvus, žiūrėta 2011-09-15]. <http://www.law.cornell.edu/uscode/usc_sec_18_00001029----000-.html>.

telių sukčiavimu. Naujajame įstatyme numatyta, kad pakanka pasinaudoti prieigos įrenginiu, kad būtų galima įvykdyti sukčiavimą, o prieigos įrenginį apibrėžė kaip bet ką, kas naudojama atliekant kreditinės kortelės operaciją, t. y. į šią sąvoką patenka kortelės, sąskaitų numeriai ir asmens identifikavimo numeriai (PIN), taip pat elektroninė įranga, skirta vykdyti kreditinei kortelės operacijai, pavyzdžiui, kortelių skaitytuvai ir modemai, skirti autorizuoti kortelėms. Federaliniu nusikaltimu laikoma suklastotų (padirbtų) prieigos įrenginių gaminimas, naudojimas, turėjimas ar pardavimas. Tačiau jei naudojamas neautorizuotas prieigos įrenginys – tikras įrenginys, kuris buvo pavogtas ar nustojęs veikti – tai bus laikoma federaliniu nusikaltimu, tik jei toks įrenginys buvo naudojamas siekiant gauti prekių ar paslaugų, kurių vertė sudaro daugiau nei 1 000 dolerių per metus. Įstatyme numatyta atsakomybė ir už elektroninės įrangos laikymą, turint tikslą ją panaudoti vykdant kreditinių kortelių sukčiavimą. Įstatymas taip pat įtvirtina, kad pasikėsinimas įvykdyti kreditinių kortelių sukčiavimą prilyginamas faktiniam tokios veikos įvykdymui, nepriklausomai nuo to, ar pasikėsinimas buvo sėkmingas, asmeniui kyla tokia pati bausmė. Už minėto įstatymo pažeidimą numatoma iki 15 metų laisvės atėmimo bausmė, taip pat baudos ir restitucija, kurios gali būti skiriamos teismo nuožiūra. Maksimali bausmė – laisvės atėmimas iki 20 metų ir sukčiaujant įgyto turto konfiskavimas.

Padirbtų prieigos įrenginių, kompiuterinio klastojimo ir piktnaudžiavimo įstatymas (angl. *Counterfeit Access Device and Computer Fraud and Abuse Act*[293]) (1984): tai pirmasis federalinis įstatymas, skirtas kompiuteriniam sukčiavimui ir piktnaudžiavimui. Iki 1984 m. nebuvo įstatymo, numatančio baudžiamąją atsakomybę už kompiuterinius nusikaltimus, o federaliniai prokurorai remdavosi federaliniais įstatymais tokiais, kaip, Sukčiavimo, susijusio su ryšio priemonėmis, įstatymu. Kongresas priėmė Padirbtų prieigos įrenginių, kompiuterinio klastojimo ir piktnaudžiavimo įstatymą, siekdamas užtikrinti aiškesnį draudžiamų veikų reglamentavimą. Iš pradžių įstatymas numatė baudžiamąjį persekiojimą už tris nusikalstamas kompiuterines veikas, kurios įvykdomos naudojant kompiuterį: neteisėta prieiga prie valstybės paslaptį sudarančios informacijos, susiju-

[293] Codified in Fraud and Related Activity in Connection with Computers, Title 18, United States Code, Section 1030. [interaktyvus, žiūrėta 2011-09-15]. <http://www.panix.com/~eck/computer-fraud-act.html>.

sios su nacionaliniu saugumu ir užsienio santykiais; netinkama prieiga prie finansinių institucijų saugomos finansinės informacijos; netinkama prieiga prie vyriausybės kompiuteryje saugomos informacijos. Tobulėjant technologijoms, pastebėta, kad įstatymo veikimo sritis yra gana siaura, todėl buvo daromos įstatymo pataisos ir bėgant laikui įstatyme kriminalizuoti 7 kompiuterinio piktnaudžiavimo būdai (1996 m.) ir numatyta galimybė pareikšti civilinį ieškinį (1990) už kompiuterinį nusikaltimą. Nors Kongresas priėmė ir kitus baudžiamuosius įstatymus, į kurių veikimo sritį patenka tokio pobūdžio nusikaltimai, minėtas įstatymas vis dar yra vienas iš tų, kuriais dažniausiai remiasi federaliniai kaltintojai, palaikydami kaltinimą už kompiuterinį nusikaltimą. Šiuo metu baudžiamoji atsakomybė pagal minėtą įstatymą kyla už šnipinėjimą elektroninėje erdvėje, neteisėtą prieigą prie finansinės informacijos, veiksmus, susijusius su vyriausybės kompiuteryje esančių duomenų peržiūra, vagystę iš apsaugotų kompiuterių, žalos sukėlimą netinkamai perduodant duomenis, prekybą slaptažodžiais, elgesį, susijusį su įsilaužimu į apsaugotą kompiuterį. Už minėto įstatymo nuostatų pažeidimą numatoma bauda ir laisvės atėmimas iki 10 metų. Maksimali bausmė – laisvės atėmimas iki 20 metų.

Sąžiningų kredito ataskaitų įstatymas (angl. *Fair Credit Reporting Act*[294]) (1970): užtikrina informacijos privatumą vartotojų kredito ataskaitose ir apsaugo vartotojus nuo netinkamo informacijos atskleidimo; riboja vartotojų ataskaitas ir vartotojams suteikia prieigos galimybę prie ataskaitų bei numato galimybę ištaisyti pastebėtas klaidas. Nenustatomi apribojimai renkamos informacijos kiekiui ir rūšiai, tačiau institucijos, teikiančios vartotojų ataskaitas, asmeninę informaciją tretiesiems asmenims gali atskleisti tik esant atitinkamoms aplinkybėms. 616 Įstatymo paragrafe numatyta, kad asmeniui, kuris tyčia nesilaiko įstatymo reikalavimų, kyla civilinė atsakomybė: pažeidimo atveju vartotojas gali reikalauti atlyginti patirtą žalą, kurios dydis ne mažesnis nei 100 dolerių ir ne didesnis nei 1 000 dolerių, taip pat advokato išlaidas. 617 įstatymo paragrafe numatyta civilinė atsakomybė, kai teisės normos pažeidžiamos dėl nerūpestingumo. Tokiu atveju vartotojui turi būti atlyginta jo patirta žala ir advokato išlaidos. 618 straipsnyje įtvirtinta, kad vartotojas su ieškiniu gali kreiptis tiek į valstijos, tiek į federalinį teismą, tačiau ne vėliau kaip

[294] Fair Credit Reporting Act [interaktyvus, žiūrėta 2011-09-19]. <http://www.ftc.gov/os/statutes/031224fcra.pdf>.

per 2 metus nuo pažeidimo nustatymo ir ne vėliau kaip per 5 metus nuo pažeidimo padarymo.

Sąžiningų kredito sąskaitų įstatymas (angl. *The Fair Credit Billing Act*[295]) (1974): numato vartotojų apsaugą nuo nesąžiningo sąskaitų tvarkymo, įtvirtina procedūras kredito sąskaitų klaidoms spręsti. Į veikimo sritį patenka sąskaitų klaidos ir tos klaidos, kurios kyla dėl apgaulingų mokesčių, atliktų pasinaudojant vartotojo kredito sąskaitomis. Vartotojas, nukentėjęs dėl to, kad kredito paslaugas teikiantys subjektai nesilaikė minėto įstatymo reikalavimų, gali pateikti ieškinį valstijos ar federaliniam teismui ir reikalauti, kad jam būtų atlyginta padaryta žala, t. y. įstatymo numatyta žala, kurios dydis yra du kartus didesnis nei per kredito paslaugas teikiančio subjekto klaidą patirtos išlaidos, taip pat advokato išlaidos (ieškinio tenkinimo atveju). Jei įtariamas neteisėtas elgesys yra plataus masto, vartotojas gali pareikšti grupinį ieškinį ir reikalauti atlyginti žalą, kurios dydis iki 500 000 dolerių arba iki 1 procento kreditoriaus bendro turto vertės.

Privatumo įstatymas (angl. *Privacy Act*[296]) (1974): tai Teisingos informacijos praktikos kodeksas, kuris nustato asmeninės informacijos, kuri leidžia identifikuoti asmenį, tvarkomos federalinių institucijų informacinėse sistemose, rinkimą, laikymą, naudojimą ir platinimą. Įstatymas numato informacijos rinkimo apribojimus valdžios institucijoms ir draudžia susipažinti su slaptais valdžios dokumentais, išskyrus tam tikras išimtis. Nė viena institucija bet kokio įrašo, esančio sistemoje, jokiomis priemonėmis negali atskleisti kitam asmeniui ar institucijai, išskyrus, kai yra rašytinis prašymas paties asmens, ar prašymas, pateiktas turint asmens sutikimą, su kuriuo tas įrašas yra susijęs, nebent tas įrašas būtų atskleidžiamas teisėtais valdžios tikslais. Įstatymas įtvirtina įpareigojimą, kad kiekviena Jungtinių Valstijų valdžios institucija imtųsi administracinių ir fizinių saugumo priemonių, kad apsaugotų asmeninės informacijos įrašus nuo neteisėtos prieigos.

1988 m. Kompiuterių suderinamumo ir privatumo apsaugos įstatymas (angl. *Computer Matching and Privacy Protection Act*) nustato Privatumo įstatymo pataisas: įstatymas buvo papildytas nuostatomis, numatančiomis apsaugą įrašams, kurie naudojami automatinėse suderinamumo prog-

[295] The Fair Credit Billing Act [interaktyvus, žiūrėta 2011-09-19]. <http://www.ftc.gov/os/statutes/fcb/fcb.pdf>.

[296] Privacy Act of 1974. [interaktyvus, žiūrėta 2011-09-19]. <http://www.justice.gov/opcl/privstat.htm>.

ramose. Apsaugą numatančios taisyklės buvo skirtos užtikrinti vienodai procedūrai vykdant suderinamumo programas; apsaugoti duomenų subjektų teises; atliekant minėtų programų priežiūrą. Už reikalavimų nesilaikymą numatoma baudžiamoji atsakomybė: bet kuris pareigūnas ar darbdavys, kuris pasinaudodamas padėtimi turi galimybę prieiti prie institucijos tvarkomų įrašų, kuriuose saugoma asmenį identifikuojanti informacija, kurios atskleidimas yra draudžiamas, ir kuris žino, kad tokios informacijos atskleidimas yra draudžiamas, tačiau tyčia ją bet kokiu būdu atskleidžia trečiajam asmeniui ar institucijai, neturintiems teisės su ja susipažinti, laikomas padaręs baudžiamąjį nusižengimą ir baudžiamas bauda iki 5 000 dolerių. Jei institucijos pareigūnas ar darbdavys atlieka įrašų sistemos priežiūrą tyčia nesilaikydamas numatytų reikalavimų arba pateikia užklausą ar įgyja bet kokį įrašą, susijusį su asmeniu, apsimetęs kitu asmeniu, laikomas padaręs baudžiamąjį nusižengimą ir baudžiamas bauda iki 5 000 dolerių.

Šeimos švietimo teisių ir privatumo įstatymas (angl. *Family Educational Rights and Privacy Act*[297]) (1974): saugo studentų mokymo įrašų privatumą. Taikomas visoms mokykloms, kurios gauna lėšas pagal Jungtinių Valstijų Mokslo departamento paraiškų programą. Mokslo įstaigos be sutikimo gali atskleisti tokią informaciją, kaip studento vardas, adresas, telefono numeris, gimimo data ir vieta, garbės raštai ir apdovanojimai, lankomumas. Tačiau mokyklos turi informuoti tėvus ir moksleivius, sulaukusius 18 metų, apie tvarkomą informaciją ir leisti tėvams ir moksleiviams, sulaukusiems 18 metų, nustatyti protingą laikotarpį, kurio metu mokykla apie juos tokios informacijos neskelbtų. Įstatymas numato skundų nagrinėjimo procedūrą (skundus nagrinėja Jungtinių Valstijų Mokslo departamentas). Griežčiausia sankcija – federalinio finansavimo nutraukimas. Studentai gali reikalauti patraukti atsakomybėn tiek universitetą, tiek atskirus asmenis. Taip pat, įvertinus individualias aplinkybes, fakulteto personalas, pažeidęs įstatymo formuojamą politiką, gali būti patrauktas drausminėn atsakomybėn.

Vairuotojų privatumo apsaugos įstatymas (angl. *Drivers Privacy Protection Act*[298]) (1994): draudžia valstijų transporto priemonių departa-

[297] Family Educational Rights and Privacy Act of 1974. [interaktyvus, žiūrėta 2011-09-19]. <www.ed.gov/policy/gen/guid/fpco/ferpa/index.html>.

[298] Drivers Privacy Protection Act [interaktyvus, žiūrėta 2011-09-19]. <http://www.accessreports.com/statutes/DPPA1.htm>.

mentams, jų darbuotojams ar rangovams atskleisti asmeninę informaciją tretiesiems asmenims, taip pat atskleisti tam tikro pobūdžio informaciją be asmens sutikimo. Vėliau buvo priimta pataisa, draudžianti valstijai parduoti ar perduoti transporto priemonių departamento įrašus prekybininkams be specialaus leidimo. Asmeninė informacija apibrėžiama kaip informacija, kuri leidžia nustatyti asmens tapatybę, įskaitant asmens nuotrauką, socialinio draudimo numerį, vairuotojo identifikavimo numerį, vardą, adresą (išskyrus 5 skaitmenų pašto kodą), telefono numerį, medicininę ar nedarbingumo informaciją, išskyrus informaciją apie autoįvykius, kelių eismo taisyklių pažeidimus ir vairuotojo statusą. Asmeniui, kuris pažeidžia įstatymo nuostatas, reglamentuojančias asmeninės informacijos gavimą, atskleidimą ar naudojimą, kyla atsakomybė. Neteisėtomis laikomos ir tokios veikos, kaip asmeninės informacijos įgijimas neteisėtais tikslais, t. y. neteisėtais veiksmais laikoma tyčinis asmeninės informacijos, kuri yra motorinės transporto priemonės įrašo dalis, įgijimas ar atskleidimas pažeidžiant įstatymo nuostatas; ir apsimetimas kitu asmeniu, siekiant įgyti bet kokios asmeninės informacijos, kuri yra motorinės transporto priemonės įrašo dalis. Fizinis asmuo gali būti patrauktas baudžiamojon atsakomybėn, baudžiamas bauda, o jei pažeidimą padaro valstijos transporto priemonių departamentas, – jam kyla civilinė atsakomybė, kuri negali viršyti 5 000 dolerių per dieną už esminio pažeidimo dieną.

Sveikatos draudimo ir atsakomybės aktas (angl. *Health Insurance Portability and Accountability Act*[299]) (1996): tikslas – siekti, kad būtų užtikrintas toks pats elektroninių dokumentų saugumas kaip ir fizinėje erdvėje, gerinant visą informacijos saugumą[300]. Aktas priimtas atsižvelgiant į vis spartesnį interneto vartojimą ir medicininių įrašų perkėlimą į elektroninę erdvę. Jis taikomas sveikatos priežiūros įstaigoms ir informacinėms agentūroms, kurios teikia informaciją elektroninėje erdvėje. Apsaugota sveikatos informacija apibrėžiama kaip asmeniškai atpažįstama sveikatos informacija, sukurta arba gauta bet kokios formos. Saugoma, kad tokia informacija nebūtų naudojama, atskleista ar ja nepiktnaudžiautų draudimo kompanijos, darbdaviai ar bet koks kitas asmuo. Daugeliu atvejų,

[299] Health Insurance Portability and Accountability Act [interaktyvus, žiūrėta 2011-09-19]. <http://www.cms.gov/HIPAAGenInfo/Downloads/HIPAALaw.pdf>.

[300] Higgins, G. E. 2010. *Cybercrime: An Introduction to an Emerging Phenomenon*. McGraw-Hill, p. 69.

norint atskleisti informaciją, reikalingas paciento sutikimas, atskleidžiant tik minimalų informacijos kiekį – tik tokį, koks reikalingas. Nesilaikant įstatymo numatytų reikalavimų, numatoma bauda iki 100 dolerių už kiekvieną pažeidimą, tačiau bendras baudos dydis už tą patį pažeidimą negali būti didesnis kaip 25 000 dolerių per kalendorinius metus. Tačiau asmuo, kuris tyčia naudojasi ar priverčia pasinaudoti unikaliu sveikatos identifikatoriumi arba įgyja asmenį identifikuojančią sveikatos informaciją arba tokią informaciją atskleidžia kitam asmeniui, gali būti patrauktas baudžiamojon atsakomybėn. Asmuo baudžiamas bauda iki 50 000 dolerių arba laisvės atėmimu iki vienerių metų, arba ir bauda ir laisvės atėmimu; jei pažeidimas įvykdomas apgaulės būdu – bauda iki 100 000 dolerių arba laisvės atėmimu iki penkerių metų, arba ir bauda, ir laisvės atėmimu; o jei pažeidimas padaromas turint tikslą parduoti, perduoti ar asmenį identifikuojančią sveikatos informaciją panaudoti komerciniais tikslais, siekiant asmeninės naudos ar tyčinės žalos, – bauda iki 250 000 dolerių arba laisvės atėmimu iki 10 metų, arba ir bauda ir laisvės atėmimu.

Tapatybės vagystės ir apsimetinėjimo atgrasymo aktas (angl. *Identity Theft and Assumption Deterrence Act*[301]) (1998): 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 sunkus nusikaltimas pagal galiojančius Valstijos ar vietinius teisės aktus. Šis aktas išplėtė identifikavimo priemonių sampratą, į ją įtraukė socialinio draudimo numerį, kreditines korteles, mobiliuosius telefonus, elektroninius serijos numerius ir kitą informaciją, kuri gali būti naudojama tiek viena, tiek su kita informacija. Įstatymas numato, kad asmuo, kurio tapatybė buvo pavogta, yra pripažįstamas auka. Iki tol tik kredito paslaugas teikiantys asmenys, kurie patirdavo finansinių nuostolių, buvo laikomi tokio nusikaltimo aukomis. Įstatymas numatė įgaliojimus Slaptumo tarnyboms, Federaliniam tyrimų biurui ir kitoms įstatymą įgyvendinančioms institucijoms kovoti su tapatybės vagystės nusikaltimu. Numato galimybę nukentėjusiajam nuo tapatybės vagystės

[301] Identity Theft and Assumption Deterrence Act [interaktyvus, žiūrėta 2011-09-19]. <http://www.ftc.gov/os/statutes/itada/itadact.htm>.

reikalauti atlyginti nuostolius, jei priimamas apkaltinamasis nuosprendis. Taip pat įstatymas įtvirtina, kad Federalinė prekybos komisija yra centrinė institucija, kuriai paskirta nagrinėti ginčus, pagalbos tapatybės vagystės aukoms klausimus. Už nusikaltimą numatoma bausmė – laisvės atėmimas iki 15 metų, o maksimali bauda gali siekti net iki 250 000 dolerių.

Bausmės už tapatybės vagystę padidinimo aktas (angl. *Identity Theft Enhancement Penalty Act*[302]) (2004): padidino laisvės atėmimo bausmę už tapatybės vagystę, kai įvykdomas kitas nusikaltimas, t. y. kai tapatybės vagyste pasinaudojama kaip priemone kitiems nusikaltimams, tokiems kaip terorizmas, nelegali imigracija, šaunamųjų ginklų kontrabanda, įvykdyti. Įstatymas numato, kad už tapatybės vagystę, įvykdytą sunkinančiomis aplinkybėmis, įprasta laisvės atėmimo bausmė prailginama 2 metais, o jei tapatybės vagystė buvo įvykdyta tam, kad vėliau ja pasinaudojant būtų galima įvykdyti terorizmo veiksmus – laisvės atėmimo bausmė už tapatybės vagystę prailginama 5 metais.

Finansinių paslaugų modernizavimo aktas (angl. *Financial Modernization Act, Gramm-Leach-Bliley Act*[303]) (1999): leido komerciniams bankams, investiciniams bankams, apsaugos firmoms ir draudimo kompanijoms vienytis. Įtvirtina nuostatas, skirtas vartotojų finansinei informacijai apsaugoti, kurią turi finansų institucijos, apibrėžiamos kaip kompanijos, kurios siūlo asmenims finansinius produktus ar paslaugas (tokias, kaip paskolos, finansinės ar investavimo konsultacijos, draudimas). Tikslas – užkirsti kelią minėtoms kompanijoms parduoti asmeninę finansinę informaciją be kliento žinios ar sutikimo. Sudaro 3 pagrindinės dalys: finansinio privatumo taisyklės (reglamentuoja kliento asmeninės finansinės informacijos rinkimą ir atskleidimą; reikalaujama, kad finansinės institucijos informuotų savo klientus apie dalijimosi informacija tvarką ir sudarytų savo klientams galimybę tam tikromis aplinkybėmis atsisakyti tokio informacijos dalijimosi su nepriimtinomis trečiosiomis šalimis), apsaugos priemonių taisyklės (reikalauja, kad visos finansų institucijos kurtų, tobulintų ir palaikytų fizines, technines ir procedūrines apsaugos priemones, skirtas

[302] Identity Theft Enhancement Penalty Act [interaktyvus, žiūrėta 2011-09-19]. <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ275.108.pdf>.

[303] Financial Modernization Act, Gramm-Leach-Bliley Act [interaktyvus, žiūrėta 2011-09-19]. <http://www.ftc.gov/privacy/glbact/glbsub1.htm>.

klientų informacijai apsaugoti, reikalaujama, kad kompanijos turėtų apsaugos strategijas, skirtas klientų informacijos konfidencialumui, vientisumui užtikrinti bei užkirsti kelią neteisėtai prieigai prie tokio pobūdžio informacijos) ir dingsčių (pretekstų) normos (normos, skirtos vartotojams apsaugoti nuo fizinių ir juridinių asmenų, kurie siekia gauti asmeninę finansinę informaciją prisidengdami melaginga dingstimi). Kiekviena finansų institucija turi pareigą gerbti savo klientų privatumą ir užtikrinti jų asmeninės informacijos apsaugą ir konfidencialumą. B poskyris reglamentuoja prieigą prie finansinės informacijos apgaulės būdu. Teisės normų pažeidimu laikomas įgijimas ar pasikėsinimas įgyti arba atskleidimas ar pasikėsinimas atskleisti trečiajam asmeniui kliento informaciją apie finansinę instituciją, kai ta informacija susijusi su kitu asmeniu – pareigūnu, darbuotoju, agentu ar finansine institucija, arba finansinės institucijos klientui pateikus netikrą, suklastotą ar apgaulingą įgaliojimą arba kitą dokumentą, žinant, kad tas dokumentas yra suklastotas, netikras, pamestas ar pavogtas, įgytas apgaulės būdu arba jame nurodytos netikros, suklastotos ar apgaulingos teisės. Taip pat draudžiama prašyti kitą asmenį, kad šis, prisidengdamas melaginga dingstimi, iš finansų institucijos gautų informaciją apie klientą. Jei įstatymo normų nesilaikoma ir padaromos minėtos veikos, asmeniui kyla baudžiamoji atsakomybė pagal 523 straipsnį, kuris numato, kad toks asmuo baudžiamas bauda arba laisvės atėmimu iki 5 metų, arba ir bauda, ir laisvės atėmimu. Už nusikalstamas veikas, padarytas sunkinančiomis aplinkybėmis, kai pažeidžiamas kitas Jungtinių Valstijų įstatymas, arba kurios yra būdas kitoms neteisėtoms veikoms atlikti, numatoma dvigubai didesnė bauda, nei numatyta Jungtinių Valstijų kodekso 18 skyriaus 3571 straipsnio (b) (3) ar (c) (3) dalyse, t. y. fiziniam asmeniui skiriama bauda iki 500 000 dolerių, o juridiniam – bauda iki 1 000 000 dolerių arba laisvės atėmimas iki 10 metų arba ir bauda, ir laisvės atėmimas.

USA PATRIOT įstatymas – įstatymas dėl Amerikos vienijimo ir stiprinimo tinkamų priemonių, reikalingų sulaikant ir užkertant kelią terorizmui (angl. *USA PATRIOT (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act*[304]) (2001). Tai vienas iš pinigų plovimo ir terorizmo finansavimo

[304] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act [interaktyvus, žiūrėta 2011-09-19]. <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107.pdf>.

prevenciją reglamentuojančių įstatymų, priimtas po rugsėjo 11 išpuolių (2001). Pagrindinis įstatymo tikslas –nustatyti bausmes už teroro išpuolius Jungtinėse Valstijose ir visame pasaulyje, sugriežtinti priemones, kuriomis siekiama užkirsti kelią terorizmui, aptikti asmenis ir patraukti baudžiamojon atsakomybėn už tarptautinį pinigų plovimą ir terorizmo finansavimą; skirtas užsienio jurisdikcijai, užsienio finansų institucijoms, tarptautinėms transakcijoms ir sąskaitoms, kurios gali būti naudojamos nusikalstamais tikslais, persvarstyti; numatyti finansines paslaugas teikiančioms institucijoms reikalavimą pranešti apie galimus pinigų plovimo atvejus; taip pat skirtas priemonėms, galinčioms apsaugoti Jungtinių Valstijų finansų sistemą nuo korumpuotų užsienio pareigūnų, kurie siekia asmeninės naudos, stiprinti ir pasisavintų lėšų grąžinimui asmenims, kuriems jos iš tikrųjų priklauso, supaprastinti. Įstatymas išplėtė vykdomosios valdžios galias sekimo ir galimybės dalytis informacija su valdžios institucijomis srityje: jos gali klausytis įtariamųjų telefono pokalbių, išduoti kratos orderius, kai krata atliekama be įtariamojo žinios, gauti prieigą prie svarbių asmens duomenų, – dėl to kritikų vertinamas kaip antikonstitucinis ir pažeidžiantis tokias žmogaus teises, kaip teisė į privatumą ir teisė į asmeninio gyvenimo neliečiamumą. Taip pat įstatymas įtvirtino papildomas priemones, tokias kaip sustiprinta įtariamųjų terorizmu priežiūra, sienos apsauga, pinigų plovimo prevencijos programos, dalijimasis informacija, sugriežtintos baudžiamųjų įstatymų sankcijos už terorizmą, valstybės institucijų pareigūnų ir visuomenės bendradarbiavimas. Skirtingai nuo kitų įstatymų, skirtų asmens privačios informacijos apsaugai, šis įstatymas įpareigoja finansų institucijas saugoti duomenis, kurie gali būti vertingi nustatant ir tiriant pinigų plovimo atvejus, kad finansų institucijos tokiu būdu prisidėtų kovojant su terorizmu. Užsienio bankų vardu administruojamoms, atidaromoms ar laikomoms korespondentinėms sąskaitoms[305] nustatomas sertifikavimo reikalavimas. Įstatymo 311 punkte nurodoma, kad JAV administracija, nustačiusi, kad egzistuoja pagrįsta priežastis įtarti, jog užsienio institucija, transakcija ar sąskaita gali būti siejama su pinigų plovimu, prieš tokią instituciją gali taikyti specialias priemones arba sankcijas. Paminėtinas VIII įstatymo skyrius, nustatantis baudžiamąją atsakomybę už kompiuterinį terorizmą

[305] Korespondentinė sąskaita – sąskaita privalomosioms atsargoms laikyti ir atsiskaitymo operacijų rezultatams sistemoje fiksuoti.

(angl. *cyberterrorism*). Bausmės numatomos asmenims, sugadinantiems ar įgyjantiems neteisėtą prieigą prie apsaugoto kompiuterio ir įvykdantiems kitus nusikaltimus, tokius, dėl kurių nukentėjęs asmuo patiria didesnę nei 5 000 dolerių žalą, nusikaltimai, kuriais klaidinami sveikatos patikrinimo rezultatai, diagnozė ar gydymas, darant neigiamą poveikį, kurie apima tokius veiksmus, kuriais asmeniui sukeliamas kūno sužalojimas, sudaroma grėsmė visuomenės sveikatai ir saugumui arba padaroma žala valstybinės valdžios kompiuteriui, kuris naudojamas kaip įrankis administruoti teisingumą, nacionalinę gynybą ar nacionalinį saugumą. Bausmė už pasikėsinimą sugadinti apsaugotus kompiuterius, užkrečiant juos virusais ar kitomis kenkėjiškomis programomis, – laisvės atėmimas iki 10 metų; už neteisėtą prieigą ir dėl to padarytą žalą apsaugotam kompiuteriui – laisvės atėmimas daugiau kaip 5 metams, o jei nusikaltimas padaromas antrą kartą – iki 20 metų. Įstatymas detalizavo saugumo elektroninėje erdvėje paramos ir plėtros galimybes: įtvirtino reikalavimą įkurti regionines kompiuterines teismo laboratorijas, kuriose būtų vykdomas teisminis elektroninių įrodymų, susijusių su nusikalstamais veiksmais ir terorizmu elektroninėje erdvėje, tyrimas; būtų sudarytos sąlygos ugdyti ir mokyti federacijos, valstijų ir vietinių įstatymo vykdymo institucijų darbuotojus ir ikiteisminio tyrimo pareigūnus tirti elektroninius nusikaltimus bei palengvinti ir skatinti federalinius įstatymus įgyvendinančių institucijų dalijimąsi patirtimi ir informacija su valstijų ir vietinių institucijų darbuotojais ir ikiteisminį tyrimą atliekančiomis institucijomis apie elektroninių nusikaltimų tyrimą, analizę ir baudžiamąjį persekiojimą.

Neužsakytos pornografijos ir rinkodaros atakų kontrolės įstatymas (angl. *Controlling the Assault of Non-Solicited Pornography and Marketing Act, CAN-SPAM Act*[306]) (2003): nustato komercinio pobūdžio elektroninių laiškų siuntimo reikalavimus, įtvirtina bausmes už nepageidaujamų elektroninio pašto žinučių siuntimą asmenims ir kompanijoms, kurių produktai reklamuojami tokio pobūdžio žinutėmis, jei taip pažeidžiami įstatymai, suteikia vartotojui teisę atsisakyti siunčiamų pranešimų. Įstatyme draudžiama netikra ar klaidinanti antraščių informacija ir temos, reikalaujama, kad elektroninio pašto adresas būtų laikomas sudedamąja skelbimo dalimi, nurodant siuntėjo fizinį pašto adresą ir įtvirtinant *opt-out* principą.

[306] Controlling the Assault of Non-Solicited Pornography and Marketing Act [interaktyvus, žiūrėta 2011-09-19]. <http://uscode.house.gov/download/pls/15C103.txt>.

Įstatymas buvo pirmasis Jungtinių Valstijų bandymas nacionaliniu lygiu sureguliuoti komercinių pranešimų siuntimą elektroniniu paštu, tačiau jis vertinamas gana skeptiškai: daugelis laikosi nuomonės, kad tai nevykęs bandymas sureguliuoti nepageidaujamas elektroninio pašto žinutes ir net vadina minėtą įstatymą leidžiančiu siuntinėti nepageidaujamas elektroninio pašto žinutes (angl. *You-Can-Spam*), kadangi jame nereikalaujama gauti asmens, kuriam bus siunčiama tiesioginės rinkodaros žinutė, sutikimo, prieš siunčiant tokią žinutę. Be to, įstatymas draudžia atskiroms valstijoms priimti griežtesnius įstatymus, reglamentuojančius nepageidaujamų elektroninių pašto žinučių siuntimą, o asmeniui, kuris gavo tokio pobūdžio žinutę, nenumatoma galimybės pareikšti ieškinį žinutės siuntėjui; numato baudžiamąją atsakomybę už sukčiavimą naudojant elektroninį paštą. Už minėtą nusikalstamą veiką baudžiama bauda ar laisvės atėmimu iki 5 metų arba ir bauda, ir laisvės atėmimu. Įstatymas draudžia apgaulingos ar klaidinančios informacijos siuntimą; klaidinančias pranešimų antraštes; laiko pažeidimu, jei siunčiamame pranešime nėra nurodyto siuntėjo kontaktinio elektroninio pašto adreso, kuriuo būtų galima išsiųsti atsakymą į gautą pranešimą; draudžia pakartotinai siųsti elektroninio pašto žinutes po to, kai buvo gautas asmens, gavusio tokio pobūdžio žinutę, prieštaravimas – už šių reikalavimų nesilaikymą gresia civilinė atsakomybė.

Vaikų privatumo elektroninėje erdvėje apsaugos įstatymas (angl. *Children's Online Privacy Protection Act*[307]) (1998): reglamentuoja asmeninės informacijos iš vaikų iki 13 metų rinkimą elektroninėje erdvėje ir reikalauja, kad būtų tėvų sutikimas prieš renkant ar dalijantis tokio pobūdžio informacija; numato, kad internetinio tinklalapio operatorius, apibrėždamas saugumo politiką, numatytų, kada ir kaip turi būti gautas tėvų ar globėjų sutikimas, ir įtvirtina operatoriaus pareigą apsaugoti vaikų privatumą bei saugumą elektroninėje erdvėje, įskaitant reklaminių pasiūlymų asmenims, jaunesniems nei 13 metų, sugriežtinimą. Asmeninė informacija apibrėžiama kaip individualiai atpažįstama informacija apie asmenį, surinkta elektroninėje erdvėje, įskaitant vardą, pavardę, namų ar kitą fizinį adresą (gatvės pavadinimas, miestas, rajonas), elektroninio pašto adresą, telefono numerį, socialinio draudimo numerį, bet kurį kitą identifikatorių, kurį Komisija pripažįsta susijusiu su konkrečiu asmeniu fizinėje ar elektroninėje erdvėje,

[307] Children's Online Privacy Protection Act [interaktyvus, žiūrėta 2011-09-19]. <http://www.ftc.gov/ogc/coppa1.htm>.

taip pat informacija apie vaiką ar jo tėvus, surinkta elektroninėje erdvėje vaiko naršymo internete metu ir susieta su minėtais identifikatoriais. Federaliniu lygiu įstatymo pažeidimai laikomi nesąžininga ar apgaulinga verslo praktika pagal Federalinės prekybos komisijos įstatymo 5 paragrafą ir Komisija gali patraukti civilinėn atsakomybėn už tokius pažeidimus. Tam, kad užtikrintų įstatymo reikalavimų laikymąsi, Komisija turi atlikti interneto kontrolę ir skatinti vaikų tėvus pareikšti nusiskundimus interneto tinklalapyje. Pažeidėjams gali būti skirta bauda iki 11 000 dolerių. Valstijos lygiu gali būti pareiškiamas ieškinys federaliniame apygardos teisme dėl įstatymo reikalavimų pažeidimo, reikalaujant atlyginti žalą.

Teisingų ir tikslių kredito transakcijų aktas (angl. *Fair and Accurate Credit Transactions Act*[308]) (2003): buvo patvirtintos tam tikros priemonės, skirtos vartotojų apsaugai, taip pat įtvirtinta daug naujų priemonių, skirtų kovai su tapatybės vagyste. Reikalaujama sukurti sukčiavimo pranešimo sistemą vartotojams, kurie galėjo tapti tapatybės vagystės aukomis, sutrumpinti kredito kortelės sąskaitos numerį, pateikiant elektroninius išrašus, blokuojant sąskaitas iš karto po to, kai vartojas užpildo pareiškimą policijoje, „raudonų vėliavėlių" indikatorių sukūrimą finansų institucijoms ir kreditoriams, pastebėjus tapatybės vagystę, ir kt. Įstatymas įtvirtina tokią tapatybės vagystes sąvoką: tapatybės vagystė – tai sukčiavimas, įvykdytas pasinaudojant kitą asmenį identifikuojančia informacija; taip pat nurodoma, kad tapatybės vagystė turėtų būti suprantama taip, kaip ją apibrėžia Komisija; priimtas siekiant mažinti tapatybės vagystės ir vartotojų apgaulių riziką; įtvirtina reikalavimą, kad verslo subjektai, nepriklausomai nuo jų dydžio ir pramonės šakos, tinkamai saugotų ir disponuotų asmenine informacija, kurią jie renka apie savo vartotojus ir darbuotojus.

Tikros tapatybės įstatymas (angl. *Real ID Act*[309]) (2005): įtvirtina griežtus, vienodus standartus dėl privalomo tapatybės nustatymo patikrinimo, kurių turi laikytis asmenys, siekiantys gauti naują arba atnaujinti vairuotojo pažymėjimą ar tapatybės kortelę (gimimo liudijimų patikra, nacionalinės imigracijos duomenų bazės siekiant patikrinti, ar pareiškėjai yra Amerikos

[308] Fair and Accurate Credit Transactions Act [interaktyvus, žiūrėta 2011-09-19]. <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ159.108>.

[309] Real ID Act [interaktyvus, žiūrėta 2011-09-19]. <http://www.ncsl.org/default.aspx?tabid=13582>.

piliečiai, ar teisėti nuolatiniai gyventojai). Taip siekiama apsisaugoti nuo teroristų ir nelegalių imigrantų, norinčių gauti vairuotojo pažymėjimą. Jungtinėse Valstijose vairuotojų pažymėjimus išduoda valstijos. Kadangi Jungtinėse Valstijose nėra nacionalinės identifikavimo kortelės, vairuotojo pažymėjimas paprastai naudojamas kaip tapatybės nustatymo formos standartas. Asmenims, kurie neturi vairuotojo pažymėjimo, valstijos išduoda identifikavimo korteles, tačiau jos nėra privalomos. Iki įstatymo priėmimo kiekviena valstija turi nustatyti atitinkamas taisykles ir kriterijus, susijusius su vairuotojo pažymėjimo ar identifikavimo kortelės išdavimu, t. y. kortelės dizainą, joje įrašomus duomenis, dokumentus, kuriuos reikia pateikti, kad kortelė būtų išduota, informaciją, saugomą valstijos duomenų bazėje apie vairuotojus ir asmenis, kuriems buvo išduota identifikavimo kortelė. Įstatymas reglamentuoja tapatybę patvirtinantį dokumentą, pripažįstamą federaliniu lygiu, kuris privalo būti pateikiamas komercinėse oro linijose, prieš patenkant į valstybės valdžios institucijas, atidarant sąskaitą banke ir pan. Kritikų teigimu, įstatymas yra didžiulė administravimo našta valstijų valdžios institucijoms, kadangi sudėtingoms nuostatoms įgyvendinti numatyta skirti minimalų federacijos finansavimą. Dar daugiau – įstatymo normos nėra veiksmingos kovojant su terorizmu, be to, didinama privatumo pažeidimo ir tapatybės vagystės rizika: vienos duomenų bazės sukūrimas ir reikalavimas, kad kiekvienas transporto priemonių departamentas saugotų gimimo liudijimų ir kitų jam pateiktų dokumentų kopijas, yra tarsi „viena didžiulė parduotuvė“ tapatybės vagystes vykdantiems asmenims.

3.3.2. JAV ir Lietuvos teisės aktų, nukreiptų prieš tapatybės vagystę elektroninėje erdvėje, lyginamoji analizė

Viena iš valstybių lyderių tapatybės vagystės teisinių santykių reglamentavimo srityje yra JAV (joje taip pat yra didelis tokių pavojingų veikų skaičius). Šioje dalyje teisinė aplinka analizuojama lyginant dviejų valstybių – JAV ir Lietuvos – teisės aktus, susijusius su tapatybės vagyste elektroninėje erdvėje. Lyginamos šios teisinio reguliavimo sritys, nuo kurių, autorių nuomone, priklauso sėkminga kova su tapatybės vagyste elektroninėje erdvėje: asmens duomenų apsauga, elektroninių duomenų saugumas, tapatybės nustatymas, baudžiamoji atsakomybė ir specialūs teisės aktai dėl tapatybės vagystės elektroninėje erdvėje.

Asmens duomenų apsaugos teisinis reguliavimas

Pažymėtina, kad asmens duomenų apsaugos teisiniam reguliavimui Lietuvoje daro įtaką tarptautinio ir regioninio teisinio reguliavimo teisės aktai. Tarptautiniu mastu galioja 1981 m. Strasbūro konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu[310] (toliau – Strasbūro konvencija, Konvencija), prie kurios šalys jungiasi savarankiškai ir savanoriškai. Europos Sąjungos lygiu asmens duomenų teisinės apsaugos reguliavimas remiasi 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva Nr. 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo[311] (toliau – Direktyva). Tai yra du pagrindiniai privalomojo pobūdžio teisės aktai, reglamentuojantys asmens duomenų apsaugą tarptautiniu ir Europos Sąjungos (regioniniu) lygiu, todėl per šių dviejų teisės aktų prizmę bus lyginamas asmens duomenų teisinis reguliavimas Lietuvoje ir JAV.

Lietuvoje, kaip ir kiekvienoje Europos Sąjungos valstybėje narėje, Direktyvą įgyvendina Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas[312], kurio tikslas – ginti žmogaus privataus gyvenimo neliečiamumo teisę tvarkant asmens duomenis. Be to, Lietuva 2000 m. vasario 11 d. pasirašė, o 2001 m. birželio 1 d. ratifikavo Strasbūro konvenciją, kuri įsigaliojo nuo 2001 m. spalio 1 d. Tuo tarpu JAV nėra prisijungusi prie 1981 m. Strasbūro konvencijos[313] ir šioje valstybėje asmens duomenų apsaugos reguliavimo srityje nedaro įtakos jokios regioninės ar tarptautinės iniciatyvos.

Lietuva priklauso europietiškajam asmens duomenų apsaugos reguliavimo modeliui, kurio esmė yra visapusiškas teisinis reguliavimas: asmens duomenų apsaugos sritį reglamentuoja vienas bendras Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas, įtvirtinantis

[310] Konvencija „Dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu“ ETS Nr. 108. *Valstybės žinios*. 2001, Nr. 32-1059.

[311] Europos Parlamento ir Tarybos 1995 m. spalio 24 d. direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo [interaktyvus]. [1995] *OL L281/31*. [žiūrėta 2011-09-19]. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1995L0046:20031120:LT:PDF>.

[312] Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas. *Valstybės žinios.* 1996, Nr. 63-1479, 2003, Nr. 15-597, 2008, Nr. 22-804.

[313] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (entered into force on 1 October 1985) [interaktyvus]. CETS 108 [žiūrėta 2011-09-19]. <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=8&DF=26/04/2011&CL=ENG>.

pagrindinius teisėto asmens duomenų tvarkymo reikalavimus, duomenų subjekto teises; reglamentuojantis duomenų saugumo ir duomenų teikimo klausimus; nustatantis instituciją, atsakingą už asmens duomenų apsaugą, užtikrinantis asmens duomenų valdytojų registracijos minėtos institucijos duomenų bazėje privalomumą; nustatantis reikalavimą gauti išankstinį leidimą norint tvarkyti asmens duomenis; numatantis skundų nagrinėjimo ir tyrimo tvarką bei atsakomybę už įstatymo nuostatų pažeidimus.

Nepaisant JAV ir Europos Sąjungos bendro siekio užtikrinti asmenų teisę į privatumą, JAV požiūris į privatumą yra skirtingas, lyginant su Europos sąjunga[314]. JAV asmens duomenų apsaugos reguliavimas pasižymi sektorinių įstatymų ir savireguliavimo modelių bruožais: skirtingais įstatymais reguliuojamos atskiros asmens duomenų apsaugos sritys, pavyzdžiui, asmens duomenų tvarkymas telekomunikacijų sektoriuje, taip pat taikomi tam tikri elgesio kodeksai asmens duomenų apsaugos srityje. Dėl tokio asmens duomenų apsaugos reguliavimo JAV susiduriama su tokiomis problemomis, kaip pakankamai silpna asmens duomenų apsauga, ribotas įstatymų, reglamentuojančių asmens duomenų apsaugą taikymas ir problemiškas jų įgyvendinimas.

Taigi JAV asmens duomenų apsaugos teisinė sistema labai skiriasi nuo Lietuvos asmens duomenų reguliavimo modelio, nors abi valstybės turi bendrą tikslą – stiprinti savo piliečių privatumo apsaugą. JAV duomenų tvarkymo atžvilgiu yra taikomi kitokie apsaugos standartai, kurie daugeliu požiūrių yra žemesni nei Lietuvoje ir apskritai Europos Sąjungoje. Valstijos per bendrąją teisę ir įstatymus pateikė skirtingus asmeninės informacijos apsaugos lygius. Panašiai JAV privatumo apsauga federaliniu lygmeniu plėtojosi sektorius po sektoriaus, kuriant daugybę įstatymų, numatančių skirtingus asmens duomenų apsaugos standartus, priklausomai nuo asmeninės informacijos rūšies ir pobūdžio, kai kurią informaciją, netgi labai svarbią, paliekant visai be jokios įstatymų apsaugos[315].

Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas įtvirtina pagrindinius asmens duomenų apsaugos principus, tokius

[314] Kuner, C. 2003. *European Data Privacy law and Online Business*. Oxford: Oxford University Press, p. 279.

[315] Civilka, M. Asmens duomenų apsaugos teisinis reguliavimas interneto kontekste [interaktyvus], p. 29 [žiūrėta 2011-09-20]. <http://www.google.lt/url?q=http://ututi.lt/subject/VU/EF/elektroninis_verslas/file/3412/get&sa=U&ei=CIrBTYTrGcqYOsXO7Z0I&ved=0CAsQFjAA &usg=AFQjCNGhewAzJu8FWWwu2xDHpalcdnv-sg>.

kaip: tikslo nustatymo, teisėtumo, asmens duomenų kokybės, proporcingumo, saugumo užtikrinimo, panaudojimo apribojimo, draudimo tvarkyti ypatingus asmens duomenis, individualaus dalyvavimo (duomenų subjekto teisių), atvirumo, priežiūros ir sankcijų. Be to, įstatymas įtvirtina, kad asmens duomenys teikiami duomenų gavėjams trečiosiose valstybėse, jeigu šiose valstybėse yra tinkamas asmens duomenų teisinės apsaugos lygis[316]. Būtent dėl paskutiniojo reikalavimo JAV, siekiant nutiesti tiltą tarp skirtingų požiūrių į asmens duomenų apsaugą, Prekybos departamentas, pasitaręs su Europos Komisija, sukūrė saugaus uosto sistemą (Europoje patvirtinta 2000 m.), kurios pagrindas yra septyni saugaus uosto principai[317]: pranešimo, pasirinkimo, perdavimo tretiesiems asmenims, prieigos, saugumo, duomenų vientisumo ir įgyvendinimo.

Pažymėtina, kad Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatyme įtvirtinti teisėto asmens duomenų tvarkymo principai yra imperatyvaus pobūdžio, o JAV saugaus uosto programa, priešingai, – remiasi savanoriškumo principu: organizacijos, kurios nori tapti šios programos narėmis, turi užsiregistruoti; be to, jos turi atitikti daugelį standartų, kurie yra nustatyti jų atitikimo Direktyvos 25 str. numatytam reikalavimui įvertinimui.

Saugaus uosto sistema yra svarbi tuo, kad JAV organizacija, kuri yra saugaus uosto narė, garantuoja pakankamą privatumo apsaugą, kaip tai apibrėžia Direktyva. Vis dėlto JAV yra taikomi kitokie asmens duomenų apsaugos standartai, kurie daugeliu požiūrių yra žemesni nei Lietuvoje. Be to, laikoma, kad JAV numatyti principai negali pakeisti nacionalinio teisinio reguliavimo asmens duomenų teisinės apsaugos srityje[318].

Vis dėlto, nepaisant tam tikrų asmens duomenų teisinės apsaugos trūkumų, ES yra pripažinusi, kad su tam tikromis išlygomis ir taikant

[316] Asmens duomenų teisinės apsaugos lygis vertinamas atsižvelgiant į visas aplinkybes, susijusias su duomenų teikimu, ypač į trečiąją valstybę, į kurią ketinami teikti asmens duomenys, galiojančius įstatymus, kitus teisės aktus bei duomenų valdytojo parengtus dokumentus, užtikrinančius asmens duomenų teisinę apsaugą, į teikiamų duomenų pobūdį, duomenų tvarkymo būdus, tikslus, trukmę, saugumo priemones, kurių bus laikomasi toje valstybėje.

[317] „Saugaus uosto“ principai [interaktyvus, žiūrėta 2011-09-20]. <https://www.export.gov/safeharbor/eu/eg_main_018476.asp>.

[318] Kuner, C. 2003. *European Data Privacy law and Online Business*. Oxford: Oxford University Press, p. 279 .

tam tikras sąlygas, JAV saugaus uosto principai gali užtikrinti tinkamą asmens duomenų apsaugos lygį[319].

Už Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo, išskyrus 8 straipsnį, vykdymo priežiūrą ir kontrolę atsakinga Valstybinė duomenų apsaugos inspekcija, kurios svarbiausi veiklos tikslai yra plėtoti duomenų apsaugą, prižiūrėti asmens duomenų valdytojų veiklą tvarkant asmens duomenis, kontroliuoti asmens duomenų tvarkymo teisėtumą, kovoti su duomenų tvarkymo pažeidimais ir užtikrinti duomenų subjekto teisių apsaugą[320]. JAV pagrindinės institucijos, atsakingos už saugaus uosto principų laikymąsi yra Federalinė prekybos komisija, Transporto departamentas ir Prekybos departamentas. Pavyzdžiui, JAV Federalinė prekybos komisija gali pareikalauti laikytis administracinių nurodymų ir skirti baudą iki 12 000 dolerių už kiekvieną pažeidimo dieną. Jei organizacija nuolat pažeidžia „saugaus uosto reikalavimus ir dėl to pradedama abejoti jos patikimumu, organizacija privalo apie tai pranešti Prekybos departamentui. Už nepranešimą numatyta baudžiamoji atsakomybė[321].

Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo 53 straipsnis įtvirtina banketinę teisės normą, kad asmenims, pažeidusiems šį įstatymą, taikoma įstatymų nustatyta atsakomybė. Pavyzdžiui, Administracinių teisės pažeidimų kodekso[322] $214^{(16)}$ straipsnis numato atsakomybę už duomenų subjekto teisių pažeidimą, $214^{(17)}$ straipsnis – už Valstybinės duomenų inspekcijos pareigūnų teisėtų nurodymų nevykdymą, $214^{(14)}$ straipsnis – už neteisėtą asmens duomenų tvarkymą, $214^{(23)}$ straipsnis – už neteisėtą asmens duomenų tvarkymą ir privatumo apsaugos pažeidimą elektroninių ryšių srityje. Sankcijos už šiuos pažeidimus yra labai nedidelės, iki 2 000 Lt. Taigi, Lietuvoje už asmens duomenų teisinės apsaugos reikalavimų pažeidimą iš esmės taikoma administracinė atsakomybė, tačiau sankcijos už pažeidimus yra kelis kartus mažesnės nei JAV.

[319] Komisijos sprendimas 2000 m. liepos 26 d. dėl Europos Parlamento ir Tarybos direktyvos 95/46/EB dėl „saugaus uosto“ privatumo principų teikiamos apsaugos pakankamumo ir su tuo susijusių JAV komercijos departamento pateiktų „Dažnai užduodamų klausimų“. [2000] OL L 215, preambulės 5 p.

[320] Valstybinė duomenų apsaugos inspekcija [interaktyvus]. Vilnius, [žiūrėta 2011-09-03]. <http://www.ada.lt>.

[321] False Statements Act (18 U.S.C. § 1001). [interaktyvus]. [žiūrėta 2011-09-19]. <http://www.law.cornell.edu/uscode/18/usc_sec_18_00001001----000-.html>.

[322] Lietuvos Respublikos administracinių teisės pažeidimų kodeksas. *Valstybės žinios*. 1985, Nr. 1-1.

Atlikus JAV ir Lietuvos asmens duomenų apsaugos teisinio reguliavimo analizę, galima daryti išvadą, kad JAV asmens duomenų apsaugos teisinė sistema labai skiriasi nuo Lietuvos: JAV požiūris į asmens duomenų apsaugą remiasi sektoriniu reguliavimu ir savireguliacija, o Lietuvoje – visapusišku teisiniu reguliavimu. JAV nėra vieno bendro pagrindinio asmens duomenų apsaugą reglamentuojančio įstatymo, o duomenų tvarkymo atžvilgiu vadovaujamasi saugaus uosto sistema ir taikomi kitokie apsaugos standartai, kurie daugeliu požiūrių yra žemesnio lygio nei Lietuvoje. JAV, priešingai nei Lietuvoje, yra gana silpnai reglamentuota asmens duomenų apsauga, ribotas įstatymų, reglamentuojančių asmens duomenų apsaugą, taikymas ir problemiškas jų įgyvendinimas. Nepaisant to, kad, Europos Sąjungos nuomone, JAV užtikrina tinkamą asmens duomenų apsaugą, visos minėtos problemos sudaro prielaidas tapatybės vagystei elektroninėje erdvėje įvykdyti ir už šią veiką išvengti atsakomybės. Tačiau reikėtų atkreipti dėmesį į sankcijas už asmens duomenų apsaugos pažeidimus, kurios JAV yra kelis kartus didesnės nei Lietuvoje ir turėtų labiau atgrasinti potencialius pažeidėjus.

Teisinė aplinka elektroninės informacijos saugos srityje

Pastaruoju metu elektroninės informacijos saugai skiriama vis daugiau dėmesio tiek techniniu, tiek ir teisiniu požiūriu visame pasaulyje. Informacijos sauga (saugumas) suprantamas kaip informacijos bei sistemos infrastruktūros apsauga nuo atsitiktinio ar tyčinio, natūralaus ar dirbtinio pobūdžio poveikio, galinčio sukelti žalą informacijos ar sistemos infrastruktūros savininkams ir vartotojams.

Elektroninės informacijos saugos aplinkos klausimus galima būtų suskirstyti į keturias pagrindines grupes: normatyvinę (įstatymai, įstatymų įgyvendinamieji aktai, standartai ir kt.), administracinę (organizacijos vadovybės vykdomi bendro pobūdžio veiksmai), procedūrinę (konkretūs su konkrečiais asmenimis susiję saugumo veiksmai), programinę techninę (vykdomi konkretūs techninio pobūdžio veiksmai)[323].

Atsižvelgiant į šio straipsnio tikslą šioje dalyje bus plačiau nagrinėjami būtent pirmosios, t. y. normatyvinės, elektroninės informacijos saugos klausimai Lietuvoje ir JAV.

[323] Kiškis, M., *et al*. 2006. *Teisės informatika ir informatikos teisė*. Vilnius: Mykolo Romerio universiteto Leidybos centras, p. 38–39.

Vienas iš pagrindinių teisės aktų JAV, reguliuojančių informacijos saugos sritį, yra Federalinis informacijos saugos valdymo įstatymas[324], kuris buvo priimtas 2002 m., kaip e. valdžios įstatymo dalis, ir kuriame pabrėžiama informacijos saugos svarba ekonomikai ir nacionaliniam saugumui JAV. Tačiau Lietuva elektroninės informacijos saugos reguliavimo prasme neturi tokių senų tradicijų kaip Europos valstybės[325]. Lietuvoje nėra įstatymo, kuris būtų skirtas tik informacijos saugai reguliuoti, o elektroninės informacijos saugos klausimus reglamentuoja daugybė įstatymų ir įstatymų įgyvendinamųjų teisės aktų[326]. Pavyzdžiui, teisės normos, reglamentuojančios elektroninės informacijos saugą, įtvirtintos Lietuvos Respublikos asmens duomenų teisinės apsaugos (30 straipsnis), Elektroninių ryšių (62 straipsnis), Elektroninio parašo ir Valstybės registrų įstatymuose (20 straipsnis), taip pat daugelyje įstatymų įgyvendinamųjų teisės aktų. Manytina, kad Lietuvoje elektroninės informacijos saugos reguliavimas įstatymo lygmeniu yra fragmentiškas ir nepakankamas[327].

JAV Federalinis informacijos saugos valdymo įstatymas specifines funkcijas informacijos saugos srityje numato federalinėms agentūroms, Nacionaliniam standartų ir technologijų institutui bei Valdymo ir biudžeto tarnybai (angl. *Office of Management and Budget*). Tuo tarpu Lietuvoje už elektroninės informacijos saugos priežiūrą, įgyvendinimą ir politikos formavimą atsakingos šios pagrindinės institucijos: Vidaus reikalų ministerija, Informacinės visuomenės plėtros komitetas, Ryšių reguliavimo tarnyba, Valstybinė duomenų apsaugos inspekcija, Valstybės kontrolė.

JAV Federalinėms agentūroms informacijos saugos srityje suteikiama ir priskiriama daug pareigų ir teisių. Federalinis informacijos saugos valdy-

[324] Federal Information Security Management Act. 2002 // US code, Title 44, Chapter 35, Subchapter III [interaktyvus, žiūrėta 2011-09-19]. < http://www.law.cornell.edu/uscode/44/usc_sup_01_44_10_35_20_III.html >.

[325] Štitilis, D.; Paškauskas, Ž. 2007. Valstybės elektroninės informacijos saugos strategija – vienas iš pagrindinių elektroninės informacijos saugos reguliavimo instrumentų: lyginamoji analizė, *Jurisprudencija* 92 (2): 38.

[326] Holistinio teisinio elektroninės informacijos saugos reguliavimo apraiška galima vadinti Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymo projektą (buvo parengtas 2007 metais), tačiau šis projektas nebuvo priimtas.

[327] Petrauskas, R.; Štitilis, D.; Rotomskis, I.; Paškauskas, Ž. 2006. International legislative Regulation Provisions Concerning the Security of Informations Systems and Information. Implementation of the Provisions in Lithuania. *Databases and Information Systems: seventh International baltic Conference on Databases and Information Systems*. Vilnius: Technika, p. 225.

mo įstatymas iš kiekvienos agentūros vadovo reikalauja įgyvendinti tinkamą informacijos saugos politiką, taip pat vykdyti veiksmus, efektyviai ir priimtinomis sąnaudomis mažinant informacijos saugos riziką, siekiant priimtinos rizikos lygio. Įstatymas taip pat reglamentuoja, kad kiekviena federalinė agentūra pagal savo veiklos apimtį plėtotų ir įgyvendintų informacijos ir informacinių sistemų saugos programą. Nacionalinis standartų ir technologijų institutas atsakingas už standartus ir su jais susijusias metodikas, skirtas adekvačiai informacijos saugai federalinių agentūrų veikloje užtikrinti. Institutas glaudžiai bendradarbiauja su federalinėmis agentūromis, siekdamas gerinti įstatymo reikalavimų užtikrinti informacijos saugą supratimą bei įgyvendinimą, skelbia standartus ir nurodo gaires, kurios sudaro pagrindą tinkamoms informacijos saugos programoms šiose agentūrose.

Lietuvoje pagrindinės funkcijos elektroninės informacijos saugos srityje numatytos Vidaus reikalų ministerijai (formuoja valstybės politiką informacinių technologijų saugos srityje, organizuoja, koordinuoja ir kontroliuoja jos įgyvendinimą), Valstybinei duomenų apsaugos inspekcijai (plėtoja duomenų apsaugą, kontroliuoti asmens duomenų tvarkymo teisėtumą, kovoja su duomenų tvarkymo pažeidimais) ir Ryšių reguliavimo tarnybai (vykdo nacionalinio elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinio CERT (*Computer Emergency Response Team)* veiklą, rengia rekomendacijas dėl elektroninės informacijos saugos grėsmės). Autorių nuomone, Lietuvoje trūksta bendros už informacijos saugą atsakingos institucijos, esamų institucijų funkcijos tam tikrais atvejais dubliuojasi, o viena iš pagrindinių institucijų – Lietuvos Respublikos vidaus reikalų ministerija – kontroliuoja kitas sau nepavaldžias ministerijas ir įstaigas ar institucijas (taikoma ydinga praktika).

JAV Federalinis informacijos saugos valdymo įstatymas įtvirtina, kad visos informacinės sistemos turi būti priskirtos tam tikroms kategorijoms, kurios nustatomos pagal tikslus užtikrinti atitinkamą informacijos saugos lygį, atsižvelgiant į kylančios rizikos lygį. Saugos kategorijas nustato pirmasis privalomas įstatymo reikalaujamas saugos standartas – Federalinės informacijos ir informacinių sistemų priskyrimo saugos kategorijoms standartas[328]. Tuo tarpu Lietuvoje valstybės institucijų ir įstaigų informacinių

[328] FIPS PUB 199 "Standards for Security Categorization of Federal Information and Information Systems" [interaktyvus]. 2004 [žiūrėta 2011-09-19]. < http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf>.

sistemų klasifikavimą pagal informacinėse sistemose tvarkomos elektroninės informacijos svarbą reglamentuoja 2007 m. Lietuvos Respublikos vidaus reikalų ministro įsakymu Nr. 1V-247 patvirtintos Valstybės institucijų ir įstaigų informacinių sistemų klasifikavimo pagal jose tvarkomą elektroninę informaciją gairės ir Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos saugos reikalavimai[329].

Pažymėtina, kad tiek JAV federalinės informacinės sistemos, tiek Lietuvos viešojo sektoriaus informacinės sistemos turi atitikti nustatytus saugos reikalavimus, kuriuos nustato įstatymo įgyvendinamasis teisinio reguliavimo aktas: „Minimalūs saugos reikalavimai Federalinei informacijai ir informacinėms sistemoms“[330] (JAV) ir 2007 m. balandžio 25 d. Vyriausybės nutarimu Nr. 410 patvirtinti Bendrieji elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimai[331] bei 2008 m. įsakymu Nr. 1V-384 patvirtinti Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos techniniai saugos reikalavimai (Lietuvoje).

Už informacijos saugos reikalavimų nesilaikymą kyla atsakomybė. Pavyzdžiui, Lietuvoje Administracinių teisės pažeidimų kodekso 214(15) straipsnis numato administracinę atsakomybę už neteisėtą valstybės informacinių sistemų duomenų tvarkymą, o Baudžiamojo kodekso XXX skyriuje numatyta baudžiamoji atsakomybė už nusikaltimus elektroninių duomenų ir informacinių sistemų saugumui[332]. Tuo tarpu, JAV atsakomybė už elektroninės informacijos saugos pažeidimus didžiąja dalimi numatyta kaip atsakomybė už elektroninius nusikaltimus (neteisėta prieiga ir kt.).

Atlikus pagrindinių Lietuvos ir JAV teisės aktų, reglamentuojančių elektroninės informacijos saugą ir analizę, darytina išvada, kad šiuo metu

[329] Lietuvos Respublikos vidaus reikalų ministro įsakymu Nr. 1V-247 patvirtintos Valstybės institucijų ir įstaigų informacinių sistemų klasifikavimo pagal jose tvarkomą elektroninę informaciją gairės ir Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos saugos reikalavimai. *Valstybės žinios.* 2007, Nr. 78-3160.

[330] FIPS 200 “Minimum Security Requirements for Federal Information and Information Systems” [interaktyvus]. 2006 [žiūrėta 2011-09-19]. <http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf >.

[331] 2007 m. balandžio 25 d. Vyriausybės nutarimu Nr. 410 patvirtinti Bendrieji elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimai. *Valstybės žinios.* 2007, Nr. 49-1891.

[332] Lietuvos Respublikos baudžiamasis kodeksas, *Valstybės žinios.* 2000, Nr. 89-2741; XXX skyrius „Nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui.

Lietuvoje elektroninės informacijos saugos reguliavimas yra fragmentiškas, t. y. nėra teisės aktų, kurie išsamiai ir sistemiškai reglamentuotų tinklų ir elektroninės informacijos saugumą, o galiojantys teisės aktai neužtikrina visapusiško ir nuoseklaus tinklų ir elektroninės informacijos saugumo visuomeninių santykių reglamentavimo, nesudaro sąlygų vartotojų pasitikėjimui informacine visuomene ir saugios informacinės visuomenės plėtrai. Nors abiejose lyginamose valstybėse galioja daug teisės aktų, reglamentuojančių elektroninės informacijos saugos klausimus viešajame sektoriuje, elektroninės informacijos sauga privačiame sektoriuje nėra reguliuojama[333], išskyrus tam tikras išimtis. Toks teisinis reguliavimas kritikuotinas, kadangi elektroninės informacijos sauga negali būti veiksmingai užtikrinama reguliuojant tik viešąjį sektorių, o privatųjį sektorių paliekant savireguliacijai. Taip pat atkreiptinas dėmesys, kad Lietuvoje trūksta bendros elektroninės informacijos saugos institucinės kontrolės.

Neužtikrinus veiksmingo elektroninės informacijos saugos reguliavimo, sudaromos prielaidos tapatybės vagystei elektroninėje erdvėje.

Asmens identifikavimo teisinis reguliavimas

JAV teisinį tapatybės turinio elementų reguliavimą užtikrina savarankiškai, o Lietuva, kaip Europos Sąjungos valstybė narė, turi užtikrinti nacionalinių teisės aktų atitiktį Europos Sąjungos keliamiems reikalavimams.

Pagrindiniai asmens tapatybės dokumentai JAV yra pasas, paso kortelė ir socialinio draudimo pažymėjimas, Lietuvoje – pasas ir asmens tapatybės kortelė. Minėtų dokumentų išdavimas abiejose valstybėse yra centralizuotas, tačiau mažiau svarbių dokumentų išdavimo tvarka yra labai skirtinga: JAV yra federacinė valstybė ir valstijose šie dokumentai išduodami vadovaujantis skirtingą tvarką nustatančiais teisės aktais. Be to, JAV ypatumas asmens identifikavimo teisinio reguliavimo srityje lyginant su Lietuva yra tas, kad JAV nenaudoja oficialių, privalomų įvairios paskirties identifikavimo kortelių ir asmens kodų taip, kaip jie suprantami Lietuvoje: vietoje vieno kodo, naudojamo nusakant asmens tapatybę bet kurioje situacijoje, naudojami įvairūs siaurai taikomi žymenys.

[333] Išskyrus (Lietuvoje) kelis fragmentinius teisės aktus – Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymą (dėl asmens duomenų saugumo), Lietuvos Respublikos elektroninių ryšių įstatymą (dėl elektroninių ryšių saugumo) ir kt.

Pastebėtina, kad JAV vairuotojų pažymėjimus išduoda valstijos, o atsižvelgiant į tai, kad šioje valstybėje nėra nacionalinės identifikavimo kortelės, vairuotojo pažymėjimas paprastai naudojamas kaip tapatybės nustatymo formos standartas. Asmenims, kurie neturi vairuotojo pažymėjimo, valstijos išduoda identifikavimo korteles, tačiau jos nėra privalomos. Lietuvoje, skirtingai nei JAV, asmens tapatybės kortelė yra vienas iš pagrindinių asmens tapatybę patvirtinančių dokumentų, tačiau naujo pavyzdžio vairuotojo pažymėjimas Lietuvoje taip pat, kaip ir JAV, faktiškai naudojamas kaip tapatybės nustatymo dokumentas, nors teisės aktuose jis nėra įvardijamas kaip asmens tapatybę patvirtinantis dokumentas. Peržvelgus Lietuvoje veikiančių finansinių institucijų paslaugų teikimo sutartis, nustatyta, kad, pavyzdžiui, visi komerciniai bankai Lietuvoje kaip tapatybę patvirtinantį dokumentą pripažįsta ir vairuotojo pažymėjimą, išduotą po 2002 m. gruodžio 31 d. (naujo pavyzdžio).

Elektroninės tapatybės reguliavimo srityje JAV paminėtinas Elektroninių parašų globalioje ir nacionalinėje komercijoje aktas[334], kuris nustato elektroninio sertifikato teisinę galią. Šiame įstatyme nurodoma, kad viena iš elektroninio parašo funkcijų yra pasirašančio asmens identifikavimas. JAV didžioji dalis elektroninių paslaugų sistemų naudoja panašias asmens identifikavimo priemones. Galima išskirti svarbiausius asmens elektroninėje erdvėje identifikavimo elementus ir identifikavimo pavyzdžius JAV:[335]

1) identifikavimas pagal tai, ką vartotojas turi žinoti: asmuo elektroninėje erdvėje gali būti identifikuojamas pagal unikalų pavadinimą (vardą) ir slaptažodį. Fizinėje erdvėje asmenų vardai gali kartotis, tačiau toje pačioje elektroninėje sistemoje asmens tapatybė turi būti nustatoma naudojant unikalų identifikatorių;

2) identifikavimas pagal tai, ką vartotojas turi: šiuo principu grindžiamas kliento atpažinimas pagal turimas priemones: elektroninį parašą (patvirtintą elektroniniu sertifikatu), kodų generatorius, kodų lenteles;

3) identifikavimas pagal tai, kas vartotojas yra: šiuo atveju naudojami

[334] *Electronic signatures in global and national commerce act* [interaktyvus, žiūrėta 2011-09-19]. <http://www.ftc.gov/os/2001/06/esign7.htm>.

[335] Burr, W. E.; Dodson, D. F.; Polk, W. T. 2006. *Electronic Authentication Guideline. Recommendations of the National Institute of Standards and Technology* [interaktyvus]. *Gaithersburg: NIST Special Publication* 800-63 Version 1.0.2., [žiūrėta 2011 09 19]. <http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf>.

biometriniai tapatybės elementai, kurie leidžia identifikuoti asmenį pagal asmens specifines fiziologines arba elgesio charakteristikas.

Lietuvoje svarbiausi asmens elektroninėje erdvėje identifikavimo elementai ir identifikavimo pavyzdžiai analogiški JAV. Abiejose valstybėse įstatymiškai pripažįstamas ir reguliuojamas asmens identifikavimo būdas elektroninėje erdvėje – elektroninis parašas, patvirtintas elektroniniu sertifikatu. Lietuvoje elektroninį parašą ir elektroninį sertifikatą, kaip asmens tapatybės patvirtinimo būdą elektroninėje erdvėje, reguliuoja Elektroninio pašašo ir Asmens tapatybės kortelės įstatymai.

Paminėtina ir tai, kad abiejų lyginamų valstybių elektroninės bankininkystės paslaugų srityje naudojama sava identifikavimo sistema, apimanti du identifikavimo elektroninėje erdvėje elementus: „Tai, kas žinoma" ir „Tai, kas turima", ir kurią pripažįsta valstybė. Pavyzdžiui, Lietuvoje toks identifikavimas remiasi Elektroninio parašo įstatymo 8 str. 3 d. nuostata: „Elektroninis parašas visais atvejais turi šio straipsnio 1 dalyje įtvirtintą teisinę galią, jeigu parašų naudotojai tarpusavyje dėl to susitaria"[336] ir ši tapatybė turi įstatymo teisinę galią. Banko ir kliento susitarimas, kad atitinkama banko sistema atitinka saugios sistemos požymius, minima įstatymo teises norma bei identifikavimas remiantis šia sistema ir suponuoja tą faktą, kad tokia identifikavimo sistema yra pripažįstama valstybės.

Atlikus JAV ir Lietuvos pagrindinių teisės aktų, reglamentuojančių asmens identifikavimą, analizę galima daryti išvadą, kad elektroninėje erdvėje elektroninis parašas (patvirtintas kvalifikuotu sertifikatu) (valstybės sureguliuota saugi identifikavimo priemonė) arba asmens identifikavimas naudojant bankines sistemas (valstybės pripažįstama tapatybė[337]), atitinka valstybės reguliuojamus tapatybės nustatymo būdus fizinėje erdvėje (kai tapatybė nustatoma dokumentais).

Atlikta asmens tapatybės dokumentų teisinio reguliavimo analizė rodo, kad asmens dokumentų įvairovė JAV yra labai didelė, lyginant su asmens dokumentais, išduodamais Lietuvoje, o asmens identifikavimo dokumentų išdavimo tvarka JAV yra gana lanksti. Taip pat atkreiptinas dėmesys, kad JAV įvykdomas didelis skaičius nusikaltimų (tiek fizinėje erdvėje, tiek elektroninėje), kuriems atlikti neretai pasisavinami tapatybės duomenys. JAV daug dėmesio skiriama terorizmo prevencijai, todėl

[336] Lietuvos Respublikos elektroninio parašo įstatymas. *Valstybės žinios.* 2000, Nr. 61-1827.

[337] Jei naudojamasi sutartiniu elektroniniu parašu.

šioje valstybėje būtina užtikrinti minimalius asmens dokumentų apsaugos reikalavimus. Tam, kad būtų įvykdyti minimalūs dokumentams keliami reikalavimai, JAV valstijos, išduodamos asmens tapatybės korteles ir vairuotojo pažymėjimus, turi užtikrinti tinkamą dokumentų apsaugos lygį ir fiksuoti būtiną informaciją[338], priešingu atveju sudaromos prielaidos tapatybės vagystei įvykdyti.

Specialūs teisės aktai dėl tapatybės vagystės elektroninėje erdvėje

Tapatybės vagystės elektroninėje erdvėje kriminalizavimas (baudžiamųjų įstatymų normos)

Tapatybės vagystės elektroninėje erdvėje kriminalizavimas JAV ir Lietuvoje nagrinėjamas monografijos 3.4.1. dalyje. Tačiau paminėtina, kad baudžiamųjų normų lyginamoji analizė parodė, kad JAV tapatybės vagystė elektroninėje erdvėje yra kriminalizuota ir traktuojama kaip savarankiška veika, ir tai turėtų gerinti tokios veikos tyrimą, o Lietuvoje už tam tikrus tapatybės vagystės elektroninėje erdvėje elementus baudžiamoji atsakomybė galima tik pagal tradicines pavojingas veikas (sukčiavimas ir pan.), dėl ko tokią veikią įrodyti yra daug sunkiau.

Kiti specialūs teisės aktai

Specialūs teisės aktai JAV analizuojami monografijos 3.3.1 dalyje.

Analizuojant lyginamų valstybių teisės aktus, susijusius su tapatybės vagyste elektroninėje erdvėje, nustatyta, kad Lietuvoje nėra specialiųjų teisės aktų dėl tapatybės vagystės elektroninėje erdvėje. Tačiau JAV tokie teisės aktai egzistuoja, nepaisant to, kad tapatybės vagystė šioje valstybėje yra kriminalizuota. Toks JAV teisinis reguliavimas vertintinas kaip veiksminga kovos su tokio pobūdžio veikomis priemonė[339].

Būtina pažymėti ir tai, kad su tapatybės vagyste susijusių visuomeninių santykių teisiniam reguliavimui papildyti naudotinos savireguliaci-

[338] Division a emergency supplemental appropriations act for defense, the global war on terror, and tsunami relief. Sec. 202. Minimum document requirements and issuance standards for federal recognition [interaktyvus]. 2005 [žiūrėta 2011-05-02]. <http://www.dsca.mil/programs/LPA/2005/getdoc.cgi_dbname=109_cong_public_laws&docid=f_publ013.109.pdf>.

[339] Štitilis, D.; Pakutinskas, P.; Dauparaitė, I.; Laurinaitis, M. 2011. Teisinė aplinka siekiant išvengti tapatybės vagystės elektroninėje erdvėje: JAV ir Lietuvos teisės aktų lyginamoji analizė, *Socialinės technologijos* 1 (1): 74.

jos priemonės. Autorių apklausti ekspertai dėl savireguliacijos pažymėjo: 9-as ekspertas teigė, kad savireguliacija kibernetinio saugumo srityje nėra veiksminga, todėl reikalauja didesnio reguliavimo, panašiai mano ir 2-as ekspertas. 1-as ekspertas paminėjo, kad reikia daugiau atsakomybės iš verslo subjektų pusės. 1-as ir 4-as ekspertai nurodė, kad reikalingas informavimas ir švietimas. 6-as ekspertas teigė, kad taikant priemones reikia vertinti siekiamo tikslo ir sąnaudų balansą.

Apibendrinančios išvados

• Jungtinėse Valstijose nėra vieno įstatymo, skirto asmens duomenų teisinei apsaugai, tačiau atskirus sektorius reguliuojančių įstatymų veikimo sritis gana detaliai reglamentuoja privatumą ir asmens duomenų apsaugą bei numato atsakomybę už tokius minėtų vertybių pažeidimus, kaip tapatybės vagystė, kreditinių kortelių sukčiavimas, kitos neteisėtos veikos, susijusios su fizinių asmenų ir verslo institucijų privatumo pažeidimais, grėsme ekonomikai, finansų sektoriui, visuomenės tvarkai ar net nacionaliniam saugumui.

• JAV įstatymai numato atsakomybę ne tik už atskirus tapatybės vagystės elementus, bet ir kriminalizuoja tapatybės vagystę *per se*, už kurią numatomos ypač griežtos sankcijos, įskaitant laisvės atėmimą iki 30 metų. Tai leidžia teigti, kad tapatybės vagystė yra pavojingas nusikaltimas, kurį įvykdžius gali nukentėti ne tik pavieniai elektroninių paslaugų vartotojai, bet gali būti pasikėsinta ir į nacionalinį saugumą (pavyzdžiui, terorizmo atveju).

• Kai kuriuos įstatymus (pavyzdžiui, USA PATRIOT įstatymas), reglamentuojančius privatumą ir asmens duomenų apsaugą, galima vertinti kaip ypač griežtus JAV Konstitucijoje įtvirtintų asmens ir piliečio teisių ir laisvių atžvilgiu, kai dėl visuomenės saugumo ir siekiant užkirsti kelią tokiems pavojingiems nusikaltimams, kaip terorizmas, nustatomi Konstitucijoje įtvirtintų atskirų individų teisių ribojimai.

• Pagrindinės apžvelgtų įstatymų saugomos vertybės yra asmens teisė į privatumą, asmens gyvenimo neliečiamumą; vartotojų teisių apsauga, finansų institucijų interesų apsauga, elektroninių dokumentų saugumas, sąžininga verslo praktika, viešoji tvarka, visuomenės sveikata, nacionalinis saugumas. Visos šios vertybės gali būti pažeidžiamos įvykdant tapatybės vagystę arba pasinaudojant tapatybės vagyste kaip priemone kitoms nusikalstamoms veikoms atlikti.

• Atitinkamų teisės aktų asmens duomenų teisinės apsaugos srityje lyginamoji analizė parodė, kad Lietuvoje asmens duomenų teisinis reguliavimas yra pakankamas, išskyrus sankcijas už asmens duomenų teisinės apsaugos reikalavimų pažeidimus, kurios turėtų būti sugriežtintos.

• Elektroninių duomenų saugumo teisinio reguliavimo analizė atskleidė, kad Lietuvoje trūksta holistinio požiūrio reglamentuojant elektroninės informacijos saugą (įskaitant ir institucinės kontrolės aspektą). Abiejose valstybėse elektroninės informacijos sauga turėtų būti reguliuojama ir privačiame sektoriuje. Šie elektroninės informacijos saugos teisinio reguliavimo trūkumai sudaro prielaidas tapatybės vagystei elektroninėje erdvėje plisti.

• Atlikus asmens tapatybės dokumentų teisinio reguliavimo analizę, nustatyta, kad asmens dokumentų įvairovė JAV yra labai didelė, lyginant su asmens dokumentais, išduodamais Lietuvoje, o asmens identifikavimo dokumentų išdavimo tvarka JAV yra pakankamai lanksti. JAV įvykdomas didelis skaičius nusikaltimų (tiek fizinėje erdvėje, tiek ir elektroninėje), kuriems atlikti neretai pasisavinami tapatybės duomenys. Be to, JAV daug dėmesio skiriama terorizmo prevencijai, todėl šioje valstybėje būtina užtikrinti minimalius asmens dokumentų apsaugos reikalavimus. Tam, kad būtų įvykdyti minimalūs dokumentams keliami reikalavimai, JAV valstijos, išduodamos asmens tapatybės korteles ir vairuotojo pažymėjimus, turi užtikrinti tinkamą dokumentų apsaugos lygį ir fiksuoti būtiną informaciją, priešingu atveju sudaromos prielaidos tapatybės vagystei įvykdyti.

• Specialių teisės aktų, susijusių su tapatybės vagyste elektroninėje erdvėje lyginamoji analizė parodė, kad JAV yra ne vienas specialus teisės aktas, susijęs su tapatybės vagyste elektroninėje erdvėje (tai pagerina kovą su šiuo socialiniu teisiniu reiškiniu), o Lietuvoje nėra nė vieno specialaus teisės akto, kuris reglamentuotų minimus santykius, ir tai, autorių nuomone, sudaro palankias sąlygas tapatybės vagystei elektroninėje erdvėje plisti.

• Baudžiamųjų normų lyginamoji analizė parodė, kad JAV tapatybės vagystė elektroninėje erdvėje yra kriminalizuota kaip savarankiška veika, ir tai turėtų gerinti tokios veikos tyrimą, o Lietuvoje už tam tikrus tapatybės vagystės elektroninėje erdvėje elementus baudžiamoji atsakomybė galima tik pagal tradicines pavojingas veikas (sukčiavimas ir pan.), dėl ko tokią veiką įrodyti tampa daug sunkiau.

• Tiek Lietuvoje, tiek JAV identifikuotas teisinio reguliavimo, susijusio su tapatybės vagyste elektroninėje erdvėje trūkumas. Tai daro neigiamą poveikį kovai su šiuo pavojingu socialiniu teisiniu reiškiniu.

• Nustatyti šie teisinio reguliavimo, susijusio su tapatybės vagyste elektroninėje erdvėje, trūkumai Lietuvoje: specialių teisės aktų, skirtų tapatybės vagystei elektroninėje erdvėje, srityje ir nustatant baudžiamąją atsakomybę už tapatybės vagystę elektroninėje erdvėje (tapatybės vagystę elektroninėje erdvėje įvardijant kaip savarankišką pavojingą veiką). Lietuvos įstatymų leidėjas, numatydamas pagrindines teisinio reguliavimo, susijusio su tapatybės vagyste elektroninėje erdvėje, tobulinimo sritis, turėtų atsižvelgti į tyrimo metu identifikuotas problemas. Be to, autorių apklausti ekspertai taip pat nurodė, kad kai kurias teisinio reguliavimo priemones reikėtų tobulinti.

• Be esamo teisinio reguliavimo, tam tikrose srityse siūlytina naudoti ir savireguliaciją (pavyzdžiui, bendradarbiavimui kibernetinio saugumo srityje).

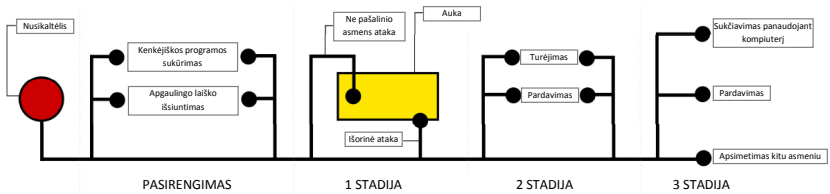
3.4. Tapatybės vagystės elektroninėje erdvėje elementų kriminalizavimas (baudžiamoji atsakomybė už tapatybės vagystę elektroninėje erdvėje)

Tapatybės vagystės elektroninėje erdvėje, kaip pavojingos veikos, vertinimo sudėtingumas lemia nevienodą praktiką[340]. Vis dažniau kyla diskusijų dėl baudžiamosios atsakomybės. Išsiskiria dvi konfrontuojančios pozicijos: vieni teigia, kad tapatybės vagystė turėtų būti kvalifikuojama kaip atskira nusikalstama veika, t. y. siūloma šią veiką kriminalizuoti. Pavyzdžiui, Ekonominio bendradarbiavimo ir plėtros organizacija[341] yra tos nuomonės, kad tapatybės vagystę reikia kriminalizuoti, laikant savarankiška nusikalstama veika. Šios pozicijos oponentai tapatybės vagystę traktuoja kaip priemonę teisės pažeidimams ir (ar) nusikalstamoms veikoms atlikti ir teigia, kad ši veika patenka į jau kriminalizuotas veikas reglamentuojančių straipsnių veikimo sritį, todėl tapatybės vagystės kriminalizavimas nėra būtinas.

[340] Štitilis, D.; Laurinaitis, M. 2009. Tapatybės vagystė elektroninėje erdvėje, *Informacijos mokslai* 50: 244.

[341] < http://www.oecd.org>.

Toliau šioje monografijoje bus nagrinėjama baudžiamoji atsakomybė už tapatybės vagystės elektroninėje erdvėje elementus. Šiuo tikslu autoriai vadovausis tapatybės vagystės elektroninėje erdvėje stadijomis. Mokslinėje literatūroje dažniausiai skiriamos trys tapatybės vagystės stadijos: 1 stadija – su tapatybe susijusios informacijos gavimas, 2 stadija – sąveika su tapatybe susijusia informacija, 3 stadija – su tapatybe susijusios informacijos panaudojimas siekiant padaryti nusikaltimą[342].



19 pav. Tapatybės vagystės trijų stadijų modelis
(šaltinis: Gercke Marco. Internet-related identity thef. Project on Cybercrime, 2007[343])

Kai kurie autoriai laikosi pozicijos, kad yra tik dvi tapatybės vagystės stadijos: 1 stadija – su tapatybe susijusios informacijos gavimas, 2 stadija – neteisėtas su tapatybe susijusios informacijos panaudojimas[344], tačiau šioje monografijoje vadovaujamasi naujausioje literatūroje siūlomo tapatybės vagystės skirstymu į tris stadijas, o nagrinėjant užsienio valstybių ir Lietuvos baudžiamuosius įstatymus, siekiama nustatyti, ar šiuose įstatymuose yra įtvirtinta tapatybės vagystės, kaip savarankiškos nusikalstamos veikos, sudėtis, ar yra kriminalizuotos tik atskiros tapatybės vagystės stadijos ir kokios sankcijos numatomos už tapatybės vagystę ar atskirus jos elementus.

[342] Gercke, M. *Internet-related identity thef. Project on Cybercrime* [interaktyvus]. 2007, p. 17-20. [žiūrėta 2011-09-19] <http://www.coe.int/T/DG1/LegalCooperation/Economiccrime/cybercrime/cy%20activity_events_on_identity_theft/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf>.

[343] *Ibid*..

[344] Rannenberg, K.; Royer, D.; Deuker, A. 2009. *The Future of Identity in the Information Society: Challenges and Opportunities*. Berlin: Springer, p. 321.

3.4.1. Tapatybės vagystės elektroninėje erdvėje elementų kriminalizavimas pasirinktose valstybėse: lyginamoji analizė

Siekiant visapusiškai išnagrinėti tapatybės vagystės elektroninėje erdvėje elementų kriminalizavimą, visų pirma lyginamuoju metodu išnagrinėtinos pasirinktų užsienio valstybių atitinkamos baudžiamųjų įstatymų normos. Toliau šioje monografijoje bus analizuojamos pasirinktų aštuonių užsienio valstybių (Jungtinių Amerikos Valstijų, Jungtinės Karalystės, Nigerijos, Prancūzijos, Suomijos, Estijos, Rusijos ir Pietų Korėjos) baudžiamųjų įstatymų teisės normos, nagrinėjant tapatybės vagystės elementų kriminalizavimo būklę lyginamuoju aspektu. Konkrečių valstybių pasirinkto kriminalizavimo motyvai atskleidžiami tolesnėse dalyse.

Tapatybės vagystės elementų kriminalizavimas Jungtinėse Amerikos Valstijose

Jungtinės Amerikos Valstijos (toliau – JAV) baudžiamosios teisės normų, nustatančių atsakomybę už tapatybės nusikaltimus, analizei buvo pasirinktos dėl to, kad JAV pagal nusikaltėlių, veikiančių elektroninėje erdvėje, skaičių, užima pirmą vietą pasaulyje[345] ir turi didžiulę patirtį kovojant su elektroniniais nusikaltimais. Šioje valstybėje pagal visus interneto nusikaltimus tapatybės vagystė elektroninėje erdvėje užima antrąją vietą (pagal kreipimosi skaičių)[346]. JAV yra viena iš Konvencijos dėl elektroninių nusikaltimų iniciatorių (Konvenciją ratifikavo 2006 m. rugsėjo 29 d., kuri šalyje įsigaliojo nuo 2007 m. sausio 1 d.) ir ėmėsi daugybės priemonių, siekdama užkirsti kelią tapatybės nusikaltimams. Pajėgos, nukreiptos prieš tapatybės vagystę (angl. *Identity Theft Task Force*), remia pastangas skatinti kitas valstybes, OECD nares, imtis veiksmų, kad tapatybės vagystė būtų kriminalizuota.

Atkreiptinas dėmesys, kad JAV baudžiamosios teisės sistema yra labai sudėtinga, kadangi tuos pačius baudžiamosios teisės klausimus reguliuoja ir federalinė, ir valstijų baudžiamoji teisė, o federalinio baudžiamojo kodekso nėra. 1948 m. Kongreso įstatymu buvo iš naujo apsvarstyti ir pirmą kartą kodifikuoti visi federaliniai įstatymai. Įstatymai, reglamen-

[345] Internet Crime Report, 2010. *Internet Crime Complaint Center* [interaktyvus, žiūrėta 2011-09-19] <http://www.ic3.gov/media/annualreport/2010_ic3report.pdf>.

[346] *Ibid.*

tuojantys baudžiamosios teisės santykius, buvo įtraukti į JAV įstatymų sąvado 18 skirsnį „Nusikaltimai ir baudžiamasis procesas“.

JAV įstatymų sąvado 18 skirsnio 1 dalies 47 skyrius įtvirtina nusikaltimų, susijusių su sukčiavimu ir melagingais pareiškimais, sudėtį. Iš šio skyriaus detaliau reikėtų paanalizuoti keletą veikų, kurios susijusios su tapatybės vagystės atskirų stadijų kriminalizavimu. Pavyzdžiui, 1002 str. kriminalizuotas suklastotų dokumentų turėjimas, siekiant suklaidinti Jungtines Valstijas: tas, kas turėdamas tikslą suklaidinti Jungtines Valstijas ar bet kokią instituciją, turi suklastotą dokumentą, siekdamas suteikti kitam asmeniui gauti iš Jungtinių Valstijų bet kurios institucijos, valstybės tarnautojo ar atstovo bet kokią sumą pinigų, baudžiamas laisvės atėmimu iki 5 metų.

1028 str. numato baudžiamąją atsakomybę už sukčiavimą, susijusį su tapatybės nustatymo dokumentais, autentifikavimo priemonėmis ir informacija. Atskiruose šio straipsnio punktuose įtvirtintos atskirų nusikalstamų veikų sudėtys: 1 punkte – neteisėtas tapatybės nustatymo dokumento, autentifikavimo priemonės gaminimas ar tapatybės nustatymo dokumento klastojimas; 2 punkte – minėtų objektų perdavimas žinant, kad tokio pobūdžio dokumentas arba priemonė buvo pavogtas arba neteisėtai pagamintas; 3 punkte – 5 ir daugiau tapatybės nustatymo dokumentų, autentifikavimo priemonių ar suklastotų tapatybės nustatymo dokumentų turėjimas siekiant juos neteisėtai panaudoti ar perduoti; 4 punkte – tapatybės nustatymo dokumento, autentifikavimo priemonės ar suklastoto tapatybės nustatymo dokumento turėjimas tam, kad būtų galima panaudoti tokį dokumentą ar priemonę siekiant apgauti Jungtines Valstijas; 5 punkte – įrankių, skirtų dokumentams ar autentifikavimo priemonėms gaminti, gaminimas, perdavimas ar turėjimas, turint tikslą, kad toks dokumentų gaminimo įrankis ar autentifikavimo priemonė bus naudojama suklastotiems tapatybės nustatymo dokumentams gaminti arba kitam dokumentų gaminimo įrankiui ar autentifikavimo priemonei, kurie būtų naudojami tam pačiam tikslui, gaminti; 8 punkte – prekyba suklastotomis ar tikromis autentifikavimo priemonėmis, kurios naudojamos suklastotuose tapatybės nustatymo dokumentuose, dokumentų gamybos ar tapatybės nustatymo priemonėse. Baudžiamoji atsakomybė už minėtas veikas, atsižvelgiant į jų padarymo aplinkybes, gali būti iki 30 metų laisvės atėmimo (jei nusikalstama veika padaryta, siekiant palengvinti terorizmo aktą).

1998 m. JAV Kongresas Tapatybės vagystės ir apsimetinėjimo atgrasymo akte[347] (angl. *Identity Theft and Assumption Deterrence Act*) įtvirtino specifinės nusikalstamos veikos – tapatybės vagystės – sudėtį, kuri buvo įtvirtinta JAV įstatymų sąvado 18 skirsnio 1 dalies 47 skyriaus 1028 straipsnio (a) dalies (7) punkte. Baudžiamoji atsakomybė numatyta už tai, 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[348]. Bausmė, numatoma už tokį nusikaltimą, yra laisvės atėmimas iki penkerių metų, o jei nusikaltimas padarytas sunkinančiomis aplinkybėmis[349] – laisvės atėmimas iki penkiolikos metų.

1030 str. numato atsakomybę už sukčiavimą, naudojant kompiuterį. Pavyzdžiui, minėto straipsnio 2 d. numatyta baudžiamoji atsakomybė tam, kas naudojasi kompiuteriu, neturėdamas prisijungimo teisių arba viršydamas suteiktas prisijungimo teises, tokiu būdu gauna informaciją apie finansinių institucijų įrašus arba kortelės naudotoją, arba informaciją apie vartotojus, informaciją iš bet kurio JAV departamento ar agentūros ar informaciją iš bet kurio apsaugoto kompiuterio. Jei nusikalstama veika buvo atlikta siekiant komercinės naudos ar turint asmeninio finansinio pasipelnymo tikslą arba tokia nusikalstama veika buvo padaryta siekiant palengvinti nusikaltimo ar deliktinio pažeidimo padarymą, kuris laikomas Konstitucijos, Federacijos įstatymo ar bet kurios valstijos įstatymo pažeidimu, arba kai gautos informacijos vertė yra didesnė kaip 5 000 dolerių, baudžiama laisvės atėmimu iki 5 metų. 4 d. nustato atsakomybę tam, kas, turėdamas tikslą suklaidinti, prisijungia prie apsaugoto kompiuterio, neturėdamas prisijungimo teisių arba viršydamas prisijungimo teises, kad galėtų įvykdyti sukčiavimą, ir įgyja tai, kas turi vertę, išskyrus atvejus, kai sukčiavimo objektas ir įgytas dalykas susideda tik iš kompiuterio naudojimo ir jei tokio kompiu-

[347] Identity Theft and Assumption Deterrence Act, 1998 [interaktyvus, žiūrėta 2011-09-19]. <http://www.ftc.gov/os/statutes/itada/itadact.htm >.

[348] United States Code („U. S. C"), Title 18, Part I, Chapter 47, Section 1028 (a) (7). [interaktyvus, žiūrėta 2011-09-19]. <http://www.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00001028----000-.html>.

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

terio naudojimo vertė sudaro ne daugiau kaip 5 000 dolerių per vienerius metus. Už šį nusikaltimą baudžiama laisvės atėmimu iki 5 metų.

1037 str. kriminalizuotas sukčiavimas naudojant elektroninį paštą. Pavyzdžiui, pagal šio straipsnio 4 d. baudžiamojon atsakomybėn bus patrauktas tas asmuo, kuris naudodamas informaciją, kurios pagrindu suklastoja tikrojo vartotojo tapatybę, sukuria 5 ir daugiau elektroninio pašto dėžučių arba vartotojų, arba 2 ar daugiau domenų vardų ir inicijuoja masinį komercinio turinio elektroninio pašto žinučių siuntimą, naudodamasis sukurtomis pašto dėžutėmis ar domenų vardais. Už tokį nusikaltimą baudžiama laisvės atėmimu iki vienerių metų, o jei suklastojama 20 ir daugiau pašto dėžučių ar vartotojų registracijų arba buvo suklastojama 10 ir daugiau domenų vardų registracijų – laisvės atėmimu iki 3 metų, o jeigu darant nusikaltimą buvo siekiama įvykdyti nusikaltimą, kuris pagal Federacijos ar bet kurios valstijos įstatymus laikomas sunkiu, – laisvės atėmimu iki 5 metų.

Atlikus JAV įstatymų sąvado baudžiamosios teisės normų, reglamentuojančių atskirų nusikalstamų veikų sudėtis, galima daryti išvadą, kad visos trys tapatybės vagystės stadijos – su tapatybe susijusios informacijos gavimas, tokios informacijos turėjimas ir panaudojimas siekiant įvykdyti nusikaltimą – yra kriminalizuotos. Pirmoji stadija patenka į JAV įstatymų sąvado 18 skirsnio 1 dalies 47 skyriaus 1030 str., reglamentuojančio sukčiavimą, naudojant kompiuterį, veikimo sritį, antroji stadija patenka į 1002 str. (suklastotų dokumentų turėjimas) bei 1028 str., numatančio baudžiamąją atsakomybę už sukčiavimą, susijusį su tapatybės nustatymo dokumentais, autentifikavimo priemonėmis ir informacija (perdavimas, turėjimas, prekyba), veikimo sritį, o trečioji tapatybės vagystės stadija kriminalizuota minėtame 1028 str. (neteisėtas dokumentų, autentifikavimo priemonių ir informacijos gaminimas, klastojimas) bei 1037 str., kuriame numatoma baudžiamoji atsakomybė už sukčiavimą naudojant elektroninį paštą. Pažymėtina, kad antroji ir trečioji tapatybės vagystės stadijos kriminalizuotos 1028 straipsnio (a) dalies (7) punkte, įtvirtinančiame tapatybės vagystės, kaip savarankiškos nusikalstamos veikos, sudėtį.

Tapatybės vagystės elementų kriminalizavimas Jungtinėje Karalystėje

Jungtinė Karalystė – tai viena iš Konvencijos dėl elektroninių nusikaltimų iniciatorių, turinti didelę praktiką kovojant su elektroniniais nusikaltimais; šioje šalyje ypač daug dėmesio skiriama su tapatybe susiju-

sių nusikalstamų veikų prevencijai. Jungtinė Karalystė pagal nusikaltėlių, veikiančių elektroninėje erdvėje, skaičių užima antrą vietą pasaulyje[350].

Atkreiptinas dėmesys, kad Jungtinės Karalystės teisės aktuose, tapatybės nusikaltimai, kaip specifiniai teisės pažeidimai, nėra išskiriami, o tapatybės vagystė laikoma sudedamąja teisės pažeidimų arba nusikaltimų dalimi. Tačiau Kredito pramonės sukčiavimų prevencijos organizacija (angl. *Credit Industry Fraud Avoidance System*, toliau – CIFAS) tapatybės vagystės kriminalizavimu laiko 2006 m. Jungtinės Karalystės Tapatybės kortelių akto[351] (angl. *Identity Cards Act*) 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[352], ir Apgaulės aktą[353] (angl. *Fraud Act*), kuris įtvirtino apgaulę, kaip savarankišką baudžiamosios teisės pažeidimą, kuris gali būti atliekamas trim būdais: *neteisėtai atstovaujant*, *nesąžiningai nesuteikiant informacijos*, *piktnaudžiaujant įgaliojimais*. Pavyzdžiui, Tapatybės kortelių akto 25 skyriuje numatoma atsakomybė už suklastotų dokumentų turėjimą: pirmame poskyryje numatoma atsakomybė už suklastotų tapatybę patvirtinančių dokumentų arba tapatybę patvirtinančių dokumentų, kuriuos turintis asmuo žino, kad jie yra suklastoti, turėjimas, bet kokio tapatybę patvirtinančio dokumento, kuris buvo nesąžiningai įgytas, ir kai asmuo, turintis tokį dokumentą žino arba mano, kad jis buvo įgytas tokiu būdu, turėjimas, taip pat svetimų dokumentų turėjimas. Būtina sąlyga, kad kiltų atsakomybė, yra tikslas panaudoti tokį dokumentą siekiant įrodyti registruojamus faktus apie save arba tikslas leisti arba priversti kitą asmenį panaudoti tokį dokumentą siekiant įrodyti, nustatyti ar patvirtinti registruojamus faktus apie save arba apie kitą asmenį. Trečiame poskyryje nusikalstamu laikomas toks asmens elgesys, kai asmuo siekia

[350] Internet Crime Report, 2010. Internet Crime Complaint Center [interaktyvus, žiūrėta 2011-09-19]. <http://www.ic3.gov/media/annualreport/2010_ic3report.pdf>

[351] Identity Cards Act 2006 [interaktyvus, žiūrėta 2011-09-19]. <http://www.legislation.gov.uk/ukpga/2006/15/introduction>.

[352] Interneto tinklapis „Tapatybės vagystė; netapk auka“, sukurtas bendradarbiaujant Jungtinės Karalystės vyriausybei ir privačiam sektoriui [interaktyvus, žiūrėta 2011-09-19]. <https://www.identitytheft.org.uk/criminal-offences.asp>.

[353] Fraud Act 2006 [interaktyvus, žiūrėta 2011-09-19]. <http://www.opsi.gov.uk/acts/acts2006/pdf/ukpga_20060035_en.pdf>.

pagaminti, turėti ir kontroliuoti bet kokį įrenginį, gaminį ar duomenis, kurie yra arba buvo specialiai sukurti arba pritaikyti gaminti suklastotus tapatybę patvirtinančius dokumentus. Penktame poskyryje įtvirtinama, kad nusikalstamu laikomas toks asmens elgesys, kai jis be pateisinamos priežasties turi arba kontroliuoja suklastotą ar nesąžiningai įgytą arba svetimą asmens tapatybę patvirtinantį dokumentą arba įrenginį, gaminį ar duomenis, kurie yra arba buvo specialiai sukurti ar pritaikyti gaminti suklastotus tapatybę patvirtinančius dokumentus, arba skirti panaudoti klastojant dokumentus. Asmeniui, padariusiam pirmame arba trečiame poskyryje įtvirtintas nusikalstamas veikas, numatoma bauda arba laisvės atėmimas iki 10 metų, arba ir bauda, ir laisvės atėmimas iki 10 metų. Jei asmuo padaro nusikalstamą veiką, numatytą penktame poskyryje, jis baudžiamas bauda arba laisvės atėmimu iki 2 metų, arba ir bauda, ir laisvės atėmimu iki 2 metų; Anglijoje ir Velse, jei nuosprendis priimamas be prisiekusiųjų, – bauda arba laisvės atėmimu iki 12 mėn., arba ir bauda ir laisvės atėmimu iki 12 mėn., o Škotijoje ir Šiaurės Airijoje – bauda arba laisvės atėmimu iki 6 mėn., arba ir bauda, ir laisvės atėmimu iki 6 mėn.

Apgaulės akto 1 str. baudžiamoji atsakomybė numatoma už apgaulę, kuri gali būti įvykdoma trim būdais: *neteisėtai atstovaujant* (nesąžiningai, turint tikslą gauti naudos, padaryti arba sukelti pavojų patirti nuostolių), *nesąžiningai nesuteikiant informacijos* (kai asmuo turi teisinę pareigą tokią informaciją suteikti, tačiau jos nesuteikia, siekdamas gauti naudos sau ar kitam asmeniui arba sukelti nuostolių kitam asmeniui, arba kitam asmeniui sukelti pavojų patirti nuostolių), *piktnaudžiaujant įgaliojimais*. Už šias alternatyvias nusikalstamas veikas asmuo baudžiamas bauda arba laisvės atėmimu iki 12 mėn., arba ir bauda, ir laisvės atėmimu iki 12 mėn. (jei nuosprendis priimamas be prisiekusiųjų) arba bauda ar laisvės atėmimu iki 10 metų, arba ir bauda, ir laisvės atėmimu iki 10 metų.

Taip pat įtvirtinti nauji nusikaltimai, pavyzdžiui, nesąžiningas paslaugų gavimas. Apgaulės akto 11 str. numatyta, jog tas, kas gauna paslaugas sau arba kitam asmeniui su sąlyga, kad už jas buvo, yra arba bus sumokėta, tačiau šias paslaugas asmuo gauna už jas nesumokėjęs arba sumokėjęs ne visą sumą, siekdamas ir toliau už jas nemokėti arba mokėti ne visą sumą, už tokią veiką numatoma bauda arba laisvės atėmimas iki 5 metų, arba ir bauda, ir laisvės atėmimas iki 5 metų, arba bauda ar laisvės atėmimas iki 12 mėn., arba ir bauda, ir laisvės atėmimas iki 12 mėn. (jei

nuosprendis priimamas be prisiekusiųjų). 6 str. numatoma atsakomybė už priemonių, įskaitant bet kokių programų ar asmens duomenų, laikomų elektronine forma, skirtų apgaulei įvykdyti, ir kurios yra susijusios su tapatybės klastote, turėjimą; už šią veiką baudžiama bauda arba laisvės atėmimu iki 12 mėn. arba ir bauda, ir laisvės atėmimu iki 12 mėn. (jei nuosprendis priimamas be prisiekusiųjų), arba bauda ar laisvės atėmimu iki 5 metų, arba ir bauda, ir laisvės atėmimu iki 5 metų. 7 str. kriminalizuoja minėtų priemonių gaminimą ir tiekimą, žinant, kad jos sukurtos ar pritaikytos atlikti apgavikiškus veiksmus; už šią veiką baudžiama bauda arba laisvės atėmimu iki 12 mėn., arba ir bauda, ir laisvės atėmimu iki 12 mėn. (jei nuosprendis priimamas be prisiekusiųjų) arba bauda ar laisvės atėmimu iki 10 metų, arba ir bauda, ir laisvės atėmimu iki 10 metų.

Taip pat reikia paminėti 1990 m. Netinkamo naudojimosi kompiuteriais aktą[354] (angl. *Computer Misuse Act*), kurio pakeitimus vėliau nustatė 2006 m. Policijos ir teisingumo aktas[355] (angl. *Police and Justice Act*), numatantį baudžiamąją atsakomybę už elektroninius nusikaltimus. Pavyzdžiui, 1 str. kriminalizuota neteisėta prieiga prie kompiuterio duomenų: tas, kas pasinaudoja kompiuteriu atlikti bet kokią funkciją, turėdamas tikslą užtikrinti prieigą prie bet kokios kompiuterinės programos ar elektroninių duomenų, baudžiamas bauda arba laisvės atėmimu iki 2 metų, arba ir bauda, ir laisvės atėmimu iki 2 metų; Anglijoje ir Velse, jei nuosprendis priimamas be prisiekusiųjų, – bauda arba laisvės atėmimu iki 12 mėn., arba ir bauda, ir laivės atėmimu iki 12 mėn.; Škotijoje, jei nuosprendis priimamas be prisiekusiųjų, – bauda arba laisvės atėmimu iki 6 mėn., arba ir bauda, ir laisvės atėmimu iki 6 mėn. 2 str. kriminalizuota neteisėta prieiga prie kompiuterio duomenų, turint tikslą įvykdyti arba palengvinti kitas nusikalstamas veikas. Už šią veiką baudžiama laisvės atėmimu iki 5 metų; Anglijoje, Velse ir Škotijoje, jei nuosprendis priimamas be prisiekusiųjų, numatoma tokia pati bausmė, kaip nurodyta 1 str.

Atlikus Jungtinės Karalystės teisės aktų, numatančių baudžiamąją atsakomybę už nusikalstamas veikas, į kurių sudėtį patenka ir atskiri tapatybės vagystės elementai, galima teigti, jog nors Jungtinės Karalystės

[354] Computer Misuse Act 1990 [interaktyvus, žiūrėta 2011-09-19]. <http://www.legislation.gov.uk/ukpga/1990/18/contents>.

[355] Police and Justice Act 2006 [interaktyvus, žiūrėta 2011-09-19]. <http://www.legislation.gov.uk/ukpga/2006/48/contents>.

baudžiamuosiuose įstatymuose tapatybės vagystės, kaip savarankiškos nusikalstamos veikos, sudėtis nėra įtvirtinta, tapatybės vagystės pirmąją stadiją, t. y. su tapatybe susijusios informacijos gavimą, kriminalizuoja 1990 m. Netinkamo naudojimosi kompiuteriais akto 1 str. ir 2 str. (neteisėta prieiga prie kompiuterio duomenų), o antroji stadija – sąveika su tapatybe susijusia informacija – patenka į Tapatybės kortelių akto 25 skyriaus straipsnių (suklastotų, nesąžiningai įgytų, svetimų dokumentų turėjimas; įrenginio, gaminio ar duomenų, skirtų gaminti suklastotus tapatybę patvirtinančius dokumentus arba panaudoti klastojant dokumentus, turėjimas), Apgaulės akto 6 str. ir 7 str. (numato baudžiamąją atsakomybę už priemonių, laikomų elektronine forma, skirtų apgaulei įvykdyti, turėjimą, gaminimą ir tiekimą) veikimo sritį. Trečiosios tapatybės vagystės stadijos – su tapatybe susijusios informacijos panaudojimo siekiant įvykdyti nusikaltimą – kriminalizavimu galima laikyti Apgaulės akto 1 str. (neteisėtas atstovavimas, nesąžiningas informacijos nesuteikimas, piktnaudžiavimas įgaliojimais) ir 11 str. (nesąžiningas paslaugų gavimas).

Tapatybės vagystės elementų kriminalizavimas Nigerijoje

Nigerijos baudžiamojo įstatymo normų, kriminalizuojančių tapatybės vagystės elementus, analizė pasirinkta dėl to, kad Nigerija laikoma falsifikuotų internetinių tinklapių pradininke, o neįtikėtinas kiekis nepageidaujamų elektroninio pašto žinučių, platinamų iš Nigerijos, vis dar kelia didelį susirūpinimą ne tik pačiai Nigerijai, bet ir visam pasauliui. Be to, elektroninių nusikaltimų įvykdymo būdai vis sudėtingėja, ir Nigerijos rūpesčiu tapo nusikaltėliai, kurie pagrobia kreditinių ir debetinių banko kortelių PIN kodus, pasinaudodami tokiais metodais kaip falsifikuoti internetiniai tinklapiai, t. y. atakomis, kurios pagrįstos padirbtu kokios nors institucijos (pvz., banko) tinklalapiu: tinklalapis yra tiksliai nukopijuotas arba gali būti pavogtas ir atrodo bei funkcionuoja visiškai taip pat kaip reali svetainė, o asmuo gauna elektroninį paštą, kur teigiama, kad elektroninės bankininkystės sistema yra atnaujinama, todėl prašoma nurodyti prisijungimo duomenis, banko kortelės PIN kodą ir kitą asmeninio pobūdžio informaciją.

Nigerija pagal nusikaltėlių, veikiančių elektroninėje erdvėje, skaičių užima trečią vietą pasaulyje[356], todėl šalis šiuo metu bendradarbiauja su

[356] Internet Crime Report, 2009. Internet Crime Complaint Center [interaktyvus, žiūrėta 2011-09-19]. <http://www.ic3.gov/media/annualreport/2010_ic3report.pdf>.

JAV vyriausybe, mėgindama gelbėti savo reputaciją ir atsikratyti įvaizdžio, kad ji yra elektroninių nusikaltimų ir liūdnai pagarsėjusių falsifikuotų internetinių tinklapių ašis, bei kovoti su elektroniniais nusikaltimais. Šalies įvaizdžiui didžiulę neigiamą įtaką padarė elektroniniai laiškai su nuorodomis į falsifikuotus internetinius tinklapius; šie laiškai, kaip juose melagingai buvo teigiama, buvo platinami Nigerijos institucijų.

Iš elektroninių nusikaltimų įvykdymo būdų Nigerijoje labiausiai paplitę būtent apgaulingi elektroniniai laiškai, kurie Nigerijoje ir visame pasaulyje žinomi kaip „apgaulė 419". Skaičius 419 yra nuoroda į straipsnį Nigerijos baudžiamajame kodekse, kuris numato baudžiamąją atsakomybę už sukčiavimą, kai neteisėtais būdais mėginama iš kito asmens išvilioti pinigus. Tokie sukčiai visuomet veikia pagal tą pačią schemą: asmuo paprastai gauna elektroninį laišką iš užsienio, kuriame banko ar kokios nors šeimos atstovu prisistatantis sukčius siūlo pasidalyti didelę sumą pinigų. Iš aukos paprašoma asmens duomenų, pavyzdžiui, banko sąskaitos numerio, ir pasiūloma susimokėti pinigų pervedimo, tarpininkavimo ar kitus neegzistuojančius mokesčius. Gavę reikalaujamą sumą, sukčiai tiesiog dingsta.

Nigerijos baudžiamojo kodekso[357] 38 skyrius numato baudžiamąją atsakomybę už nuosavybės įgijimą apgaulės būdu, sukčiavimą. 419 str. numatoma, kad asmuo, kuris apgaulės būdu, turėdamas tikslą suklaidinti, iš kito asmens įgyja bet ką, kas gali būti pavogta, arba įtikina kitą asmenį perduoti bet ką, kas gali būti pavogta, yra laikomas padariusiu sunkų nusikaltimą ir baudžiamas laisvės atėmimu iki trejų metų, o jei nusikaltimo dalyko vertė 1 tūkst. ir daugiau narių[358] – laisvės atėmimu iki septynerių metų. 421 str. numato, kad asmuo, kuris, naudodamasis apgavikiškomis priemonėmis ar įrenginiais, iš kito asmens įgyja bet ką, kas gali būti pavogta, arba įtikina kitą asmenį perduoti bet ką, kas gali būti pavogta, arba sumokėti ar perduoti pinigus arba prekes, arba didesnę sumą pinigų, arba didesnį kiekį prekių, nei kad turėjo būti sumokėta ar pristatyta, yra laikomas padaręs baudžiamąjį nusižengimą ir baudžiamas laisvės atėmimu iki dvejų metų.

17 skyrius reglamentuoja nusikalstamas veikas, susijusias su pašto ir telekomunikacijų paslaugomis. Pavyzdžiui, 161 str. įtvirtinta, kad asmuo,

[357] Nigerijos baudžiamasis kodeksas [interaktyvus, žiūrėta 2011-09-19]. <http://www.nigeria-law.org/Criminal%20Code%20Act-Tables.htm>.

[358] Naira (NGN) – Nigerijos nacionalinis piniginis vienetas. 1 LTL ~ 61 NGN.

kuris sulaiko paštą, turėdamas tikslą apieškoti ar pagrobti pašto korespondencijos siuntą, laikomas padaręs sunkų nusikaltimą ir baudžiamas laisvės atėmimu iki gyvos galvos. 162 str. nustatyta, kad asmuo, kuris neteisėtai paslepia ar sunaikina bet kokią pašto korespondencijos siuntą ar telegramą arba dalį jų, laikomas padaręs sunkų nusikaltimą ir baudžiamas laisvės atėmimu iki 7 metų, o jei pašto korespondencijos siuntoje, kuri buvo paslėpta ar sunaikinta, bus pinigų ar kitokio kilnojamojo turto, ar bet koks vertingas vertybinis popierius, baudžiamas laisvės atėmimu iki gyvos galvos.

44 skyrius įtvirtina nusikalstamų veikų, susijusių su klastojimu, sudėtis. Pavyzdžiui, šio skyriaus 467 str. numato baudžiamąją atsakomybę už klastojimą: asmuo, kuris suklastoja bet kokį dokumentą ar antspaudą, laikomas padaręs sunkų nusikaltimą ir baudžiamas laisvės atėmimu iki 3 metų, jeigu nenumatyta kitaip.

Pažymėtina, kad Nigerijos baudžiamajame kodekse yra atskiras 46 skyrius, kuris numato baudžiamąją atsakomybę už apsimetimą kitu asmeniu. Šio skyriaus 484 str. įtvirtinta, kad asmuo, siekdamas apgauti kitą asmenį, melagingai save pristato kaip kitą asmenį, kuris yra gyvas ar miręs, laikomas padaręs sunkų nusikaltimą ir baudžiamas laisvės atėmimu iki 3 metų, o jei tokiu būdu save pristatantis nusikaltimo subjektas apsimeta kitu asmeniu, kuris turi teises į testamente ar įstatyme nustatytą nuosavybę, ir jis įvykdo nusikalstamą veiką, kad įgytų tokią nuosavybę ar pareigas, baudžiamas laisvės atėmimu iki 14 metų.

486 str. numato baudžiamąją atsakomybę asmeniui, kuris išleidžia į apyvartą bet kokį dokumentą, kurį kitam asmeniui išdavė teisėta institucija, kai toks dokumentas patvirtina asmens įgytą kvalifikaciją, užimamas pareigas, teisę užsiimti tam tikra profesija, prekyba, verslu ar turimas teises arba privilegijas, arba laipsnį ar padėtį, ir apgaulės būdu save pristato kaip tą asmenį, kurio vardu išduotas dokumentas, laikomas padaręs tokį patį nusikaltimą ir baudžiamas tokia pačia bausme kaip už dokumentų klastojimą – laisvės atėmimu iki 3 metų, išskyrus specialiai numatytas išimtis. Tokia pati bausmė numatoma ir už teisėto savininko minėto pobūdžio dokumentų pardavimą, perdavimą ar paskolinimą kitam asmeniui, kad šis galėtų apsimesti tuo asmeniu, kuriam toks dokumentas buvo išduotas (487 str.).

488 str. įtvirtinta baudžiamojo nusižengimo sudėtis: asmuo, kuris turėdamas tikslą gauti darbą, išleidžia į apyvartą tokį dokumentą, kaip

kito asmens rekomendacija ar charakteristika, laikomas padaręs baudžiamąjį nusižengimą ir baudžiamas laisvės atėmimu iki vienerių metų. Jei tokio pobūdžio dokumentą asmuo, kuriam jis buvo suteiktas, perduoda, parduoda ar paskolina kitam asmeniui, žinodamas, kad tas asmuo gali panaudoti tokį dokumentą, siekdamas gauti darbą, baudžiamas laisvės atėmimu iki 3 metų.

Atlikus Nigerijos baudžiamojo kodekso teisės normų analizę, galima daryti išvadą, kad Nigerijos baudžiamajame kodekse tapatybės vagystės, kaip savarankiškos nusikalstamos veikos, sudėtis nėra įtvirtinta, tačiau atskiri tapatybės vagystės elementai patenka į kitas nusikalstamas veikas reglamentuojančių straipsnių veikimo sritį. Už pirmąją tapatybės vagystės stadiją – su tapatybe susijusios informacijos gavimą – baudžiamoji atsakomybė numatoma pagal 161 str., 162 str. reglamentuojančias nusikalstamas veikas, susijusias su pašto ir telekomunikacijų paslaugomis, ar pagal 419 str., 421 str., numatančius baudžiamąją atsakomybę už nuosavybės įgijimą apgaulės būdu, sukčiavimą. Atsakomybė už antrąją stadiją – sąveiką su tapatybe susijusia informacija (pardavimą, perdavimą, paskolinimą) – numatyta 487 str., tačiau antrosios stadijos elementas – su tapatybe susijusios informacijos turėjimas – pagal Nigerijos baudžiamąjį kodeksą baudžiamosios atsakomybės neužtraukia. Trečioji tapatybės vagystės stadija patenka į Nigerijos baudžiamojo kodekso 44 skyriaus normų (pavyzdžiui, 467 str.), įtvirtinančių nusikalstamų veikų, susijusių su klastojimu, sudėtis, veikimo sritį, 46 skyriaus normų (484 str., 486 str., 488 str.), numatančių baudžiamąją atsakomybę už apsimetimą kitu asmeniu, bei į jau minėtų 419 str., 421 str., kriminalizuojančių nuosavybės įgijimą apgaulės būdu, sukčiavimą, veikimo sritį.

Tapatybės vagystės elementų kriminalizavimas Prancūzijoje

Prancūzija – Europos Sąjungos valstybė, civilinės teisės atstovė, padariusi didžiulį poveikį civilinės teisės raidai Europoje. Prancūzijos teisė tapo pavyzdine daugeliui valstybių, kuriančių savo teisę (pvz., Belgijai, Olandijai, Italijai), atsižvelgiant į tai, buvo pasirinkta ir šios valstybės baudžiamojo kodekso normų analizė, siekiant nustatyti, ar Prancūzijoje tapatybės vagystė yra kriminalizuota.

2006 m. sausio 10 d. Prancūzija ratifikavo Konvenciją dėl elektroninių nusikaltimų, kuri šalyje įsigaliojo 2006 m. gegužės 1 d., tačiau paste-

bėtina, kad Prancūzijos baudžiamasis įstatymas tapatybės vagystės, kaip atskiros nusikalstamos veikos sudėties, nenumato, o tapatybės vagystės elementai patenka į kitų nusikalstamų veikų sudėtis.

Prancūzijos baudžiamojo kodekso[359] 226-15 str. numato atsakomybę už susižinojimo slaptumo pažeidimą: tyčinis siunčiamos korespondencijos atidarymas, sunaikinimas, sulaikymas ar nukreipimas, nepriklausomai nuo to, ar ji pasiekia adresatą, arba jos turinio sužinojimas apgaulės būdu, baudžiamas laisvės atėmimu ir 45 000 EUR bauda. Analogiška bausmė numatoma ir už tyčinį siunčiamos korespondencijos perėmimą, nukreipimą, naudojimą ar paskelbimą, kai susirašinėjimas perduodamas ar gaunamas telekomunikacijos priemonėmis arba įdiegiant įrenginius, specialiai sukurtus tokiam susirašinėjimui perimti.

Paminėtinas ir 226-18 str., kuriame numatoma baudžiamoji atsakomybė už duomenų rinkimą apgaulingomis, nesąžiningomis ar neteisėtomis priemonėmis, ar informacijos apie asmenį apdorojimą prieš jo valią, kai prieštaravimas turi teisinį pagrindą. Už šį nusikaltimą baudžiama laisvės atėmimu iki 5 metų ir 300 000 EUR bauda.

313-1 str. numato atsakomybę už turto įsigijimą apgaulės būdu: asmuo, kuris klaidina kitus asmenis, naudodamasis netikru vardu arba netikromis pareigomis, piktnaudžiaudamas įgaliojimais arba naudodamasis neteisėtomis priemonėmis, ir taip įtikina kitą asmenį jo arba trečiosios šalies nenaudai perduoti pinigines lėšas, brangenybes ar kitą turtą, suteikti paslaugas arba sutikti prisiimti įsipareigojimus ar atleisti nuo jų, baudžiamas laisvės atėmimu iki 5 metų ir 375 000 EUR bauda.

Pažymėtina, kad 3 skyrius reglamentuoja neteisėtą prieigą prie automatizuotų duomenų tvarkymo sistemų. Pavyzdžiui, šio skyriaus 323-1 str. kriminalizuota neteisėta prieiga apgaulės būdu prie automatizuotos duomenų tvarkymo sistemos, už kurią baudžiama laisvės atėmimu iki 1 metų ir 15 000 EUR bauda. Jei tokiais veiksmais sistemos duomenys pakeičiami arba sutrikdomas sistemos darbas, baudžiama laisvės atėmimu iki 2 metų ir 30 000 EUR bauda.

Prancūzijos baudžiamojo kodekso 441-2 str. kriminalizuotas valstybės institucijos išduoto dokumento klastojimas turint tikslą suteikti teisę, tapatybę ar kompetenciją arba suteikti įgaliojimus. Asmuo už

[359] Prancūzijos baudžiamasis kodeksas [interaktyvus, žiūrėta 2011-09-19]. <http://www.legislationline.org/documents/section/criminal-codes>.

šį nusikaltimą baudžiamas laisvės atėmimu iki 5 metų ir 75 000 EUR bauda. 441-3 str. numato baudžiamąją atsakomybę už neteisėtą bet kokio dokumento gavimą iš viešojo administravimo ar viešąsias paslaugas teikiančios institucijos apgaulės būdu, siekiant suteikti teisę, tapatybę ar kompetenciją arba suteikti įgaliojimus. Už šį nusikaltimą nustatyta bausmė – laisvės atėmimas iki 2 metų ir 30 000 EUR bauda.

Atlikus Prancūzijos baudžiamojo kodekso normų analizę, matyti, kad tapatybės vagystės, kaip atskiros nusikalstamos veikos, sudėtis nėra įtvirtinta, tačiau Prancūzijos baudžiamojo įstatymo tam tikros normos numato atsakomybę už atskirus tapatybės vagystės elementus. 1-ąją tapatybės vagystės stadiją – su tapatybe susijusios informacijos gavimą – kriminalizuoja Prancūzijos baudžiamojo kodekso 226-15 str. (susižinojimo slaptumo pažeidimas: korespondencijos atidarymas, sulaikymas, nukreipimas), 226-18 str. (duomenų rinkimas apgaulingomis, nesąžiningomis ar neteisėtomis priemonėmis), 323-1 str. (neteisėta prieiga prie automatizuotų duomenų tvarkymo sistemų), 441-3 str. (neteisėtas dokumento gavimas). Antroji tapatybės vagystės stadija – sąveika su tapatybe susijusia informacija (naudojimas, paskelbimas, apdorojimas) – patenka į 226-15 str., 226-18 str. veikimo sritį, tačiau antrosios stadijos elementas – su tapatybe susijusios informacijos turėjimas – Prancūzijos baudžiamajame kodekse nėra kriminalizuotas. Trečiosios tapatybės vagystės stadijos – su tapatybe susijusios informacijos panaudojimas siekiant įvykdyti nusikaltimą – kriminalizavimu galima laikyti 313-1 str. (turto įgijimas apgaulės būdu) ir 441-2 str., numatančius atsakomybę už dokumentų klastojimą.

Tapatybės vagystės elementų kriminalizavimas Suomijoje

Suomija – Europos Sąjungos valstybė, turinti gilias informacijos saugos tradicijas. Pirmoji nacionalinė informacijos apsaugos strategija Suomijoje buvo priimta 2003 m. 2005 m. Duomenų apsaugos ombudsmenas Reijo Aarnio savo ataskaitoje[360] pabrėžė, kad tapatybės vagystė Suomijoje, lyginant su kitomis valstybėmis, yra santykinai nedidelė problema, vis dėlto padidėjęs elektroninių paslaugų ir mobiliojo ryšio naudojimas lėmė tai, jog problema tapo aktuali ir Suomijai. 2008 m. buvo susirūpinta, kad Suomijoje tapatybės vagystė tampa įprastu reiškiniu. 2007 m. gegužės

[360] Review 2005 of the Data Protection Ombudsman [interaktyvus, žiūrėta 2011-09-19]. <www.tietosuoja.fi/uploads/q0vw1ft5.rtf>.

24 d. ši valstybė ratifikavo Konvenciją dėl elektroninių nusikaltimų, kuri šalyje įsigaliojo nuo 2007 m. rugsėjo 1 d.

Suomijos baudžiamojo kodekso[361] 16 skyriaus 5 str. numatoma baudžiamoji atsakomybė už apgaulingą identifikuojančios informacijos pateikimą: tas, kas, turėdamas tikslą suklaidinti valdžios instituciją, nurodo klaidingą vardą arba kitaip pateikia neteisingą ar klaidinančią informaciją, nustatant tapatybę, ar šiam tikslui panaudoja kito asmens tapatybės kortelę, pasą, vairuotojo pažymėjimą ar kitą identifikuojantį dokumentą, baudžiamas bauda arba laisvės atėmimu iki 6 mėn. 8 str. 1 d. kriminalizuoja suklastotų dokumentų pateikimą valstybinei institucijai: tas, kas valstybinei institucijai pateikia teisiškai svarbų suklastotą rašytinį dokumentą ar panašų procedūrinį protokolą, arba pagamintą tokį dokumentą ar protokolą perduoda kitam asmeniui, kad šis asmuo juos naudotų tam pačiam tikslui, baudžiamas bauda arba laisvės atėmimu iki 6 mėn. 9 str. numato baudžiamąją atsakomybę už apsimetimą valdžios pareigūnu: tas, kas siekdamas suklaidinti kitą asmenį, neturėdamas teisės imasi priemonių, kurių imtis gali tik kompetentingas pareigūnas, vykdantis viešosios valdžios funkcijas, arba kitu būdu pristato save kaip valstybės pareigūną, atliekantį pareigas ir vykdantį viešosios valdžios funkcijas, baudžiamas bauda arba laisvės atėmimu iki 6 mėn.

24 skyriaus 5 str. kriminalizuotas slaptas pasiklausymas: asmuo, kuris neteisėtai klausosi arba naudodamasis techninėmis priemonėmis įrašo diskusiją, pokalbį arba kitus privataus gyvenimo garsus privačioje teritorijoje, arba slapta neteisėtai kitose vietose klausosi pokalbio tokiomis aplinkybėmis, kai pokalbio dalyvis neturi pagrindo manyti, kad trečioji šalis klausosi pokalbio, baudžiamas bauda arba laisvės atėmimu iki vienerių metų. 8 str. 1 d. numatyta baudžiamoji atsakomybė už informacijos, pažeidžiančios asmens privatumą, platinimą: asmuo, kuris neteisėtai, naudodamasis masinėmis informavimo priemonėmis arba pasinaudodamas kitu būdu, daugeliui asmenų platina informaciją, šmeižiančius prasimanymus ar privataus gyvenimo vaizdus apie kitą asmenį, ir šie veiksmai padaro asmeniui žalos arba priverčia kentėti, arba užtraukia asmeniui nešlovę, baudžiamas bauda arba laisvės atėmimu iki 2 metų.

[361] Suomijos baudžiamasis kodeksas [interaktyvus, žiūrėta 2011-09-19]. <http://www.legislationline.org/documents/section/criminal-codes>.

36 skyrius kriminalizuoja sukčiavimą ir kitus nesąžiningus veiksmus. 1 str. įtvirtinama, kad asmuo, kuris siekdamas neteisėtai įgyti finansinės naudos sau ar kitam asmeniui arba kitam asmeniui padaryti žalos, suklaidina kitą asmenį arba dėl kito asmens klaidos gauna naudos, kai šis asmuo atlieka tam tikrus veiksmus arba susilaiko nuo tam tikrų veiksmų atlikimo ir dėl to patiria ekonominių nuostolių arba nuostolius patiria kitas asmuo, kurio turtu disponuoja apgautasis, baudžiamas bauda arba laisvės atėmimu iki 2 metų. Jei asmuo, turėdamas minėtą tikslą, gali prieiti prie duomenų ir juos pakeisdamas, sunaikindamas, ištrindamas ar kitaip sutrikdydamas duomenų sistemos darbą suklastoja galutinį duomenų apdorojimo procesą ir dėl to kitas asmuo patiria ekonominių nuostolių, baudžiamas tokia pačia bausme, kuri numatyta už sukčiavimą.

38 skyriuje įtvirtintos nusikalstamų veikų, susijusių su duomenimis ir susižinojimu, sudėtys. 3 str. numato baudžiamąją atsakomybę už žinutės perėmimą: asmuo, kuris neteisėtai atplėšia laišką ar kitą pranešimą, adresuotą kitam asmeniui, ar susipažįsta su elektroninės ar kitokiu techniniu būdu įrašytos žinutės turiniu, kuris yra apsaugotas nuo trečiųjų asmenų, arba įgyja informacijos iš telefoninio pokalbio, telegramos, siunčiamo teksto, vaizdų ar duomenų arba kitokios panašios žinutės, perduodamos telekomunikacijų tinklais perdavimo ar gavimo metu, baudžiamas bauda arba laisvės atėmimu iki vienerių metų. 7 d. str. kriminalizuoja įsilaužimą į kompiuterinę sistemą: asmuo, kuris siekdamas kitam padaryti žalos ar sukelti ekonominių nuostolių, įsilaužia į kompiuterinę sistemą, perduoda, sugadina, pakeičia ar ištrina duomenis ar kitokiais panašiais neteisėtais veiksmais sutrikdo kompiuterinės sistemos veikimą, baudžiamas bauda arba laisvės atėmimu iki 2 metų. 8 str. numatoma atsakomybė už įsilaužimą į kompiuterį: asmuo, kuris naudodamasis svetimu prisijungimo kodu arba kitokiu būdu apeina apsaugos sistemą ir neteisėtai įsilaužia į kompiuterinę sistemą, kurioje duomenys apdorojami, saugomi ar elektroniniu arba kitu panašiu techniniu būdu perduodami, arba įsilaužia į atskirą apsaugotą tokios sistemos dalį, baudžiamas bauda arba laisvės atėmimu iki vienerių metų. Analogiška bausme asmuo baudžiamas už tai, kad naudodamas specialius techninius įrenginius, net neįsilaužęs į kompiuterinę sistemą, įgyja kompiuterinėje sistemoje esančią informaciją. 9 str. numato, kad asmuo, kuris apdoroja kito asmens duomenis, turėdamas tikslą, nesuderinamą su Asmens duomenų įstatymo reikalaujamu tikslu, kai bū-

tina tokio apdorojimo sąlyga yra būtinumas ir duomenų integralumas, svarbūs duomenys, identifikavimo kodai ar asmens duomenys apdorojami specifiniais tikslais ar pažeidžiant numatytas asmens duomenų apdorojimo sąlygas, arba pateikdamas suklastotą ar klaidinančią informaciją neleidžia arba siekia neleisti asmens duomenų subjektui pasinaudoti savo teise patikrinti, arba perduoda asmens duomenis šalims, kurios nėra Europos Sąjungos ar Europos ekonominės erdvės narės, pažeidžia Asmens duomenų įstatymo 5[362] skyrių ir asmens duomenų subjekto privatumą arba sukelia jam žalos ar sudaro didelių nepatogumų, baudžiamas bauda arba laisvės atėmimu iki vienerių metų.

Atlikus Suomijos baudžiamojo kodekso teisės normų analizę, nustatyta, kad elektroniniai nusikaltimai kriminalizuoti plačiu mastu, tačiau tapatybės vagystės, kaip savarankiškos nusikalstamos veikos, sudėtis nėra įtvirtinta. Tačiau tapatybės vagystės elementai patenka į baudžiamojo įstatymo straipsnių veikimo sritį ir už juos numatyta baudžiamoji atsakomybė. Tapatybės vagystės pirmąją stadiją – su tapatybe susijusios informacijos gavimą – kriminalizuoja Suomijos baudžiamojo kodekso 24 skyriaus 5 str., 38 skyriaus 3 str., 8 str., tapatybės vagystės antrosios stadijos – sąveikos su tapatybe susijusios informacijos (platinimas, apdorojimas, perdavimas) – kriminalizavimu galima laikyti 25 skyriaus 8 str. 1 d., 38 skyriaus 9 str. Tapatybės vagystės trečioji stadija – su tapatybe susijusios informacijos panaudojimas siekiant įvykdyti nusikaltimą – patenka į Suomijos baudžiamojo kodekso 16 skyriaus 5 str., 9 str., 36 skyriaus 1 str., 38 skyriaus 8 str. veikimo sritį. Tačiau pažymėtina, kad tapatybės vagystės antrosios stadijos elementas – su tapatybe susijusios informacijos turėjimas – Suomijos baudžiamajame kodekse nėra kriminalizuotas.

Tapatybės vagystės elementų kriminalizavimas Estijoje

Estija – valstybė, panaši į Lietuvą, tačiau pagal naujausius ekonominės ir socialinės raidos Baltijos šalyse rodiklius vis labiau lenkia savo kaimynes Lietuvą ir Latviją. Ši valstybė yra viena iš tų, kuri gali didžiuotis labiausiai išvystytomis informacinėmis technologijomis. Tačiau tai dar nereiškia,

[362] Pagrindinis šiame skyriuje įtvirtintas asmens duomenų perdavimo už Europos Sąjungos ribų principas yra tas, kad asmens duomenys gali būti perduodami šalims, kurios nėra Europos Sąjungos ar Europos ekonominės erdvės narės, tik su sąlyga, kad kita šalis užtikrins pakankamą duomenų apsaugos lygį.

kad, lyginant Estiją su kitomis valstybėmis, pažeidėjų dalis yra proporcingai mažesnė. Pažymėtina, kad Estija labai pasitiki savo informacinių technologijų infrastruktūra, pavyzdžiui, elektroninėje erdvėje atliekamos dauguma banko operacijų, taip pat įgyvendinta elektroninio balsavimo galimybė, funkcionuoja daugybė elektroninės valdžios paslaugų.

2003 m. gegužės 12 d. Estija ratifikavo Konvenciją dėl elektroninių nusikaltimų, kuri įsigaliojo 2004 m. liepos 1 d. Estija tarptautinėje bendruomenėje ėmėsi iniciatyvos kovoti su elektroniniais nusikaltimais po plataus masto išpuolių prieš privataus ir viešojo sektoriaus kompiuterines sistemas 2007 m.

Kalbant apie tapatybės vagystės ar jos elementų kriminalizavimą, Estijos baudžiamojo kodekso[363] 156 str. numato, kad už pranešimo konfidencialumo pažeidimą baudžiama pinigine bauda, o jei šis pažeidimas buvo atliktas asmens, kuris turi prieigą prie siunčiamų pranešimų dėl savo oficialių pareigų, baudžiama pinigine bauda arba laisvės atėmimu iki vienerių metų.

157(1) str. yra numatyta atsakomybė už neteisėtą svarbių asmens duomenų atskleidimą. Baudžiamajame kodekse numatyta, kad neteisėtas svarbių asmens duomenų atskleidimas, prieigos prie tokio pobūdžio duomenų sudarymas arba tokių duomenų perdavimas siekiant asmeninės naudos, jei padaroma didelė žala kito asmens teisėms ar teisėtiems interesams, baudžiamas pinigine bausme arba laisvės atėmimu iki vienerių metų. Svarbių asmens duomenų sąrašas įtvirtintas Estijos asmens duomenų apsaugos įstatymo 4 str., kuriame svarbiais asmens duomenimis laikoma: duomenys, atskleidžiantys politinius, religinius, filosofinius įsitikinimus, duomenys, susiję su etnine ar rasine kilme, sveikata ar negalia, duomenys apie genetinę informaciją, biometriniai duomenys, duomenys, susiję su lytiniu gyvenimu, naryste prekybos organizacijose, informacija, susijusi su teisės pažeidimo padarymu arba nukentėjusiuoju iki viešo teismo posėdžio, kurio metu byla nagrinėjama iš esmės arba teisminė byla nutraukiama.

209 str. įtvirtina sukčiavimo sudėtį: asmuo, kuris gauna asmeninės naudos priversdamas tyčia klaidingai įvertinti egzistuojančius faktus, baudžiamas pinigine bauda arba laisvės atėmimu iki 3 metų.

[363] Estijos baudžiamasis kodeksas [interaktyvus, žiūrėta 2011-09-19]. <http://www.legislationline.org/download/action/download/id/1280/file/4d16963509db70c09d23e52cb8df.htm/preview>.

213 str. numato atsakomybę už sukčiavimą, susijusį su kompiuteriu: asmuo, kuris gauna asmeninės naudos neteisėtai prisijungdamas prie kompiuterio, pakeisdamas, ištrindamas ar užblokuodamas kompiuterines programas arba duomenis arba kitokiu būdu neteisėtai įsikišdamas į duomenų apdorojimo procesą, baudžiamas pinigine bauda arba laisvės atėmimu iki 5 metų.

217 str. kriminalizuoja neteisėtą kompiuterių, kompiuterinių sistemų ar tinklų naudojimą, kai pašalinami kodai, slaptažodžiai ar kitos apsaugos priemonės. Už šią nusikalstamą veiką baudžiama pinigine bauda, o jei ji sukelia didelės žalos arba padaroma pasinaudojant valstybės paslaptimi ar kompiuteriu, kompiuterine sistema ar tinklu, kuriuose esanti informacija skirta tik tarnybos reikmėms, – pinigine bauda arba laisvės atėmimu iki 3 metų. 217^1 str. numato baudžiamąją atsakomybę už galinių įrenginių, kai neteisėtai pašalinamos ar pakeičiamos identifikavimo priemonėmis, naudojimą, baudžiant pinigine bauda arba laisvės atėmimu iki 3 metų.

280 str. kriminalizuotas apgaulingos informacijos pateikimas: asmuo, kuris pateikia apgaulingą informaciją viešojo administravimo institucijai, siekdamas įgyti oficialų dokumentą ar bet kokios naudos ar pelno, baudžiamas pinigine bauda arba laisvės atėmimu iki vienerių metų.

Estijos baudžiamojo kodekso 299 str. numatyta baudžiamoji atsakomybė už pareigūnų atliekamą oficialių dokumentų klastojimą: pareigūnas, kuris klastoja dokumentą ar išleidžia suklastotą dokumentą, baudžiamas pinigine bauda arba laisvės atėmimu iki 3 metų.

347 straipsnyje numatyta baudžiamoji atsakomybė už svarbaus identifikuojančio dokumento klastojimą. Nurodyta, kad asmuo už svarbaus tapatybės dokumento klastojimą baudžiamas pinigine bauda arba laisvės atėmimu iki 5 metų, o už tą patį nusikaltimą juridinis asmuo gali būti baudžiamas bauda.

Taip pat numatyta atsakomybė už apgaulingą svarbių tapatybės dokumentų naudojimą: 349 str. įtvirtinta laisvės atėmimo bausmė iki 3 metų asmeniui, kuris naudoja svarbų tapatybės dokumentą, išduotą kitam asmeniui, arba suteikia leidimą kitam asmeniui naudotis svarbiu tapatybės dokumentu, išduotu jo vardu, turėdamas tikslą įgyti teisių arba būti atleistas nuo įsipareigojimų. 350 str. pateikiamas baigtinis svarbių tapatybės dokumentų sąrašas, į kurį patenka tokie dokumentai, kaip tapatybės kortelė, Estijos piliečio pasas, diplomatinis pasas, jūreivio tarnybos

įrašų knyga, užsieniečio pasas, laikinas kelionės dokumentas, pabėgėlio kelionės dokumentas, Estijos laivų sertifikatas teikti paslaugas, grįžimo pažymėjimas, motorinės transporto priemonės vairuotojo pažymėjimas.

Atlikus Estijos baudžiamojo kodekso teisės normų analizę, nustatyta, kad tapatybės vagystės, kaip savarankiškos nusikalstamos veikos, sudėtis nėra įtvirtinta. Tačiau tam tikri tapatybės vagystės elementai patenka į baudžiamojo įstatymo straipsnių veikimo sritį ir už juos numatyta baudžiamoji atsakomybė. Tapatybės vagystės pirmąją stadiją – su tapatybe susijusios informacijos gavimą – kriminalizuoja Estijos baudžiamojo kodekso 156 str., 217 str. tapatybės vagystės antrosios stadijos – sąveikos su tapatybe susijusios informacijos atskleidimas ir perdavimas – kriminalizavimu galima laikyti 157(1) str., 349 str. Tapatybės vagystės trečioji stadija – su tapatybe susijusios informacijos panaudojimas siekiant įvykdyti nusikaltimą – patenka į Estijos baudžiamojo kodekso 209 str., 213 str., 280 str., 299 str., 347 str., 349 str. Tačiau pažymėtina, kad tapatybės vagystės antrosios stadijos elementas – su tapatybe susijusios informacijos turėjimas – Estijos baudžiamajame kodekse nėra kriminalizuotas.

Tapatybės vagystės elementų kriminalizavimas Rusijoje

Analizuoti tapatybės vagystės kriminalizavimą Rusijoje lėmė tai, kad šioje šalyje itin klesti nusikaltimai elektroninėje erdvėje. Rusijoje, ypač Maskvoje ir Sankt Peterburge, neteisėtas informacijos apie privačius asmenis ir įvairias organizacijas rinkimas ir tokio pobūdžio informacijos platinimas yra įprastas reiškinys. Gana populiarios yra duomenų bazės apie perkamus / parduodamus automobilius, jų savininkus; kaupiami pasų duomenys, duomenys apie nekilnojamąjį turtą (pirkimą, pardavimą, parametrus, buvimo vietą, savininkus), taip pat apie mokesčių mokėtojus, ieškomus asmenis, kurie įtariami padarę nusikalstamas veikas, ir tuos, kurie buvo nuteisti. Pigūs kompaktiniai diskai su minėto turinio informacija yra lengvai prieinami tiesiog gatvėje arba internetu. Pavyzdžiui, 2003 m. sausio mėn. pasirodė diskas su detalia informacija apie 5 mln. vieno Rusijos mobiliojo ryšio operatoriaus klientus[364], 2004 m. rudenį – diskas su detalia informacija apie mokesčių mokėtojų pajamas.

[364] Personal Data Is Pirated From Russian Phone Files. *The New York Times* [interaktyvus]. 2003-01-23 [žiūrėta 2011 09 19]. < http://www.nytimes.com/2003/01/23/business/personal-data-is-pirated-from-russian-phone-files.html>.

Manoma, kad vien Rusijos bankai dėl tapatybės vagysčių praranda daugiau nei 4 mlrd. eurų per metus. Pasauliniai technologijų ir finansų verslo lyderiai kartu su teisėsaugos institucijomis, orientuotomis į tapatybės vagysčių prevenciją, 2007 m. gruodžio mėn. Rusiją pripažino viena iš trijų pasaulio šalių, kuriose tapatybės vagysčių išpuolių internete daugiausia. Taip pat Rusija buvo viena iš šešių pasaulio valstybių, pagal interneto tinklapių, kuriuose yra kenkėjiškos programos, skirtos duomenims rinkti, kriterijumi[365]. Tačiau nepaisydama minėtų rodiklių, Rusija iki šiol nėra ratifikavusi 2001 m. lapkričio 23 d. Konvencijos dėl elektroninių nusikaltimų.

Pažymėtina, kad iki 1997 m. Rusijoje galiojo senasis baudžiamasis kodeksas ir nebuvo galimybės veiksmingai kovoti su elektroniniais nusikaltimais. Tačiau atlikus šiuo metu galiojančio Rusijos Federacijos baudžiamojo įstatymo[366] analizę, galima teigti, kad tapatybės vagystė, kaip atskira nusikalstama veika, nėra kriminalizuota, nors minėtas įstatymas numato baudžiamąją atsakomybę už kai kuriuos tapatybės vagystės elementus, pavyzdžiui, 137 str. 1 d. numatyta baudžiamoji atsakomybė už privataus gyvenimo neliečiamumo pažeidimą (už neteisėtą be asmens sutikimo informacijos apie asmens privatų gyvenimą rinkimą arba platinimą, kai tokia informacija yra to asmens arba jo šeimos paslaptis, arba tokios informacijos atskleidimą, sakant viešą kalbą, viešai atliekamo darbo metu arba visuomenės informavimo priemonėmis, numatoma bauda iki 200 tūkst. rublių[367], šią sumą išskaičiuojant iš nuteisto asmens atlyginimo, darbo užmokesčio arba bet kokių kitų pajamų laikotarpiu iki 18 mėnesių, arba viešieji darbai nuo 120 iki 180 valandų, arba pataisos darbai iki vienerių metų arba areštas iki keturių mėnesių), taip pat numatoma baudžiamoji atsakomybė už susižinojimo slaptumo pažeidimą (138 str.).

159 str. numatoma baudžiamoji atsakomybė už sukčiavimą, kuris suprantamas kaip svetimo turto pasisavinimas arba teisės į kito asmens turtą įgijimas apgaulės būdu arba piktnaudžiaujant pasitikėjimu. Už šį nusikaltimą baudžiama iki 120 tūkst. rublių bauda arba šią sumą išskaičiuojant iš nuteisto asmens atlyginimo, darbo užmokesčio arba bet kokių

[365] Biegelman, M. T. 2009. *Identity Theft Handbook: Detection, Prevention, and Security*, p. 224–225.

[366] Rusijos Federacijos baudžiamasis kodeksas [interaktyvus, žiūrėta 2011-09-19] <http://www.legislationline.org/download/action/download/id/1697/file/0cc1acff8241216090943e97d5b4.htm/preview>.

[367] 100 RUB ~ 8 LTL

kitų pajamų iki vienerių metų laikotarpiu, arba viešaisiais darbais iki 180 valandų, arba pataisos darbais nuo 6 mėn. iki vienerių metų, arba areštu nuo 2 iki 4 mėn., arba laisvės atėmimu iki 2 metų.

Rusijos federacijos baudžiamojo kodekso 187 str. 1 d. numatyta atsakomybė už kreditinių ar debetinių kortelių ar kitų mokėjimo priemonių gaminimą ar paleidimą į apyvartą: kreditinių ar debitinių kortelių, taip pat kitų mokėjimo dokumentų gaminimas turint tikslą juos paleisti į apyvartą užtraukia baudžiamąją atsakomybę iki 6 metų ir baudą nuo 100 iki 300 tūkstančių rublių. 187 str. 2 dalyje numatyta, kad ta pati veika, įvykdyta grupės asmenų, baudžiama laisvės atėmimu iki 8 metų ir bauda iki 1 mln. rublių.

Rusijos baudžiamajame kodekse yra atskiras 28 skyrius „Nusikaltimai kompiuterinės informacijos srityje“, kuriame kriminalizuotos trys veikos. 272 str. numato baudžiamąją atsakomybę už *neteisėtą prieigą prie kompiuterinės informacijos* (teigiama, kad atsakomybė kyla už tyčinę neteisėtą prieigą prie įstatymu saugomos kompiuterinės informacijos, jei tai sukėlė tam tikras pasekmes, tokias kaip informacijos sunaikinimą, blokavimą, modifikavimą, kopijavimą arba kompiuterių, kompiuterinių sistemų ir tinklų darbo sutrikdymą. Už šią veiką baudžiama bauda iki 200 tūkst. rublių arba šią sumą išskaičiuojant iš nuteisto asmens atlyginimo, darbo užmokesčio arba bet kokių kitų pajamų laikotarpiu iki 18 mėnesių, arba pataisos darbais nuo 6 iki 12 mėnesių, arba laisvės atėmimu iki dvejų metų. 273 str. kriminalizuotas *kenkėjiškų programų kūrimas, naudojimas ar platinimas*, už kurį numatoma 200 tūkst. rublių bauda šią sumą išskaičiuojant iš nuteisto asmens atlyginimo, darbo užmokesčio arba bet kokių kitų pajamų laikotarpiu iki 18 mėnesių, o jei tokia veika buvo atlikta dėl nusikalstamo nerūpestingumo ir sukėlė sunkias pasekmes, – laisvės atėmimu nuo trejų iki septynerių metų. 274 str. kriminalizuotas *kompiuterių, kompiuterinių sistemų ar tinklų naudojimo taisyklių pažeidimas*, už kurį numatomas nušalinimas nuo tam tikrų pareigų arba teisės dirbti tam tikrą darbą atėmimas iki penkerių metų arba viešieji darbai nuo 180 iki 240 valandų, arba laisvės apribojimas iki ketverių metų.

Rusijos Federacijos baudžiamojo kodekso 327 str. numatyta baudžiamoji atsakomybė už klastojimą, falsifikuotų dokumentų gaminimą ir pardavimą, už ką numatytas laisvės atėmimas iki dvejų metų. Ta pati veika, įvykdyta turint tikslą įvykdyti kitą nusikaltimą ar palengvinti kito nusikaltimo įvykdymą, užtraukia laisvės atėmimą iki ketverių metų (2 dalis). Trečioje straipsnio dalyje numatyta atsakomybė už dokumento naudojimą,

žinant, kad jis suklastotas, užtraukia baudą iki 80 tūkstančių rublių arba viešuosius darbus nuo 180 iki 240 valandų, arba areštą iki 6 mėnesių.

Atlikus Rusijos baudžiamojo kodekso teisės normų analizę, nustatyta, kad tapatybės vagystės, kaip savarankiškos nusikalstamos veikos, sudėtis nėra įtvirtinta. Tačiau tam tikri tapatybės vagystės elementai patenka į baudžiamojo įstatymo straipsnių veikimo sritį ir už juos numatyta baudžiamoji atsakomybė. Tapatybės vagystės pirmąją stadiją – su tapatybe susijusios informacijos gavimą – kriminalizuoja Rusijos baudžiamojo kodekso 137 str. 1 d., 138 str., 272 str.; tapatybės vagystės antrosios stadijos – sąveikos su tapatybe susijusios informacijos (atskleidimas, platinimas) – kriminalizavimu galima laikyti 137 str. 1 d. Tapatybės vagystės trečioji stadija – su tapatybe susijusios informacijos panaudojimas siekiant įvykdyti nusikaltimą – patenka į Rusijos baudžiamojo kodekso 159 str., 187 str. ir 327 str. Tačiau pažymėtina, kad tapatybės vagystės antrosios stadijos elementas – su tapatybe susijusios informacijos turėjimas – Rusijos baudžiamajame kodekse nėra kriminalizuotas.

Tapatybės vagystės elementų kriminalizavimas Kinijoje

Kinijos baudžiamojo įstatymo normų analizė, siekiant nustatyti, ar šioje valstybėje kriminalizuoti tapatybės vagystės elementai, pasirinkta dėl to, kad ši šalis, turėdama 220 mln. interneto vartotojų, pirmauja pasaulyje pagal interneto vartojimą[368]. 2007 m. gruodžio mėn. darbo grupės, skirtos kovai su duomenų vagystėmis (angl. *Anti-Phishing Working Group)* **atliktų tyrimų duomenimis, Kinija** buvo pirmoji pasaulyje pagal interneto svetaines, kuriose pasitaikydavo kenksmingas programinis kodas, pagrįstas raktiniais kaupikliais[369]. 2010 m. vasario mėn. Kinija buvo antroje vietoje iš pasaulio šalių pagal sukčiavimą, naudojant falsifikuotas internetines svetaines[370].

Kinijos baudžiamojo kodekso[371] 3 skyriaus 5 dalis įtvirtina nusikalstamų veikų, susijusių su sukčiavimu finansų sektoriuje, sudėtis. 193 str.

[368] Biegelman, M. T. 2009. *Identity Theft Handbook: Detection, Prevention, and Security*, p. 226.

[369] APWG Phishing Activity Trends Report for the Month of December 2007, p. 8 [interaktyvus, žiūrėta 2011-09-19]. <http://www.antiphishing.org/reports/apwg_report_dec_2007.pdf>.

[370] APWG Phishing Activity Trends Report. 1st Quarter 2010, p. 7 [interaktyvus, žiūrėta 2011-09-19]. <http://www.antiphishing.org/reports/apwg_report_Q1_2010.pdf>.

[371] Kinijos baudžiamasis kodeksas [interaktyvus, žiūrėta 2011-09-19]. <http://www.cecc.gov/pages/newLaws/criminalLawENG.php>.

įtvirtinta, kad asmuo, išgalvojantis apgaulingas priežastis, kad gautų lėšų, užsakymų ir kt. iš užsienio valstybių, naudojasi suklastota sutartimi, dokumentu ar nuosavybės teisės liudijimu, kaip garantija arba pakartotinai įkeičiant tą patį turtą viršijant jo vertę, arba apgaulės būdu skolinantis, siekiant suklaidinti banką ar kitą finansų instituciją, teikiančią paskolas, ir jei mastas yra santykinai didelis, baudžiamas laisvės atėmimu iki 5 metų arba areštu ir bauda nuo 20 000 iki 200 000 juanių[372]; jei mastas yra didelis arba jei yra kitų svarbių priežasčių, – laisvės atėmimu nuo 5 iki 10 metų ir bauda nuo 50 000 iki 500 000 juanių; jei mastas yra itin didelis arba jei yra kitų svarbių priežasčių, – laisvės atėmimu ne mažiau kaip 10 metų arba laisvės atėmimu iki gyvos galvos ir bauda nuo 50 000 iki 500 000 juanių arba turto konfiskavimu.

Analogiška bausmė numatyta 194 str. už suklastotų, negaliojančių, svetimų vekselių, skolos raštų ar čekių naudojimą, pasirašymą ar išdavimą, siekiant išvilioti pinigų ar kito turto; 195 str. už suklastotų, pakeistų, negaliojančių, laiškų iš kreditą teikiančių institucijų, naudojimą, įgijimą, suklastotų sąskaitų, dokumentų naudojimą; 196 str. – už suklastotos, negaliojančios, svetimos kredito kortelės naudojimą, kredito perviršimą, turint neteisėtų ketinimų.

6 skyriaus 1 dalis numato baudžiamąją atsakomybę už nusikalstamas veikas viešajai tvarkai. 279 str. įtvirtinta, kad asmuo, kuris apsimeta valstybės valdininku, siekdamas suklaidinti žmones, baudžiamas laisvės atėmimu iki 3 metų, areštu, skiriama valstybinė priežiūra arba atimamos politinės teisės; jei yra svarbių aplinkybių arba jei apsimetama policijos pareigūnu baudžiama laisvės atėmimu nuo 3 iki 10 metų.

280 str. įtvirtinta, kad asmuo, kuris klastoja, perdirba, parduoda ar pasisavina, naudodamas prievartą pagrobia ar sunaikina oficialius dokumentus, pažymėjimus arba valstybinių institucijų antspaudus, baudžiamas laisvės atėmimu iki 3 metų, areštu, skiriama valstybinė priežiūra arba atimamos politinės teisės; jei yra svarbių aplinkybių, – laisvės atėmimu nuo 3 iki 10 metų, o asmuo, kuris klastoja ar perdirba tapatybės korteles, baudžiamas laisvės atėmimu nuo 3 iki 7 metų.

283 str. numatyta, kad asmuo, kuris neteisėtai gamina ar parduoda bet kokią specialią šnipinėjimo įrangą arba priemones, skirtas slaptam

[372] 10 CNY ~3,82 Lt.

pasiklausymui ar fotografavimui, baudžiamas laisvės atėmimu iki 3 metų, areštu arba skiriama valstybinė priežiūra.

286 str. įtvirtinta, kad asmuo, kuris atšaukia, pakeičia, pagreitina ar slopina kompiuterio informacinės sistemos darbą taip, kad sistema negali normaliai veikti, ir jei tai sukelia rimtų padarinių, baudžiamas laisvės atėmimu iki 5 metų arba areštu; jei padariniai labai rimti, – laisvės atėmimu iki 5 metų. Tokia pati bausmė numatoma ir už duomenų, kurie saugomi, tvarkomi arba perduodami naudojant informacinę sistemą, išbraukimą, pakeitimą ar įrašymą ir už kenkėjiškų programų, tokių kaip kompiuteriniai virusai, kurie sutrikdo kompiuterinės sistemos darbą, kūrimą ir platinimą, jei tai sukelia rimtų padarinių.

287 str. numatyta, kad asmuo, kuris naudoja kompiuterį įvykdyti tokias nusikalstamas veikas, kaip sukčiavimas finansų srityje, vagystė, svetimo turto pasisavinimas, valstybinio turto išeikvojimas ir valstybės paslapčių atskleidimas, baudžiamas pagal straipsnius, numatančius baudžiamąją atsakomybę už šias veikas.

7 skyriaus 372 str. numato baudžiamąją atsakomybę asmeniui, kuris apsimeta kariškiu, turėdamas tikslą suklaidinti kitus asmenis. Už tai nusikalstamos veikos subjektas baudžiamas laisvės atėmimu iki 3 metų, areštu, skiriama valstybinė priežiūra arba atimamos politinės teisės, o jei tai sukėlė rimtų padarinių, – laisvės atėmimu nuo 3 iki 10 metų.

Atlikus Kinijos baudžiamojo kodekso teisės normų analizę, nustatyta, kad Tapatybės vagystės, kaip savarankiškos nusikalstamos veikos, sudėtis nėra įtvirtinta, tačiau tapatybės vagystės elementai patenka į baudžiamojo įstatymo straipsnių veikimo sritį ir už juos numatyta baudžiamoji atsakomybė. Tapatybės vagystės pirmąją stadiją – su tapatybe susijusios informacijos gavimą – kriminalizuoja Kinijos baudžiamojo kodekso 195 str.; tapatybės vagystės antrosios stadijos – sąveikos su tapatybe susijusios informacijos (pardavimas) – kriminalizavimu galima laikyti 280 str.; tapatybės vagystės trečioji stadija – su tapatybe susijusios informacijos panaudojimas siekiant įvykdyti nusikaltimą – patenka į Kinijos baudžiamojo kodekso 193 str., 194 str., 195 str., 196 str., 279 str., 280 str. veikimo sritį. Atkreiptinas dėmesys, kad Kinijos baudžiamajame kodekse yra specialus 287 str., kuriame nustatyta, kad baudžiamoji atsakomybė už kompiuterio naudojimą nusikalstamoms veikoms, tokioms kaip sukčiavimas finansų srityje, vagystė, svetimo turto pasisavinimas, valstybinio

turto išeikvojimas ir valstybės paslapčių atskleidimas, numatyta pagal straipsnius, numatančius atsakomybę už minėtas veikas: į šių straipsnio veikimo sritį patenka tapatybės vagystės elektroninėje erdvėje pirmoji ir trečioji stadijos: su tapatybe susijusios informacijos gavimas ir tokio pobūdžio informacijos panaudojimas siekiant įvykdyti nusikalstamą veiką. Tačiau pažymėtina, kad tapatybės vagystės antrosios stadijos elementas – su tapatybe susijusios informacijos turėjimas – Kinijos baudžiamajame kodekse nėra kriminalizuotas.

Tapatybės vagystės elementų kriminalizavimas Lietuvoje

Detaliai tapatybės vagystės elementų kriminalizavimas Lietuvoje nagrinėjamas 3.4.2 monografijos dalyje.

Atlikus Lietuvos Respublikos baudžiamojo kodekso teisės normų analizę, nustatyta, kad tapatybės vagystės, kaip savarankiškos nusikalstamos veikos, sudėtis nėra įtvirtinta, tačiau tam tikri tapatybės vagystės elektroninėje erdvėje elementai gali būti vertinami kaip pavojingos veikos. Tapatybės vagystės pirmąją stadiją – su tapatybe susijusios informacijos gavimą – kriminalizuoja Lietuvos Respublikos baudžiamojo kodekso 166 str., 167 str., 198 str., 198$^{(1)}$, 214 str. Tapatybės vagystės trečioji stadija – su tapatybe susijusios informacijos panaudojimas siekiant įvykdyti nusikaltimą – patenka į Lietuvos Respublikos 182 str., 207 str., 215 str., 300 str. Tapatybės vagystės antroji stadija (laikymas, perdavimas) – iš dalies patenka į 198 str. ir 214 str. veikimo sritį, tačiau tapatybės vagystės antrosios stadijos elementas – su tapatybe susijusios informacijos turėjimas – Lietuvos Respublikos baudžiamajame kodekse nėra kriminalizuotas, o baudžiamąją atsakomybę užtraukia tik neviešų elektroninių duomenų ir svetimų, netikrų ar suklastotų elektroninių mokėjimo priemonių laikymas.

Pažymėtina, kad Lietuvoje už tapatybės vagystės elementus numatytos gana įvairios sankcijos: bauda, viešieji darbai, areštas, laisvės apribojimas arba laisvės atėmimas. Dažniausiai Lietuvoje už tapatybės vagystės elektroninėje erdvėje elementus baudžiama pinigine bauda arba laisvės atėmimu. Maksimali Lietuvoje numatyta laisvės atėmimo bausmė už tapatybės vagystės elektroninėje erdvėje antrąją stadiją, patenkančią į sukčiavimo sudėtį, yra laisvės atėmimas iki aštuonerių metų, o piniginė bauda gali siekti iki 300 MGL (iki 39 000 Lt). 1 lentelėje pavaizduotos piniginės baudos ir laisvės atėmimo bausmės už tapatybės vagystės elementus Lietuvoje.

1 lentelė. Baudos ir laisvės atėmimo bausmės už tapatybės vagystės elementus Lietuvoje

LR BK str. / str. d.	Nusikaltimo rūšis	Baudos dydis*	Laisvės atėmimo terminas (kriterijus baudos dydžiui nustatyti)
166 str.	nesunkus	**iki 100 MGL** (iki 13 000 Lt)	iki dvejų metų
167 str.	nesunkus	**iki 100 MGL** (iki 13 000 Lt)	iki trejų metų
168 str.	nesunkus	**iki 100 MGL** (iki 13 000 Lt)	iki trejų metų
182 str. 1 d.	nesunkus	**iki 100 MGL** (iki 13 000 Lt)	iki trejų metų
182 str. 2 d.	sunkus	**iki 300 MGL** (iki 39 000 Lt)	iki aštuonerių metų
207 str.	nesunkus	**iki 100 MGL** (iki 13 000 Lt)	iki trejų metų
198 str. 1 d.	apysunkis	**iki 200 MGL** (iki 26 000 Lt)	iki ketverių metų
198 str. 2 d.	apysunkis	**iki 200 MGL** (iki 26 000 Lt)	iki šešerių metų
198$^{(1)}$ str. 1 d.	nesunkus	**iki 100 MGL** (iki 13 000 Lt)	iki vienerių metų
198$^{(1)}$ str. 2 d.	nesunkus	**iki 100 MGL** (iki 13 000 Lt)	iki trejų metų
214 str.	apysunkis	**iki 200 MGL** (iki 26 000 Lt)	iki šešerių metų
215 str.	apysunkis	**iki 200 MGL** (iki 26 000 Lt)	iki šešerių metų
300 str. 1 d.	nesunkus	**iki 100 MGL** (iki 13 000 Lt)	iki trejų metų
300 str. 2 d.	apysunkis	**iki 200 MGL** (iki 26 000 Lt)	iki ketverių metų
300 str. 3 d.	apysunkis	**iki 200 MGL** (iki 26 000 Lt)	iki šešerių metų

Tapatybės vagystės elektroninėje erdvėje kriminalizavimo tirtose užsienio valstybėse pagrindiniai apibendrinantys aspektai

Tapatybės vagystės elektroninėje erdvėje kriminalizavimo tyrimo rezultatai pateikiami 2 lentelėje. Tapatybės vagystės elektroninėje erdvėje kriminalizavimo būklė aprašoma remiantis pateiktu trijų stadijų modeliu.

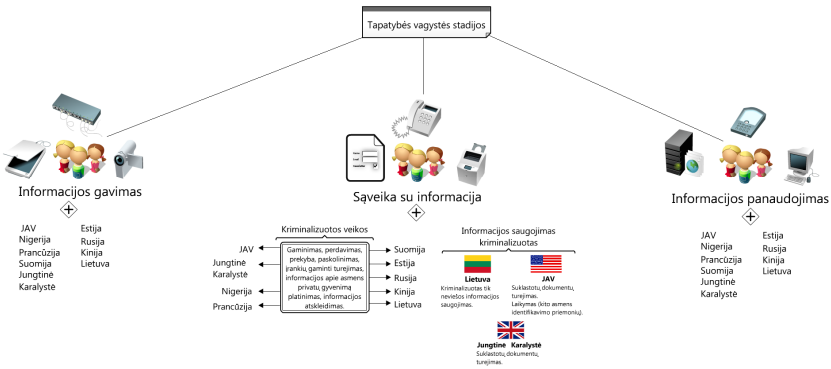
2 lentelė. Tapatybės vagystės elektroninėje erdvėje kriminalizavimas pasirinktose užsienio valstybėse

Šalis / ar įtvirtinta tapatybės vagystės, kaip savarankiškos nusikalstamos veikos, sudėtis?	**Informacijos gavimas**	**Sąveika su informacija**	**Informacijos panaudojimas**
JAV / Taip	Sukčiavimas naudojant kompiuterį (naudotis kompiuteriu neturint teisių, viršyti suteiktas teises, gauti informaciją)	1) Suklastotų dokumentų turėjimas, siekiant suklaidinti 2) Sukčiavimas, susijęs su tapatybės nustatymo dokumentais, autentifikavimo priemonėmis ir informacija (gaminimas, turėjimas, perdavimas, įrankių gaminti turėjimas, prekyba) **3) Tyčia perdavimas, laikymas, naudojimas, neturint tam teisės, kito asmens identifikavimo priemones, turint tikslą padaryti bet kokią neteisėtą veiką** 4) Neteisėtas dokumentų, autentifikavimo priemonių ir informacijos gaminimas, klastojimas 5) Sukčiavimas naudojant elektroninį paštą	
Jungtinė Karalystė / Ne	Netinkamo naudojimosi kompiuteriais aktas (neteisėta prieiga prie kompiuterio duomenų Prieiga prie duomenų, turint tikslą padaryti arba palengvinti nusikalstamas veikas)	Tapatybės kortelių aktas (suklastotų dokumentų turėjimas apima ir autentiškus dokumentus, jei buvo gauti neteisėtu būdu ar išduoti ne tam asmeniui be pateisinamos priežasties) Apgaulės aktas (priemonių, laikomų elektronine forma, skirtų apgaulei įvykdyti, turėjimas, gaminimas ir tiekimas)	Atsakomybė už apgaulę: Apgaulės akto 1 str. (neteisėtas atstovavimas, nesąžiningas informacijos nesuteikimas, piktnaudžiavimas įgaliojimais) ir 11 str. (nesąžiningas paslaugų gavimas)
Nigerija / Ne	Veikos, susijusios su pašto ir telekomunikacijų paslaugomis (pašto sulaikymas, turint tikslą apieškoti ar pagrobti pašto korespondencijos siuntą Paslėpimas, sunaikinimas) Nuosavybės įgijimas apgaulės būdu, sukčiavimas	Dokumentų pardavimas, perdavimas, paskolinimas *Informacijos turėjimas baudžiamosios atsakomybės neužtraukia*	Apsimetimas kitu asmeniu Dokumento (išduoto kitam asmeniui) realizavimas Dokumento ar antspaudo klastojimas Atskiros sudėtys dėl sukčiavimo

Prancūzija / Ne	Slaptumo pažeidimas (tyčinis korespondencijos atplėšimas, perėmimas, sulaikymas) Duomenų rinkimas (apgaulingomis, nesąžiningomis, neteisėtomis priemonėmis) Neteisėta prieiga prie automatizuotų duomenų tvarkymo sistemų	Informacijos apie asmenį naudojimas prieš jo valią (kai priešTaravimas turi teisinį pagrindą) *Informacijos turėjimas baudžiamosios atsakomybės neužtraukia*	Dokumento klastojimas (turint tikslą suteikti teisę, tapatybę, įgaliojimus) Turto įgijimas apgaulės būdu
Suomija / Ne	Slaptas pasiklausymas (neteisėtas klausymasis techninėmis priemonėmis) Žinutės perėmimas (laiškai, elektroninės žinutės, informacija iš telefoninio pokalbio, telegramos, siunčiami teksto, vaizdo duomenys) Įsilaužimas į kompiuterį	Informacijos, pažeidžiančios asmens privatumą, platinimas Asmens duomenų naudojimas *Informacijos turėjimas baudžiamosios atsakomybės neužtraukia*	Apgaulingas identifikuojančios informacijos pateikimas Suklastotų dokumentų pateikimas valstybinei institucijai Finansinės naudos siekimas, suklaidinant kitą asmenį (pakeičiant duomenis, sunaikinant, ištrinant, sutrikdant duomenų sistemos darbą, klastojant galutinį duomenų apdorojimo procesą)
Estija / Ne	Pranešimo konfidencialumo pažeidimas Neteisėtas kompiuterių, kompiuterinių sistemų, tinklų naudojimas pašalinant kodus, slaptažodžius ar kitas apsaugos priemones	Svarbių asmens duomenų atskleidimas *Informacijos turėjimas baudžiamosios atsakomybės neužtraukia*	Privertimas klaidingai įvertinti egzistuojančius faktus Sukčiavimas naudojant kompiuterį (naudos gavimas, įsikišimas į duomenų apdorojimo procesus) Apgaulingos informacijos pateikimas siekiant įgyti oficialų dokumentą ar gauti kitokios naudos Tapatybės dokumento, išduoto kitam asmeniui, naudojimas arba leidimas kitam asmeniui naudotis svarbiu tapatybės dokumentu, išduotu leidusiojo vardu Dokumentų klastojimas, atliekamas pareigūnų Svarbaus identifikuojančio dokumento klastojimas

Rusija / Ne	Privataus gyvenimo neliečiamumo pažeidimas (neteisėtas informacijos apie asmens privatų gyvenimą rinkimas, kai tokia informacija yra to asmens arba jo šeimos paslaptis) Susižinojimo slaptumo pažeidimas. Neteisėta prieiga prie kompiuterinės informacijos	Neteisėtas informacijos apie asmens privatų gyvenimą platinimas, tokios informacijos atskleidimas Informacijos turėjimas baudžiamosios atsakomybės neužtraukia	Sukčiavimas (turto pasisavinimas arba teisės į kito asmens turtą įgijimas apgaulės būdu arba piktnaudžiaujant pasitikėjimu) Kreditinių ar debetinių kortelių ar kitų mokėjimo priemonių gaminimas ar paleidimas į apyvartą Klastojimas, falsifikuotų dokumentų gaminimas ir pardavimas
Kinija / Ne	Suklastotų, pakeistų, negaliojančių laiškų iš kreditą suteikiančių institucijų įgijimas Kompiuterio naudojimas vagystei, svetimam turtui pasisavinti	Su tapatybe susijusios informacijos pardavimas Informacijos turėjimas baudžiamosios atsakomybės neužtraukia	Naudojimasis suklastota sutartimi, dokumentu ar nuosavybės teisės liudijimu, siekiant gauti naudos Suklastotų, pakeistų sąskaitų, dokumentų naudojimas Suklastotos, negaliojančios, svetimos kredito kortelės naudojimas Apsimetimas valstybės tarnautoju, siekiant suklaidinti žmones Duomenų klastojimas, perdirbimas, pasisavinimas, pagrobimas prievarta
Lietuva / Ne	Asmens susižinojimo neliečiamumo pažeidimas (paštas, siunčiami pranešimai) Informacijos apie privatų asmens gyvenimą rinkimas Elektroninių duomenų perėmimas ir panaudojimas Neteisėtas prisijungimas prie informacinės sistemos Netikros elektroninės mokėjimo priemonės gaminimas	Laikymas, pasisavinimas, paskleidimas ar kitas panaudojimas neviešų elektroninių duomenų Laikymas, perdavimas ar realizavimas svetimų, netikrų ar suklastotų elektroninių mokėjimo priemonių Informacijos turėjimas baudžiamosios atsakomybės neužtraukia	Sukčiavimas Kreditinis sukčiavimas Netikros elektroninės mokėjimo priemonės gaminimas, tikros elektroninės mokėjimo priemonės klastojimas ar neteisėtas disponavimas elektronine mokėjimo priemone Neteisėtas elektroninės mokėjimo priemonės ar jos duomenų panaudojimas Dokumento klastojimas ar disponavimas suklastotu dokumentu

Kaip matyti iš 2 lentelės, tik vienoje valstybėje (t. y. JAV) yra įtvirtinta savarankiška tapatybės vagystės elektroninėje erdvėje sudėtis. Tik trijose valstybėse kriminalizuotas (skirtinga apimtimi) vienas iš antrosios stadijos elementų – neteisėtas tapatybės informacijos turėjimas, turint tikslą padaryti nusikaltimą. Apibendrintai tapatybės vagystės elektroninėje erdvėje stadijų kriminalizavimas tirtose valstybėse pavaizduotas 20 pav.[373]:



20 pav. Tapatybės vagystės elektroninėje erdvėje stadijų kriminalizavimas

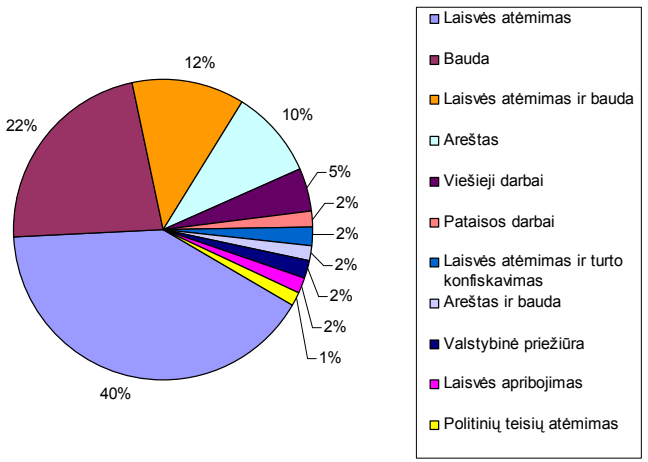
Autorių nuomone, vieno iš antrosios stadijos elementų, t. y. neteisėto tapatybės informacijos turėjimo, kriminalizavimo trūkumas paaiškinamas istoriniu aspektu. Tapatybės vagystė elektroninėje erdvėje yra naujas socialinis teisinis reiškinys ir ne visų užsienio valstybių įstatymų leidėjai skyrė deramą dėmesį, kad uždraustų šią pavojingą veiką elektroninėje erdvėje. Kita vertus, tokia padėtis gali daryti neigiamą įtaką kovai su šia pavojinga veika. Nesant tinkamai nustatytos atsakomybės, gali susidaryti sąlygos toliau šiai pavojingai veikai sparčiai plisti.

Tais atvejais, kai užsienio valstybėje nėra įstatymų, kuriais tapatybės vagystė elektroninėje erdvėje būtų kriminalizuota kaip savarankiška veika, 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

[373] Štitilis, D., Pakutinskas, P., Dauparaitė, I., Laurinaitis, M. 2011. Tapatybės vagystės elektroninėje erdvėje kriminalizavimas: lyginamieji aspektai, *Socialinių mokslų studijos* 3(1): 166.

ir tarptautiniu lygiu. Nesant galimybės surinkti įrodymų elektroniniu pavidalu, neužtikrinamas 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.

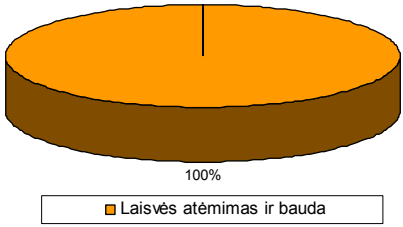
Tačiau ne vien veikos kriminalizavimo faktas svarbus tiriant tapatybės vagystę elektroninėje erdvėje ir teisinės prevencijos priemones. Šis autorių pristatomas tyrimas neapsiribojo vien tik kriminalizavimo būklės įvertinimu tirtose valstybėse. Taip pat buvo tiriamos ir sankcijos už įvairius tapatybės nusikaltimus. Toliau pateikiami sankcijų už tapatybės vagystės elektroninėje erdvėje neteisėtas veikas tyrimo rezultatai.



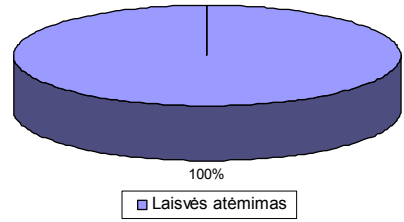
21 pav. Sankcijos už tapatybės vagystės elektroninėje erdvėje nusikaltimus

Taigi, kaip matyti iš 2 pav., sankcijos už tapatybės vagystes elektroninėje erdvėje tirtose užsienio valstybėse yra labai įvairios: nuo laisvės atėmimo iki arešto ir viešųjų darbų. Tačiau kai kuriose valstybėse sankcijos įvairove nepasižymi. Tai Prancūzija, JAV ir Nigerija.

Pačių sankcijų dydžiai irgi skiriasi. Pavyzdžiui, bauda už atitinkamas pavojingas veikas, susijusias su tapatybės vagyste, gali siekti iki 300 000 eurų (Prancūzijoje). Laisvės atėmimas vienose valstybėse gali siekti iki 30 metų ar net iki gyvos galvos, o kitose svyruoja nuo 3 iki 6 metų (pvz., Prancūzijoje). Nigerijoje už tapatybės vagystės elektroninėje erdvėje elementus gali būti baudžiama laisvės atėmimu iki gyvos galvos.

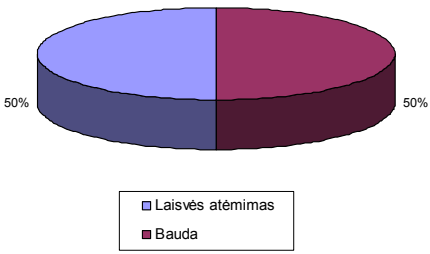


22 pav. Sankcijos už tapatybės vagystės elementus Prancūzijoje

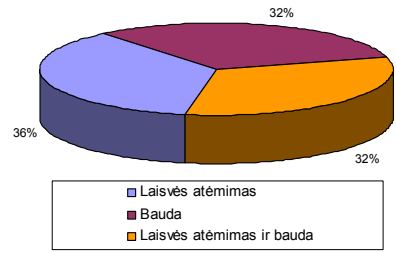


23 pav. Sankcijos už tapatybės vagystės elementus JAV ir Nigerijoje

Panaši padėtis yra ir Suomijoje, Estijoje bei Jungtinėje Karalystėje sankcijos už tapatybės vagystės elektroninėje erdvėje nusikaltimus apsiriboja laisvės atėmimu ir bauda.

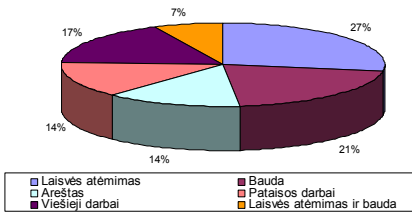


24 pav. Sankcijos už tapatybės vagystės elementus Suomijoje ir Estijoje

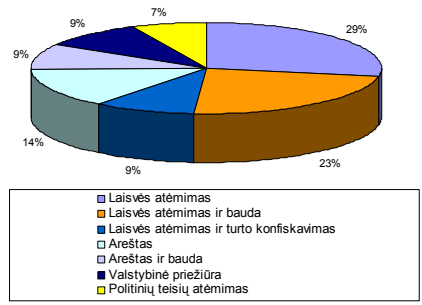


25 pav. Sankcijos už tapatybės vagystės elementus Jungtinėje Karalystėje

Tuo tarpu sankcijos už tapatybės vagystės nusikaltimus Rusijoje ir Kinijoje labai įvairios.

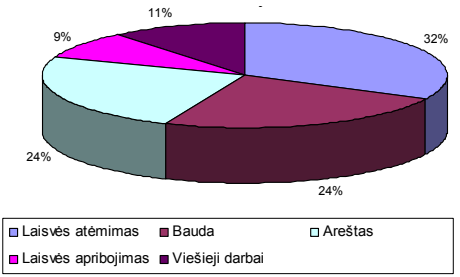


26 pav. Sankcijos už tapatybės vagystės elementus Rusijoje



27 pav. Sankcijos už tapatybės vagystės elementus Kinijoje

Bauda už atitinkamas pavojingas veikas, susijusias su tapatybės vagyste, Lietuvoje gali siekti iki 39 000 Lt, o laisvės atėmimas grėsti iki 3–8 metų.



28 pav. Sankcijos už tapatybės vagystės elementus Lietuvoje

Apibendrinant pasirinktų užsienio valstybių baudžiamuosiuose įstatymuose numatytas sankcijas už tapatybės vagystės nusikaltimus, galima pažymėti, kad sankcijos yra labai įvairios: vienos valstybės tapatybės vagystę elektroninėje erdvėje vertina kaip mažiau pavojingą veiką, kitos – atvirkščiai. Tai, kad valstybėse numatytos nevienodo pobūdžio ir dydžio sankcijos, yra paskata nusikaltimus daryti tose valstybėse, kuriose sankcijos už tapatybės vagystę elektroninėje erdvėje yra mažesnės. Todėl įstatymų leidėjams taip pat svarbu suvienodinti sankcijas už šią pavojingą veiką elektroninėje erdvėje.

3.4.2. Tapatybės vagystės elektroninėje erdvėje elementų kriminalizavimas Lietuvoje

Lietuva yra viena iš Konvencijos dėl elektroninių nusikaltimų narė (Konvenciją ratifikavo 2004 m. kovo 18 d., kuri šalyje įsigaliojo nuo 2004 m. liepos 1 d.), tačiau, nors elektroninių nusikaltimų (taip pat ir tapatybės vagystės elektroninėje erdvėje) atvejų vis daugėja, šalyje itin trūksta teismų praktikos ir mokslinių tyrimų elektroninių nusikaltimų srityje. Tapatybės vagystė elektroninėje erdvėje, kuri, pavyzdžiui, JAV yra kriminalizuota ir įvardijama kaip labiausiai plintanti XXI amžiaus nusikalstama veika, Lietuvoje vis dar mistifikuojama ir vertinama gana skeptiškai: jei veika ir pavojinga, tai Lietuvoje nepaplitusi (pavyzdžiui, pagal autorių atliktą vartotojų tyrimą, 46 proc. vartotojų nurodė, kad tokia veika nėra paplitusi Lietuvoje),

o už tokio pobūdžio veikas numatyti baudžiamąją atsakomybę netikslinga, nes esamas teisinis reguliavimas yra pakankamas (pagal autorių atliktą ekspertų apklausą, 4 ekspertai nurodė, tapatybės vagystės elektroninėje erdvėje kriminalizuoti kaip savarankiškos veikos nereikia).

Tokią poziciją galima paaiškinti tuo, kad tiek valstybės, tiek verslo institucijoms, o ypač vartotojams, trūksta informacijos apie tai, kas yra tapatybės vagystė elektroninėje erdvėje ir kokius įvairius ir pavojingus padarinius ji gali sukelti, jei asmens duomenys ir asmeninė informacija elektroninėje erdvėje bus naudojami neatsakingai ar neapdairiai.

Interneto vartotojų supratimo apie tapatybės vagystę didinimas turėtų būti prioritetinė sritis tiek valstybės, tiek privataus sektoriaus institucijoms, nes atlikti tyrimai rodo, kad vartotojai vis dar nesuvokia elektroninėje erdvėje jų tykančių pavojų masto. Pavyzdžiui, Jungtinėse Valstijose, 2005–2006 m. 20 % apklaustų šeimų savo kompiuteriuose nebuvo įdiegę antivirusinių programų, o Jungtinėje Karalystėje 2006 m. 1/5 apklaustųjų antivirusinių programų nebuvo atnaujinę per pastarąjį mėnesį, o 23 % apklaustųjų atidarydavo elektroniniu paštu iš nežinomo siuntėjo gautus elektroninio laiško priedus[374].

Lietuvos vartotojų instituto 2010 m. antroje pusėje atliktas sociologinis tyrimas parodė, kad vartotojams trūksta informacijos, kaip saugiai atsiskaityti negrynaisiais pinigais ir apie jų, kaip vartotojų, teises. Tyrimas, kurio tikslas buvo nustatyti, kaip vartotojai supranta riziką, kylančią atsiskaitant negrynaisiais pinigais, ir kokių saugumo priemonių imasi, parodė, jog vartotojai saugo asmens duomenis, stengdamiesi riboti jų pateikimą internete (52 proc.), naudoja antivirusines programas, ugniasienes (50 proc.), o 34 proc. teigė, kad net vengia atsiskaitinėti internetu. Tik 8 proc. nurodė, jog jie nenaudoja jokių priemonių savo asmeninei informacijai apsaugoti, nes nieko apie tai nesupranta. Tyrimas taip pat parodė, kad vartotojai nėra pakankamai susipažinę su asmens duomenų sąvokos turiniu, ir tai gali būti viena iš priežasčių, lemiančių per didelį duomenų atskleidimą internete, tuo sudarant galimybes sukčiams juos pasisavinti, o vėliau ir panaudoti finansiniams nusikaltimams elektroninėje erdvėje atlikti[375].

[374] Online Identity Theft. OECD, 2009, p. 59 [interaktyvus, žiūrėta 2011-09-19]. < http://browse.oecdbookshop.org/oecd/pdfs/browseit/9309021E.PDF>.

[375] Lietuvos vartotojų instituto interneto tinklapis [interaktyvus, žiūrėta 2011-09-19]. <http://www.vartotojai.lt/index.php?id=7324>.

Visi vartotojai, nepriklausomai nuo to, ar jie yra viešojo, ar privataus sektoriaus atstovai, kurie bendrai stengiasi įgyvendinti tapatybės vagystės prevencines priemones, turėtų suprasti problemą, žinoti, kaip tapatybės vagystė gali būti įvykdyta, kam ji gali sukelti neigiamus padarinius ir kokių priemonių turėtų būti imtasi, kad būtų galima jos išvengti.

Manytina, kad tapatybės vagystės elektroninėje erdvėje kaip savarankiškos veikos kriminalizavimas palengvintų tokių veikų susekimą, tyrimą ir baudžiamąjį persekiojimą nacionaliniu ir tarptautiniu lygiu, todėl ankstesnėje dalyje apžvelgus tapatybės vagystės elementų kriminalizavimą užsienio valstybių baudžiamuosiuose įstatymuose, tikslinga atlikti nuodugnesnę Lietuvos Respublikos baudžiamojo kodekso[376] (toliau – LR BK) normų analizę, siekiant nustatyti, ar visi tapatybės vagystės elektroninėje erdvėje elementai yra kriminalizuoti ir ar šio pavojingo reiškinio įvertinimas iš baudžiamosios teisės pozicijų yra pakankamas, t. y. ar už visas tris tapatybės vagystės elektroninėje erdvėje stadijas – su tapatybe susijusios informacijos gavimą, sąveiką su tapatybe susijusia informacija ir su tapatybe susijusios informacijos panaudojimą siekiant padaryti nusikaltimą[377] – yra numatyta baudžiamoji atsakomybė.

LR BK normų analizė bus atliekama aptariant pavojingas veikas, kurių sudėtys yra įtvirtintos baudžiamajame įstatyme, ir į kurių veikimo sritį patenka vienas ar keli tapatybės vagystės elektroninėje erdvėje elementai, bei pateikiant kritines įžvalgas dėl esamo teisinio reguliavimo.

Pažymėtina, kad Lietuvoje, kaip ir daugelyje kitų valstybių (pavyzdžiui, Prancūzijoje, Jungtinėje Karalystėje, Suomijoje, Estijoje, Rusijoje, Kinijoje, Nigerijoje), tapatybės vagystė *per se* nėra laikoma teisės pažeidimu, o patenka į įvairias išimtis, susijusias su duomenų slaptumu, apsauga, neteisėta prieiga, sukčiavimu, klastote ar intelektinės nuosavybės teisių pažeidimais, už kuriuos galima asmenį patraukti baudžiamojon atsakomybėn.

Kaip jau minėta, JAV ši veika yra kriminalizuota, o jos sudėtis įtvirtinta JAV įstatymų sąvado 18 skirsnio 1 dalies 47 skyriaus 1028 straipsnio (a) dalies (7) punkte, numatančiame baudžiamąją atsakomybę už tai, kai

[376] Lietuvos Respublikos baudžiamasis kodeksas. *Valstybės žinios*, 2000, Nr. 89-2741.

[377] Gercke, M. Internet-related identity thef. *Project on Cybercrime* [interaktyvus], 2007. p. 17–20 [žiūrėta 2011-09-19]. <http://www.coe.int/T/DG1/LegalCooperation/Economiccrime/cybercrime/cy%20activity_events_on_identity_theft/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf>.

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[378].

Pažymėtina, kad Lietuvoje tam tikri tapatybės vagystės elektroninėje erdvėje elementai yra vertinami kaip pavojingos veikos, pavyzdžiui, LR BK 166 str. kriminalizuotas asmens susižinojimo neliečiamumo pažeidimas: tas, kas neteisėtai perėmė paštu ar per pasiuntinių paslaugos teikėją siunčiamą siuntą ar siuntinį arba neteisėtai perėmė, fiksavo ar stebėjo asmens elektroninių ryšių tinklais siunčiamus pranešimus, arba neteisėtai fiksavo, klausėsi ar stebėjo asmens pokalbius elektroninių ryšių tinklais, arba kitaip pažeidė asmens susižinojimo neliečiamumą, baudžiamas viešaisiais darbais arba bauda, arba laisvės apribojimu, arba areštu, arba laisvės atėmimu iki dvejų metų.

LR BK 167 str. numato baudžiamąją atsakomybę už neteisėtą informacijos apie privatų asmens gyvenimą rinkimą: tas, kas neteisėtai rinko informaciją apie privatų asmens gyvenimą, baudžiamas viešaisiais darbais arba bauda, arba laisvės apribojimu, arba areštu, arba laisvės atėmimu iki trejų metų; o 168 str. – už neteisėtą informacijos apie asmens privatų gyvenimą atskleidimą ar panaudojimą: tas, kas be asmens sutikimo viešai paskelbė, pasinaudojo ar kitų asmenų labui panaudojo informaciją apie kito žmogaus privatų gyvenimą, jeigu tą informaciją jis sužinojo dėl savo tarnybos ar profesijos arba atlikdamas laikiną užduotį, arba ją surinko darydamas kodekso 165–167 straipsniuose numatytą veiką (neteisėtai pažeisdamas asmens būsto, susižinojimo neliečiamumą arba neteisėtai rinkdamas informaciją apie privatų asmens gyvenimą) baudžiamas viešaisiais darbais arba bauda, arba laisvės apribojimu, arba areštu, arba laisvės atėmimu iki trejų metų.

LR BK 182 str. kriminalizuotas sukčiavimas: tas, kas apgaule savo ar kitų naudai įgijo svetimą turtą ar turtinę teisę, išvengė turtinės prievolės arba ją panaikino, baudžiamas viešaisiais darbais arba bauda, arba laisvės apribojimu, arba areštu, arba laisvės atėmimu iki trejų metų; 2 d.

[378] United States Code („U. S. C“), Title 18, Part I, Chapter 47, Section 1028 (a) (7) [interaktyvus, žiūrėta 2011-09-19]. <http://www.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00001028----000-.html>.

numatyta kvalifikuota nusikaltimo sudėtis – tas, kas savo ar kitų naudai įgijo didelės vertės svetimą turtą ar turtinę teisę arba didelės mokslinės, istorinės ar kultūrinės reikšmės turinčias vertybes arba išvengė didelės vertės turtinės prievolės, arba ją panaikino, arba sukčiavo dalyvaudamas organizuotoje grupėje, baudžiamas laisvės atėmimu iki aštuonerių metų.

LR BK 207 str. įtvirtinta kreditinio sukčiavimo sudėtis: tas, kas apgaule gavo kreditą, paskolą, subsidiją, laidavimo ar banko garantijos raštus arba kitus kreditinius įsipareigojimus, baudžiamas bauda arba areštu, arba laisvės atėmimu iki trejų metų.

LR BK XXX skyrius įtvirtina nusikaltimų elektroninių duomenų ir informacinių sistemų saugumui sudėtis. LR BK 198 str. kriminalizuoja neteisėtą elektroninių duomenų perėmimą ir panaudojimą: tas, kas neteisėtai stebėjo, fiksavo, perėmė, įgijo, laikė, pasisavino, paskleidė ar kitaip panaudojo neviešus elektroninius duomenis, baudžiamas bauda arba laisvės atėmimu iki ketverių metų, o jei minėti veiksmai buvo atliekami su strateginę reikšmę nacionaliniam saugumui arba didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinčiais neviešais elektroniniais duomenimis, – laisvės atėmimu iki šešerių metų. LR BK 198$^{(1)}$ str. numatyta baudžiamoji atsakomybė už neteisėtą prisijungimą prie informacinės sistemos: tas, kas neteisėtai prisijungė prie informacinės sistemos pažeisdamas informacinės sistemos apsaugos priemones, baudžiamas viešaisiais darbais arba bauda, arba areštu, arba laisvės atėmimu iki vienerių metų, o jei prisijungta buvo prie strateginę reikšmę nacionaliniam saugumui arba didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinčios informacinės sistemos, – bauda arba areštu, arba laisvės atėmimu iki trejų metų.

LR BK 214 str. numato baudžiamąją atsakomybę už netikros elektroninės mokėjimo priemonės gaminimą, tikros elektroninės mokėjimo priemonės klastojimą ar neteisėtą disponavimą elektronine mokėjimo priemone arba jos duomenimis: tas, kas gamino vieną ar daugiau netikrų elektroninių mokėjimo priemonių ar jų dalių ar suklastojo vieną ar daugiau tikrų elektroninių mokėjimo priemonių arba neteisėtai įgijo, laikė, perdavė ar realizavo vieną ar daugiau svetimų, netikrų ar suklastotų elektroninių mokėjimo priemonių, arba neteisėtai įgijo, laikė, perdavė ar realizavo vienos ar daugiau svetimų elektroninių mokėjimo priemonių ar jų naudotojo tapatybės patvirtinimo priemonių duomenis, pakankamus finansinei operacijai

inicijuoti, arba gamino, įgijo, laikė, perdavė ar realizavo techninę įrangą, programinę įrangą ar kitokias priemones, tiesiogiai skirtas ar pritaikytas netikroms elektroninėms mokėjimo priemonėms ar jų dalims gaminti ar tikroms elektroninėms mokėjimo priemonėms klastoti, baudžiamas bauda arba areštu, arba laisvės atėmimu iki šešerių metų. 215 str. kriminalizuotas neteisėtas elektroninės mokėjimo priemonės ar jos duomenų panaudojimas: tas, kas neteisėtai inicijavo ar atliko vieną ar daugiau finansinių operacijų viena ar daugiau svetimų, netikrų ar suklastotų elektroninių mokėjimo priemonių arba neteisėtai panaudodamas vieną ar daugiau svetimų elektroninių mokėjimo priemonių ar jų naudotojo tapatybės patvirtinimo priemonių duomenis, arba panaudodamas žinomai netikrus vienos ar daugiau tapatybės patvirtinimo priemonių duomenis, arba žinomai neteisėtą vienos ar daugiau svetimų, netikrų ar suklastotų elektroninių mokėjimo priemonių panaudojimą pripažino teisėtu, baudžiamas bauda arba areštu, arba laisvės atėmimu iki šešerių metų.

LR BK 300 str. įtvirtinta dokumento suklastojimo ar disponavimo suklastotu dokumentu sudėtis: tas, kas pagamino netikrą dokumentą, suklastojo tikrą dokumentą arba žinomai netikrą ar žinomai suklastotą tikrą dokumentą laikė, gabeno, siuntė, panaudojo ar realizavo, baudžiamas bauda arba areštu, arba laisvės atėmimu iki trejų metų. 2 d. įtvirtinta kvalifikuota nusikaltimo sudėtis: tas, kas pagamino netikrą asmens tapatybės kortelę, pasą, vairuotojo pažymėjimą ar valstybinio socialinio draudimo pažymėjimą arba suklastojo tikrą asmens tapatybės kortelę, pasą, vairuotojo pažymėjimą ar valstybinio socialinio draudimo pažymėjimą, arba žinomai netikrą ar žinomai suklastotą tikrą asmens tapatybės kortelę, pasą, vairuotojo pažymėjimą ar valstybinio socialinio draudimo pažymėjimą laikė, gabeno, siuntė, panaudojo ar realizavo, baudžiamas areštu arba laisvės atėmimu iki ketverių metų. Jeigu dėl minėtų veikų buvo padaryta didelės žalos arba buvo pagamintas didelis kiekis netikrų asmens tapatybės kortelių, pasų, vairuotojo pažymėjimų ar valstybinio socialinio draudimo pažymėjimų, arba suklastotas didelis kiekis tikrų asmens tapatybės kortelių, pasų, vairuotojo pažymėjimų ar valstybinio socialinio draudimo pažymėjimų, arba žinomai netikrų ar žinomai suklastotų tikrų didelis kiekis asmens tapatybės kortelių, pasų, vairuotojo pažymėjimų ar valstybinio socialinio draudimo pažymėjimų buvo laikoma, gabenta, siųsta, naudota ar realizuota, – laisvės atėmimu iki šešerių metų.

Atlikus LR BK teisės normų analizę, nustatyta, kad tapatybės vagystės, kaip savarankiškos nusikalstamos veikos, sudėtis nėra įtvirtinta, tačiau tam tikri tapatybės vagystės elektroninėje erdvėje elementai gali būti vertinami kaip pavojingos veikos. Pirmąją tapatybės vagystės stadiją – su tapatybe susijusios informacijos gavimą – kriminalizuoja LR BK 166 str., 167 str., 198 str., 198$^{(1)}$, 214 str. Trečioji tapatybės vagystės stadija – su tapatybe susijusios informacijos panaudojimas siekiant įvykdyti nusikaltimą – patenka į LR BK 182 str., 207 str., 215 str., 300 str. reglamentavimo sritį. Tapatybės vagystės antroji stadija (laikymas, perdavimas) – iš dalies patenka į LR BK 198 str. ir 214 str. veikimo sritį, tačiau tapatybės vagystės antrosios stadijos elementas – su tapatybe susijusios informacijos turėjimas – LR BK nėra kriminalizuotas, o baudžiamąją atsakomybę užtraukia tik neviešų elektroninių duomenų ir svetimų, netikrų ar suklastotų elektroninių mokėjimo priemonių laikymas.

Už tapatybės vagystės elektroninėje erdvėje atskiras stadijas LR BK, lyginant su kitomis užsienio valstybėmis, numatytos gana įvairios sankcijos: laisvės atėmimas, laisvės apribojimas, areštas, viešieji darbai, bauda. Prancūzijoje už tapatybės vagystės elektroninėje erdvėje elementus numatytos sankcijos yra laisvės atėmimas ir bauda, Suomijoje ir Estijoje – baudžiama laisvės atėmimu arba bauda. Tuo tarpu Rusijoje ir Kinijoje sankcijų už tapatybės vagystės elektroninėje erdvėje spektras dar platesnis ir, be jau paminėtų sankcijų, šiose valstybėse asmeniui, įvykdžiusiam minėtą veiką, gali būti skiriami pataisos darbai (Rusijoje), taip pat laisvės atėmimas ir turto konfiskavimas, areštas ir bauda, nustatoma valstybinė priežiūra ar politinių teisių atėmimas (Kinijoje).

Dažniausiai Lietuvoje už tapatybės vagystės elektroninėje erdvėje elementus baudžiama pinigine bauda arba laisvės atėmimu (detaliau apie sankcijas nurodyta monografijos 3.4.1 dalyje), tačiau minėtos sankcijos, lyginant jas su kitų užsienio valstybių baudžiamuosiuose įstatymuose įtvirtintomis sankcijomis už tokio pobūdžio veikas, nėra itin griežtos. Maksimali laisvės atėmimo bausmė Lietuvoje numatyta už tapatybės vagystės elektroninėje erdvėje antrąją stadiją, patenkančią į sukčiavimo sudėtį, yra laisvės atėmimas iki aštuonerių metų, o piniginė bauda gali siekti iki 300 MGL (iki 39 000 Lt). Tuo tarpu JAV ir Nigerijoje už tapatybės vagystės elektroninėje erdvėje elementus numatyta pati griežčiausia bausmė – laisvės atėmimas iki 30 metų (JAV) ar net iki gyvos galvos (Ni-

gerijoje), o pavyzdžiui, Prancūzijoje, maksimali galima bausmė yra ne tik laisvės atėmimas iki 5 metų, bet ir 300 000 EUR bauda.

Taigi, kai kurių užsienio valstybių baudžiamuosiuose įstatymuose numatomos gana įvairios ir kartais labai griežtos bausmės: nuo piniginės baudos iki laisvės atėmimo iki gyvos galvos. Galima daryti išvadą, kad ne tik tapatybės vagystės elektroninėje erdvėje kriminalizavimas, bet ir sankcijų rūšių bei dydžių už tapatybės vagystę elektroninėje erdvėje įvairovė turėtų neigiamai veikti šios pavojingos veikos plitimą.

Iš paminėtų LR BK straipsnio normų, į kurių veikimo sritį patenka ir tapatybės vagystės elektroninėje erdvėje elementai, matyti, kad tapatybės vagystės elektroninėje erdvėje atveju reikia kalbėti apie nusikalstamų veikų daugetą,[379] 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 pažeidžiant garbę ir orumą); 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 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, susijusiai su dokumentų klastojimu) ir pan.

Tačiau tapatybės vagystė, atliekama fizinėje erdvėje, Lietuvoje traktuojama kaip priemonė, pasiruošimas kitai neteisėtai veikai padaryti ir

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

per se nusikalstama veika nėra laikoma. Todėl 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[380]. Minėtu atveju tokia veika dažniausiai 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.

Praktikoje kyla problemų už tapatybės vagystę taikant LR BK įtvirtintas normas dėl sukčiavimo. Spaudoje buvo pranešta, kad policijai pavyko sulaikyti sukčius, per „Gmail" elektroninio pašto sistemą išviliojusius įvairias sumas iš dešimčių žmonių[381]. Gavę prisijungimo prie „Gmail" pašto slaptažodžius ir prisijungimo vardus, šie asmenys prisijungdavo prie kitų asmenų e. pašto ir susirašinėdavo su adresatais, apsimesdami dėžutės savininkais, prašydavo pervesti pinigų. Policijos duomenimis, nuo šių asmenų visoje Lietuvoje nukentėjo bent 30 žmonių, o dalis nukentėjusiųjų – užsienyje gyvenantys emigrantai. Bandymų galėjo būti kur kas daugiau, nes daugelis žmonių į prašymus pervesti pinigų nereaguodavo – sukčiams pavykdavo tik tuo atveju, jeigu jie pataikydavo susisiekti su dėžutės savininkui artimu žmogumi. Pareigūnų teigimu, elektrėniškiai išmano įstatymus ir siekė išvilioti sumas, nesiekiančias vieno minimalaus gyvenimo lygio (MGL), 130 litų. Už tokios sumos išviliojimą taikoma tik administracinė atsakomybė[382]. Taigi, tapatybės vagystė elektroninėje erdvėje gali būti masinė, tačiau dėl atitinkamos sumos ribojimų baudžiamoji atsakomybė pagal LR BK 182 str. gali nekilti.

[380] Piesliakas,V. 2008. *Lietuvos baudžiamoji teisė*. Kn. 2. Vilnius: Justitia, p. 125.

[381] Gmail.com siaubas – jaunuoliai iš Elektrėnų. *Kauno diena* [interaktyvus] 2010-06-03 [žiūrėta 2011-09-19]. <http://kauno.diena.lt/naujienos/kriminalai/-gmail-com-siaubas-jaunuoliai-is-elektrenu-281729>.

[382] *Ibid.*

Autorių nuomone, veiką būtų galima vertinti kaip neteisėtą elektroninių duomenų perėmimą ir panaudojimą pagal LR BK 198 str. Atkreiptinas dėmesys, kad nors, kaip minėta, tam tikri tapatybės vagystės 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, 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 (nebent užtrauktų baudžiamąją atsakomybę pagal LR BK 167–168 str.). Kaip šiuo 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 Respublikoje nėra teisės akto, kurio normomis remiantis būtų galima patraukti asmenį atsakomybėn už tokių veiksmų atlikimą. Taigi, pagal minimą straipsnį neįmanoma įvertinti visų pavojingų epizodų, pavyzdžiui, tuo atveju, jei neteisėtai perimti duomenys laikomi turint tikslą įvykdyti teisės pažeidimą.

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, be to, apsunkinamas tokių veikų susekimas, tyrimas ir baudžiamasis persekiojimas nacionaliniu ir tarptautiniu lygiu. Nesant galimybės rinkti įrodymų 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.

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? Arba kaip reikėtų vertinti gana dažnai pasitaikančią situaciją, kai asmuo, pasinaudodamas turima informacija apie kitą asmenį, socialiniame tinkle sukuria profilį kito asmens vardu, įdeda jame kito asmens nuotrauką ir skelbia to asmens privataus gyvenimo detales? Ar ši situacija turėtų būti vertinama iš civilinės teisės pozicijų ir tokiam asmeniui turėtų būti taikoma civilinė atsakomybė už neteisėtą atvaizdo naudojimą ar teisės į privatų gyvenimą pažeidimą (LR CK 2.22 str., 2.23 str.)? Ar tokie veiksmai galėtų būti kvalifikuojami pagal LR BK atitinkamus straipsnius ir vertinami kaip nusikalstamos veikos asmens garbei ir orumui (jei skelbiama tikrovės neatitinkanti informacija), ar kaip nusikaltimai asmens privataus gyvenimo neliečiamumui?

Pavyzdžiui, paminėtinas atvejis, kai asmuo, neteisėtai panaudodamas prisijungimo duomenis, neteisėtai prisijungė prie kito asmens *Facebook* profilio ir pastarojo asmens vardu per šį profilį pradėjo platinti seksualinio pobūdžio informaciją[383];[384]. Tokie pažeidėjo veiksmai JAV Kalifornijos valstijos teisėjo buvo įvertinti kaip nusikaltimas – tapatybės vagystė[385]. Tačiau pagal dabartinį teisinį reguliavimą Lietuvoje už tokio pobūdžio veiką baudžiamoji atsakomybė nekiltų.

Kaip vieną iš probleminių situacijų galima iliustruoti parašo fizinėje erdvėje ir elektroninio parašo pavyzdžiais. Abejonių nekyla, kad fizinėje erdvėje savo valią patvirtinus kito asmens parašu, tokie veiksmai patenka į LR BK 300 str. reglamentavimo sritį ir yra kvalifikuojami kaip do-

[383] Judge Rules Facebook Trolling = Identity Theft. *Techmento* [interaktyvus, žiūrėta 2011-09-20]. <http://techmento.com/2011/08/03/judge-rules-facebook-trolling-identity-theft>.

[384] Using Someone Else's Facebook Is ID Theft: CA Judge. *Findlaw* [interaktyvus]. 2011-08-05 [žiūrėta 2011-09-20]. <http://blogs.findlaw.com/blotter/2011/08/using-someone-elses-facebook-is-id-theft-ca-judge.html>.

[385] Judge Rules Facebook Trolling = Identity Theft. *Techmento* [interaktyvus, žiūrėta 2011-09-20]. <http://techmento.com/2011/08/03/judge-rules-facebook-trolling-identity-theft>.

kumentų klastojimas. Tačiau elektroninėje erdvėje, kurioje asmens valia informacinėje sistemoje išreiškiama įrašant atitinkamą vartotojo vardą ir slaptažodį ar PIN kodą, bendros 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 šie veiksmai turėtų būti kvalifikuojami kaip nusikalstama veika.

Pradine išeities pozicija būtų galima laikyti Lietuvos Respublikos elektroninių ryšių įstatymo[386] (toliau – Įstatymo) 2 str. 1 ir 3 d. Įstatymo 2 str. 1 d. įtvirtinta, kad 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, atliekančioms 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 vagystė elektroninėje erdvėje vertinama gana kontraversiškai. Be to, Lietuvoje vis dar nėra pakankamai praktikos, kaip galiojančios teisės normos taikomos tapatybės vagystės elektroninėje erdvėje atvejais. Tai nurodė ir kai kurie autorių apklausti ekspertai (2-asis ir 3-iasis).

Taigi, ar reikia kriminalizuoti veiką, kai asmuo, neturėdamas tam teisės disponuoja kito asmens duomenimis ir (ar) asmenine informacija, ir kyla nusikalstamų veikų rizika, kurios potencialiai gali būti padarytos pasinaudojant tapatybės vagystės metu įgytais duomenimis ir (ar) informacija? Kada laikoma, kad veika pavojinga ir ją reikia kriminalizuoti? Kokios yra atitinkamos savarankiškos pavojingos veikos kriminalizavimo prielaidos?

Visų pirma pabrėžtina, kad remiantis demokratine teisės samprata baudžiamieji įstatymai skirti ne veikoms uždrausti, o bausti už nevykdy-

[386] Lietuvos Respublikos elektroninių ryšių įstatymas. *Valstybės žinios*, 2004-04-30, Nr. 69-2382.

mą tų draudimų, kuriuos nustatė konstitucinės ar kitos bendrosios reguliacinės teisės normos[387]. Pavyzdžiui, visi nusikaltimai žmogaus privatumui kaip draudžiami yra nurodyti ne Baudžiamojo kodekso XXIV skyriaus normose[388], bet Konstitucijos[389] 22 straipsnyje „Žmogaus privatus gyvenimas neliečiamas“. Tačiau baudžiamasis įstatymas nustato konkrečius minėtos konstitucinės normos pažeidimų būdus ir sankcijas už jas[390]. Minėtas Konstitucijos 22 straipsnis, taip pat ir kiti ypač svarbūs tuo, kad jų draudimai nėra orientuoti tik į šiuo momentu žinomus konkrečius asmens privatumo pažeidimo būdus, bet ir į visus galimus pažeidimo būdus ateityje, tai labai svarbu, žinant, kad tapatybės vagystės atlikimo būdai nuolatos keičiasi, o dalis jų net nėra įvardyti Baudžiamajame kodekse. Asmens privatumo pažeidimo būdai, kurie šiuo momentu aprašyti Baudžiamajame kodekse, yra baigtiniai, pateikiant visų galimų pažeidimų atlikimo būdų sąrašą. Atsakomybė numatyta tik už tam tikru metu įstatymų leidėjui žinomus pažeidimų būdus, tačiau konkrečios normos nebuvimas nereiškia, kad neaprašytas kėsinimosi būdas yra neuždraustas ir tokia veikia yra nepavojinga. Konstitucinės normos nustato universalius draudimus, nepalieka spragų[391]. Spragos galimybė paliekama tik baudžiamuosiuose įstatymuose dėl operavimo baigtiniu pažeidimų būdų sąrašu[392]. Remiantis vyraujančia teisės samprata Lietuvoje, kai konkretus, naujas asmens privatumo pažeidimo būdas neaprašytas baudžiamajame kodekse, toks pažeidimas, nors jį ir draudžia minėta Konstitucijos norma, nėra laikomas nusikaltimu. Tačiau, remiantis A. Vaišvilos teorija, antroji tapatybės vagystės elektroninėje erdvėje stadija yra uždrausta Lietuvos Respublikos Konstitucijos 22 straipsnio, todėl Lietuvos Respublikos baudžiamajame kodekse turėtų būti įtvirtintos normos dėl sankcijų skyrimo už šią pavojingą savarankišką veiką.

Tapatybės vagystės elektroninėje erdvėje kaip savarankiškos veikos kriminalizavimo klausimas keltinas atsižvelgiant į veikos pavojingumo požymį. Anot V. Piesliako, ne visi socialiai žalingi poelgiai tampa nusi-

[387] Vaišvila, A. 2009. *Teisės teorija*. 3-iasis leid. Vilnius: Mykolo Romerio universitetas.

[388] Lietuvos Respublikos baudžiamasis kodeksas. *Valstybės žinios*, 2000, Nr. 89-2741.

[389] Lietuvos Respublikos Konstitucija. *Valstybės Žinios*, 1992, Nr. 33-1014.

[390] Vaišvila, A. 1998. Baudžiamoji justicija – juridinė asmens teisinio statuso identifikacija, *Teisės problemos* 3–4 (21, 22): 131.

[391] *Ibid*., p. 135.

[392] *Ibid.*

kalstamomis veikomis. Vienas iš pagrindinių reikalavimų tokiam poelgiui – žmogaus poelgio (veikos) pavojingumas[393]. Žmogaus poelgio pavojingumas yra pirmasis nusikalstamos veikos požymis ir veikos kriminalizavimo prielaida. Žodis „pavojingas“ baudžiamojoje teisėje aiškinamas kaip kas nors, keliantis pavojų, darantis žalą, besikėsinantis ar kažką pažeidžiantis. Galiausiai, anot V. Piesliako, nusikalstama – tai pavojinga viešpataujančiai vertybių sistemai veika[394], taip pat kaip nusikalstamos pripažįstamos ne šiaip pavojingos veikos, o pačios pavojingiausios – veikos, kuriomis kėsinamasi į didžiausias vertybes[395].

Tapatybės vagystės elektroninėje erdvėje veikos pavojingumas nekelia abejonių. Šia veika kėsinamasi į vienas iš svarbiausių vertybių: asmens teisę į privatumą ir nuosavybės teisinius santykius. Gali kilti klausimas, gal tapatybės vagystę elektroninėje erdvėje kaip savarankišką veiką užtektų pripažinti ne nusikaltimu, o kitu teisės pažeidimu (pavyzdžiui, administracinės teisės pažeidimu)? Anot V. Piesliako, iš principo nusikaltimai skiriasi nuo kitų teisės pažeidimų didesniu pavojingumu. Nusikaltimo statusas suteikiamas pavojingiausioms žmogaus elgesio formoms. Atskiriant nusikaltimus ir kitus teisės pažeidimus vadovaujamasi panašiais kriterijais kaip ir atskiriant nusikaltimus ir baudžiamuosius nusižengimus, t. y. pagal tam tikrus nusikalstamos veikos sudėties požymius. Vienas iš tokių požymių, dažnai naudojamas įstatymo leidėjo, yra nusikalstamos veikos dalykas, materiali jo vertė ar kiti dalyko požymiai[396]. Autorių nuomone, tapatybės vagystės elektroninėje erdvėje atveju labai svarbūs kiti dalyko požymiai: grėsmė ir tikslas atlikti kitas nusikalstamas veikas. Pavyzdžiui, su asmens tapatybe susijusios informacijos laikymas yra būtina sąlyga įvykdyti kitus nusikaltimus, tarkim, lėšų grobimą. Kaip pavyzdį galima paminėti ir LR BK 309 str. 2 d., kurioje kriminalizuotas pornografinės medžiagos apie vaikus laikymas, keliantis pavojų, kad nusikaltėlis, laikydamas tokią medžiagą, realybėje gali imtis neteisėtų veiksmų prieš vaikus.

Paminėtini ir autorių atliktos ekspertų apklausos rezultatai. Pasisakantys už veikos kriminalizavimą ekspertai grindė savo nuomonę šiais

[393] Piesliakas, V. 2009. *Lietuvos baudžiamoji teisė*. Antra pataisyta ir papildyta laida. Kn. 1. Vilnius: Justitia, p. 125.
[394] *Ibid.*, p. 126.
[395] *Ibid.*, p. 128.
[396] *Ibid*., p. 157.

argumentais: 2-asis ekspertas siūlė tapatybės vagystę elektroninėje erdvėje kriminalizuoti kaip savarankišką nusikalstamą veiką dėl specifikos. nes šią intelektinio pobūdžio veiką paprasta išskaidyti į atskiras dalis, kurias galima realizuoti lygiagrečiai, todėl labai sparčiai, kai kurie jų dalyviai gali net nesuprasti, kad jie dalyvauja nusikalstamoje veikloje. Labai sudėtinga įvertinti, kokiems tolesniems nusikaltimams planuojami ir galimi panaudoti TVEE duomenys; 7-asis ekspertas atsakydamas į šeštąjį klausimą teigė, kad atsakomybė už tapatybės vagystę elektroninėje erdvėje yra fragmentiška ir tik dalis veikų kriminalizuota, todėl siūlė tapatybės vagystę kriminalizuoti; 8-asis ekspertas nurodė, kad kriminalizavimas drausmintų potencialius vagystės vykdytojus; 9-asis ekspertas savo nuomonę grindė didėjančia šio neigiamo reiškinio žala ir mastu.

Taigi, LR BK normų sisteminė analizė ir atlikti tyrimai patvirtino, kad tapatybės vagystės elektroninėje erdvėje vertinimas iš baudžiamosios teisės pozicijų yra pakankamai sudėtingas, todėl LR BK būtų tikslinga įtvirtinti tapatybės vagystės elektroninėje erdvėje kaip savarankiškos nusikalstamos veikos sudėtį – tai leistų panaikinti tapatybės vagystės teisinio reguliavimo spragas, palengvintų minėtos veikos įrodinėjimą ir kvalifikavimą, be to, siekiant patraukti asmenį baudžiamojon atsakomybėn, tai padėtų išvengti gana sudėtingo nusikalstamų veikų daugeto įrodinėjimo.

TAPATYBĖS VAGYSTĖS ELEKTRONINĖJE ERDVĖJE, KAIP NUSIKALSTAMOS VEIKOS, 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, 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 reikšmingas nusikalstamos veikos kaip atitinkamo poelgio požymių atskleidimas ir jų formalizavimas įstatyme. Šiuo aspektu nusikalstama veika apibrėžiama kaip sąmoningas ir valingas, pavojingas, prieštaraujantis 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[397]. 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[398].

Nusikalstamos veikos sudėtį sudaro tam tikri požymiai, kurie skirstomi į objektyviuosius ir subjektyviuosius. Kadangi, autorių nuomone, galiojančios baudžiamojo įstatymo normos neapima visų tapatybės vagystės elektroninėje erdvėje elementų, ši veika turėtų būti kriminalizuota kaip savarankiška nusikalstama veika. Atsižvelgiant į tai, toliau bus nagrinėjami objektyvieji ir subjektyvieji tapatybės vagystės elektroninėje erdvėje požymiai, konstruojant tapatybės vagystės elektroninėje erdvėje sudėties modelį, kuris įstatymo leidėjo galėtų būti vertinamas kaip galimas LR BK specialiosios dalies pakeitimo projektas.

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[399].

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. ar kitų LR BK straipsnių 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

[397] Piesliakas, V. 2009. *Lietuvos baudžiamoji teisė*. Antra pataisyta ir papildyta laida. Kn. 1. Vilnius: Justitia, p. 175.

[398] *Ibid.*, p. 178.

[399] *Ibid.*, p. 180, 181.

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 ir dalykas. Nagrinėjant bendruosius tapatybės vagystės kriminalizavimo aspektus, buvo minėta, kad 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 informacinėmis ir ryšio technologijomis. Be to, tapatybės vagystės atveju gali būti pasikėsinta ne tik į duomenų saugumą, bet kartu ir į privataus gyvenimo neliečiamumą, nuosavybę, turtines teises ir interesus, valdymo tvarką, finansų sistemą ar net nacionalinį saugumą, t. y. tapatybės vagystė elektroninėje erdvėje gali būti nukreipta prieš žmogaus teises, laisves ir saugumą, tautos puoselėjamas vertybes, valstybės nepriklausomybę, konstitucinę santvarką, valstybės teritorijos vientisumą, aplinką ir kultūros paveldą, visuomenės sveikatą (pavyzdžiui, terorizmo išpuoliai, energetikos sektoriaus darbo sutrikdymas, valstybės paslapties atskleidimas ir pan.). Pažymėtina, kad elektroniniai nusikaltimai gali būti nukreipti prieš strateginę reikšmę nacionaliniam saugumui ar didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinčias informacines sistemas ar šiose sistemose esančius elektroninius duomenis[400].

Atsižvelgiant į tai, kad tapatybės vagystė gali būti įvykdoma ne tik elektroninėje, bet ir fizinėje erdvėje, 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, kad vagystės objektas yra visų rūšių ir

[400] *LR Baudžiamojo kodekso komentaras*, II dalis, 2009, p. 417.

formų nuosavybė, o turtas pagal LR BK 178 str. – tai turintys vertę ir fizinius parametrus (matmenis, svorį, skaičių, kiekį) daiktai (pavyzdžiui, namų apyvokos daiktai, transporto ir gamybos priemonės, asmeniniai daiktai, taip pat pinigai ir vertybiniai popieriai)[401]. Taigi, remiantis LAT pozicija, vagystės dalykas yra svetimas materialus judamas (kilnojamo pobūdžio), turtas, turintis ekonominę vertę, tačiau 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, kad sąvoka „tapatybės vagystė" apskritai vartojama netinkamai, kadangi informacija pati savaime negali būti pavogta. Veika tokiu atveju kaip vagystė galėtų būti kvalifikuojama tik tada, jei duomenys, kuriais remiantis galima identifikuoti asmenį, yra kokios nors apčiuopiamos formos, nuosavybės teise priklausančios kitam asmeniui, pavyzdžiui, pavogta mokėjimo kortelė[402].

Toks požiūris kritikuotinas. Sparčiai tobulėjant 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 atitinkančių daiktų, o neteisėtai disponuojant tokia informacija ir (ar) duomenimis nukentėjusiajam gali būti padaryta didelė žala.

Jungtinių Tautų tarpvyriausybinė ekspertų grupė, kuri 2007 m. atliko mokslinį tyrimą sukčiavimo ir nusikalstamo piktnaudžiavimo tapatybe ir jos klastojimo tema, laikosi požiūrio, kad tapatybės vagystė apima tokius atvejus, kai informacija, susijusi su asmens tapatybe, įskaitant asmenį identifikuojančią informaciją ir kai kuriais atvejais – kitą asmeninę informaciją, faktiškai yra paimama vagystei ar sukčiavimui analogiškais būdais, įskaitant materialių dokumentų ir informacijos, esančios materialioje laikmenoje, vagystę, dokumentų ar informacijos, kurie palikti be priežiūros ar yra laisvai prieinami, paėmimas, taip pat apgaulės būdu iš kitų asmenų tokių dokumentų ar informacijos išviliojimas[403].

[401] 2005 m. birželio 23 d. Lietuvos Aukščiausiojo Teismo Senato nutarimas Nr. 52 „Dėl teismų praktikos vagystės ir plėšimo baudžiamosiose bylose", 4 punktas [interaktyvus, žiūrėta 2011-09-19]. <http://www.lat.lt/4_tpbiuleteniai/senos/nutartis.aspx?id=29259>.

[402] Walden, I. 2007. *Computer Crimes and Digital Investigations*, p.116.

[403] Online Identity Theft. OECD, 2009. p. 49 [interaktyvus, žiūrėta 011-09-19]. < http://browse.oecdbookshop.org/oecd/pdfs/browseit/9309021E.PDF>.

Autorių nuomone, tapatybės vagystės dalyku turėtų būti laikoma informacija ir (ar) duomenys, kuriuos naudojant gali būti nustatyta asmens tapatybė, nesvarbu, ar tokia informacija ir (ar) duomenys yra elektronine forma, ar saugomi 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, tačiau elektroninėje erdvėje – ne tik prieš konkretų asmenį (pavyzdžiui, panaudojant nepageidaujamas elektroninio pašto žinutes), bet ir prieš informacines sistemas bei elektroninių ryšių tinklus, kuriuos naudojant tvarkomi duomenys. 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 šioje monografijoje 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 saugomą teisinį gėrį, atlikimu. Kiekvieną veikimo veiksmą sudaro sąmoningas ir valingas žmogaus kūno judesys. Tapatybės vagystė elektroninėje erdvėje taip pat padaroma veikiant, 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, skleidžiant ar kitaip naudojant 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

būtų padaryta atitinkama žala, norint patraukti asmenį atsakomybėn. Atsakomybė užtraukiama 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. Kodėl tapatybės vagystės elektroninėje erdvėje sudėtis turėtų būti formali, pagrindinis argumentas 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 leidėjų formuluojant nusikalstamų veikų sudėtis[404]. 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

[404] Piesliakas, V. 2009. *Lietuvos baudžiamoji teisė*. Antra pataisyta ir papildyta laida. Kn. 1. Vilnius: Justitia, p. 298.

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; o 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.

Tačiau atsižvelgiant į tai, kad sparčiai tobulėjant informacinėms ir ryšio technologijoms informacinėje visuomenėje įprastai vartojamos sąvokos įgauna naujas prasmes ir požymius, ir šiuo atveju, nagrinėjant tapatybę elektroninėje erdvėje, galima atsiriboti nuo įrankio materialaus pobūdžio. Tokiu atveju į „įrankio“ kategoriją patektų nepageidaujamos elektroninio pašto žinutės, falsifikuoti interneto tinklapiai, kurie naudojami turint tikslą išgauti prisijungimo prie informacinių sistemų slaptažodžius ar kitus konfidencialius duomenis, 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 elektroninėje terpėje (įskaitant 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.

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[405].

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[406].

LR BK nepateikiama pakaltinamumo sąvoka, tačiau ji nesunkiai suformuluojama pasitelkiant nepakaltinamumo apibrėžimą, įtvirtintą 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 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[407].

LR BK skiriamos dvi kaltės formos: tyčinė ir neatsargi kaltė. Pabrėžtina tai, kad tapatybės vagystė elektroninėje erdvėje gali būti 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

[405] Piesliakas, V. 2009. *Lietuvos baudžiamoji teisė*. Antra pataisyta ir papildyta laida. Kn. 1. Vilnius: Justitia, p. 180, 181, 319.

[406] *Ibid.*, p. 325.

[407] *Ibid.*, p. 336.

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"[408]. Iš pirmo žvilgsnio gali pasirodyti, kad 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 naudodamas tokius duomenis ir (ar) asmeninę informaciją, 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, kurį identifikuojantys duomenys ir asmeninė informacija buvo pasisavinti (pvz., vartotojo vardas, slaptažodis, PIN kodas, kodų kortelės ir kita), bei atlikti nusikalstamas veikas – nusikaltimus ir (ar) baudžiamuosius nusižengimus. Tuo tarpu piktnaudžiaudamas tapatybe subjektas nesiekia įvykdyti jokios nusikalstamos veikos, o minėtus

[408] *Ibid.*, p. 414, 415.

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 gali realizuoti 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.

LIETUVOS RESPUBLIKOS BAUDŽIAMOJO KODEKSO SPECIALIOSIOS DALIES PAKEITIMO PROJEKTAS

Ankstesnėse monografijos dalyse aptarus tapatybės vagystės elektroninėje erdvėje, kaip savarankiškos nusikalstamos veikos, objektyviuosius ir subjektyviuosius sudėties požymius, siūlytinas alternatyvus LR BK specialiosios dalies 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 specialiąją dalį 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, kurį identifikuojančios priemonės buvo gauto, tačiau *neturėdamas tikslo įvykdyti nusikalstamą veiką*.

Taigi siūlomas trečias ir, atrodo, optimalus problemos sprendimo variantas – LR BK specialiąją dalį papildyti nauju straipsniu, kuriame būtų numatoma atsakomybė už skirtingas tapatybės vagystės rūšis. Tapatybės vagystės įvykdymas elektroninėje erdvėje pasinaudojant informacinėmis ir ryšio technologijomis 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 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 įsibroveęs į patalpą, saugyklą ar saugomą teritoriją <...>“); BK 187 str. 1 d. reglamentuoja svetimo turto sunaikinimą ar suga-

dinimą, 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, kad tapatybės vagystė elektroninėje erdvėje yra pavojingesnė už tapatybės vagystę fizinėje erdvėje: fizinėje erdvėje apsisaugoti nuo tapatybės vagystės yra santykinai paprasta, o 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, kad tapo minėtos veikos aukomis. Reikia pabrėžti, kad 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, į abiejų veikų sudėtį turėtų būti įtrauktas ir įtvirtintas nusikalstamų ketinimų požymis. Tame pačiame straipsnyje, be minėtų nusikalstamų veikų sudėties, 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, neteisėtai perėmė, įgijo, laikė, naudojo, paskleidė, ar atliko kitokius veiksmus su asmens duomenimis ir (ar) asmenine informacija apie kitą asmenį, siekdamas identifikuotis kaip asmuo, kurį identifikuojantys duomenys ir (ar) asmeninė informacija buvo pasisavinta ar kitaip surinkta, 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...

Apibendrinančios išvados

• Atlikus Jungtinių Amerikos Valstijų, Jungtinės Karalystės, Nigerijos, Prancūzijos, Suomijos, Estijos, Rusijos, Kinijos ir Lietuvos baudžiamųjų įstatymų teisės normų analizę, nustatyta, kad tapatybės vagystės, kaip savarankiškos nusikalstamos veikos, sudėtis yra įtvirtinta tik Jungtinių Amerikos Valstijų baudžiamajame įstatyme; šios valstybės teisės aktai numato baudžiamąją atsakomybę už visas tris tapatybės vagystės stadijas: su tapatybe susijusios informacijos gavimą, sąveiką su tokio pobūdžio informacija bei su tapatybe susijusios informacijos panaudojimą siekiant įvykdyti nusikaltimą. Tuo tarpu kitose valstybėse tapatybės vagystė laikoma kitų nusikalstamų veikų sudedamąja dalimi.

• Analizei pasirinktų valstybių baudžiamuosiuose įstatymuose, išskyrus Jungtinių Amerikos Valstijų, yra kriminalizuoti pirmosios, antrosios ir trečiosios tapatybės vagystės stadijų elementai, tačiau antrosios tapatybės vagystės stadijos elementas – su tapatybe susijusios informacijos turėjimas – baudžiamosios atsakomybės pagal galiojančius baudžiamuosius įstatymus neužtraukia.

• Tapatybės vagystės elektroninėje erdvėje kaip pavojingos veikos vertinimas baudžiamosios teisės požiūriu įvairiose valstybėse skiriasi, ir tai, kad tapatybės vagystė nėra kriminalizuota kaip savarankiška nusikalstama veika, apsunkina tokių veikų susekimą, tyrimą ir baudžiamąjį persekiojimą nacionaliniu ir tarptautiniu lygiu.

• Už tapatybės vagystę dažniausiai baudžiama pinigine bauda arba laisvės atėmimu, tačiau kai kurių užsienio valstybių baudžiamuosiuose įstatymuose numatomos gana įvairios ir kartais labai griežtos bausmės: nuo piniginės baudos iki laisvės atėmimo iki gyvos galvos. Didžiausia sankcijų įvairovė už tapatybės vagystės elementus įtvirtinta Rusijos ir Kinijos baudžiamuosiuose įstatymuose, griežčiausios – Jungtinių Amerikos Valstijų, Nigerijos ir Rusijos baudžiamuosiuose įstatymuose, vienos iš švelniausių – Estijos ir Suomijos baudžiamuosiuose kodeksuose.

• Išanalizavus tapatybės vagystės kaip savarankiškos nusikalstamos veikos požymius, akcentuotinas šios veikos pavojingumas ir siūlytina

tapatybės vagystę kriminalizuoti. Lietuvoje 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 specialiąją dalį papildyti nauju straipsniu, kuriame būtų numatoma atsakomybė už skirtingas tapatybės vagystės rūšis.

• Tapatybės vagystės (tapatybės pasisavinimo nusikalstamais tikslais) įvykdymas elektroninėje erdvėje pasinaudojant informacinėmis ir ryšio technologijomis 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 nei tapatybės vagystė (tapatybės pasisavinimas nusikalstamais tikslais) fizinėje erdvėje.

3.5. Kitos atsakomybės rūšys Lietuvoje už tapatybės vagystę elektroninėje erdvėje

Už tapatybės vagystę elektroninėje erdvėje gali kilti ne tik baudžiamoji, bet ir civilinė ar administracinė atsakomybė[409]. Vertybės gali būti ginamos ir civilinės ar administracinės teisės normų[410]. Šios atsakomybės rūšys panagrinėtinos detaliau.

3.5.1. Civilinė atsakomybė už tapatybės vagystę elektroninėje erdvėje

Tapatybės vagystės elektroninėje erdvėje termino dalis – vagystė – suponuoja, kad ši pavojinga veika turėtų būti traktuojama kaip nusikalstama veika arba bent jau kaip administracinės teisės pažeidimas. Tačiau įvertinant tai, kad tapatybės vagystė elektroninėje erdvėje yra kompleksinis, sudėtingas ir įvairiose užsienio valstybėse skirtingai vertinamas socialinis teisinis reiškinys, monografijos autoriai siekia aptarti visas galimas

[409] Rannenberg, K.; Royer, D.; Deuker, A. 2009. *The Future of Identity in the Information Society*. Springer-Verlag, p. 327.

[410] Piesliakas, V. 2009. *Lietuvos baudžiamoji teisė*. Antra pataisyta ir papildyta laida. Kn. 1. Vilnius: Justitia, p. 127.

atsakomybės už šią veiką rūšis, neapsiribodami lingvistine šio reiškinio reikšme. Taigi, šioje dalyje bus nagrinėjama civilinė atsakomybė už tapatybės vagystę elektroninėje erdvėje.

Tapatybės vagystės elektroninėje erdvėje auka gali patirti ne tik didžiulius finansinius nuostolius, bet ir emocinės, psichologinės žalos, todėl tokiu atveju veiksminga patirtos žalos atlyginimo priemone tampa civilinės atsakomybės institutas.

Piniginiai nuostoliai tapatybės vagystės atveju vidutiniškai sudaro 6 000 dolerių, o nukentėjusieji nuo šios pavojingos veikos praranda daug laiko (vidutiniškai 40 valandų) ir patiria neigiamų emocijų, siekdami pašalinti esamus ir užkirsti kelią galimiems neigiamiems padariniams[411]. Dažniausiai tapatybės vagystės elektroninėje erdvėje aukos patiria skausmingus emocinius išgyvenimus, susiduria su nepatogumais kasdienio gyvenimo situacijose, patiria gėdos ir pažeminimo jausmą, kai, pavyzdžiui, kreipęsi dėl paskolos gauna neigiamą atsakymą ir informuojami, kad jie yra įtraukti į asmenų, turinčių neįvykdytų skolinių įsipareigojimų ir (arba) prieš kuriuos pradėtas išieškojimo procesas, sąrašą.

Nors atsigauti nukentėjus nuo tokio pobūdžio veikos nėra lengva, tiek baudžiamoji, tiek civilinė teisė užtikrina teisę reikalauti aukos patirtų nuostolių atlyginimo ir siekti teisingumo, kad teisės pažeidėjas ir (arba) atsakinga trečioji šalis būtų patraukti atsakomybėn.

Paprastai tapatybės vagystės elementai užtraukia baudžiamąją atsakomybę, kai neteisėtai panaudojus kitą asmenį identifikuojančią informaciją pasisavinami pinigai arba gaunamos paslaugos, įvykdomas sukčiavimas ar kita neteisėta veika. Nagrinėjant tapatybės vagystę elektroninėje erdvėje asmens turtinių santykių srityje, daugiausia tapatybės vagyste pasinaudojama siekiant įvykdyti kreditinių kortelių sukčiavimą, tačiau taip pat gali būti pasikėsinta į banko sąskaitas, ryšio operatorių paslaugas, viešojo sektoriaus teikiamas pašalpas ir į daugybę kitų finansinio pobūdžio transakcijų.

Tapatybės vagystės elektroninėje erdvėje auka gali ginti savo pažeistas teises pasinaudodama civilinės atsakomybės priemone – restitucija, kurios metu būtų atlyginti patirti finansiniai nuostoliai, tačiau valstybėse, kur tapatybės vagystė yra kriminalizuota, dažnos situacijos, kai nukentė-

[411] Johannes, R. 2006 Identity Fraud Survey Report (abridged) (Javelin Strategy Research Jan. 2006) [interaktyvus, žiūrėta 2011-09-19]. <www.javelinstrategy.com/products/99DEBA/27/delivery.pdf>.

jusieji pareiškia civilinį ieškinį baudžiamojoje byloje. Pavyzdžiui, 2008 m. JAV Tapatybės vagystės vykdymo ir jos sukeltos žalos atlyginimo akte[412] (angl. *Identity Theft Enforcement and Restitution Act of 2008*) įtvirtinta, kad asmuo, įvykdęs tapatybės vagystę, nukentėjusiajam turi sumokėti kompensaciją už jo pagrįstai sugaištą laiką, siekiant užkirsti kelią būsimiems ar pašalinti jau kilusius tapatybės vagystės padarinius. Taigi tapatybės vagystės elektroninėje erdvėje auka gali pareikšti kaltinimus įtariamajam, siekdama piniginės kompensacijos tiek už patirtus piniginius nuostolius, tiek už neturtinę žalą, pavyzdžiui, už sielvartą, fizines kančias, neigiamus emocinius išgyvenimus.

Kai kuriose Jungtinių Amerikos valstijų valstijose, pavyzdžiui, Kalifornijoje[413], Ajovoje[414], Luizianoje[415], Naujajame Džersyje[416], Pensilvanijoje[417], galiojantys teisės aktai numato, kad tapatybės vagystės bylos gali būti nagrinėjamos civilinio proceso tvarka, ir asmenims, tapusiems tapatybės vagystės aukomis, gali būti priteista tris kartus didesnė suma nei jų patirti nuostoliai bei advokato išlaidos.

Pažymėtina, kad civilinė atsakomybė gali kilti ne tik neteisėtus veiksmus atlikusiam asmeniui, bet ir trečiajai šaliai, dėl kurios veiksmų asmuo tapo tapatybės vagystės elektroninėje erdvėje auka, ar net pačiai tapatybės vagystės elektroninėje erdvėje aukai.

Trečiosios šalies veiksmai, už kuriuos jai gali kilti civilinė atsakomybė, gali būti suskirstyti į keturias pagrindines kategorijas[418]:

---

412 Identity Theft Enforcement and Restitution Act of 2008 [interaktyvus, žiūrėta 2011-09-20]. <http://www.govtrack.us/congress/billtext.xpd?bill=h110-5938>.

413 Cal. Civ. Code [section] 1798.92-1798.97. [interaktyvus, žiūrėta 2011-09-20]. <http://www.leginfo.ca.gov/cgi-bin/calawquery?codesection=civ&codebody=&hits=20>.

414 Iowa Code [section] 714.16B. [interaktyvus, žiūrėta 2011-09-20]. <http://coolice.legis.state.ia.us/coolice/default.asp?category=billinfo&service=iowacode&ga=83&input=714>.

415 La. Stat. Ann. [section] 9:3568. [interaktyvus, žiūrėta 2011-09-20] <http://www.legis.state.la.us/lss/lss.asp?folder=83>.

416 N.J. Stat. Ann. [section] 56:11-50. [interaktyvus, žiūrėta 2011-09-20]. <http://www.njleg.state.nj.us/2004/bills/pl05/226_.htm>.

417 42 Pa. Consol. Stat. Ann. [section] 8315. [interaktyvus, žiūrėta 2011-09-20]. <http://law.onecle.com/pennsylvania/judiciary-and-judicial-procedure/index.html>.

418 Civil liability for identity theft: identity theft can cause catastrophic financial damage, but many victims also suffer emotional, psychological, and even physical injuries. Civil claims against the responsible parties can help repair the damage [interaktyvus]. 2007-02-01 [žiūrėta 2011-09-20]. <http://goliath.ecnext.com/coms2/gi_0199-6285492/Civil-liability-for-identity-theft.html>.

1) nerūpestingumas asmeninės informacijos saugumo srityje: asmenį identifikuojanti informacija suteikia prieigą prie to asmens banko sąskaitų, be to, ja remiantis suteikiamos paskolos, todėl juridiniai asmenys, tvarkantys asmens duomenis, privalo imtis atitinkamų saugumo priemonių ir užtikrinti, kad tokie duomenys nebūtų panaudoti neteisėtiems tikslams. Nors nė viena organizacija negali šimtu procentų apsisaugoti nuo neteisėtų trečiųjų asmenų veiksmų, ji neabejotinai gali sumažinti tokio pobūdžio veiksmų tikimybę, nesudarydama galimybės lengvai prieiti prie svarbios informacijos. Priežastinio ryšio įrodinėjimas teisminio proceso metu yra pakankamai sudėtingas, tačiau technologijų amžiuje turi būti įvertintos visos aplinkybės, kurios leidžia iš anksto numatyti neteisėtų veiksmų riziką.

2) nerūpestingas tokios informacijos perdavimas: galimos situacijos, kai verslo subjektai parduoda asmeninio pobūdžio informaciją tretiesiems asmenims, nesiimdami priemonių nustatyti, kokiais tikslais tokia informacija bus naudojama. Kaip pavyzdį galima paminėti Naujojo Hempšyro *Remsburg v. Docusearch, Inc.* persekiojimo ir žmogžudystės bylą[419], kurioje Liam Youens sukūrė interneto tinklalapį, kuriame atvirai dalijosi savo ketinimais nužudyti Amy Boyer. Pasinaudodamas tyrimų elektroninėje erdvėje tinklalapiu Docusearch.com, L. Youens gavo asmeninės informacijos apie A. Boyer. Per šešias savaites atlikęs penkias transakcijas už 204 dolerius, kuriuos sumokėjo Docusearch.com, L. Youens gavo duomenis apie A. Boyer gimimo datą, socialinio draudimo numerį, darbovietę ir gyvenamosios vietos adresą. Tada L. Youens nuėjo į A. Boyer darbovietę ir ją, išeinančią iš darbo, nušovė, po to nusišovė pats. Teismo pozicija buvo tokia, kad kompanija galėtų būti patraukta atsakomybėn, kadangi kiekvienas asmuo turi teisinę pareigą kitam asmeniui nesukelti neprotingo žalos pavojaus, kai pavojų galima iš anksto numatyti.

3) bankų nesugebėjimas apsisaugoti nuo tapatybės vagystės arba sumažinti jos padarytą žalą. Šios kategorijos veiksmus galima iliustruoti Pietų Karolinos *Murray v. Bank of America, N. A.*[420] byla: 1997 m. gegužę Margareta Murray pametė savo vairuotojo pažymėjimą. Po mėnesio

[419] Remsburg v. Docusearch, Inc. [interaktyvus, žiūrėta 2011-09-20]. <http://www.courts.state.nh.us/supreme/opinions/2003/remsb017.htm>.

[420] Murray v. Bank of America, N.A. [interaktyvus, žiūrėta 2011-09-20]. <http://www.judicial.state.sc.us/opinions/displayOpinion.cfm?caseNo=3634>.

kita moteris Amerikos banke M. Murray vardu atidarė sąskaitą ir išrašė 60 suklastotų čekių, kurių bendra vertė sudarė 7 500 dolerių. Tų pačių metų birželio mėnesį M. Murray nuėjo į banką ir išsiaiškinusi pareikalavo banko darbuotojų šią apgaulingą sąskaitą uždaryti bei paprašė informuoti apie tai asmenis, gavusius suklastotus čekius, bei apie šį įvykį pranešė policijai. Bankas tik po mėnesio uždarė sąskaitą ir neįspėjo nė vieno, kuris gavo suklastotą čekį, apie tai, kad M. Murray yra nekalta. Lapkritį M. Murray buvo suimta ir apkaltinta bankiniu sukčiavimu. M. Murray kalėjime praleido 12 valandų, po kurių paleista už užstatą. Vėliau ji gavo laišką iš banko, patvirtinantį, kad ji nebuvo tas asmuo, kuris atidarė apgaulingą sąskaitą, taigi, jai buvo panaikinti visi kaltinimai. Tačiau dėl patirtos prievartos arešto metu, streso ir rūpesčių M. Murray pateikė bankui ieškinį dėl nerūpestingumo, kurį teismas patenkino.

4) finansines ataskaitas teikiančių institucijų nesugebėjimas apsisaugoti nuo sukčiavimo. Pavyzdžiui, JAV Sąžiningų kredito ataskaitų įstatymas (angl. *Fair Credit Reporting Act*[421]) nustato, kad institucijos, teikiančios vartotojų ataskaitas, asmeninę informaciją tretiesiems asmenims gali atskleisti tik esant tam tikroms aplinkybėms. Institucijai, kuri tyčia nesilaiko įstatymo reikalavimų, kyla civilinė atsakomybė: pažeidimo atveju vartotojas gali reikalauti atlyginti patirtą žalą ir advokato išlaidas. Taip pat civilinė atsakomybė kyla, kai teisės normos pažeidžiamos dėl nerūpestingumo. Vartotojas su ieškiniu gali kreiptis tiek į valstijos, tiek į federalinį teismą, tačiau ne vėliau kaip per 2 metus nuo pažeidimo paaiškėjimo ir ne vėliau kaip per 5 metus nuo pažeidimo padarymo.

Panagrinėkime, kaip tapatybės vagystės elektroninėje erdvėje atveju nukentėjęs asmuo galėtų ginti savo pažeistas teises Lietuvoje, pasinaudodamas civilinės atsakomybės institutu.

Aptariant civilinę atsakomybę retais atvejais gali pasitaikyti, kad asmens duomenys pavagiami, kai auką ir subjektą sieja sutartiniai santykiai (pvz., viena sutarties šalis pažeidžia konfidencialumo, gautos informacijos saugojimo ar kitokius įsipareigojimus ir panaudoja teisėtai gautus duomenis ne pagal teisės normas, sutartį ir asmens duomenų subjekto valią), tačiau didžia dalimi atvejų aukos ir subjekto nesieja sutartiniai santykiai, todėl kyla deliktinė atsakomybė.

[421] Fair Credit Reporting Act. [interaktyvus, žiūrėta 2011-09-20] <http://www.ftc.gov/os/statutes/031224fcra.pdf>.

Tapatybės vagystės elektroninėje erdvėje atveju pasikėsinama į vieną iš pagrindinių žmogaus teisių – teisę į privataus gyvenimo neliečiamumą. Lietuvos Respublikos Konstitucijos[422] (toliau – Konstitucija) 22 straipsnis įtvirtinta, kad *žmogaus privatus gyvenimas neliečiamas. Asmens susirašinėjimas, pokalbiai telefonu, telegrafo pranešimai ir kitoks susižinojimas neliečiami. Informacija apie privatų asmens gyvenimą gali būti renkama tik motyvuotu teismo sprendimu ir tik pagal įstatymą. Įstatymas ir teismas saugo, kad niekas nepatirtų savavališko ar neteisėto kišimosi į jo asmeninį ir šeimyninį gyvenimą, kėsinimosi į jo garbę ir orumą.*

Pažymėtina, kad privataus gyvenimo apibrėžimas pirmą kartą buvo pateiktas 2002 m. rugsėjo 19 d. Konstitucinio Teismo nutarime[423], kuriame buvo išaiškinta, kad privatus žmogaus gyvenimas – tai individo asmeninis gyvenimas: gyvenimo būdas, šeimyninė padėtis, gyvenamoji aplinka, santykiai su kitais asmenimis, individo pažiūros, įsitikinimai, įpročiai, jo fizinė bei psichinė būklė, sveikata, garbė, orumas ir kt.

Iš Konstitucijoje įtvirtinto žmogaus privataus gyvenimo neliečiamumo kyla asmens teisė į privatumą. Konstitucinis Teismas 1999 m. spalio 21 d. nutarime[424] konstatavo, kad *asmens teisė į privatumą apima privatų, šeimos ir namų gyvenimą, asmens fizinę ir psichinę neliečiamybę, garbę ir reputaciją, asmeninių faktų slaptumą, draudimą skelbti gautą ar surinktą konfidencialią informaciją ir kt.* Taigi Konstitucinis Teismas teisės į privatų gyvenimą apsaugą susiejo su asmens garbės ir orumo apsauga, tačiau Lietuvos Respublikos civiliniame kodeksas (toliau – LR CK)[425] ir teismų praktika skiria teisę į privatų gyvenimą bei asmens garbės ir orumo gynimą kaip dvi savarankiškas asmens neturtines teises.

Atsižvelgiant į išdėstytas nuostatas, tapatybės vagystės elektroninėje erdvėje auka savo pažeistą teisę į privataus gyvenimo neliečiamumą gali ginti pasinaudodama Konstitucijos normas detalizuojančiomis civilinės teisės normomis. Pavyzdžiui, LR CK 2.23 straipsnis reglamentuoja teisę į privatų gyvenimą ir jo slaptumą. Minėto straipsnio 4 dalyje įtvirtinta,

[422] Lietuvos Respublikos Konstitucija. *Valstybės žinios*, 1992, Nr. 33-1014.

[423] Konstitucinio Teismo 2002 m. rugsėjo 19 d. nutarimas „Dėl Telekomunikacijų, Operatyvinės veiklos įstatymų ir Baudžiamojo proceso kodekso". *Valstybės žinios.* 2002, Nr. 93-4000.

[424] Konstitucinio Teismo 1999 m. spalio 21 d. nutarimas „Dėl vardų ir pavardžių rašymo Lietuvos Respublikos piliečio pase". *Valstybės žinios.* 1999, Nr. 90-2662.

[425] Lietuvos Respublikos civilinis kodeksas. *Valstybės žinios.* 2000, Nr. 74-2262.

kad *privataus asmens gyvenimo duomenų, nors ir atitinkančių tikrovę, paskelbimas, taip pat asmeninio susirašinėjimo paskelbimas pažeidžiant nustatytą tvarką, taip pat įėjimas į asmens gyvenamąjį būstą be jo sutikimo, išskyrus įstatymų numatytas išimtis, asmens privataus gyvenimo stebėjimas ar informacijos rinkimas apie jį pažeidžiant įstatymą bei kiti neteisėti veiksmai, kuriais pažeidžiama teisė į privatų gyvenimą, yra pagrindas pareikšti ieškinį dėl tokiais veiksmais padarytos turtinės ir neturtinės žalos atlyginimo*.

LR CK 2.22 straipsnyje reglamentuojama teisė į atvaizdą. Minėto straipsnio 1 dalyje įtvirtinta bendra taisyklė, kad *fizinio asmens nuotrauka (jos dalis), portretas ar kitoks atvaizdas gali būti atgaminami, parduodami, demonstruojami, spausdinami, taip pat pats asmuo gali būti fotografuojamas tik jo sutikimu*. 2 dalyje įtvirtinta bendros taisyklės išimtis, numatanti, kad *asmens sutikimo nereikia, jeigu šie veiksmai yra susiję su visuomenine asmens veikla, jo tarnybine padėtimi, teisėsaugos institucijų reikalavimu arba jeigu fotografuojama viešoje vietoje. Tačiau asmens nuotraukos (jos dalies), padarytos šiais atvejais, negalima demonstruoti, atgaminti ar parduoti, jeigu tai pažemintų asmens garbę, orumą ar dalykinę reputaciją*.

LR CK 2.21 straipsnis reglamentuoja teisės į vardą gynimą: *fizinis asmuo, kurio teisė į vardą yra pažeista dėl to, kad kitas asmuo neteisėtai veikia jo vardu ar kitokiu būdu neteisėtai pasisavina svetimą vardą, ar kliudo juo naudotis, turi teisę kreiptis į teismą ir reikalauti, kad teismas įpareigotų kaltą asmenį nutraukti tokius veiksmus bei atlyginti tokiais neteisėtais veiksmais padarytą turtinę ir neturtinę žalą.*

Pažymėtina, kad siekiant apginti savo pažeistas teises, pasinaudojant civilinę atsakomybę reglamentuojančiomis normomis, informacinėje visuomenėje susiduriama su tam tikromis problemomis. Šiuo metu yra gausybė socialinių tinklapių, kuriuose žmonės gali susikurti savo profilį, t. y. įkelti savo nuotrauką (-as), nurodyti asmeninius pomėgius, kontaktinius duomenis, atskleisti įvairaus pobūdžio asmeninę ir privataus gyvenimo informaciją ir pan. – asmeniui suteikiama teisė pačiam nuspręsti, kokią informaciją ir kiek jos atskleisti viešai apie privatų gyvenimą. Taigi, asmeniui, užsiregistravusiam socialiniame tinklapyje, suteikiama galimybė palaikyti kontaktą su socialinio tinklalapio bendruomenės nariais, kurie gali vertinti įkeltas nuotraukas, rašyti komentarus, dalyvauti diskusijose ir pan.

Kuo daugiau asmuo atskleidžia savo privataus gyvenimo detalių, tuo didesnė rizika tapatybės vagystės elektroninėje erdvėje atveju patirti didesnę žalą. Dažnai pasitaiko atvejų, kai iš kerštо, pykčio, pavydo ar kitų piktavališkų motyvų, asmuo socialiniame tinklapyje sukuria profilį kito – realaus – asmens vardu, t. y. įvykdo tapatybės vagystę ir naudodamasis tokiais profiliais skleidžia šmeižikišką, asmens, kurio vardu sukurtas profilis, garbę ir orumą žeminančią informaciją ir (arba) viešina to asmens privataus gyvenimo detales. Tokiu atveju asmuo, tapęs tapatybės vagystės elektroninėje erdvėje auka, gali ginti savo pažeistą teisę, pasinaudodamas ne tik LR CK 2.23 straipsnio 4 dalimi, bet ir LR CK 2.22 straipsnio 3 dalimi, numatančia, kad *fizinis asmuo, kurio teisė į atvaizdą buvo pažeista, turi teisę teismo tvarka reikalauti nutraukti tokius veiksmus bei atlyginti turtinę ir neturtinę žalą*, tačiau įrodinėjimas tokio pobūdžio bylose yra pakankamai sudėtingas. Labai svarbu įvertinti ir aplinkybę, kad elektroninėje erdvėje, pvz., internete padaryta žala gali būti daug kartų didesnė negu realioje erdvėje (pvz., neigiamos informacijos apie asmenį išplatinimas internete gali turėti daug didesnę sklaidą negu realioje erdvėje).

Taip pat asmuo, kurio garbė ir orumas nukentėjo nuo tokio pobūdžio veikos, savo pažeistas teises gali ginti pasinaudodamas LR CK 2.24 straipsniu, kurio 1 dalis įtvirtina bendrą taisyklę, kad *asmuo turi teisę reikalauti teismo tvarka paneigti paskleistus duomenis, žeminančius jo garbę ir orumą ir neatitinkančius tikrovės, taip pat atlyginti tokių duomenų paskleidimu jam padarytą turtinę ir neturtinę žalą*. Tuo atveju, *jei nevykdomas teismo sprendimas, įpareigojantis paneigti tikrovės neatitinkančius duomenis, žeminančius asmens garbę ir orumą, teismas nutartimi gali išieškoti iš atsakovo baudą už kiekvieną teismo sprendimo nevykdymo dieną. Baudos dydį nustato teismas ir ji yra išieškoma ieškovo naudai, nepaisant neturtinės žalos atlyginimo* (LR CK 2.24 straipsnio 7 dalis).

Paminėtina dar viena sritis, kurioje asmenys dažnai tampa tapatybės vagystės elektroninėje erdvėje aukomis – elektroninės paslaugos, kurioms naudojamos elektroninės bankininkystės tapatybės patvirtinimo priemonės.

Atlikus Lietuvos komercinių bankų elektroninių paslaugų teikimo sutartyse įtvirtintų tipinių sąlygų dėl banko, kliento bei naudotojo atsakomybės, kai tapatybės patvirtinimo priemonės tapo žinomos arba kilus grėsmei, kad jos gali tapti žinomos tretiesiems asmenims, galima daryti

išvadą, kad tapatybės vagystės elektroninėje erdvėje atveju banko klientas (naudotojas) susidurtų su sunkumais įrodinėdamas šios pavojingos veikos požymius ir savo nekaltumą, kadangi sutarčių nuostatos yra pakankamai griežtos, kategoriškos ir gana nepalankios naudotojo atžvilgiu. Manytina, kad tapatybės vagystės elektroninėje erdvėje atvejai kiekvieną kartą turėtų būti nagrinėjami individualiai, įvertinant visas pavojingos veikos padarymo aplinkybes.

Kaip pavyzdį panagrinėkime „Swedbank", AB tipinės elektroninių paslaugų teikimo sutarties sąlygas, numatančias sutarties šalių atsakomybę.

Sutartyje įtvirtinta, kad siekiant užtikrinti elektroninių kanalų (interneto bankas, bankas telefonu, automatinė paslauga, mobilus bankas) saugumą ir tai, kad operacijų sąskaitoje negalėtų atlikti kliento[426] neįgalioti asmenys, tapatybės patvirtinimo priemonės turi būti žinomos tik naudotojui[427], kuris privalo rūpestingai jas saugoti (nelaikyti kartu visų tapatybės patvirtinimo priemonių, atskirai saugoti identifikavimo kodų generatorių, identifikavimo kodų kortelę, nerašyti naudotojo identifikavimo kodo ir (arba) nuolatinio slaptažodžio ant identifikavimo kodų nustatymo priemonių ar kartu su jomis laikomų daiktų, nerašyti ant identifikavimo kodų generatoriaus jo slaptažodžio ir pan.). Naudotojas jokiais atvejais neturi teisės perduoti tretiesiems asmenims identifikavimo kodų nustatymo priemonių, leisti jiems sužinoti konkrečius identifikavimo kodus, nuolatinį slaptažodį ir (arba) identifikavimo kodų generatoriaus slaptažodį arba su minėtomis tapatybės patvirtinimo priemonėmis ir (arba) identifikavimo kodų nustatymo priemonėmis leisti kitaip susipažinti tretiesiems asmenims.

Iškilus grėsmei, kad tapatybės patvirtinimo priemones gali sužinoti tretieji asmenys, arba jeigu jos tapo žinomos tretiesiems asmenims ar atsiradus kitoms priežastims, dėl kurių elektroniniais kanalais naudotojo vardu gali pasinaudoti arba jau pasinaudojo tretieji asmenys, taip pat naudotojui praradus mobilųjį telefoną arba identifikavimo kodų nustatymo priemones, naudotojas privalo nedelsdamas pateikti bankui prašymą blokuoti naudotojui suteiktą identifikavimo kodą ir (arba) pakeisti tapa-

[426] Sutartyje nurodytas sąskaitos savininkas, sutartimi suteikiantis teisę naudotojui atlikti operacijas elektroniniais kanalais.

[427] Sutartyje nurodytas fizinis asmuo, kuriam klientas suteikia teisę atlikti operacijas elektroniniais kanalais. Naudotojas ir klientas gali būti tas pats fizinis asmuo.

tybės patvirtinimo priemones. Jeigu klientas sužino apie aplinkybes, dėl kurių elektroniniais kanalais naudotojo vardu gali pasinaudoti arba jau pasinaudojo tretieji asmenys, apie tokias aplinkybes klientas taip pat privalo nedelsdamas informuoti banką ir, savo nuožiūra, gali pateikti bankui prašymą panaikinti naudotojui teisę atlikti operacijas kliento vardu. Bankas, gavęs tokį pranešimą, taip pat turi teisę blokuoti atitinkamam naudotojui suteiktą naudotojo identifikavimo kodą.

Nuostoliai, atsiradę iki pranešimo pateikimo bankui momento, tenka klientui, o nuostoliai, atsiradę po pranešimo bankui momento, tenka bankui, išskyrus tuos atvejus, kai nuostoliai atsirado dėl kliento ar naudotojo tyčios arba didelio neatsargumo. Ši sutarties sąlyga yra gana nepalanki naudotojui, nes sąvoka „nuostoliai, atsiradę iki pranešimo pateikimo bankui momento“ yra neapibrėžtas ir logiškai negalimas apibrėžti laikotarpis. Asmuo, kuris nesinaudoja elektroninėmis paslaugomis kasdien, gali ne iš karto pastebėti tapatybės vagystę elektroninėje erdvėje ir nuo jos faktiško įvykdymo iki momento, kai naudotojas tai pastebėjo, naudotojas gali patirti didžiulius finansinius nuostolius, pavyzdžiui, gali būti ištuštinta naudotojo sąskaita, pasisavinti taupomieji indėliai ir pan. Aplinkybė, kad naudotojas ne iš karto pastebėjo, kad tapo tapatybės vagystės elektroninėje erdvėje auka, neturėtų didinti naudoto atsakomybės už pranešimo nepateikimą bankui „laiku“.

Dar vienas probleminis sutarties aspektas yra tas, kad joje nėra įtvirtintos didelio nerūpestingumo sąvokos. Atsižvelgiant į tai, kad minėta sąvoka yra vertinamojo pobūdžio, manytina, kad kilus ginčams dėl tapatybės vagystės elektroninėje erdvėje požymių įrodinėjimo, bankas būtų stipresnė šalis, kuri remdamasi didelio neatsargumo kriterijumi, turėtų pranašumą prieš naudotoją sprendžiant nuostolių, susijusių su naudotojo tapatybės patvirtinimo priemonių praradimu, atskleidimu, netinkamu saugojimu, paskirstymo tarp banko ir kliento klausimą.

Sutartyje įtvirtinta, kad tuo atveju, kai įstatymas numato maksimalią kliento atsakomybės už nuostolius sumą, klientui tenka tik nuostolių suma, neviršijanti įstatymo nustatytos maksimalios atsakomybės sumos, išskyrus atvejį, kai nuostoliai atsirado dėl kliento ar naudotojo tyčios ar didelio neatsargumo ar kitus įstatymo numatytus atvejus, kai ši maksimali atsakomybės riba netaikoma. Tokiu atveju lieka neišspręstas klausimas – kam kyla atsakomybė atlyginti kliento patirtus nuosto-

lius, jei jie yra didesni nei maksimali kliento atsakomybės už nuostolius suma?

Dar viena diskutuotina sutarties nuostata yra ta, kad klientas visiškai atsako už visas operacijas, atliktas elektroniniais kanalais panaudojant naudotojui suteiktas tapatybės patvirtinimo priemones, taip pat atsako už elektroniniais kanalais pateikiamų nurodymų atlikti operacijas ir kitos informacijos teisingumą. Ši sutarties sąlyga taip pat nepalanki naudotojui, nes tapatybės vagystės elektroninėje erdvėje atveju gali būti pasisavintos naudotoją elektroninėje erdvėje identifikuojančios priemonės naudotojui to net nežinant, taip pat naudotojas gali ne iš karto pastebėti, kad tapo tapatybės vagystės elektroninėje erdvėje auka. Tačiau visos operacijos, kol apie pavojingą veiką bus pranešta bankui ir atitinkamoms teisėsaugos institucijoms, naudotojo vardu sėkmingai bus vykdomos pavojingos veikos subjekto, o visa atsakomybė už tai teks naudotojui.

Atsižvelgiant į tai, autorių nuomone, vartotojų atsakomybės, nustatytos sutartyse su bankais, ribos turėtų būti persvarstytos, siekiant užtikrinti geresnę sąžiningo ir rūpestingo vartotojo interesų apsaugą. Valstybinė vartotojų teisių apsaugos tarnyba, kaip vartotojų teises ginanti institucija, galėtų išleisti rekomendacijas, įtvirtinančias pagrindinius atsakomybės nustatymo principus vartotojų su bankais sudaromose sutartyse.

Apžvelgus pagrindines civilinės teisės nuostatas, numatančias civilinę atsakomybę už asmens teisės į privataus gyvenimo neliečiamumą pažeidimą, galima daryti išvadą, kad pažeista teisė į privatų gyvenimą gali būti ginama:

1) pareiškiant ieškinį dėl veiksmų, kuriais pažeidžiama teisė į privatų gyvenimą, nutraukimo;
2) pareiškiant prevencinį ieškinį dėl veiksmų, kurie dar nebuvo atlikti, uždraudimo;
3) reikalaujant atlyginti turtinę arba neturtinę žalą.

Taigi, asmuo, tapęs tapatybės vagystės elektroninėje erdvėje auka, savo pažeistas teises gali ginti ne tik baudžiamosios, bet ir pasinaudodamas civilinės teisės normomis, reglamentuojančiomis atsakomybę už tokius civilinės teisės pažeidimus, kaip teisės į vardą, teisės į atvaizdą, teisės į privatų gyvenimą ir jo slaptumą, teisės į garbę ir orumą pažeidimas, tačiau tapatybės vagystės elektroninėje erdvėje požymių ir patirtos neturtinės žalos įrodinėjimas civiliniame procese yra gana sudėtingas.

3.5.2. Administracinė atsakomybė už tapatybės vagystę elektroninėje erdvėje

Administracinės atsakomybės pagrindai už tapatybės vagystę elektroninėje erdvėje

Užkertant kelią teisės pažeidimams, susijusiems su tapatybės vagyste elektroninėje erdvėje, plačiai taikomos visų teisinės atsakomybės rūšių priemonės. Šiuo atveju labai svarbus administracinės atsakomybės vaidmuo[428]. Deja, tenka konstatuoti, kad šiuo klausimu užsienio teisinės literatūros beveik nėra. Tokią padėtį lemia ir tai, kad administracinių teisės pažeidimų kodeksų, kaip atskirai egzistuojančių teisės aktų, nustatančių teisinę atsakomybę už administracinės teisės pažeidimus, daugelyje užsienio valstybių iš viso nėra. Kai kuriose iš tokių valstybių nusižengimai inkorporuoti į šių valstybių baudžiamuosius įstatymus. Antai Vokietijos baudžiamasis kodeksas visas nurodytas veikas skirsto į nusikaltimus ir nusižengimus[429]. Anglijoje, Skandinavijoje ir JAV nusikaltimais laikomi visi teisės pažeidimai, taigi ir, mūsų supratimu, administraciniai teisės pažeidimai[430]. Todėl pažeidimai elektroninėje erdvėje nagrinėjami šių valstybių baudžiamosios teisės literatūroje.

Tiesa, pavyzdžių, kai atskirai galioja administracinių teisės pažeidimų kodeksai, yra: pvz., Latvija, Rusija ir kt. Šių valstybių teisės literatūroje ir praktikoje daug dėmesio skiriama baudžiamajai atsakomybei už nusikaltimus, susijusius su kompiuteriais, nustatyti, tačiau administracinės atsakomybės nustatymo už mažesnio pavojingumo pažeidimus problemų kol kas nesprendžiama, nors kai kurie mokslininkai jau siūlo tam tikras veikas įvardyti administraciniais teisės pažeidimais.

Nagrinėjant tapatybės vagystės elektroninėje erdvėje neteisėtas veikas, kurių dalis yra elektroniniai nusikaltimai, reikia paminėti, kad administracinė atsakomybė kaip alternatyva baudžiamosioms sankcijoms už elektroninius nusikaltimus, buvo iškelta kriminalinės policijos tarptautinėje apžvalgoje, susijusioje su kompiuteriniais nusikaltimais, kurioje nurodyta, jog kompiuterinė informacija turi būti apsaugota ir administracinės teisės

[428] Petkevičius, P. 1996. *Administracinė atsakomybė*. Vilnius: Justitia, p. 7.

[429] Piesliakas, V. 1996. *Mokymas apie nusikaltimą ir nusikaltimo sudėtį*. Vilnius: Lietuvos policijos akademija, p. 30.

[430] Piesliakas, V. 1993. Ekonominiai nusikaltimai Europos valstybių bei JAV teisėje, *Lietuvos policijos akademijos mokslo darbai* 1: 40–41.

priemonėmis, tačiau pažymėta, jog nuomonės dėl apsaugos skirtingų teisės šakų normomis laipsnio kardinaliai skiriasi[431]. Tokiai nuomonei pritarė ir Ulrich Sieber, nurodydamas, kad pavojingos veikos turi būti ne tik kriminalizuotos, tačiau galimas ir administracinės atsakomybės pagrindų nustatymas[432]. Konvencijoje dėl elektroninių nusikaltimų taip pat yra nuostatos, tokios kaip ,*turi būti nustatyta baudžiamoji atsakomybė arba imtasi kitų teisinių priemonių atsakomybei nustatyti*, iš kurių galima daryti išvadą, kad valstybėms narėms paliekama teisė ne tik nustatyti baudžiamąją atsakomybę už nusikaltimus, susijusius su kompiuteriais, tačiau tam tikras veikas elektroninėje erdvėje įvardyti kaip administracinės teisės pažeidimus.

Atskirose užsienio valstybėse šiuo metu beveik jokio dėmesio neskiriama administracinei atsakomybei nustatyti už teisės pažeidimus elektroninėje erdvėje (daugelyje valstybių dėmesio neskiriama dėl to, kad, kaip jau minėta anksčiau, administracinių teisės pažeidimų kodeksų iš viso nėra). Tačiau kaip išimtis paminėtina Latvija, kurioje, atsižvelgiant į Konvencijos dėl elektroninių nusikaltimų nuostatas, imtasi aktyvių veiksmų keisti ne tik baudžiamąjį kodeksą, tačiau buvo parengti ir atitinkami Latvijos administracinių teisės pažeidimų kodekso pakeitimai[433]. Apie galimybę kaip administracinius pažeidimus įvardyti pavojingas veikas elektroninėje erdvėje užsimena ir Rusijos autoriai *(*V. O. Černišova*[434]* ir kt.).

Administracinės atsakomybės pagrindų nustatymo už pavojingas veikas elektroninėje erdvėje, susijusias su tapatybės vagyste, galimybės

Užkertant kelią teisės pažeidimams ir stiprinant teisėtvarką, turėtų būti plačiai taikomos visų teisinės atsakomybės rūšių priemonės. Labai svarbus yra administracinės atsakomybės vaidmuo[435]. P. Petkevičius nu-

[431] United Nations Manual on Computer-Related Crime. International Review of Criminal Policy Nos. 43/44, 1994, p. 29 [interaktyvus, žiūrėta 2011-09-20]. <http://www.uncjin.org/Documents/EighthCongress.html>.

[432] Sieber U. Legal Aspects of Computer-Related Crime in the Information Society. Comcrime study, prepared for European Commission [interaktyvus]. 1998 [žiūrėta 2011-09-20], p. 204. <http://www.archividelnovecento.it/archivinovecento/CAPPATO/Cappato/Faldone64-12Dirittiumanipaesiextracom/DonneAfghanistan/Desktop/sieber.pdf >.

[433] The Following Countries Are in the Process of developing laws to Prosecute Cyber Crime [interaktyvus, žiūrėta 2011-09-20]. <http://www.mcconnellinternational.com >.

[434] Černišova V.O. Internet i prestupnost. Computer Crime Research Center [interaktyvus, žiūrėta 2011-09-20]. <http://www.crime-research.org/library/Chernish1.htm>.

[435] Petkevičius, P. *Administracinė atsakomybė*. Vilnius: Justitia, 1996, p. 7.

rodo, kad administracinės atsakomybės reikšmė labai padidėjo pastaraisiais metais, kai reikia tobulinti valstybingumo stiprinimo ir rinkos ekonomikos sąlygomis intensyviai besiplėtojančių visuomeninių santykių teisinį reguliavimą ir stiprinti jų apsaugą. Administracinė atsakomybė yra savarankiška teisinės atsakomybės rūšis. Jai būdingi visi bendrieji teisinės atsakomybės bruožai[436].

Administraciniu teisės pažeidimu (nusižengimu) Lietuvoje laikomas priešingas teisei, kaltas (tyčinis ar neatsargus) veikimas arba neveikimas, kuriuo kėsinamasi į valstybinę arba viešąją tvarką, nuosavybę, piliečių teises ir laisves, nustatytą valdymo tvarką, už kurį įstatymai nustato administracinę atsakomybę[437]. Administracinė atsakomybė už Lietuvos Respublikos administracinių teisės pažeidimų kodekse nurodytus pažeidimus atsiranda, jeigu savo pobūdžiu šie pažeidimai pagal galiojančius įstatymus neužtraukia baudžiamosios atsakomybės[438]. Taigi administracinės atsakomybės skirtumas nuo baudžiamosios atsakomybės pasireiškia pirmiausia jos taikymo pagrindu. Administracinės atsakomybės pagrindas – administracinis teisės pažeidimas, nustatytas Lietuvos Respublikos įstatymų. Baudžiamosios atsakomybės pagrindas – nusikaltimas, kurio požymiai nustatyti Lietuvos Respublikos įstatymų[439].

Pagrindinis administracinio teisės pažeidimo atribojimo nuo nusikaltimo kriterijus yra veikos pavojingumo visuomenei laipsnis[440]. Nusikaltimas yra pavojingesnis visuomenei nei administracinis teisės pažeidimas. Taigi, administracinė atsakomybė nustatoma už mažiau pavojingas veikas. Gali kilti klausimas, ar nustatytini administracinės atsakomybės pagrindai už veikas, vykdomas elektroninėje erdvėje, kurios yra mažiau pavojingos nei nusikalstamos veikos. Paminėtina, kad veikomis elektroninėje erdvėje sukeliamas pavojus įvairiems visuomeniniams santykiams. Lietuvos Respublikos administracinių teisės pažeidimų kodekso 1 straipsnyje yra nustatyti visuomeniniai santykiai, kurie saugomi administracinių teisės normų. Šiame straipsnyje nurodoma, kad Lietuvos Respublikos

[436] Petkevičius, P. *Administracinė atsakomybė*. Vilnius: Justitia, 1996, p. 9.

[437] Lietuvos Respublikos administracinių teisės pažeidimų kodeksas. *Valstybės žinios*. 1985, Nr. 1-1, 9 str. 1 d.

[438] *Ibid*., 9 str. 2 d.

[439] Petkevičius, P. *Administracinė atsakomybė*. Vilnius: Justitia, 1996, p. 28.

[440] *Valstybės ir teisės teorija*. Vilnius: Mintis, 1989, p. 148.

įstatymų dėl administracinių teisės pažeidimų tikslas yra saugoti Lietuvos Respublikos visuomeninę santvarką, nuosavybę, socialines, ekonomines, politines ir asmenines piliečių teises ir laisves, taip pat įmonių, įstaigų ir organizacijų teises ir teisėtus interesus, nustatytą valdymo tvarką, valstybinę ir viešąją tvarką …[441]. Veikos elektroninėje erdvėje pažeidžia asmenų teises ir teisėtus interesus (pvz., neteisėta prieiga), asmenų ekonomines teises (pvz., sukčiavimas) ir t. t. Galima teigti, kad tokiomis veikomis kėsinamasi taip pat ir į administracinės teisės saugomus visuomeninius santykius, todėl, autoriaus nuomone, egzistuoja galimybė nustatyti administracinės atsakomybės pagrindus už neteisėtas veikas elektroninėje erdvėje, kurios yra mažiau pavojingos nei nusikalstamos veikos.

Autorių nuomone, atsižvelgiant į Lietuvoje egzistuojančią teisinę sistemą, Konvencijos dėl elektroninių nusikaltimų nuostatas, paliekančias tam tikrą laisvę valstybėms pačioms spręsti atsakomybės pagrindų už veikas elektroninėje erdvėje nustatymo klausimus, nagrinėtina administracinės atsakomybės pagrindų nustatymo už kai kurias neteisėtas veikas, vykdomas elektroninėje erdvėje ir susijusias su tapatybės vagyste, galimybė. Taip pat, paminėtina, kad ekspertų apklausoje 7-asis ekspertas nurodė, kad galėtų būti svarstomos administracinės atsakomybės už TVEE tobulinimo galimybės.

Administracinės atsakomybės nustatymas subalansuotų teisinės atsakomybės taikymą už kai kurias neteisėtas veikas elektroninėje erdvėje (ypač už neteisėtą prieigą, neteisėtų prieigos priemonių platinimą ir kt.) ir įgyvendintų kai kurias Konvencijos dėl elektroninių nusikaltimų nuostatas, susijusias su teisinės atsakomybės nustatymu už pavojingas veikas elektroninėje erdvėje. Be to, administracinė atsakomybė taikoma daug operatyviau bei paprasčiau negu baudžiamoji atsakomybė[442], todėl kai kuriais atvejais administracinės atsakomybės taikymas padėtų greičiau, efektyviau įvertinti pavojingas veikas elektroninėje erdvėje. Tokios atsakomybės taikymas vietoje baudžiamosios atsakomybės valstybei kainuotų ir mažiau lėšų.

Gali kilti klausimas, kas ir kokiais pagrindais remdamasis sprendžia, kokie teisei priešingi ir visuomenei pavojingi veiksmai turi būti laikomi

[441] Lietuvos Respublikos administracinių teisės pažeidimų kodeksas. *Valstybės žinios*. 1985, Nr. 1-1, 1 str.

[442] Petkevičius, P. 1996. *Administracinė atsakomybė*. Vilnius: Justitia, p. 29.

administraciniais teisės pažeidimais. P. Petkevičius (1996) nurodo, kad šį klausimą sprendžia įstatymo leidėjas, atsižvelgdamas į atitinkamas vietos, laiko, politines, socialines, ekonomines sąlygas ir kitas konkrečias aplinkybes. Vis dėlto egzistuoja tam tikri požymiai, kuriais remiantis galima tam tikras veikas priskirti prie nusikaltimų arba administracinių teisės pažeidimų (padariniai, žala; pažeidimo mastas; kaltės forma ir žalos dydis; pakartotinumas; pažeidimo padarymo būdas, įrankiai ir priemonės bei kiti požymiai, kuriuos įvertina įstatymų leidėjas[443]). Toliau šiame darbe išdėstyti autorių samprotavimai remsis užsienio autorių diskusijomis dėl veikų kriminalizavimo, kurios rodo tam tikrų veikų mažesnį pavojingumą, bei vidiniu įsitikinimu, grindžiamu išvardytų požymių buvimu.

Įstatymų leidėjas Lietuvos Respublikos administracinių teisės pažeidimų kodekse[444] jau yra nustatęs tam tikrą administracinę atsakomybę už kai kuriuos teisės pažeidimus internete. Lietuvos Respublikos administracinių teisės pažeidimų kodekso 214[10] str. nustatyti atsakomybės pagrindai už galimą autorių teisių pažeidimą, t. y. už neteisėtą literatūros, mokslo ar meno kūrinio (įskaitant kompiuterių programas ir duomenų bazes) ar gretutinių teisių objekto arba jų dalies viešą atlikimą, atgaminimą, viešą paskelbimą, kitokį panaudojimą bet kokiais būdais ir priemonėmis nekomerciniais tikslais, taip pat neteisėtų kopijų platinimą, gabenimą ar laikymą komerciniais tikslais[445]. Nors ši norma yra „tradicinė“, tačiau ją galima pritaikyti ir veikoms elektroninėje erdvėje.

Autoriai nori pažymėti, jog vienas iš administracinės atsakomybės bruožų yra tas, kad administracinė atsakomybė labai svarbi ne tik užkertant kelią administraciniams pažeidimams, bet ir kriminaliniams nusikaltimams. Šiuo atveju yra ypač didelis profilaktinis administracinės atsakomybės vaidmuo. Jos taikymas už įvairius administracinius teisės pažeidimus – tai veiksminga kovos su pavojingais baudžiamaisiais nusikaltimais priemonė[446]. Autorių nuomone, kai nusikaltimai

[443] Petkevičius, P. 1996. *Administracinė atsakomybė*. Vilnius: Justitia, p. 70.

[444] Aut. past.: šios monografijos rengimo metu naujojo Lietuvos Respublikos administracinių teisės pažeidimų kodekso projektas, nors ir parengtas, dar nebuvo priimtas, todėl analizuojamos galiojančio Lietuvos Respublikos administracinių teisės pažeidimų kodekso nuostatos.

[445] Lietuvos Respublikos administracinių teisės pažeidimų kodeksas. *Valstybės žinios*. 1985, Nr. 1-1, 214[10] str. 1 d.

[446] Petkevičius, P. 1996. *Administracinė atsakomybė*. Vilnius: Justitia, p. 9.

elektroninėje erdvėje pagal pavojingumą lenkia kai kuriuos tradicinius nusikaltimus, svarstytinas administracinės atsakomybės pagrindų nustatymo už kai kurias mažiau pavojingas veikas internete nustatymo klausimas, siekiant užkirsti kelią iš tikrųjų pavojingiems kompiuteriniams nusikaltimams.

Lietuvos Respublikos baudžiamajame kodekse ir Lietuvos Respublikos administracinių teisės pažeidimų kodekse galima surasti nemažai pavyzdžių, kai už panašias veikas, kurios skiriasi tik pavojingumo laipsniu, nustatyta ir baudžiamoji, ir administracinė atsakomybė. Kaip pavyzdį galima pateikti šiuo metu galiojančio Lietuvos Respublikos baudžiamojo kodekso 178 straipsnį, kuriame nurodytas atsakomybės pagrindas už svetimo turto pagrobimą. Už mažiau pavojingą veiką, kai nėra Lietuvos Respublikos baudžiamojo kodekso 178, 182, 183, 184 straipsniuose numatytų sunkinančių aplinkybių, nustatyta administracinė atsakomybė: pagal Lietuvos Respublikos administracinių teisės pažeidimų kodekso 50 str., administracine tvarka yra baudžiamas smulkus svetimo turto pagrobimas vagystės, sukčiavimo, pasisavinimo arba iššvaistymo būdu[447]. Autoriaus nuomone, analogiškas atsakomybės nustatymas galimas ir dėl pavojingų veikų internete. Todėl toliau bus analizuojama administracinės atsakomybės pagrindų už tam tikras veikas nustatymo galimybė, atsižvelgiant į Lietuvos Respublikos baudžiamojo kodekso ir Lietuvos Respublikos administracinių teisės pažeidimų kodekso santykį.

Autoriai norėtų atkreipti dėmesį ir į vieną reikšmingą veikų elektroninėje erdvėje įvardijimo kaip administracinių teisių pažeidimą problemą. P. Petkevičius nurodo, jog administracinės atsakomybės operatyvumas pasireiškia ir tuo, kad jos poveikio priemonės taikomos tuojau pat, dažnai net teisės pažeidimo padarymo vietoje, o baudžiamosios atsakomybės taikymas yra susijęs su sudėtingais baudžiamojo proceso veiksmais[448]. Pavojingos veikos elektroninėje erdvėje, susijusios su tapatybės vagyste, dažnai pasižymi tyrimo sudėtingumu bei sunkiu veiką įvykdžiusių asmenų nustatymu. Jos įvykdomos elektronine forma ir nustatyti įvykdžiusį asmenį dažnai būna pakankamai sudėtinga. Tokiais atvejais, be abejo, veikai tirti efektyvesnis būtų baudžiamojo proceso normų taikymas.

[447] Lietuvos Respublikos administracinių teisės pažeidimų kodeksas. *Valstybės žinios*. 1985, Nr. 1-1,50 str. 1 d.

[448] Petkevičius, P. 1996. *Administracinė atsakomybė*. Vilnius: Justitia, p. 29.

Iškėlus baudžiamąją bylą, tyrėjai turi daugiau teisių nei administracinio teisės pažeidimo padarymo atveju. Be to, administracinė byla dažniausiai keliama jau suradus pažeidėją. Autorių nuomone, administracinės atsakomybės taikymas už veikas elektroninėje erdvėje gali būti problemiškas dėl sudėtingo pažeidimų tyrimo. Tačiau nepaisant to, kai teisės pažeidėjo nustatymo procesas yra paprastesnis, tam tikrų veikų laikymas administraciniais teisės pažeidimais gana tikslingas.

Administracinės atsakomybės pagrindai už neteisėtas veikas elektroninėje erdvėje, susijusias su tapatybės vagyste ir Lietuvos Respublikos administracinių teisės pažeidimų kodeksu

Atsakomybė už neteisėtą prieigą

Viena iš neteisėtų veikų, susijusių su tapatybės vagyste elektroninėje erdvėje – neteisėta prieiga. Neteisėta prieiga dažniausiai vykdoma turint tikslą pasisavinti asmeninę informaciją, t. y. asmens duomenis. Todėl keltinas atsakomybės už šią neteisėtą veiką klausimas.

Kai kuriose valstybėse jau nustatyti baudžiamosios atsakomybės pagrindai už neteisėtą prieigą prie kompiuterinių sistemų per internetą, tačiau nusikaltimo sudėties elementai pastebimai skiriasi[449]. Dalyje tokių valstybių (pvz., Ispanija ir kt.) reikalaujama papildomų kvalifikavimo aplinkybių, kaip nurodo Rekomendacija Nr. (89)9 ir 1985 m. Europos bendradarbiavimo ir vystymo organizacijos darbo grupės siūlymai. Be to, Konvencijoje dėl elektroninių nusikaltimų nurodyta, kad, *kiekviena šalis turi imtis įstatymų ir kitokių priemonių, kokių būtina nustatyti baudžiamąją atsakomybę už neteisėtą prieigą prie kompiuterio. Šalis gali reikalauti, kad pažeidimas būtų padaromas pažeidžiant saugumo priemones, turint tikslą pasisavinti kompiuterinę informaciją ar turint kitą nesąžiningą tikslą, arba jei tai susiję su kompiuterine sistema, kuri sujungta su kita kompiuterine sistema*[450]. Konvencijoje siūloma nustatant baudžiamąją atsakomybę už neteisėtą prieigą prie kompiuterio, naudoti tokius būtinus nusikaltimo sudėties požymius (kartu arba atskirai): saugumo priemonių pažeidimas; tikslas pasisavinti kompiuterinę informaciją; ki-

[449] Explanatory Report of Convention on Cybercrime, p. 49. [interaktyvus, žiūrėta 2011-09-20] <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>.

[450] Convention on Cybercrime. Strasbourg, 19.09.2001. art. 2. [interaktyvus, žiūrėta 2011-09-20] <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>.

tas nesąžiningas tikslas; pažeidimas padaromas, kai tai susiję su kompiuterine sistema, kuri sujungta su kita kompiuterine sistema[451]. Taip pat ir kai kurie mokslininkai pabrėžia mažesnį neteisėtos prieigos, kai nėra žalingų pasekmių (nepadaroma žalos), pavojingumą. Konvencijos dėl elektroninių nusikaltimų aiškinamajame rašte pažymima, kad vien neteisėtas įsibrovimas, t. y. neteisėta prieiga prie kompiuterinės sistemos (angl. *Hacking, Cracking, Computer Trespass*), turėtų būti nelegalus, nes tokie veiksmai sukelia pavojų kompiuteriniams duomenims ir t. t.[452] Taip pat kai kuriose valstybėse (pvz., Didžioji Britanija), kuriose nusikaltimo terminas apima ir pažeidimus (Lietuvos atžvilgiu – administracinius teisės pažeidimus), už analogišką veiką yra nustatyta lengvesnė atsakomybė, tuo lyg ir priskiriant veiką prie pažeidimų. *U. Proske, P. J. Schick, G. Schmolzer* už tolias veikas siūlo nustatyti būtent administracinę atsakomybę.

Šiuo metu Lietuvos Respublikos baudžiamajame kodekse neteisėta prieiga kriminalizuota 198-1 straipsnyje „Neteisėtas prisijungimas prie informacinės sistemos". Tam, kad kiltų baudžiamoji atsakomybė, įstatymo leidėjas pasirinko vieną esminį požymį – turi būti pažeidžiamos informacinės sistemos apsaugos priemonės.

Turint omenyje ankščiau išdėstytus teiginius, galėtų būti svarstoma galimybė geriau subalansuoti teisinę atsakomybę už tapatybės vagystę elektroninėje erdvėje, už tam tikras mažiau pavojingas veiką, įsilaužimą į kompiuterių sistemą, kai nebūna žalingų pasekmių (pvz., nepasisavinama informacijos), taip pat nėra kitų būtinų kvalifikuojančių požymių, tačiau pažeidžiamos saugumo priemonės, įstatymo leidėjui pasirinktinai nustatant administracinę atsakomybę. Toks administracinės atsakomybės pagrindo nustatymas padėtų „subalansuoti" atsakomybę už neteisėtą prieigą prie kompiuterinės sistemos. Tačiau turint omenyje, kad Lietuva dėl Konvencijos dėl elektroninių nusikaltimų 2 straipsnio deklaravo, jog neteisėtos prieigos atveju baudžiamoji atsakomybė kyla pažeidus saugumo priemones, šia deklaracija Lietuva jau apsisprendė dėl atitinkamo neteisėtos prieigos kriminalizavimo.

[451] Explanatory Report of Convention on Cybercrime, p. 50. [interaktyvus, žiūrėta 2011-09-20]. < http://conventions.coe.int/Treaty/en/Reports/Html/185.htm >.

[452] *Ibid*., p. 44.

Atsakomybė už neteisėtus veiksmus, susijusius su neteisėtais įrenginiais / prieigos duomenimis

Lietuvoje baudžiamoji atsakomybė už veikas, kai kuriami, platinami, panaudojami ir t. t. neteisėti įrenginiai / prieigos duomenys (slaptažodžių „nulaužimo" programos ar pan.), skirti pažeidimams prieš kompiuterinių sistemų ar duomenų konfidencialumą, integruotumą ir prieinamumą įvykdyti, kyla pagal Lietuvos Respublikos baudžiamojo kodekso 198-2 str. „Neteisėtas disponavimas įrenginiais, programine įranga, slaptažodžiais, prisijungimo kodais ir kitokiais duomenimis". Šios straipsnio dispozicijoje nurodyta taip: „Tas, kas neteisėtai gamino, gabeno, pardavė ar kitaip platino įrenginius ar programinę įrangą, taip pat slaptažodžius, prisijungimo kodus ar kitokius panašius duomenis, tiesiogiai skirtus nusikalstamoms veikoms atlikti, arba tuo pačiu tikslu juos įgijo ar laikė, baudžiamas viešaisiais darbais arba bauda, arba areštu, arba laisvės atėmimu iki trejų metų."

Apie atsakomybės numatymą nurodoma ne viename šaltinyje (Tarptautinėje baudžiamosios teisės apžvalgoje 1992 metais, 1994 m. Kriminalinės policijos tarptautinėje apžvalgoje dėl kompiuterinių nusikaltimų ir kt.), tačiau juose neakcentuojama, kad už tokias veikas turi kilti baudžiamoji atsakomybė. Kaip jau minėta, už šios veikos kriminalizavimą nepasisako ir dauguma tokias veikas nagrinėjančių mokslininkų. Todėl, autorių nuomone, jas dėl mažesnio pavojingumo visuomenei tikslinga įvardyti administraciniais teisės pažeidimais. Atsižvelgiant į tai, kad baudžiamajame kodekse atsakomybė numatyta ne už vieno įrenginio neteisėtą disponavimą, o už įrenginių neteisėtą disponavimą, taip pat remiantis užsienio mokslininkų (M. Mohrenschlagerio ir kt.) nuomonėmis bei atsižvelgiant į tarptautinių dokumentų nuostatas, autoriai siūlo administracinę atsakomybę nustatyti už mažiau pavojingą veiką, disponavimą vienu neteisėtu įrenginiu ir tokio pažeidimo dispoziciją formuluoti taip:

„Neteisėtas disponavimas įrenginiu, programine įranga (vienu vienetu), slaptažodžiu, prisijungimo kodu ir kitokiu duomeniu, užtraukia <…>".

Atsakomybė už informacinės sistemos ar kompiuterių tinklo naudojimo taisyklių pažeidimą

Autorių nuomone, papildoma veika, už kurią įstatymų leidėjas turėtų svarstyti nustatyti administracinę atsakomybę – informacinės siste-

mos ar kompiuterių tinklo naudojimo taisyklių pažeidimą. Paminėtinas Rusijos pavyzdys, kurioje už informacinės sistemos ar kompiuterių tinklo naudojimo taisyklių pažeidimą, sukėlusį žalingas pasekmes, numatyta baudžiamoji atsakomybė (Rusijos baudžiamojo kodekso 274 str.). Manytina, kad mažiau pavojinga veika, kai žalingų pasekmių nebuvo, tačiau kilo tokių pasekmių grėsmė, galėtų užtraukti administracinę atsakomybę. Todėl autoriai, naują administracinio pažeidimo dispoziciją siūlo formuluoti taip:

„*Informacinės sistemos ar kompiuterių tinklo eksploatavimo taisyklių pažeidimas, užtraukia, <...>*“.

Taigi, siekiant išbalansuoti teisinę atsakomybę už tapatybės vagystę elektroninėje erdvėje, svarstytina tam tikras neteisėtas veikas įvardyti administracinės teisės pažeidimais. Tokios naujos neteisėtų veikų sudėtys minėtos ankščiau.

Apibendrinančios išvados

• Asmuo, tapęs tapatybės vagystės elektroninėje erdvėje auka, pažeistas teises gali ginti ne tik baudžiamosios ar administracinės teisės priemonėmis, bet ir pasinaudodamas civilinės teisės normomis, reglamentuojančiomis atsakomybę už tokius civilinės teisės pažeidimus, kaip teisės į vardą, teisės į atvaizdą, teisės į privatų gyvenimą ir jo slaptumą, teisės į garbę ir orumą pažeidimas, tačiau tapatybės vagystės elektroninėje erdvėje požymių ir patirtos neturtinės žalos įrodinėjimas civiliniame procese yra gana sudėtingas.

• Civilinė atsakomybė gali kilti ne tik neteisėtus veiksmus atlikusiam asmeniui, bet ir trečiajai šaliai, dėl kurios veiksmų asmuo tapo tapatybės vagystės elektroninėje erdvėje auka, ar net pačiai tapatybės vagystės elektroninėje erdvėje aukai.

• Atlikus Lietuvos komercinių bankų elektroninių paslaugų teikimo sutartyse įtvirtintų tipinių sąlygų dėl banko, kliento bei naudotojo atsakomybės, kai tapatybės patvirtinimo priemonės tapo žinomos arba kilus grėsmei, kad jos gali tapti žinomos tretiesiems asmenims, galima daryti išvadą, kad tapatybės vagystės elektroninėje erdvėje atveju banko klientas (naudotojas) susidurtų su sunkumais įrodinėjant šios pavojingos veikos požymius ir savo nekaltumą, kadangi sutarčių nuostatos yra gana griežtos, kategoriškos ir gana nepalankios naudotojo atžvilgiu.

• Vartotojų atsakomybės, nustatytos sutartyse su bankais, ribos turėtų būti persvarstytos, siekiant užtikrinti geresnę sąžiningo ir rūpestingo vartotojo interesų apsaugą. Valstybinė vartotojų teisių apsaugos tarnyba, kaip vartotojų teises ginanti institucija, galėtų išleisti rekomendacijas, įtvirtinančias pagrindinius atsakomybės nustatymo principus vartotojų su bankais sudaromose sutartyse.

• Atskirose užsienio valstybėse (išimtis – Latvija) šiuo metu neskiriama beveik jokio dėmesio administracinei atsakomybei nustatyti už teisės pažeidimus elektroninėje erdvėje, daugelyje valstybių apskritai neegzistuoja administracinių teisės pažeidimų kodeksai.

• Administracinės atsakomybės taikymas už veikas elektroninėje erdvėje gali būti problemiškas dėl sudėtingo pažeidimų tyrimo. Visgi būtų tikslinga tam tikras veikas, kurių tyrimas ir teisės pažeidėjo nustatymo procesas yra paprastesnis, laikyti administraciniais teisės pažeidimais. Siekiant išbalansuoti teisinę atsakomybę už tapatybės vagystę elektroninėje erdvėje, svarstytina galimybė tam tikras neteisėtas veikas laikyti administracinės teisės pažeidimais.

4. Tapatybės vagystės elektroninėje erdvėje prevencija

Monografijoje ištirtas neigiamas socialinis reiškinys – tapatybės vagystė elektroninėje erdvėje. Svarbu ne tik sužinoti apie neigiamo reiškinio buvimą, bet ir jį veikti taip, kad būtų galima mažinti šio reiškinio plitimą, apsaugoti pažeidžiamas visuomenės grupes. Neabejotinai neegzistuoja paprastų priemonių, galinčių panaikinti vienokį ar kitokį neigiamą reiškinį, tačiau svarbu ieškoti priemonių, leidžiančių riboti, kontroliuoti reiškinio paplitimą ir pasekmes. Prevencijos sąvoka dažnai vartojama kriminologijoje, tačiau autoriai tapatybės vagystę elektroninėje erdvėje tyrė ne tik kaip baudžiamąjį nusikaltimą ar nusižengimą, o ir kaip daugelyje šalių nekriminalizuotą, bet pavojingą veiką, todėl aptardami prevenciją autoriai vadovausis tiek kriminologijos mokslo sukaupta patirtimi, tiek bendromis socialinių mokslų žiniomis, t. y. aptariamos ne tik teisinės priemonės, bet ir socialinio reiškinio valdymas bei priežasčių kontrolė pasitelkiant psichologines, ekonomines ir kitas priemones.

Dėl šios priežasties, nors valstybės vaidmuo išlieka labai svarbus, tačiau svarbu įvertinti ir atskirų individų, organizacijų, atskirų visuomenės grupių galimą indėlį į tapatybės vagystės elektroninėje erdvėje prevenciją. Atsižvelgiant į tapatybės vagystės didelį paplitimą ir dėl elektroninės erdvės sąlyginio (lyginant su fizine erdve) neapibrėžtumo galimą didžiulę dinamiką, svarbu orientuotis ne tik į pasekmių, bet ir į reiškinio priežasčių prevenciją, tačiau tam būtinos visos visuomenės pastangos, o tai įmanoma tik suvokus reiškinio pavojingumą. Neigiamų reiškinių prevencija nuo neigiamų pasekmių apsaugo ne tik visuomenę ar konkretų asmenį, ji taip pat apsaugo ir patį linkusį potencialiai nusižengti asmenį nuo nusižengimo (ar nusikaltimo) ir kilsiančios neigiamos visuomenės reakcijos (pvz., bausmės).

Pagrindinis neteisėtų veikų prevencijos tikslas yra saugoti tokias svarbias socialines vertybes, kaip valstybės, visuomenės ir piliečių teisėti interesai[453].

[453] Bluvšteinas J.; E. Bieliūnas, E; Justickis, V. ir kt. 2006. *Kriminologija*. Pradai, p.153.

Žymus Rusijos mokslininkas A. M. Jakovlevas[454] išsamiai tyrinėja nusikaltimų kilimo priežastis, nusikaltėlio ir visuomenės sąveiką ir kitus itin svarbius kriminologinius klausimus. Jis teigia, kad „visuomenė ir jos atskiros socialinės grupės (šeima, darbo kolektyvas ir kt.) negali egzistuoti nekontroliuodamos visuomenės narių elgesio“[455]. Tuo pat metu Jakovlevas teigia, kad žmogus – ne pasyvus objektas, formuojamas socialinės aplinkos. Esmė ta, kad pati socialinė aplinka yra žmogaus aktyvaus socialinio elgesio rezultatas[456].

Atsižvelgdamas į šiuos fundamentalius teiginius, autorius išskiria tokius prevencijos lygius:

1) individualioji prevencija;
2) prevencija socialinėse grupėse ir kolektyvuose;
3) bendra socialinė prevencija, t. y. prevencija visos visuomenės mastu.

Literatūroje išskiriamas regioninis ir šakiniai lygmenys, tačiau elektroninei erdvei svarbesnis šakinis lygmuo, nes viena veiklos sritis gali daryti įtaką kitiems santykiams (pvz., tinkamai sureguliuotas ir saugus finansinis sektorius sudaro galimybę kurtis saugesniems elektroniniams santykiams kitose srityse). Regioninis lygmuo taip pat turi savo specifiką ir gali turėti teigiamą įtaką, tačiau tai tik tarpinis problemos sprendimas siekiant visuotinio tarptautinio sutarimo prevencijos klausimais.

Nė vienas iš šių prevencijos lygių nėra mažiau svarbus, ypač aptariant tokią specifinę socialinio bendravimo terpę, kaip elektroninė aplinka (įskaitant, bet neapsiribojant, internetu). Internetas aiškiai diferencijuoja atskiras individų kategorijas, kurios sugeba saugotis nuo pavojų, kylančių iš elektroninės erdvės, ir visiškai nesugeba apsisaugoti nuo nesudėtingai įveikiamų grėsmių. Antruoju prevencijos lygiu (socialinės grupės ir kolektyvai) neilgoje elektroninės erdvės egzistavimo istorijoje yra itin pozityvių poslinkių pavyzdžių (pvz., įmonės deda pakankamai daug pastangų ir užtikrina aukštą saugumo lygį, leidžiantį sumažinti grėsmes, įskaitant ir tapatybės vagystės riziką). Šis prevencijos lygis elektroninėje erdvėje

[454] Jakovlev, A. M. 2003. Socialnaja struktūra obščestva. Moskva. Ekzamen.
Jakovlev, A. M. 2001. Sociologija prestupnosti (kriminologija): Osnovi obščej teoriji. Moskva. Sodeistvije novij vek.

[455] Jakovlev, A. M. 1985. Teorija kriminologiji ir socialnaja praktika. Moskva: Nauka, p. 165.

[456] *Ibid*., p. 189.

apima ir šakinius forumus, ir kitus socialinius tinklus, kuriuose dalijamasi informacija, kaip apsisaugoti nuo tapatybės vagysčių[457], tačiau yra ir prastų tendencijų bei pavyzdžių tuo pačiu prevencijos lygiu, pavyzdžiui, paplitę socialiniai tinklai, kurie skatina vartotojus nesaugoti savo asmens duomenų, leidžia į socialinius tinklus patekti pažeidžiamiausioms asmenų grupėms (mažamečiai, jautrios arba nestabilios psichikos asmenys ir kt.). Elektroninėje erdvėje sudėtingiausiai susitariama trečiuoju prevencijos lygmeniu: kadangi vyrauja skirtingas vertybių suvokimas ir vertinimas, todėl net priimtas atitinkamas teisės normas dažnai įgyvendinti būna gana sudėtinga.

Atsižvelgdami į elektroninės terpės ir konkretaus neigiamo elgesio joje (tapatybės vagystės) specifiką, autorių nuomone, prevenciją svarbu tirti vadovaujantis šiais lygmenimis:

1. Konkretaus asmens lygmeniu,
2. Organizacijų lygmeniu:
   a. Viešajame sektoriuje,
   b. Privačiame sektoriuje,
   c. Neformalių socialinių junginių, darinių ir organizacijų lygmeniu,
3. Valstybiniu lygmeniu,
4. Tarptautiniu, dvišaliu (tarpvalstybiniu) ir (arba) regioniniu lygmeniu.

Minėti prevencijos lygiai panagrinėtini detaliau.

4.1. Tapatybės vagystės elektroninėje erdvėje prevencija konkretaus asmens lygmeniu

Siekiant minimizuoti tapatybės vagystės elektroninėje erdvėje tikimybę, būtina apsaugoti asmeninę informaciją[458]. Tyrimai rodo, kad patys vartotojai bene daugiausia prisideda prie tapatybės vagystės elektroninėje

[457] CIFAS interneto svetainė <http://www.cifas.org.uk/default.asp?edit_id=561-56>; JAV Federalinės prekybos komisijos tinklapis, skirtas kovai su tapatybės vagyste. <http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html>; Portalas, skirtas apsaugai nuo tapatybės vagystės < http://www.identity-theft-protection-made-easy.com/define-identity-theft.html>; Tapatybės vagystės tyrimų centro oficialus tinklapis <www.idtheftcenter.org>.

[458] Higgins, G. E. 2010. *Cybercrime: An Introduction to an Emerging Phenomenon*. McGraw-Hill, p. 70.

erdvėje prevencijos[459], todėl prevencija konkretaus asmens lygmeniu yra labai svarbi. Be to, pagal autorių atliktą vartotojų tyrimą dauguma vartotojų (83,6 proc.) mano, kad viešosios informacijos apie apsisaugojimo būdus nuo tapatybės vagystės elektroninėje erdvėje nepakanka. Dėlto vartotojams taip pat svarbu informaciją šiuos apsisaugojimo būdus viešinti. Autorių atliktu tyrimu taip pat nustatyta, kad tapatybės vagystės elektroninėje erdvėje prevencijos priemonių viešinimas skatintų vartotojus naudotis elektroninėmis paslaugomis ir didintų pasitikėjimą elektroninio verslo sektoriumi (taip teigia 71,9 proc. apklaustų respondentų / vartotojų). Daugiau apie autorių atliktus tyrimus pateikta 5.2.2 monografijos dalyje.

Prevencijos konkretaus asmens lygmeniu atveju paminėtina 21 taisyklė, kuri padėtų apsisaugoti nuo tapatybės vagystės grėsmės. Šias taisykles Martinas T. Biegelmanas savo knygoje *Identity Theft Handbook: Detection, Prevention and Security*[460] pristato kaip kiekvienam vartotojui žinoti privalomas taisykles, tačiau jos labiausiai pritaikomos yra JAV praktikoje. Autoriai šį 21 taisyklių rinkinį adaptavo taip, kad būtų galima pritaikyti ir Lietuvoje, atsižvelgiant į naudojamas finansines paslaugas, teisinę sistemą ir kitus svarbius aspektus. Paminėtina, kad tokių taisyklių rinkinių pateikiama ir kitoje literatūroje. Štai Rfank W. Abagnale pateikia 20 taisyklių, skirtų tapatybės vagystės elektroninėje erdvėje prevencijai[461]. Kadangi šios taisyklės pagal esmę panašios, bus remiamasi vienu šaltiniu – Martino T. Biegelmano kūriniu.

Taigi, kiekvienas vartotojas Lietuvoje, norėdamas apsisaugoti nuo galimos tapatybės vagystės rizikos, turėtų atkreipti dėmesį į šias taisykles.

1) Reikia saugoti savo asmens identifikavimo numerius (asmens kodą, kitus dokumentų numerius)

Asmens identifikavimo numeriai gali suteikti prieigą prie subjektų finansinių paslaugų, teikiamų kreditinių ataskaitų, medicininių įrašų ir kt. Negalima dalyti ir pildyti formos nurodant asmens identifikavimo nu-

[459] Javelin Study Finds Identity Fraud Reached New High in 2009, but Consumers are Fighting Back. [interaktyvus, žiūrėta 2011-09-20]. <http://www.prnewswire.com/news-releases/javelin-study-finds-identity-fraud-reached-new-high-in-2009-but-consumers-are-fighting-back-83987287.html>.

[460] Biegelman, M. T. 2009. *Identity theft handbook : detection, prevention and security*, p. 295.

[461] Abagnale, F. W. 2007. *Stealing Your Life: The Ultimate Identity Theft prevention Act*. Broadway Books, p. 105.

merius, jei tai nėra būtina paslaugų teikimo sąlyga. Negalima rašyti asmens identifikavimo numerių bet kokioje sutarties formoje – pirmiausia būtina įsitikinti, kad šie duomenys būtini. Taip pat būtina drąsiai klausti, kam ir kodėl reikia nurodyti asmens identifikavimo numerius, siekiant apsaugoti kitą asmeninę informaciją.

2) Reikia apsaugoti kitą asmeninę informaciją

Asmens identifikavimo numerių apsauga yra pirmas žingsnis asmeninės informacijos apsaugos link. Prie tokių apsaugos priemonių būtina priskirti elektroninių mokėjimo kortelių numerius, banko sąskaitų duomenis ir kt. Negalima pateikti kreditinės kortelės numerio ar kitos asmeninės informacijos asmenims, kurie skambina, net jei prisistato kaip oficialūs asmenys ir vilioja įvairiais pasiūlymais. Būtina maksimaliai susiaurinti ratą subjektų, kuriems suteikiame savo asmeninę informaciją, taip pat reikia maksimaliai sumažinti asmeninės informacijos kiekį, kurį nešiojamės su savimi. Rekomenduojama vienu metu nesinešioti daugiau nei dviejų kredito kortelių, ta pat nesinešioti užsirašytų savo kortelių asmens identifikavimo numerių (PIN). Iš piniginės ar rankinės reikia išmeti visą seną nereikalingą informaciją, čekius, apmokėtas sąskaitas. Taip pat nesaugoti svarbios asmeninės informacijos, PIN kodų, slaptažodžių mobiliuosiuose įrenginiuose, jei tokia informacija nėra apsaugota kriptografiniu būdu. Jei galima, panaikinkite visiškai nenaudojamų kreditinių kortelių sąskaitas, taip sumažindami riziką. Reikia nuolatos tikrinti sąskaitų išrašus, ypač kredito kortelių, po kiekvieno naudojimo ir apsipirkimo tiek fizinėje, tiek elektroninėje erdvėje. Neduoti kortelių į rankas, jei atsiskaitinėjama lustinėmis kortelėmis. Nenurodyti jokios kitos asmeninės informacijos ant apmokėto čekio, net jei to prašoma, nebent tokio prašymo tikslai bus visikai aiškūs. Perkant internetu iš mažmenininkų reikia pasidomėti, kas ir kiek laiko saugos finansinę informaciją – kuo mažiau informacijos leista laikyti, tuo mažesnė rizika, kad ji bus neteisėtai panaudota. Būtina nepalikinėti asmeninės informacijos automobiliuose, pavyzdžiui, draudimo polisų, nes juose nurodyta visa asmeninė informacija. Taip pat nepalikinėkite kitų svarbių daiktų, kuriuose gali būti asmens duomenų elementų. Rekomenduojama tinkamai užtikrinti svarbių dokumentų apsaugą: namų seifas, įdiegta signalizacija – visa tai papildomai apsaugos svarbią asmeninę informaciją.

3) Būtina išnagrinėti mokėjimų instrumentų ataskaitas

Būtent ši rekomendacija ir yra svarbiausią. Būtina atidžiai nagrinėti mokėjimo instrumentų ataskaitas ir tai daryti nuolat. Tokie veiksmai leis greičiausiai pastebėti tapatybės vagystę. Nuoseklus tikrinimas gali padėti nustatyti tapatybės vagystę pačioje pradžioje ir sumažinti galimą potencialią žalą. Jei viena sąskaita naudojasi keli šeimos asmenys, ataskaitas peržiūrėti derėtų dar dažniau.

4) Rekomenduojama įsigyti dokumentų naikintuvą

Vienas iš lengviausių prevencijos būdų – naikinti visus nereikalingus dokumentus. Dažna klaida, tai dokumentų, kuriuose yra asmens duomenų išmetimas į šiukšlių dėžę. Žmonės išmeta įvairių rūšių dokumentus negalvodami apie pasekmes: kreditinių kortelių paraiškos formos, čekiai (su asmenine informacija), banko sąskaitų išrašai, asmeninė korespondencija ir kt. Net vaistų receptai gali pasitarnauti asmenims, kenčiantiems nuo priklausomybės narkotinėms ar psichotropinėms medžiagoms, kaip informacija, kokių medžiagų galima rasti Jūsų namuose. Dokumentų naikintuvas galėtų būti privalomas elementas namuose, kiekvieną dieną smulkinant nereikalingus dokumentus. Tokia tvarka privaloma finansų sektoriuje ir kitose organizacijose, kuriose dirbama su asmens duomenimis. Tad namų ūkio sektoriuje reikėtų pasinaudoti šia gerąja praktika, kaip naudinga prevencine priemone. Be to, susmulkintus dokumentus lengviau fasuoti ir priduoti perdirbti, taip prisidedant prie gamtos apsaugos.

5) Būtina mažinti pašto vagysčių riziką

Pašto vagystės visada buvo problema, bet galima sumažinti ir šią riziką, tik pašto dėžutes reikia visada rakinti. Pašto vagystės, nors tai vyksta pastebimai rečiau (dėl rakinamų laiptinių), vis dar kelia rimtą grėsmę. Svarbu reguliariai tikrinti paštą. Galimos priemonės, padėsiančios apsisaugoti nuo pašto vagysčių:

- paštą tikrinti kiekvieną dieną ir pašto dėžutėje nepalikti laiškų per naktį arba savaitgaliais.
- atsisakyti popierinių sąskaitų už komunalines paslaugas, mobiliąsias paslaugas ir kt.
- pasirūpinti tvarkinga pašto dėžute.
- svarbų asmeninį paštą adresuoti sau į darbą (jei darbdavys leidžia).

- palaikyti gerus ryšius su pašto darbuotojais, pranešti, kada planuojama ilgiau netikrinti pašto.
- apie bet kokią įtartiną veiklą pranešti pašto tarnybai.
- pranešti apie negautą vertingą pašto siuntą.

6) Pasirūpinti tinkama kompiuterio apsauga

Kompiuteryje turi būti įdiegta ugniasienė ir antivirusinė programa. Būtina imtis prevencinių priemonių dėl galimų kenkėjiškų programų ar virusų. Reikia laiku atnaujinti visą apsaugos programinę įrangą, įtariai vertinti neprašytus laiškus, kuriuose prašoma pateikti asmeninės ar finansinės informacijos. Teisėti prašymai pateikti asmeninę informaciją, paprastai nėra siunčiami elektroniniu paštu. Negalima naudotis viešais kompiuteriais tokiose vietose, kaip viešbučiuose, kavinėse ar kt., ir atlikti finansinius sandorius ar tvarkyti kitą svarbią asmeninę informaciją. Minėtose vietose esantys kompiuteriai gali būti užkrėsti šnipinėjimo programomis arba virusais. Niekada neatidarinėkite nežinomų elektroninių laiškų priedų arba atsisiųstos abejotinos programinės įrangos. Nusikaltėliai gali siūlyti nemokama muziką, antivirusinę apsaugą ar kitas programas. Būtina apsaugoti ir koduoti namų bevielį kompiuterinį tinklą, taip nusikaltėliams bus sunkiau rasti neapsaugotą prieigą. Visada naudokite sunkius slaptažodžius, nenaudokite žodžių, pavadinimų, ar frazių, kurios gali būti lengvai atspėjamos. Kuo ilgesnis slaptažodis, tuo geriau. Dažnai rekomenduojama, kad slaptažodis turėtų būti bent aštuonių simbolių, atsitiktinės raidės, o skaičiai yra stipriausi slaptažodžio elementai. Taip pat reikia nustatyti slaptažodžio keitimo tvarką ir jos laikytis.

7) Būtinas atsargumas naudojantis bankomatais

Dažna vieta, kur bandoma pasisavinti mokėjimo duomenis, yra bankomatas. Būtina atkreipti dėmesį į įtartinus prietaisus. Apžiūrėkite, ar bankomatas techniškai tvarkingas, ar nematyti atvirų laidų, jungčių, paslėptų kamerų, kurias nusikaltėliai naudoja PIN slaptažodžiams įrašyti. Jei bankomatas atrodo įtartinai, pavyzdžiui, per daug iškilusi klaviatūra, prie kortelės įkišimo lizdo primontuotas neaiškus įrenginys, rekomenduojama nesinaudoti ir esant galimybei pranešti apie tai atitinkamam bankui ir teisėsaugos institucijai. Būtina atkreipti dėmesį į žmones, kurie pernelyg ilgai atlieka

paprastas operacijas ar įdėmiai stebi kitų žmonių veiksmus prie bankomatų. Tokie žmonės gali naudoti paprasčiausius žiūrėjimo per petį metodus tam, kad pamatytų PIN kodą, pinigų likutį sąskaitoje, o tai gali paskatinti juos įvykdyti apiplėšimą, o vėliau, gavus mokėjimo kortelę, ištuštinti sąskaitą. PIN kodą geriau įrašyti viena ranka, kitą naudojant kaip skydą PIN kodui apsaugoti nuo galimo pamatymo. Ypač reikia būti atsargiems naudojantis bankomatais užsienyje, nes jų modeliai atskirose šalyse skiriasi, tad nepažįstami bankomatai visada kelia didesnę riziką. Taip pat iki minimumo bankomatuose reikėtų naudotis kvitais ir iš karto juos sunaikinti, kad jais negalėtų pasinaudoti galimi nusikaltėliai, rinkdamiesi potencialią auką.

8) Uždrausti platinti asmeninę informaciją

Vartotojai gali rinktis, kiek ir kokią informaciją jie nori pateikti prekybos įmonėms, kitoms bendrovėms, tam tikroms vyriausybinėmis organizacijomis. Informacija apie asmenis dažnai dalijamasi, tai daro daugelis verslo atstovų, ypač siūlydami naujas paslaugas ir prekybines akcijas. Tačiau galima nesutikti, kad asmeninė informacija būtų atskleista tretiesiems asmenims, būtina reikalauti pašalinti asmeninius duomenis iš komercinės rinkodaros duomenų bazių, atsisakyti nepageidaujamų laiškų, įskaitant katalogus ir kt.

9) Reikia pasidaryti asmens duomenų atsarginę kopiją

Dažnai patys asmenys net nežino savo asmens dokumentų numerių, jų galiojimo laiko, išdavimo datos ir t. t. Rekomenduojama padaryti dokumentų, kuriuos nešiojamasi su savimi, aprašą. Užsirašyti arba padaryti kopijas sąskaitų numerių, kredito kortelių, užfiksuoti dokumentų galiojimo datas, emitentų pavadinimus ir reikiamus telefono numerius, kad pranešus būtų galima atšaukti prarastų dokumentų galiojimą. Toks sąrašas padės susiorientuoti, kokie dokumentai prarasti nelaimės atveju, sutikrinti, kokie buvo kartu ir kokių jau nėra. Žinoma, negalima laikyti šio sąrašo piniginėje ar rankinėje, jį reikia paslėpti saugioje vietoje, kur pasiektų tik pats savininkas, tai galėtų būti namų seifas, kurį šiais laikais privalu turėti.

10) Kiekvieną mėnesį būtina peržiūrėti gaunamas sąskaitas

Reikia įsitikinti, kad visos gautos sąskaitos yra pagrįstos, paslaugų teikėjai žinomi ir pateikti jų sąskaitų duomenys taip pat. Dažnai pasi-

taiko, kad aptinkamos fiktyvios sąskaitos už paslaugas, vartotojai nieko neįtardami jas apmoka, vėliau paaiškėja, kad už jiems įprastas pasaugas jie sumokėjo sukčiams. Reikia tinkamai sekti mokėjimus, skirti keletą minučių jiems peržiūrėti, jei kyla įtarimas, kad pateiktos sąskaitos ir mokėjimo tvarka skiriasi nuo įprastos. Būtina atkreipti dėmesį, jeigu mokėjimo gavėjo pavadinimas pasikeitė arba pakeista pastovi mokėtina suma. Tokią grėsmę gerokai sumažintų elektroninės sąskaitos, gaunamos iš paslaugų teikėjų, ir tinkamai suformuoti atskaitymų šablonai elektroninės bankininkystės sistemoje – taip bet kokie pakeitimai būtų iškart pastebimi.

11) Rekomenduojama prieš išmetant ar keičiant sunaikinti duomenis seno kompiuterio kietajame diske

Kai asmuo perka naują kompiuterį ar keičia senojo kietąjį diską, ką daro su senuoju? Daugelis žmonių tiesiog jį išmeta. Tačiau jau nebeveikiantis kietasis diskas dar gali būti nuskaitytas, iš jo įmanoma ištraukti visą ar dalį buvusios informacijos. Būtina ištrinti visą informaciją, jei planuojama keisti diską ar išmesti seną. Net jei diskas neveikia, reikia pasirūpinti, kad jo niekas nebandytų nuskaityti. Dažniausiai siūlomi sprendimai – tai diską fiziškai sunaikinti (smūgiu plaktuku, įrenginį pergręžti, neatstatomai pažeidžiant standžius diskus). Jei diskas geras ir ketinama jį parduoti ar kt., reikia pasirūpinti, kad visi ten esantys duomenys tikrai būtų pašalinti. Jį reikia paprasčiausiai suformatuoti, o jei diske buvo tikrai svarbios informacijos, galima atlikti vadinamąjį nulinį formatavimą (angl. *Zero-filling*), kai visa disko talpa užpildoma nuliais, neatstatomai panaikinant bet kokį buvusį įrašą. Tokie patys sunaikinimo veiksmai turėtų būti atliekami ir su kitomis laikmenomis (USB kištukinėmis atmintinėmis, optinėmis laikmenomis).

12) Reikia būti atsargiems dėl produkto įsigijimo ir garantijų.

Dažnai perkant kokį prietaisą ar kitą namų apyvokos daiktą prašoma užpildyti garantinius dokumentus, nurodant asmens duomenis. Daugeliu atvejų ši informacija naudojama rinkodaros tikslais. Rekomenduojama nepildyti tokių laukų, kaip asmens metinės pajamos, kita svarbi finansinė informacija, nes visa tai neturi nieko bendro su garantiniu aptarnavimu ir

gali būti panaudota tapatybės vagystės nusikaltimams atlikti, atsirenkant potencialias aukas.

13) Reikia peržiūrėti valstybines mokesčių deklaracijas, net jei ir neturima ko deklaruoti

Būtina kiekvienais metais atidžiai peržiūrėti preliminarias valstybines mokesčių deklaracijas. Tai lengvai galima padaryti elektroniniu būdu. Jei deklaracijose pastebėta neatitikimų, sutarčių, kurių asmuo nepasirašė, ar įsiskolinimų, kurių asmuo neturėjo, reikia nedelsiant kreiptis į atitinkamas institucijas.

14) Galima naudoti privatumą saugančias priemones

Jei kompiuteris naudojamas keliaujant, kavinėse ir kitose viešose vietose ir būtinai tenka naudotis elektroninėmis finansinėmis paslaugomis, reikia pasirūpinti priemonėmis, kurios užtikrintų privatumą. Kaip vienas iš siūlymų – specialios ekrano apsaugos, klijuojamos plėveles, kurios užtikrina ekrano duomenų privatumą, matoma tik, kas sėdi tiesiai prieš ekraną. Tokie ekranai gali apsaugoti nuo smalsių akių, kai keliaujama ankštose erdvėse, tokiose kaip lėktuvas, traukinys, autobusas. Nors vadinamieji privatumo ekranai yra labai veiksmingi, tačiau jų nėra standartiniame komplekte, todėl tenka pirkti atskirai.

15) Negalima lengvai tikėti atsitiktine sėkme ir laimėjimais, taip pat nelaimėmis ir problemomis

Sukčiai dažnai naudoja laiškus, telefonus, internetą, kad apgautų. Jie gali pranešti, kad asmuo laimėjo puikų prizą, ar siekti sukelti nerimą pranešdami apie menamą nelaimę, gali prisistatyti valstybės pareigūnu, banko atstovu, įmonių vadovu, taikyti tam tikrus psichologinius metodus. Rekomenduojama neatsakinėkite į laiškus, kuriuose prašoma mokesčių ar verslo susitarimų, į raginimus pateikti informaciją apie banko sąskaitą, siekiant perduoti didelę pinigų sumą. Dažnai sukčiai bando išvilioti pinigus pirkdami prekes, už kurias neva per daug sumoka, dažnai atsiunčia fiktyvius tarptautinių mokėjimo kvitus, taip pat bando išvilioti pinigų menamoms advokato išlaidoms, kurios atsiranda dėl didelio laimėjimo dokumentų tvarkymo ir t. t.

16) Būtina saugotis mokėjimo kortelių duomenų pagrobimo

Negalima duoti mokėjimo kortelių į kitas rankas, būtina patiems atlikti mokėjimus. Šalyse, kuriose veikia SEPA[462] mokėjimų sistemos elementai, visos kortelės aptarnaujamos įvedant PIN kodą, tad daugiau dėmesio būtina skirti toms šalims, kuriose vis dar naudojami magnetiniai skaitytuvai. Reikia atidžiai stebėti, kad kortelė nebūtų neleistinai nuskaityta, t. y. jos magnetiniame takelyje esantys duomenys gali būti pagrobti siekiant kortelę klonuoti. Dažniausiai duomenys pagrobiami pardavėjo vietoje, tad būtina nenuleisti akių nuo mokėjimo kortelės.

17) Reikia stengtis išvengti duomenų pažeidimų

Dėl galimų duomenų pažeidimų būtina imtis reikiamų priemonių:

- Riboti svarbių duomenų saugojimą kompiuteriuose. Per daug asmeniškos ir identifikuojančios informacijos nelaikyti nešiojamame kompiuteryje, nes jį galima prarasti.
- Organizacijose būtina įgyvendinti duomenų saugos taisykles.
- Įdiegti šifravimo programinę įrangą, jei yra naudojami svarbūs duomenys.
- Informuoti darbuotojus apie šifravimo naudą ir įsitikinti, kad jie geba ja naudotis.
- Nuolatos atnaujinti informacinės sistemos elementus.
- Naudoti saugų interneto prisijungimą keliaujant.
- Apsvarstyti galimybę naudoti biometrines autentifikavimo ir identifikavimo technologijas.
- Išjungti kompiuterį dienos pabaigoje, taip bus galima sutaupyti energijos, o ir patį įrenginį galima ilgiau naudoti.

18) Rekomenduojama aktyvuoti įspėjimų apie galimus sukčiavimus paslaugą

Perspėjimai apie galimus sukčiavimus sudaro galimybę paslaugų teikėjams asmeniškai susisiekti su registruotu asmeniu ir patikrinti, ar asmuo pats savo valia atlieka finansines operacijas. Bankas gali susisiekti su klientu, jei jam kyla pagrįsta abejonė, kad klientas gali tapti tapatybės

[462] SEPA (angl. Single Euro Payments Area) – bendra mokėjimų eurais erdvė, kurioje mokėjimai nebus skirstomi į nacionalinius ir tarptautinius. SEPA [interaktyvus, žiūrėta 2011-09-20]. <http://www.ecb.int/paym/sepa/about/html/index.en.html>.

vagysčių auka. Pavyzdžiui, jei asmuo visą dieną keliauja ir trijuose skirtinguose oro uostuose atsiskaito mokėjimo kortele, bankas gali susisiekti su klientu ir nustatyti, ar klientas tikrai keliauja per tas šalis. Dažniausiai paplitusi įspėjimų sistema – tai lėšų judėjimo sąskaitose ataskaitos, siunčiamos į mobiliuosius telefonus. Vartotojas kiekvieną kartą gaus pranešimą, kai jo sąskaitoje bus naudojamos lėšos. Taip pat plačiai taikoma informavimo apie prisijungimą prie elektroninės bankininkystės sistema, kai vartotojas kiekvieną kartą jungdamasis prie elektroninės bankininkystės yra informuojamas (dažniausiai SMS žinute), taip pat informuojamas ir apie nepavykusius prisijungimus, visa tai sudaro galimybę greičiau sureaguoti ir užkirsti kelią galimai tapatybės vagystei.

19) Rekomenduojama naudoti kredito draudimus ir limitus

Tai išties naudingas apsaugos elementas, įskaitant tai, kad Lietuvoje populiarios greitosios paskolos. Galima sukurti tokią sistema, kuri leistų informuoti savo ir kitas kredito įstaigas apie tai, kad neketinama imti kreditų, paskolų, taip pat prekių išsimokėtinai. Tokiu būdu maksimaliai sumažinama rizika, kad tapatybės vagys, pasinaudoję asmens duomenimis, bandys pasiskolinti ar kitaip sukčiauti. Sistemą neturėtų būti sudėtinga įgyvendinti, pakaktų tai numatyti elektroninėje bankininkystėje, įtraukiant asmenį į nenorinčiuosius gauti paskolų ar pirkti išsimokėtinai. O jei toks poreikis atsirastų, tai šį draudimą ar limitą panaikinti galėtų tik pats asmuo (elektroninės bankininkystės sistemoje ar asmeniškai banke).

20) Būti nuolatos informuojamiems apie grėsmes

Reikia sekti kredito įstaigų ir valstybės institucijų pranešimus apie galimas tapatybės vagystės grėsmes. Domėtis naujovėmis ir vadovautis atitinkamų institucijų rekomendacijomis, susijusiomis su asmens duomenų apsauga. Lietuvoje ataskaitas ir rekomendacijas skelbia Valstybinė duomenų apsaugos inspekcija, Valstybinė vartotojų teisių apsaugos tarnyba ir kt. institucijos. Atsižvelgiant į turimą informaciją apie galimas grėsmes, bus galima greičiau ir lengviau jas aptikti ir kreiptis į reikiamas institucijas pagalbos.

21) Jei asmuo tapo auka

Jei asmuo tapo tapatybės vagystės auka, būtina nedelsiant kreiptis į banką, jei vagys pasinaudojo asmens finansiniais instrumentais, – ir į poli-

ciją. Jei pastebėjote, kad kažkas naudoja asmens duomenis be asmens sutikimo, reikia kreiptis į Valstybinę duomenų apsaugos inspekciją. Atsiminkite svarbiausią taisyklę – pirmiausia pats asmuo turi saugoti savo duomenis ir tik pasirūpinęs tinkama apsauga, jis galės tikėtis tinkamos pagalbos, nes jei asmuo kontroliuos visus savo duomenis, žinos, kur ir kiek jų yra palikęs, labiau padės tyrėjams atskleisti įvykusią tapatybės vagystę.

Be šių taisyklių, autorių nuomone, būtina laikytis ir asmeninės informacijos valdymo kontrolės. Kaip jau minėta, asmeninės informacijos skelbimas, pavyzdžiui, socialiniame tinkle, padidina tapatybės vagystės elektroninėje erdvėje tikimybę. Todėl asmenys turi kontroliuoti asmeninės informacijos apie save skelbimą viešai.

Beje, autorių nuomone, prevencija konkretaus asmens lygmeniu labiausiai turėtų būti nukreipta į asmenis nuo 18 iki 24 metų. Tyrimai rodo, kad šios amžiaus grupės asmenims pastebėti tapatybės vagystę elektroninėje erdvėje užtrunka dvigubai ilgiau nei vyresniems žmonėms[463].

Apibendrinančios išvados

• Patys vartotojai bene daugiausia turi prisidėti prie tapatybės vagystės elektroninėje erdvėje prevencijos.

• Vartotojai turi per mažai informacijos apie apsisaugojimo nuo tapatybės vagystės elektroninėje erdvėje būdus, todėl svarbu juos kuo daugiau informuoti. Tapatybės vagystės elektroninėje erdvėje prevencijos priemonių viešinimas skatintų vartotojus naudotis elektroninėmis paslaugomis ir didintų pasitikėjimą elektroninio verslo sektoriumi.

• Prevencijos konkretaus asmens lygmeniu taikytina 21 taisyklė, kurios turėtų laikytis kiekvienas asmuo, vykdydamas tam tikrą veiklą elektroninėje erdvėje. Be to, svarbi ir asmeninės bei privačios informacijos elektroninėje erdvėje kontrolė.

• Prevencija dėl tapatybės vagystės elektroninėje erdvėje konkretaus asmens lygmeniu labiausiai turėtų būti nukreipta į asmenis nuo 18 iki 24 metų.

[463] Javelin Study Finds Identity Fraud Reached New High in 2009, but Consumers are Fighting Back [interaktyvus, žiūrėta 2011-09-20]. <http://www.prnewswire.com/news-releases/javelin-study-finds-identity-fraud-reached-new-high-in-2009-but-consumers-are-fighting-back-83987287.html>.

4.2. Tapatybės vagystės elektroninėje erdvėje prevencija organizacijų lygmeniu

4.2.1. Tapatybės vagystės elektroninėje erdvėje prevencija viešajame sektoriuje

Išskirtinos tokios pagrindinės tapatybės vagystės elektroninėje erdvėje prevencijos priemonės viešajame sektoriuje:

- teisės aktai, numatantys atsakomybę už tapatybės vagystę;
- strategijos, kaip kovoti su tapatybės vagyste, kaip išvengti tapatybės vagystės ir netapti jos auka. Tokios strategijos pavyzdžiu galėtų būti JAV Prezidento kovos su tapatybės vagyste grupės 2007 metais patvirtintas „Kovos su tapatybės vagyste strateginis planas“[464];
- vieši renginiai / akcijos tapatybės vagystės tema;
- institucijos, atsakingos už elektroninius nusikaltimus, įskaitant tapatybės vagystę;
- forumai, kuriuose dalyvauja valdžios institucijų, įstatymų leidybos ir privataus sektoriaus atstovai;
- internetiniai tinklapiai, kuriuose būtų viešinama pagrindinė informacija apie informacijos saugą ir kovos su elektroninėje erdvėje kylančiomis grėsmėmis, įskaitant tapatybės vagystę, siekiant išvengti privatumo ir informacijos saugumo pažeidimų. Kaip pavyzdį galima paminėti JAV Federalinio tyrimų biuro tinklapio skiltį apie tapatybės vagystę (pateikiama bendra informacija apie tapatybės vagystę, naujienos, apsisaugojimo būdai, pranešimo galimybės, bylos ir kt.[465]).

Nors tapatybės vagystės elektroninėje erdvėje priemonės viešajame sektoriuje taip pat gali būti skirstomos į teisines bei organizacines technines (kaip nurodyta privataus sektoriaus prevencijoje), ypač atkreiptinas dėmesys į elektroninės informacijos saugumo aspektą viešajame sektoriuje. Kiekvienos organizacijos vienas iš svarbiausių tikslų yra užtikrinti savo, kaip organizacijos, ir vartotojų duomenų saugumą. Svarbu, kad tre-

[464] Combating Identity Theft: A Strategic Plan. 2007 [interaktyvus, žiūrėta 2011-09-20]. <http://www.idtheft.gov/reports/StrategicPlan.pdf >.

[465] Federal Bureu of Investigation. Identity Theft [interaktyvus, žiūrėta 2011-09-20]. <http://www.fbi.gov/about-us/investigate/cyber/identity_theft>.

čiosioms šalims nebūtų atskleista asmeninė informacija, kurią vartotojai nurodo užmegzdami dalykinius santykius su organizacija. Dauguma organizacijų apie savo vartotojus renka techninius ir statistinius duomenis.[466] Minėta informacija renkama, o vėliau ir analizuojama, siekiant pagerinti paslaugų teikimą vartotojams.

Taip pat svarbi ir organizacijos sauga, kuri tampa viena iš pagrindinių organizacijų veiklos dalių, siekiant užsibrėžtų tikslų. Prioritetus, saugos klausimus organizacijos dažniausiai apsibrėžia saugumo politikos gairėse, kurių tikslas yra sukurti ir išsaugoti tinkamas organizacijos veiklos sąlygas, apsaugoti veiklą ir valdyti grėsmes. Organizacijos savo saugos politiką nuolatos atnaujina ir papildo. Organizacijos saugumas užtikrinamas vykdant tinkamą priežiūrą atitinkamais metodais: patvirtintomis procedūromis, tvarkomis, dokumentų rinkiniais. Kiekviena organizacija įvertina galimus pavojus ir priima reikiamas prioritetines saugos kryptis.

Organizacijos saugos politiką įgyvendina priimti vidaus dokumentai, kuriuose nurodoma:

- Organizacijoje privalomi saugos reikalavimai, kurių turi būti laikomasi.
- Detalesnės ir organizacijos patvirtintos saugos tvarkos, instrukcijos, procedūros, kurios yra privalomos, ir rekomendacijos, kurių patariama laikytis.
- Organizacijos saugos politikos dokumentai yra vieši ir prieinami visiems jos nariams ir vartotojams, o atitinkamos detalios saugos tvarkos, specialiosios instrukcijos, procedūros, rekomendacijos priskiriamos prie vidinių dokumentų, kurie prieinami tik tos organizacijos nariams.

Organizacijos, formuodamos saugos politiką, turi remtis ne tik šioje monografijoje detaliau nagrinėtais Lietuvos Respublikos teisės aktais, bet ir tarptautiniu mastu pripažintais dokumentais, tokiais kaip ISO 27001:2005 standartu. Minėtas standartas apima visas organizacijas, nepaisant jų teisinio statuso. Jis apibrėžia reikalavimus:[467]

- Nustatant ir įgyvendinant saugumo valdymo sistemas.

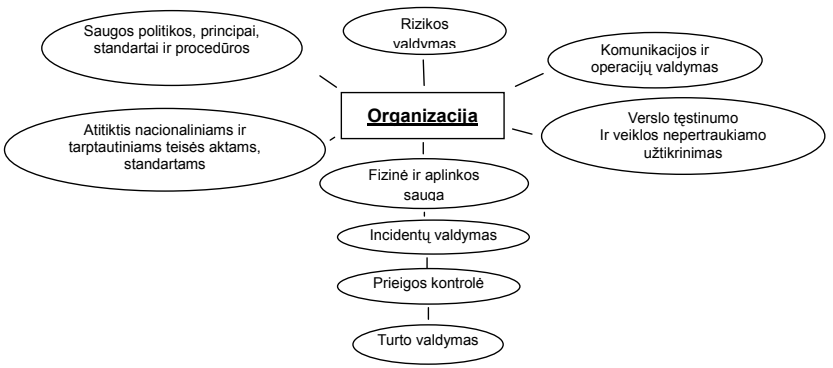
[466] Pvz., kompiuterio IP adresą, interneto naršyklės tipą, informaciją apie operacinę sistemą ir kt.

[467] ISO/IEC 27001 [interaktyvus, žiūrėta 2011-09-20]. <http://en.wikipedia.org/wiki/ISO/IEC_27001>.

- Eksploatuojant, prižiūrint, persvarstant, saugant ir gerinant dokumentų informacijos saugumo valdymo sistemas.
- Specifinius reikalavimus įgyvendinant saugumo prevencinę kontrolę, kuri yra adaptuota pagal atskiros organizacijos poreikius.

Šis standartas taip pat apima naudojamų informacinių technologijų priežiūrą, taikomų saugumo metodų parinkimą, informacinių saugumo valdymo sistemų (angl. *Information Security Management Systems* (ISMS) reikalavimus. Pagrindinis standarto tikslas – organizacijose užtikrinti tinkamą ir proporcingą saugumo kontrolę, kuri apsaugotų organizacijos informaciją ir didintų vartotojų pasitikėjimą.

Kiekviena organizacija, apibrėždama savo saugos politiką, detalizuoja procedūras, taikomas atitinkamose srityse. Panašias procedūras ir tvarką savo veikloje tvirtina ir LR valstybinės įstaigos, besiremiančios galiojančiais teisės aktais[468]. Apibendrinant galima išskirti svarbiausias organizacijos saugos sritis, kurios organizacijos saugos politikoje privalo atsispindėti (sudaryta autorių):



29 pav. Svarbiausios organizacijos saugos sritys

Pagal autorių atliktą Sodros darbuotojų apklausą, vienos iš pagrindinių priemonių kovai su tapatybės vagyste elektroninėje erdvėje buvo įvardintos teisinės, organizacinės ir techninės priemonės. Viešojo sektoriaus darbuotojų apklausa parodė, kad svarbiausios žinomos kovos su tapatybės

[468] LR vidaus reikalų ministro įsakymas „Dėl saugos dokumentų turinio gairių patvirtinimo" 2007 m. gegužės 8 d. Nr. 1V-172. *Valstybės žinios*, 2007-05-15, Nr. 53-2070.

vagyste elektroninėje erdvėje priemonės yra: techninės, teisinės (teisės aktai, vidaus dokumentai). Manytina, kad įvardytos organizacinės ir techninės priemonės taip pat turi būti įtrauktos į viešojo sektoriaus atitinkamo subjekto vidaus saugos politiką. Teisinės priemonės gali būti taikomos ir valstybiniu lygmeniu. Taip pat Sodros darbuotojai ir viešojo sektoriaus darbuotojai kaip vieną iš pagrindinių priemonių nurodė asmenų sąmoningumą ir mokymus, švietimą. Švietimą ir informavimą kaip vienas svarbiausių tapatybės vagystės elektroninėje erdvėje prevencijos priemonių nurodė ir autorių apklausti 3 ekspertai (1-asis, 2-asis ir 9-asis).

Nepaisant apsaugos nuo tapatybės vagystės viešajame sektoriuje priemonių įvairovės, manytina, kad lėšų apsaugai nuo šio pavojingo reiškinio skiriama nepakankamai. Pagal autorių atliktą tyrimą, Sodros darbuotojai mano, kad jų organizacijoje daugiau lėšų skiriama apsaugai nuo tiriamo reiškinio. Jie situaciją vertino 6,57 balo iš 10 galimų, o viešojo sektoriaus darbuotojai apskritai situaciją vertino 4,66 balo iš 10 galimų. O dėl priemonių kovai su šiuo pavojingu reiškiniu pakankamumo, skirtingai nuo Sodros darbuotojų, viešojo sektoriaus darbuotojai mano, kad jų organizacijos nepakankamai imasi priemonių kovai su tapatybės vagyste elektroninėje erdvėje ir jos prevencijai užtikrinti, taip mano net 73,7 proc., o Sodros darbuotojų, manančių, kad tokių priemonių nepakanka, yra tik 31,9 proc. Taigi, viešajame sektoriuje reikėtų didinti lėšas ir gerinti apsaugos nuo tapatybės vagystės elektroninėje erdvėje priemones.

Be to, paminėtina, kad turėtų būti gerinamas ir tarpinstitucinis bendradarbiavimas, kiek tai susiję su informacijos keitimusi apie tapatybės vagystę elektroninėje erdvėje, tyrimu ir pan. Autorių apklausti 1-asis ir 2-asis ekspertai teigė, kad tarpinstitucinį bendradarbiavimą reikėtų gerinti. Be to, viešasis sektorius turėtų geriau bendradarbiauti su privačiu sektoriumi. Ekspertai: 1-asis, 2-asis, 4-asis, 5-asis, 6-asis, 7-asis ir 8-asis teigė, kad toks bendradarbiavimas nepakankamas arba galėtų būti geresnis. Ekspertai vardijo bendradarbiavimo trūkumus: 1-asis ekspertas, kad trūksta pasitikėjimo verslu, ypač didelėmis, patikimomis įmonėmis; blogai, kad visiems taikomi vienodi kriterijai, 2-asis ekspertas nurodė, kad trūksta vienos koordinuojančios institucijos, atsakingos už problemos sprendimą, 4-asis ekspertas teigė, kad trūksta informacijos keitimosi, visuomenės sąmoningumo ir atsakingumo, 5-asis, 7-asis ir 8-asis ekspertai iškėlė panašią problema, kad privatus sektorius nėra suinteresuotas tirti ir

tyrimus viešinti, o tai trukdo efektyviai kovoti su šiuo reiškiniu. Panašios problemos turi būti sprendžiamos ir privačiame sektoriuje (apie prevenciją šiame sektoriuje žr. toliau).

Be to, viešajame sektoriuje nepakanka viešosios informacijos apie tapatybės vagystės elektroninėje erdvėje pavojingumą ir apsisaugojimo nuo šio pavojingo reiškinio būdus. Viešosios informacijos pakankamumą apskritai viešojo sektoriaus darbuotojai vertino labai panašiai, t. y. 4 balais iš 10, o Sodros – 4,79 balsais iš 10. Tai reiškia, kad viešosios informacijos dėl tapatybės vagystės elektroninėje erdvėje pavojingumo ir apsisaugojimo nuo šio pavojingo reiškinio, apimtis nukreiptas į šį sektorių, reikėtų didinti.

Detalesnė informacija apie autorių atliktus tyrimus pateikiama monografijos 5.2 dalyje.

4.2.2. Tapatybės vagystės elektroninėje erdvėje prevencija privačiame sektoriuje

Autorių atlikta ekspertų apklausa parodė, kad rizikingiausias yra privatus sektorius. Taip teigė dauguma ekspertų (5 ekspertai: 1-as, 3-as, 5-as, 7-as, ir 8-as). Todėl prevencijai šiame sektoriuje turi būti skiriama daug dėmesio.

Tapatybės vagystės elektroninėje erdvėje tikimybė

Tapatybės vagystės elektroninėje erdvėje prevenciją privačiame sektoriuje galima įvardyti kaip rizikos kompiuterinėms sistemoms ir elektroninei informacijai nustatymą ir įvairių saugumo priemonių, kurios padės apsaugoti šias sistemas, įgyvendinimą.

Istoriškai kompiuterinių sistemų apsaugos priemonės yra labiau nukreiptos į informaciją, susijusią su nacionaliniu saugumu. Šiuo metu daug dėmesio skiriama privačios informacijos ir duomenims, esantiems individualiose kompiuterinėse sistemose, taip pat organizacijų, finansinių, mokslinių ir kitų institucijų kompiuterinėse sistemose, apsaugoti.

Mažai organizacijų gali sau leisti taikyti kompiuterinių sistemų apsaugą nuo bet kokios rizikos (jei tokia apsauga iš viso galima). Tai daug kainuoja. Apsaugos kaina dažnai lyginama su rizika. Saugumo lygis, su kuriuo organizacija sutinka, vadinamas prieinama rizika.

Tapatybės vagystės elektroninėje erdvėje prevencijos įgyvendinimas betarpiškai susijęs su rizikos analize. Kiekviena rizikos analizė apima:

- grėsmes;
- pažeidžiamumą;
- kontrpriemones.

Grėsmė – tai galimas pavojus kompiuterinei sistemai. Tapatybės vagystės elektroninėje erdvėje atveju pavojų gali sukelti žmogus (vagis, profesionalus nusikaltėlis, programišius). Pažeidžiamumas – jautri pažeidimui kompiuterinės sistemos vieta. Grėsmė pasireiškia konkrečioje veikoje, susijusioje su sistemos pažeidžiamumu. Kontrpriemonės – priemonės kompiuterinei sistemai apsaugoti: slaptažodžiai, antivirusinės programos, durų užraktai ir pan.

Taigi, rizikos analizė yra procesas, kurio metu atsakoma į klausimus – pirma, apie grėsmes, antra, apie pažeidžiamumą ir galiausiai apie kontrpriemones, kurias naudojant galima užkirsti kelią pavojui[469].

Į rizikos analizę taip pat įeina ir įvertinimas, kaip gerai organizacija pasiruošusi blogiausiam variantui – kartais vadinamam atsitiktinumų planavimu arba vadovavimu krizei.

Yra du rizikos analizės vertinimo tipai:

- išankstinis – atliekamas prieš tai, kol dar neįvyko incidentas;
- pavėluotas – atliekamas jau po incidento.

Kompiuterinės sistemos pažeidžiamos vietos ir grėsmės gali būti skirstomos į statines ir dinamines. Rizikos analizė, bėgant laikui ir keičiantis sąlygoms, turi keistis, nesvarbu, ar organizacijos viduje, ar išorėje.

Keičiantis aplinkai, reikia būti budriems. Patartina keisti rizikos analizę, jei atsitinka tokie įvykiai:

1. Organizacijoje yra didelė personalo kaita. Papildomai tikrinama kvalifikacija, priimant naujus darbuotojus;
2. Organizacija valdo, tvarko naują, svarbią privačią informaciją;
3. Organizacija susijungia su kita organizacija;
4. Organizacijoje įvykdomas naujas elektroninis nusikaltimas;
5. Organizacija tapo teroristų ar kitokių nusikaltėlių taikiniu;

[469] Icove, D. 1995. *Computer crime: A Crimefighter`s Handbook*. O`Reylly Associates, Inc., p. 91.

6. Organizacijos kompiuterinėje aparatinėje ar programinėje įrangoje aptinkama pažeidžiama vieta ar virusas.

Rizikos analizė atliekama tam tikra tvarka. Tipinė rizikos analizė skirstoma į penkis punktus:

1. Klausimų uždavimas;
2. Žvalgybos pranešimai;
3. Pažeidžiamų vietų analizė;
4. Saugumo kontrpriemonių plėtra;
5. Duomenų dokumentavimas ir sprendimai[470].

1. Kiekviena rizikos analizė prasideda nuo klausimų uždavimo. Pavyzdžiui, kas kėsinsis į kompiuterinę sistemą? Kokia technika bus naudojamasi atakuojant kompiuterinę sistemą? Kokius duomenis bus stengiamasi pavogti?

2. Tai tam tikros išorinės informacijos naudojimas. Pavyzdžiui, sužinoma, kad konkurentai ieško įsilaužėlių, kurie patektų į kompiuterinę sistemą ir t. t.

3. Kita rizikos analizės pakopa irgi yra labai specifinė. Nustačius grėsmes, kurias galima numatyti, sprendžiama, kur kompiuterinėje sistemoje yra pažeidžiamų vietų. Netgi jei grėsmės gali pasirodyti mažesnės, reikia nustatyti visas galimas pažeidžiamas vietas, nes mažos grėsmės gali tapti didelėmis. Tikslas – papunkčiui jas išvardyti. Jei išanalizuotos visos galimos pažeidžiamos vietos, yra daugiau šansų, kad kompiuterinės sistemos bus apsaugotos nuo nenumatytų atvejų.

4. Dabar, kai žinomos kompiuterinės sistemos pažeidžiamos vietos ir kyla grėsmė, kad jos gali būti išnaudotos, reikia taikyti saugumo kontrpriemones. Organizacija turi įvertinti, kompiuterinės sistemos grėsmes, sistemos pažeidžiamumą, realiai esamus išteklius. Kompiuterinės sistemos trūkumų įveikimo laipsnis priklauso nuo jų pobūdžio ir nuo turimų lėšų. Kartais atliekant rizikos analizę galima išgirsti terminą „grėsmės lygis“. Jei grėsmės lygis minimalus, išlaidos irgi greičiausiai bus minimalios. Jei grėsmės lygis aukštas, išlaidos bus daug didesnės.

[470] Icove, D. 1995. *Computer crime: A Crimefighter`s Handbook.* O`Reylly Associates, Inc., p. 92.

5. Duomenų ir sprendimų dokumentavimas: gera idėja yra duomenis ir sprendimus užrašyti: pakanka ir atskiros suvestinės, parodančios esamas grėsmes kompiuterinei sistemai, galimas pažeidžiamas vietas ir apsaugos kontrpriemones, kurios sumažintų riziką iki priimtino lygio.

Rizikos analizė apima ir pažeidžiamų vietų bei atsakomųjų priemonių nustatymą. Yra daug skirtingų pažeidžiamų vietų – nuo personalo klausimų iki aparatinės ir programinės įrangos problemų. Kiekvienu atveju reikia numatyti atitinkamas kontrpriemones. Bet pirmiausia reikia jas visas nustatyti. Pavyzdžiui, pažeidžiama vieta yra neautorizuotas priėjimas prie programų, o atsakomosios priemonės – vartotojo identifikavimas, stebėjimas filmavimo kameromis ir kt.

Tapatybės vagystės elektroninėje erdvėje prevencijos priemonės privačiame sektoriuje

Atsakomosios arba saugumo prevencinės priemonės yra kelių rūšių. Jungtinių Tautų tarptautinėje kriminalinės policijos kompiuterinių nusikaltimų apžvalgoje šios priemonės skirstomos į 6 grupes (organizacijos lygmeniu):

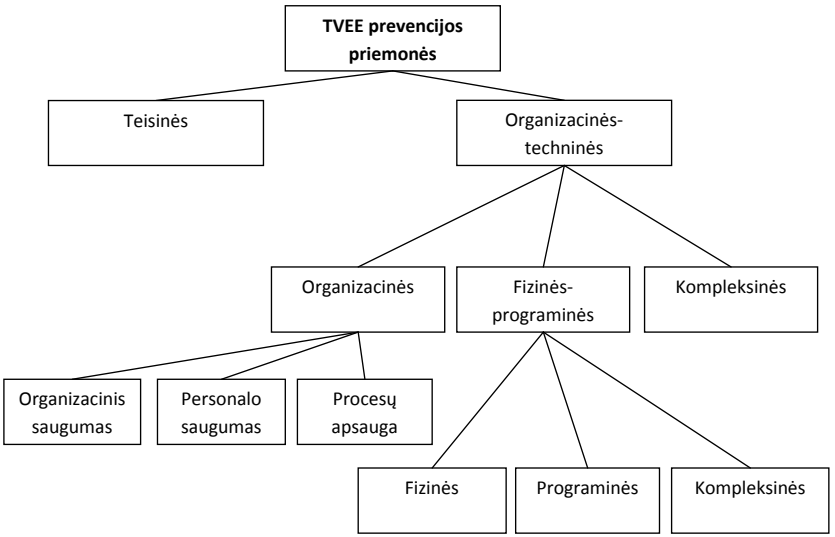
1) administracinis ir organizacinis saugumas;
2) personalo saugumas;
3) fizinė apsauga;
4) komunikacijų ir elektroninis saugumas (ryšių apsauga);
5) programinės įrangos saugumas;
6) procesų saugumas (operacijų saugumas)[471].

Remiantis duomenimis ir analizuojant specialiąją literatūrą dėl klausimų, susijusių su elektroninių nusikaltimų teoriniais ir praktiniais aspektais, galima išskirti dvi pagrindines elektroninių nusikaltimų, taigi ir tapatybės vagystės elektroninėje erdvėje, prevencijos priemones:

1) teisinės;
2) organizacinės techninės.

[471] Jungtinių Tautų tarptautinėje kriminalinės policijos kompiuterinių nusikaltimų apžvalga "International review of criminal policy - United Nations Manual on the prevention and control of compute-related crime, p. 41 [interaktyvus, žiūrėta 2011-09-20]. <http://www.ifs.univie.ac.at/-pr2gq1/rev4344.html>.

Tolesnį prevencijos priemonių skirstymą žr. 30 pav.



30 pav. Tapatybės vagystės elektroninėje erdvėje prevencijos priemonės

Teisinės tapatybės vagystės elektroninėje erdvėje prevencijos priemonės

Prie teisinių apsaugos priemonių reikia priskirti visas vidines organizacijų taisykles, reglamentuojančius saugų kompiuterinės informacijos naudojimą ir platinimą bei saugų kompiuterinių tinklų naudojimą ir kt.

Pagal autorių atliktą verslo sektoriaus apklausą, verslo sektoriaus respondentai kaip vieną iš pagrindinių kovos su tapatybės vagyste elektroninėje erdvėje priemonių nurodo teisines priemones (teisės aktai, vidaus dokumentai). Detalesnė informacija apie atliktus tyrimus pateikta 5.2.5 dalyje.

Organizacinės-techninės tapatybės vagystės elektroninėje erdvėje prevencijos priemonės

Paminėtina, kad šių priemonių svarbą išskyrė du autorių apklausti ekspertai. Kaip pavaizduota 30 pav., šios priemonės skirstomos į tris grupes:

1) organizacinės;
2) fizinės programinės;
3) kompleksinės.

1. Organizacinės priemonės

Organizacinės kompiuterinės technikos apsaugos priemonės apima veiksmus parenkant, tikrinant ir instruktuojant personalą, kuriant informacinių objektų atstatymo planą incidento atveju, organizuojant programinę techninę kompiuterinės technikos priemonių priežiūrą, apibrėžiant atsakomybę asmenims, dirbantiems su kompiuterine technika, nustatant kompiuterinių sistemų funkcionavimo konfidencialumo režimą, užtikrinant fizinės objektų apsaugos režimą, materialinį-techninį aprūpinimą.

Organizacinės priemonės savo ruožtu skirstomos į:

- bendras saugumo politikos plėtros priemones (organizacinis saugumas);
- prevencijos priemones, nukreiptas į personalą (personalo saugumas);
- procesų apsauga.

Bendros saugumo politikos plėtros priemonės (organizacinis saugumas)

Prevencijos priemonių diegimas prasideda bendros saugumo politikos plėtra ir procedūros jai įgyvendinti nustatymu (**administracinis ir organizacinis saugumas**). Jos apima šiuos elementus:

- procesų, užtikrinančių rizikos identifikavimą, diegimas;
- individualių saugumo pareigų apibrėžimas ir atsakomybės paskirstymas;
- riboto patekimo vietų nustatymas;
- autentifikavimo procedūrų nustatymas;
- nenumatytų atvejų planų rengimas ir t. t.

Prevencijos priemonės, nukreiptos į personalą (personalo apsauga)

Ši apsauga numato asmens identifikavimą ir hierarchijos nustatymą prieinant prie skirtingos svarbos informacijos tiek asmenims, dirbantiems organizacijos viduje, tiek asmenims, kontaktuojantiems su organizacija iš išorės.

Apsauga personalo lygiu taip pat apima darbuotojų atranką, testavimą, mokymą, kvalifikacijos tikrinimą ir stebėjimą.

Bet kokioje kompiuterinėje sistemoje didžiausią grėsmę kompiuteriniam saugumui kelia žmonės. Kai kurie iš jų paprasčiausiai gali būti

nekvalifikuoti, net to nenorėdami gali sunaikinti kompiuterinėse sistemose esančią svarbią informaciją. Kiti žmonės gali piktaviliškai pažeisti nustatytas taisykles.

Taigi, yra daug žmonių tipų, kurie gali kelti pavojų kompiuteriams ir informacijai, pradedant nuo naujų kompiuterių vartotojų, nepatenkintų darbuotojų iki profesionalių nusikaltėlių ir šnipinėjimo agentų.

Personalo saugumas yra svarbi kompiuterinių sistemų apsaugos dalis. Todėl personalo saugumo programa turi būti nuolat tobulinama. Daugumą aptiktų elektroninių nusikaltimų padaro darbuotojai, kurių motyvacijos gali būti skirtingos. Tačiau personalo saugumo programa turi apimti ne tik vidines grėsmes, bet ir išorines.

Taip pat reikia atkreipti dėmesį į darbuotojus. Ar jie gerai patikrinami prieš priimant į darbą? Priimti netinkami darbuotojai gali sukelti nemalonumų. Reikia turėti gerų vadovų ir personalo specialistų, orientuotų į žmogiškųjų išteklų valdymą, kurie įvertintų darbuotojų pasiruošimą ir jų moralę. Taip pat reikia mokyti darbuotojus, kad jie nepadarytų neapdairių klaidų, kurios sukeltų grėsmę elektroninės informacijos saugumui ar kompiuterinių programų veikimui.

Reikia žinoti, kad globalizacija daro didžiulę įtaką personalo saugumo programoms. Turint sudarytą gerą personalo saugumo programą, iš dalies galima kontroliuoti įvykius, kai jie kelia grėsmę kompiuterinėms sistemoms. Grėsmė, susijusi su personalu, priklauso nuo kelių veiksnių:

1) Priėjimo prie kompiuterinių sistemų tipo;
2) Pažeidėjo išsilavinimo lygio;
3) Pažeidėjo motyvacijos.

1) Priėjimo tipai. Žala kompiuterinėms sistemoms gali būti padaroma naudojant įvairaus lygio priėjimo prie kompiuterinės sistemos būdus. Jei žmogus turi tiesioginį priėjimą prie kompiuterinės sistemos, grėsmė yra daug didesnė. Tačiau ir neturintys tiesioginio priėjimo prie kompiuterinės sistemos asmenys gali į ją įsilaužti, sugadinti failus, užkrėsti virusais ar padaryti fizinę žalą.

2) Kvalifikacijos lygis.

Kuo didesnė kvalifikacija, tuo didesnis grėsmės lygis. Kita vertus, žemos kvalifikacijos darbuotojas, nepatikrinęs kompiuterinės laikmenos antivirusinėmis programomis, taip pat gali pridaryti daug žalos – kompiuterinę sistemą gali sugadinti virusai.

3) Motyvacija.

Darbuotojai, kuriems patinka darbas ir kurie gerai sutaria su darbdaviu, nėra linkę atlikti neleistinų veiksmų su asmenine informacija. O štai kita dalis darbuotojų, kurie turi papeikimų ar yra pasipiktinę dėl kitų priežasčių, – kelia didelę grėsmę.

Ne visų elektroninių nusikaltimų motyvai padaromi iš blogų paskatų tam tikros organizacijos atžvilgiu. Kai kurie nusikaltimai vykdomi norint parodyti intelektualinius gebėjimus. Vis dėlto didžioji dalis nusikaltimų daromi turint savanaudiškų motyvų ir siekiant finansinės naudos.

Norint pagerinti personalo apsaugą, reikia:

- vadovauti tarnybos kvalifikacijos tikrinimams;
- modernizuoti informaciją, taikomą šiems tikrinimams;
- patikrinti visas sutartis su pardavėjais, nustatyti, ar pardavėjai tikrina savo darbuotojus;
- organizacijai reikia turėti saugumo politiką, pageidautina išdėstytą raštu;
- mokyti darbuotojus būti budrius ir pranešti apie visas įtartinas veikas;
- kurti sistemas, kad būtų užkirstas kelias individams gauti prieigą prie aparatūros ir failų, kai jie palikti be priežiūros;
- mokyti prižiūrėtojus nustatyti darbuotojų problemas ir jas spręsti;
- atskirti teisėtos prieigos funkcijas;
- taikyti saugumo revizijos procedūras;
- žinoti, kad galimas nepatenkintų darbuotojų, *eks* darbuotojų, klientų kerštas;
- užtikrinti, kad naudojant kompiuterines sistemas būtų laikomasi visų taisyklių;
- įgyvendinti atostogų politikos ir darbuotojų kaitos paskyrimus. Kai kurioms saugumo atakoms užbaigti reikia ilgo laiko, bet ir jas galima sustabdyti;
- apriboti prieigą prie labai svarbių kompiuterinių sistemų ir duomenų;
- kai darbuotojas atleidžiamas iš pareigų: panaikinti jo prieigos teises prie kompiuterinės sistemos, ištrinti darbuotojo slaptažodžius; atsiimti raktus, praėjimo kontrolės korteles; patikrinti

darbuotojo failus ir išsaugoti juos, nes gali prireikti ateityje; jei darbuotojas buvo administratorius – pakeisti visus sistemos slaptažodžius.

Procesų apsauga

Tai toks saugumo tipas, kuris aptinka kompiuterinių sistemų saugumo pažeidimus ir užkerta kelią jiems atsirasti. Procesų apsaugą sudaro du pagrindiniai kompiuterinio saugumo aspektai:

- būdai, kuriais mokomos galimos elektroninių nusikaltimų aukos apie galimus kompiuterinius nusikaltimus;
- būdai, kuriais faktiškai sulaikomi nusikaltėliai, kad nepadarytų nusikaltimo kompiuterinėse sistemose.

Procesų apsauga negali egzistuoti atskirai nuo kitų sistemų. Ji veiksminga tik tada, kai yra integruota į organizacijos fizinės, personalo ir kt. saugumo programas. Iš tikrųjų procesų apsauga naudojama, kad padėtų šioms programoms veikti efektyviau. Yra keli paprasti būdai, kaip procesų apsauga gali sąveikauti su kitomis saugumo procedūromis:

- dažnas kompiuterio slaptažodžio keitimas, bet keitimas ne pagal tvarkaraštį, o atsitiktinai;
- jeigu pastatas būna atidarytas, keletą valandų per savaitę reikia kontroliuoti priėjimą, bet kad niekas nežinotų, kada tos valandos bus;
- maskuoti procesų pavyzdžius, kad juos būtų galima sunkiai atspėti. Pavyzdžiui, vietoje programos, kuri tikrina autorizuotas programas, paleidimo, kiekvieną naktį 2 valandą paleisti programą, dažnai 24 valandų periodu, ir kiekvieną kartą programai duoti skirtingą vardą;
- aktyviai saugoti informaciją, kuria gali pasinaudoti kompiuteriniai nusikaltėliai, planuodami nusikaltimą;
- formuluoti būdus, kurie aptiktų kompiuterinį nusikaltėlį, kai nusikaltimas jau įvyko arba tikėtina, kad įvyks.

Pagrindiniai procesų saugumo programos elementai:

- nustatyti konkrečią privačią informaciją, esančią tam tikroje kompiuterinėje sistemoje, į kurią gali bandyti kėsintis kompiuteriniai nusikaltėliai;
- nustatyti metodus, kuriuos gali taikyti elektroninis nusikaltėlis, kad gautų reikiamą informaciją;

- taikyti procesų procedūras, padedančias pasipriešinti elektroninių nusikaltėlių metodams, užkirsti priėjimo prie informacijos kelią ir aptikti bet kokius saugumo pažeidimus;
- įtraukti darbuotojus į programą (jie turi žinoti, kad operacijų saugumas ir kompiuterinis saugumas apskritai yra svarbi jų procesų dalis).

Užsienio praktika rodo, kad gana veiksminga prevencijos priemonė yra kompiuterinio saugumo specialisto arba saugos įgaliotinio pareigybės, ar atitinkamų dalinių sukūrimas.

Tam, kad būtų sudaryta efektyvi operacijų saugumo programa, reikia perprasti nusikaltėlio mąstymą:

* Kokie yra motyvai atakuoti tam tikrą taikinį?
* Ar reikia didelės kvalifikacijos, kad ataka būtų sėkminga?
* Kokia informacija reikalinga pasiruošti atakai?
* Kaip nusikaltėlis bandys gauti šią informaciją?

Darbuotojams reikia suprasti, kam reikalinga tokia apsauga, kokie yra metodai, leidžiantys kompiuteriniams nusikaltėliams įsilaužti į kompiuterines sistemas, ir ką darbuotojai asmeniškai gali padaryti, kad užkirstų kelią tokiems įsilaužimams[472].

Yra dvi priežastys, kodėl svarbus darbuotojų informuotumas. Pirma, yra būdų, kuriais darbuotojai gali sulaikyti nusikaltėlius nuo įsiveržimo į kompiuterines sistemas, pavyzdžiui, darbuotojai turi būti atsargūs ir neužrašinėti viešai slaptažodžių arba neišmetinėti svarbių ataskaitų ir kitokių dokumentų į šiukšlių dėžes. Antra, jei darbuotojai bus budrūs, jie gali atpažinti, kai žmogus kėsinasi į informaciją.

2. Fizinės-programinės priemonės

Autorių atliktos verslo sektoriaus apklausos duomenimis, verslo sektoriaus respondentai kaip pagrindinę kovos su tapatybės vagyste elektroninėje erdvėje priemonę nurodo technines priemones (slaptažodžiai, elektroninės programos ir kt.). Detalesnė informacija apie atliktus tyrimus pateikiama monografijos 5.2 dalyje.

Šios priemonės savo ruožtu skirstomos į:

1) fizines (aparatines);

2) programines;

3) kompleksines.

[472] Icove, D. 1995. *Computer crime: A Crimefighter`s Handbook*. O`Reylly Associates, Inc. p. 145.

Fizinė apsauga

Ji apima metodus, skirtus užkirsti kelią galimam konfidencialios informacijos ir duomenų nutekėjimui.

Fizinė apsauga apima visus su kompiuterine sistema susijusius įrenginius: pastatą, kompiuterio kambarį, patį kompiuterį ir kitą su juo susijusią įrangą (diskus, spausdintuvus ir pan.), saugojimo įrenginius (diskus, atspausdintus tekstus), komunikacijų įrenginius (įvairius kabelius).

Aparatinės (fizinės) apsaugos metodų realizacija dažniausiai atliekama naudojant įvairius techninius specialios paskirties įtaisus:

- aparatūros, ryšių linijų ir patalpų, kuriose yra kompiuteriai, ekranavimo aparatūrą;
- įrenginius, užtikrinančius tiktai sankcionuotą patekimą į saugomus objektus (šifruojamas spynas, asmens identifikacijos įrenginius);
- terminalų ir vartotojų identifikacijos ir fiksacijos, bandant gauti neteisėtą priėjimą prie kompiuterinio tinklo, įrenginiai;
- apsaugos ir gaisrinės signalizacijos priemonės (veiksmingos saugant kompiuterinius tinklus nuo neteisėtos prieigos ir t. t.).

Kompiuterinės sistemos fizinė apsauga yra konkretus ženklas darbuotojams ir klientams, kad apsauga yra rimtai vertinama.

Fizinė apsauga nuo žmonių yra gana sudėtinga. Pirma gynybos nuo įsilaužėlių linija yra neprileisti jų prie pastato ar kompiuterių kambario. Tai nėra taip paprasta, kaip tai būdavo, kai dauguma organizacijų turėjo vieną kompiuterį gerai rakinamame kambaryje. Šiomis dienomis daugelyje organizacijų vos ne kiekvienas darbuotojas turi kompiuterį, todėl pakankamai sunku užtikrinti jų apsaugą.

Kad patektų į pastatą ar užrakintą kompiuterinį kambarį, naudotojas turi atlikti tam tikro tipo identifikavimo testą. Yra trys klasikiniai savęs identifikavimo būdai:

* Tai, ką turi žinoti, pvz., slaptažodį;
* Tai, ką turi turėti, pvz., raktą, ženklelį, kortelę;
* Tai, kas tu pats esi, pvz., delno, pirštų antspaudai.

Visos šios identifikavimo priemonės gali būti naudojamos kompiuterinių sistemų fizinei apsaugai užtikrinti.

Labai svarbus momentas yra fizinio saugumo sistemų bandymas. Užuot laukus, kada įvyks elektroninis nusikaltimas, reikia taikyti tris fizinio saugumo programos testavimo būdus[473]:

1) sistemingi fizinio saugumo patikrinimai;
2) atsitiktiniai fizinio saugumo patikrinimai;
3) prasiskverbimo testai.

1. Reguliarūs fizinės apsaugos tikrinimai – fizinio saugumo apžiūra dažniausiai vykdoma darbuotojo, kuris dirba kompanijoje, naudojant iš anksto paruoštą sąrašą. Šis sąrašas padeda užtikrinti, kad visos galimos pažeidžiamos vietos bus patikrintos. Tokia sistema galėtų funkcionuoti geriau, kai žmonės, vykdantys apžiūrą, dirba ne toje vietoje, kuri tikrinama. Pavyzdžiui, žmonės, kurie dirba penktame aukšte, vykdo ketvirto aukšto apžiūrą.

Kartais fiziniam saugumui tikrinti pasitelkiami ekspertai. Tai patartina daryti tada, kai prarasta daug turto arba buvo suplanuoti esminiai fizinio saugumo keitimai. Profesionalios komandos ataskaita yra daug geresnė už savos komandos ataskaitą.

2. Atsitiktiniai saugumo patikrinimai – priėjimo kontrolės sistemos gali būti labai sudėtingos, bet jei darbuotojai ne visai gerai uždaro duris, sistema tampa neveiksminga. Tokiu atveju naudingi atsitiktiniai saugumo patikrinimai.

3. Prasiskverbimo testai vykdomi profesionalų didelės rizikos kompiuterinėse sistemose (pavyzdžiui, karinių padalinių ir kt.).

Daug žalos kompiuterinėms sistemoms padaro ir vadinamieji įsibrovėliai – žmonės, kurie be leidimų įvairiais būdais patenka prie kompiuterinių sistemų. Kad to būtų išvengta, reikia laikytis šių taisyklių:

- įrengti specialias atsargumo priemones patalpų, kuriose yra kompiuterinės sistemos, duryse;
- turi būti tvirtos kambarių sienos;
- turi būti tvirtos kambarių lubos ir grindys;
- turi būti maži oro kondicionavimo langeliai;
- kompiuterines sistemas reikia laikyti toliau nuo langų: juos lengva išdaužti, o jei nusikaltėlis juos išdaužia, jau vien langas gali daug kainuoti. Žmonės taip pat gali patekti pro langus ir nuskaityti informaciją;

[473] United Nations Manual on the prevention and control of computer-related crime. 2001 [interaktyvus, žiūrėta 2011-09-25]. < http://www.bcbkuwait.com/english/int_regulations/UN/CompCrims_UN_Guide.pdf>, p. 107.

- kritiniuose taškuose, tokiuose kaip išėjimas, pastatyti sargybinius;
- įrengti priėjimo prie kompiuterinių sistemų kontrolės sistemas, kuriose naudojamos korteles, skanuojami piršto antspaudai ar balso pavyzdžiai;
- įrengti standartinius įsilaužėlių signalizatorius;
- įrengti televizijos stebėjimo sistemą.

Programinė apsauga

Programinės įrangos apsauga skirta kompiuterinės sistemos saugumui užtikrinti programiniu lygmeniu. Ši apsauga apima:

- identifikavimo mechanizmus, nustatančius teisėtus vartotojus (pvz., naudojant slaptažodžius);
- hierarchijos nustatymą, t. y. užtikrinant, kad vartotojai neprieitų prie tų informacijos resursų, prie kurių jie neturi prieigos teisių;
- aptikimo priemones, kuriomis nustatomi saugumo pažeidimai programiniu lygiu;
- kitas priemones.

Siekiant apsaugoti perduodamą informaciją, paprastai taikomi įvairūs šifravimo metodai. Kriptografija grindžiami sprendimai yra kaip priemonė išvengti duomenų vagystės, elektroninių laiškų klastojimo. Kaip rodo praktika, šifravimas yra gana patikima apsaugos priemonė.

Visos apsaugos programos, užtikrinančios priėjimo prie kompiuterinės informacijos valdymą, veikia pagal atsakymo į klausimą principą: kas gali atlikti, kokias operacijas ir t. t.

Priėjimas gali būti nustatytas:

- bendras;
- priklausomas nuo įvykio;
- priklausomas nuo duomenų turinio;
- iš dalies priklausomas (pvz., vartotojui leidžiama prieiti vieną ar nustatytą skaičių kartų);
- pagal vartotojo vardą ar kitus požymius;
- susijęs su pareigomis;
- pagal leidimą (pvz., slaptažodį);
- pagal procedūrą.

Prie veiksmingiausių priemonių, nukreiptų prieš neteisėtą prieigą, priskiriamos registracijos priemonės. Šiam tikslui labiausiai tinka naujos

specialios paskirties operacinės sistemos, plačiai taikomos užsienio šalyse, kurios vadinamos „monitoringu" (automatinis galimos kompiuterinės grėsmės stebėjimas).

Monitoringą vykdo pati operacinė sistema, be to, į jos funkcijas patenka informacijos įvedimo ir pašalinimo, apdorojimo ir ištrynimo procesų kontroliavimas. Operacinė sistema fiksuoja neteisėtos prieigos laiką ir naudotas programines priemones. Be to, ji apie grėsmę tuojau pat informuoja kompiuterinio saugumo tarnybas, taip pat pateikia reikalingus duomenis.

Iš problemų, susijusių su programine apsauga, paminėtina ir apsauga nuo kompiuterinių virusų, todėl reikia aktyviai naudoti specialias antivirusines programas. Taip pat paminėtini elektroninio pašto filtrai, apsaugantys nuo kompiuterinių virusų. Tačiau vien tokių priemonių nepakanka, nes programinė įranga turi turėti informaciją apie kompiuterinius virusus dar prieš juos aptikdama[474]. Todėl veiksmingai apsaugai reikia naudoti ir kompleksines organizacines-technines priemones:

- informuoti visus įstaigos darbuotojus, naudojančius kompiuterinės technikos priemones, apie pavojų ir galimą žalą kompiuterinio virusu atveju;
- uždrausti atsinešti į darbą programines priemones iš šalies;
- uždrausti naudoti ir kompiuterio atmintyje saugoti kompiuterinius žaidimus;
- visi iš išorinio kompiuterinio tinklo patenkantys failai turi būti testuojami;
- daryti duomenų archyvą;
- nuolat tikrinti, kaip laikomasi nustatytų taisyklių, ir taikyti poveikio priemones asmenims, tyčia ar ne pirmą kartą pažeidusiems šias taisykles.

3. Kompleksinės priemonės

Kompleksinė apsauga – tai bendros sistemos, kuri galėtų atremti visas galimas atakas, nukreiptas prieš kompiuterinę sistemą – nuo durų išlaužimo ir aparatinės įrangos pavogimo iki informacijos vagystės, – sukūrimas. Į kompleksinę apsaugą integruojamos visos anksčiau minėtos apsaugos priemonės.

[474] Ghosh, S.; Turrini, E. 2010. *Cybercrimes: A Multidisciplinary Analysis*. Springer-Verlag, p. 111.

Paminėtina, kad taupymo tikslais verslas naudoja kuo pigesnes apsaugos nuo tapatybės vagystės elektroninėje erdvėje priemones ir tai identifikuotina kaip problema. Šią problemą iškėlė ir autorių apklausti ekspertai. Pavyzdžiui, 2-asis ekspertas patikslino, kad patikimesnės priemonės yra brangesnės ir mažina elektroninės erdvės patrauklumą. 9-asis ekspertas teigė, kad priemonių yra daug, bet taupymas, nežinojimas, rizikos nuvertinimas turi įtakos kompromisams, mažinantiems saugumą.

Labai svarbus ir švietimas. Pagal autorių atliktą verslo sektoriaus apklausą, verslo sektoriaus respondentai kaip vieną iš pagrindinių kovos su tapatybės vagyste elektroninėje erdvėje priemonių nurodo asmenų sąmoningumą ir švietimą. Taip pat autorių atliktas tyrimas rodo, kad elektroninio verslo paslaugas teikiančių įmonių darbuotojai negauna pakankamai viešosios informacijos apie tapatybės vagystę elektroninėje erdvėje ir jos pavojingumą.

Taip pat, vertinant, ar pakankamai respondentų įmonėje skiriama lėšų apsaugai nuo tapatybės vagystės elektroninėje erdvėje, dešimties balų skalėje daugiausia rinkosi 8 ir 5 balus, o vidurkis bubo 5,88 balo. Tai reiškia, kad verslo srityje taip pat reikėtų skirti daugiau lėšų apsaugai nuo tapatybės vagystės elektroninėje erdvėje.

Detalesnė informacija apie atliktus tyrimus pateikiama monografijos 5.2 dalyje.

„Raudonosios vėliavos" taisyklės

Autorių atliktos ekspertų apklausos duomenimis, pagrindiniu konkrečiu sektoriumi, kuriame reikėtų imtis prevencinių priemonių, laikomas finansų sektorius. Taip pat verslo atstovų tyrimas parodė, kad dažniausiai respondentai mano, jog tapatybės vagystės elektroninėje erdvėje pasekmės gali būti finansinės (detalesnė informacija apie tyrimo rezultatus pateikiama monografijos 5.2.6 dalyje). Todėl kaip prevencijos privačiame-finansiniame sektoriuje gerosios praktikos pavyzdį galima panagrinėti **JAV „Raudonosios vėliavos taisykles".** Literatūroje pabrėžiama šių taisyklių svarba, kadangi tai yra puikus netiesioginio federalinės vyriausybės elektroninės erdvės reguliavimo pavyzdys[475].

JAV Federalinės Prekybos komisijos (toliau – FPK) teigimu, JAV vartotojai dėl tapatybės vagysčių ir panašių nusikaltimų kasmet praranda

[475] Ghosh, S. ; Turrini, E. 2010. *Cybercrimes: A Multidisciplinary Analysis*. Springer-Verlag, p. 248.

maždaug 50 milijardų JAV dolerių[476]. 2007 metais FPK gavo daugiau kaip 813 tūkstančių vartotojų skundų dėl galimo sukčiavimo ir tapatybės vagystės, o tai savo ruožtu buvo 21 % daugiau, nei gauta 2006 metais. Tikėdamasi sumažinti tapatybės vagystės nusikaltimų nuostolius FPK inicijavo „*Red Flag* (Raudonos vėliavos)" programą. Ja buvo siekiama atnaujinti „Sąžiningų ir tikslių kredito operacijų įstatymo 2003 m." veikimo ribas.

Minėtos taisyklės taikomos „kreditoriams" ir „tęstiniams kreditoriams". Sąvoką „kreditorius" „Raudonos Vėliavos" taisyklės apibrėžia labai plačiai: kreditorius – tai bet kuris asmuo, kuris reguliariai pratęsia, atnaujina, ar teikia paslaugas. „Kreditas" reiškia teises, kurias suteikia kreditorius skolininkui. Daugelis paslaugų teikėjų siūlo klientams paslaugas su atidėto mokėjimo planais, kai už suteiktas paslaugas mokama vėliau. Paslaugų teikėjas apie asmenį renka visą reikiamą informaciją ir ją naudoja griežtai dalykiniams ir verslo ryšiams palaikyti. Sąvoka „tęstiniai kreditoriai" apibrėžiama kaip „tęstinis ryšys" su klientu, t. y. paslaugos teikiamos nuolatos. Pagal numatomus „Raudonosios vėliavos" reikalavimus, visoms organizacijoms, susijusioms su vartojimo kreditais, finansinės atskaitomybės operacijomis ir sandoriais, numatoma pareiga atlikti asmens tapatybės vagystės grėsmės analizę, įvertinti verslo riziką ir remiantis šiomis išvadomis parengti specialiąsias priemones, kuriomis būtų galima tinkamai nustatyti bei užkirsti kelią vartotojų duomenų vagystėms[477]. Taisyklės taip pat reikalauja, kad organizacijos tokias savo programas periodiškai atnaujintų. Buvo numatyta, kad šios taisyklės įsigalios 2008 m., tačiau daugelis organizacijų nustatytu terminu nebuvo pasiruošusios reikalaujamų programų. FPK sutiko sustabdyti „Raudonosios vėliavos" taisyklių įgyvendinimą iki 2009 m. gegužės mėnesio: iki šio termino pabaigos daugiau nei du milijonai organizacijų turėjo įdiegti tapatybės grėsmių požymių programas, kartu numatyti veiksmų planus įvykus tokiems incidentams.

„Raudonosios vėliavos" taisyklės taikomos finansinėms organizacijoms, bankams, kredito unijoms, automobilių prekybos tarpininkams, hipotekos įstaigoms, finansų makleriams, komunalinių paslaugų įmonėms, taip pat telekomunikacijų bendrovėms. Pagal minėtas taisykles, tokios bendrovės turi įgyvendinti savo parengtas rašytines programas,

[476] Swartz, N. 2009. Will Red Flags Detour ID Theft? *Information Management* 43(1): 38–41; 4.

[477] Winston & Strawn LLP. 2010. FTC Red Flags Rule Reminder to Financial Institutions and Creditors. Financial Services.

numatyti asmens identifikavimo, grėsmių aptikimo ir reagavimo į incidentus modelius, atitinkamus metodus ir konkretų veikimą – žinomą kaip „Raudonųjų vėliavėlių incidentai"[478]. Vadovaujantis „Raudonosios vėliavos" taisyklėmis ir gairėmis, kaip atskaitos taškus, būtina sudaryti tapatybės vagystės programą. Minėtose taisyklėse išskiriamos penkios pagrindinės „Raudonųjų vėliavų" rizikos kategorijos:[479]

1) įspėjimai, pranešimai iš kliento aptarnavimo centro;
2) įtartini dokumentai;
3) įtartina asmens identifikavimo informacija;
4) neįprastas sąskaitos naudojimas;
5) įspėjimai, pranešimai iš kliento, teisėsaugos organizacijų ar kitų asmenų.

3 lentelė. Kategorijos (*sudaryta remiantis: Christopher Wold*)

I – kategorija: įspėjimai, pranešimai iš kliento aptarnavimo centro
• Vartotojo sukčiavimas, perspėjimų ataskaitos. • Operacijų stabdymas, reaguojant į vartotojo prašymą. • Klientams ataskaitas teikiančios organizacijos pranešimas dėl adreso neatitikimo. • Neįprasta kreditinė veikla, didelis skaičiaus vykdomų operacijų.
II – kategorija: įtartini dokumentai
• Identifikavimo dokumentai pakeisti ar suklastoti. • Asmens nuotrauka tapatybės dokumente neatitinka kliento išvaizdos. • Asmens informacijos ir pateikiamos informacijos neatitikimas atsidarant sąskaitą. • Pateikiamos informacijos apie asmens tapatybę ir įstaigos turimos informacijos apie klientą neatitikimas. • Paraiškos forma suklastota, pakeista ar sunaikinta.
III – kategorija: įtartina asmens identifikavimo informacija
• Informacijos apie asmens tapatybę neatitikimas. • Socialinio draudimo, kurio nebuvo išduota, numeris arba asmuo miręs. • Informacija susijusi su žinomais sukčiavimo atvejais. • Įtartini adresai, telefono numeriai. • Tas pats adresas arba telefono numeris pateiktas daugelio klientų. • Sąskaitą atidarantis asmuo negali pateikti save identifikuojančios informacijos. • Informacija yra neišsami, asmeninė informacija neatitinka informacijos, kurią turi finansų organizacijos.

[478] Morrison & Foerster LLP. Identity Theft Red Flags Rule and Address Discrepancy Rule Frequently Asked Questions. Venulex Legal Summaries. 2008 Q3, Special section p1-6, 6 p.

[479] Wold, Ch. 2008. *A Practical Guide to the Red Flag Rules: Identifying and Addressing Indentity Theft Risks*. Practising Law Institute; 1st edition, p. 28.

IV – kategorija: neįprastas sąskaitos naudojimas
• Atidarantis sąskaitą asmuo negali paaiškinti sąskaitos naudojimo tikslų. • Po adreso pasikeitimo finansų įstaiga gauna prašymą pateikti papildomą sąskaitos informaciją. • Nepaaiškinami ir keisti mokėjimo būdai, naudojant turimus kreditus. • Ilgai buvęs neaktyvus, staiga pradeda neįprastą veiklą. • Laiškai, nusiųsti klientui, pakartotinai grąžinami kaip nepristatyti. • Kitų finansų įstaigų pranešimai dėl kliento įtartinų veiksmų.
V – kategorija: įspėjimai, pranešimai iš kliento, teisėsaugos organizacijų ar kitų asmenų
• Finansų įstaigos pranešimas apie neteisėtą lėšų nuskaitymą. • Finansų įstaiga pranešė, kad klientas užsiima asmens tapatybės duomenų vagystėmis ir dėl to atsidarė sąskaitą.

„Raudonos vėliavos“ programoje taip pat turi būti nurodytos priemonės, kurios užkirstų kelią ir sumažintų galimą nusikalstamumą, taip pat būtų išsamiai planuojamos ir nuolat atnaujinamos. Programa turi būti valdoma organizacijos direktorių valdybos arba viršesnių darbuotojų, įtraukiant darbuotojų mokymus ir numatytant visų paslaugų teikėjų priežiūrą.

„Raudonos vėliavos“ taisyklės numato griežtą finansinių organizacijų prieigą prie klientų tapatybių, skatina geriau apsaugoti svarbią klientų informaciją. Teigiama, kad taisyklės pastūmės finansų įstaigas labiau analizuoti vartotojų sandorius ir juos standartizuoti, reaguoti į įtartiną veiklą, kuri susijusi su klientų sąskaitomis[480]. Tačiau šis reguliavimas nepateikė gairių, kaip parengti tokią tapatybės vagystės prevencijos programą. „Raudonos vėliavos“ taisyklės tapo tiesiog našta organizacijoms, kurios ir taip jau buvo labai varžomos galiojančių teisės aktų.

Organizacijos, vadovaudamosi „Raudonos vėliavos“ programa, turi parengti ir įgyvendinti tapatybės vagysčių prevenciją, skirtą keliui nustatyti ir užkirsti bei tapatybės vagystėms, susijusioms su sąskaitų atidarymu ar naudojimu, mažinti. „Raudonos vėliavos“ gairėse nenurodoma pačios programos turinio. Yra pateiktas priedas – gairės, kurios padėtų organizacijoms kurti ir įgyvendinti programas. Taisyklės reikalauja, kad gairės būtų patvirtintos, tačiau organizacijos gali laisvai pritaikyti sau savo programas taip, kaip joms atrodo tinkama įprastinėje veikloje. Taisyklės suteikia organizacijoms daug lankstumo, todėl būtina, kad organizacijos

[480] Swartz, N. 2009. Will Red Flags Detour ID Theft? *Information Management*. 43(1): 38–41; 4 p.

parengtų ir įgyvendintų programą, adekvačią organizacijos dydžiui ir sudėtingumui bei apimančią jos veiklą. „Raudonosios vėliavos“ taisyklėse reikalaujama, kad tapatybės vagystės prevencijos programa apimtų „protingą politiką ir procedūras“[481].

Pirmasis žingsnis kuriant tapatybės vagysčių prevencijos programą, kaip reikalaujama pagal „Raudonosios vėliavos“ taisykles, yra nustatyti, su kokiomis rizikos rūšimis yra susijusi organizacija, ir kad ta rizikos rūšis atsispindėtų rengiamoje programoje. „Raudonosios vėliavos“ yra modeliai, metodai, konkreti veikla, kuri nurodo riziką ir grėsmę dėl galimos tapatybės vagystės. Organizacija turėtų išnagrinėti, kurios jos teikiamos paslaugos labiausiai veikiamos nustatytų rizikos rūšių. Taip pat organizacijos turėtų rimtai apsvarstyti kiekvieną galimą atvejį ir pasirengti reaguoti teisėtomis veikimo priemonėmis, kurios būtų išdėstytos jų parengtoje programoje. Organizacijos taip pat turėtų atsižvelgti į savo ankstesnę patirtį, susijusią su tapatybės vagyste[482]. Turėtų būti įgyvendintos procedūros, skirtos „Raudonoms vėliavoms“ nustatyti. Organizacijos privalo patikrinti asmenų tapatybes prieš padėdamos santykius. Norėdama sužinoti asmens tapatybę, organizacija turi naudotis patikrinimo procedūromis, nustatytomis klientų identifikavimo programos taisyklėse, kurios privalo būti taikomos. Sukurtos reagavimo procedūros turėtų būti proporcingos pavojaus laipsniui. Visa tai privalo būti nuolatos kontroliuojama, o esant būtinybei net susisiekiama su klientais: pvz., keičiant slaptažodžius ar pranešant apie teisių apribojimą, kai kuriose situacijose gali būti tikslinga nustatyti, kad iš kliento yra būtinas grįžtamasis ryšys. Be to, organizacijos šias programas turi periodiškai atnaujinti. Svarbu, kad organizacija, nuolat atnaujindama programas, parodytų rizikos rūšių pasikeitimus, įtrauktų naujus metodus kovai su tapatybės vagystėmis. Kiekviena organizacija turėtų žinoti, kad rizikos lygis gali keistis, kai ji keičia savo paslaugų spektrą[483].

Galima išskirti keturis pagrindinius „Raudonosios vėliavos“ programos elementus, kurie įpareigoja organizaciją:[484]

[481] Jones Day. 2008. Red Flag Rules Require Companies to Take Identity Theft Seriously. *Venulex Legal Summaries*. Q4, Special section p1-5, 5 p.

[482] *Ibid.*

[483] *Ibid.*

[484] Wold, Ch. 2008. *A Practical Guide to the Red Flag Rules: Identifying and Addressing Indentity Theft Risks*. Practising Law Institute. 1st edition. 5 p.

• nustatyti atitinkamas „Raudonas vėliavas“ siūlomoms paslaugoms ir įtraukti jas į savo programą. Pirmasis organizacijos žingsnis[485] – nustatyti atitinkamas „Raudonas vėliavas“ naujiems santykiams ir operacijoms. Vienas iš būdų tai padaryti – įvertinti kriterijus ir sąlygas, dėl kurių gali įvykti tapatybės vagystės, nustatyti tai, į ką organizacija turėtų atkreipti dėmesį, ir kokie požymiai tūrėtų rodyti, kad minėtas nusikaltimas įvyko ar gali įvykti. Procesai, kuriais organizacijos turėtų vadovautis nustatydamos „Raudonas vėliavas“:

- organizacija turi įvertinti naudojamų asmens duomenų tipą (sąskaitos, medicininių įrašų kortelės ir kt.);
- organizacija turi įvertinti visus metodus, kuriuos taiko rinkdama asmens duomenis ir pradėdama dalykinius santykius su klientu, taip pat sąskaitų išrašymo ir pateikimo tvarką (prieiga prie klientų registracijos duomenų, paciento medicininių įrašų);
- organizacija turėtų įvertinti ir taikyti turimą patirtį kovoje su minėtais tapatybės vagystės pažeidimais;
- organizacijoms gali būti naudinga netgi suburti tapatybės vagystės komitetą, kuris sukurtų tapatybės vagystės prevencijos politiką ir minėtas procedūras. Komitetas turėtų būti sudarytas iš organizacijos personalo, kurio funkcijos apima darbą su asmens duomenimis (organizacijų vadybininkai, registracijos ir atsiskaitymų personalas). Numatoma, kad tokia priežiūros veikla turėtų apimti:
  - atsakingų už programos įgyvendinimą subjektų nustatymą;
  - programos peržiūros ataskaitų formavimą;
  - esminių pasikeitimų programoje inicijavimą ir atlikimą. Be to, rekomenduojama, kad darbuotojai, atsakingi už programos administravimą, ataskaitą priežiūros institucijai turėtų teikti bent kartą per metus. Metinėje ataskaitoje turėtų atsispindėti organizacijos programos įgyvendinimas, veiksmingumas, susijęs su paslaugų teikimu.

• aptikti „Raudonas vėliavas“, kurios buvo įtrauktos į programą. Tai antras organizacijos žingsnis[486] – nustatyti „Raudonos vėliavos“ procedū-

[485] Smith, A. 2009. The Red Flag Rules: A Closer Look. *Health Care Registration: The Newsletter for Health Care Registration Professionals* 18(6): 1–11; 5 p.

[486] *Ibid.*

ras, susijusias su tęstine veikla, kurios metu tvarkomi nuolatinių klientų duomenys. Turi būti nustatyti veiksmai, kaip būtų galima greičiau aptikti pažeidimus, susijusius su galimais sąskaitų tvarkymo pažeidimais (pvz., trūksta arba pakeista tapatybės dokumento nuotrauka arba reikiamas dokumentas buvo pateiktas pavėluotai);

• tinkamai reaguoti į bet kurias „Raudonas vėliavas“, užkirsti kelią ir sumažinti tapatybės vagystės riziką. Tai trečias organizacijos žingsnis[487] – prevencijos priemonės; jei tikslinga, reikalauti iš klientų pateikti naują nuotrauką arba reguliariai atnaujinti informaciją apie jį, reikalauti informacijos apie adreso pasikeitimą. Žinoma, tai negali pažeisti įsipareigojimo teikti tinkamas paslaugas. Yra pateiktos rekomendacijos dėl tinkamų prevencinių priemonių:

- stebėti klientus, jų veiklą;
- kreiptis į klientą informuojant jį apie įtartiną veiklą;
- nuolatos reikalauti keisti slaptažodžius, saugumo kodus arba kitus identifikacinius duomenis;
- nuolatos atnaujinti paslaugų teikimo procedūras;
- nepradėti naujų verslo santykių, jeigu yra įtarimų dėl galimos tapatybės vagystės;
- nutraukti, laikinai sustabdyti nenaudojamas paslaugas;
- nekaupti perteklinės informacijos;
- informuoti teisėsaugos institucijas dėl galimo nusikaltimo.
- periodiškai atnaujinti programą ir jos „Raudonas vėliavas“, siekiant parodyti tapatybės vagystės pavojus vartotojams ir organizacijai. Tai ketvirtas organizacijos žingsnis[488] – nuolatinis programos atnaujinimas, kuris turėtų atspindėti bet kokią naują riziką, kylančią vartotojams. Atnaujinimas taip pat turėtų rodyti naujus metodus, taikomus atliekant tapatybės vagystes. Šie pokyčiai reikalingi siekiant apsisaugoti, išvengti ar sušvelninti galimus tapatybės vagystės padarinius.

Parengusios programą, organizacijos privalo užtikrinti tinkamą programos administravimą. Administruodamos programą, organizacijos turi atlikti šiuos veiksmus:

1) iš organizacijų vadovų, atitinkamų komitetų, valdybos gauti patvirtintą programą;

[487] *Ibid.*

[488] *Ibid.*.

2) įtraukti personalą į programos priežiūrą ir plėtrą, įgyvendinimą ir administravimą;
3) mokyti personalą įgyvendinti priimtą programą;
4) prižiūrėti paslaugų teikėjo priemones.

Federalinės Prekybos komisija sukūrė šabloną, kuris gali padėti organizacijoms parengti tinkamą „Raudonų vėliavų" programą[489].

Svarbu pažymėti, kad didžiausią susirūpinimą greičiausiai gali kelti tos sritys, kuriose yra aukšta tapatybės vagystės rizika. Anot FPK atstovo Franko Dormano, „bus peržiūrėti vartotojų tapatybės vagystės skundai, kurių skaičius neproporcingai didelis. Apgaulingų sąskaitų, kurios atidarytos tam tikrame sektoriuje skaičius labai didelis ir organizacijos privalo imtis priemonių tinkamai „Raudonų vėliavų" programai parengti, ypač sektoriuose, kur rizika yra aukšto lygio"[490]. Pažymėtina, kad tokios programos labai svarbios medicinos paslaugų kontekste, kur tvarkomi svarbūs asmenų duomenys gali būti panaudoti tapatybės vagystės nusikaltimams. Žala dėl medicinos duomenų vagystės gali būti didelė, o nuostoliai nekompensuojami"[491].

Lietuvoje panašaus norminio dokumento, kuriame būtų įtvirtintos tokios „Raudonos vėliavos" taisyklės, šiuo metu nėra, tačiau galioja griežtas pinigų plovimo prevencijos reguliavimas, kuris pagrindiniu finansų institucijų veiklos principu laiko principą – pažink savo klientą. Finansų įstaigose turi būti parengta vidaus tvarka, numatyta, kokios konkrečios funkcijos atliekamos tam tikroje finansų įstaigoje įgyvendinant prevencijos priemones. Finansų subjektai steigia atskirą padalinį, kuris įgyvendintų pinigų plovimo prevencijos priemones, palaikytų ryšius ir teiktų informaciją valstybės teisėsaugos institucijoms. Šių finansų institucijų darbuotojai turi būti tinkamai pasirengę ir supažindinti su pinigų plovimo ir teroristų finansavimo prevencijos priemonėmis. Finansų institucijos numato tikslus ir uždavinius, priima konkrečias rekomendacijas savo darbuotojams:

---

489 FTC FACT Act Red Flags Rule Template [interaktyvus, žiūrėta 2011-09-19]. <http://www.finra.org/web/idcplg?IdcService=GET_FILE&dDocName=p119095&RevisionSelectionMethod=LatestReleased&Rendition=primary&allowInterrupt=1>.

490 Klein Aguilar, M. 2011. Red Flags Rule Enforcement Goes Into Effect. *Compliance Week*, 888.519.9200 JANUARY

491 Smith, A. 2009. The Red Flag Rules: A Closer Look. *Health Care Registration: The Newsletter for Health Care Registration Professionals* 18(6): 1–11; 5 p.

1) administracijos darbuotojams rekomenduojama susipažinti ir supažindinti savo darbuotojus su teisės aktais, reglamentuojančiais pinigų plovimo prevencijos ir atsakomybės už pinigų plovimo prevencijos priemonių nevykdymą klausimus. Organizuoti banko darbuotojų mokymus (nuo banko vadovų iki darbuotojų, kurie tiesiogiai bendrauja su klientais);
2) banko darbuotojams rekomenduojama keistis informacija ir patirtimi su kitomis finansų įstaigomis, kurių veikla panaši;
3) sekti Lietuvos ir užsienio spaudos leidinius, kuriuose rašoma pinigų plovimo prevencijos klausimais. Susipažinti su Finansinių nusikaltimų tyrimo tarnybos parengtomis metodinėmis rekomendacijomis, skirtomis finansinėms įstaigoms, kitiems juridiniams asmenims ir įmonėms, neturinčioms juridinių asmenų teisių, ir pasinaudoti jose išdėstyta informacija[492].

Tokia vidaus tvarka nustato veiklos strategiją, kuria remiasi šios prevencijos priemonės:

1) finansų įstaigos analizuoja klientus, tikruosius kliento veiklos tikslus, dabartinius ir būsimus verslo partnerius ir jų buvimo vietą, įmonių akcininkus, planuojamas banko paslaugas ir numatomą jų apimtį, operacijas, fizinių asmenų pajamų šaltinius bei dydžius;
2) nustato nepriimtinus klientus atsižvelgiant į kliento gyvenamąją vietą, pateikiamą informaciją apie save, tikrųjų paslaugų gavėjų atskleidimą;
3) identifikuoja klientus ir saugo identifikavimo dokumentus, pvz., taiko specialią dvigubo identifikavimo tvarką klientams, kurie atidarė banko sąskaitas ne asmeniškai;
4) nustato asmenis, kurių naudai ir kurių interesais klientas iš tikrųjų veikia;
5) analizuoja klientų atliktas operacijas banke siekiant nustatyti neįprastus ar įtartinus sandorius;

[492] 2008 m. gegužės 15 d. Lietuvos Banko valdybos nutarimas Nr. 82 „Dėl kredito įstaigoms skirtų nurodymų, kuriais siekiama užkirsti kelią pinigų plovimui ir (ar) teroristų finansavimui“. *Valstybės žinios,* 2008, Nr. 62-2374.

6) skirsto klientus pagal rizikos grupes ir atidžiai stebi padidintos rizikos klientus, prašo jų pateikti papildomos informacijos bei nurodyti operacijos tikslą, tikrina operacijos pagrįstumą;
7) nustato operacijas, kurios yra neįprastos pagal Lietuvos Respublikos įstatymus;
8) praneša Kontrolės skyriui visus faktus, galinčius būti pinigų plovimo veiklos požymiu;
9) atsisako vykdyti įtartinas operacijas.

Pinigų plovimo prevencijos įstatyme nurodoma, kad finansų įstaigos gali vienašališkai nutraukti santykius su nepatikimais klientais, kurie vengia arba atsisako finansų įstaigai jos prašymu ir terminais pateikti informaciją apie piniginių lėšų ar turto kilmę[493]. Remiantis įstatymu, išskiriami supaprastinto ir sustiprinto kliento tapatybės nustatymo atvejai:

- supaprastintas tapatybės nustatymas taikomas, jei klientas yra kredito ar finansų įstaiga, bendrovė, kurios vertybiniais popieriais prekiaujama Europos Sąjungos valstybių narių ar trečiųjų šalių reguliuojamoje rinkoje, klientui, susijusiam su maža pinigų plovimo ar teroristų finansavimo grėsme bei kitais įstatyme nurodytais atvejais[494].
- sustiprintas kliento tapatybės nustatymo režimas taikomas, kai klientas fiziškai nedalyvauja nustatant tapatybę, esant tarptautinės korespondentinės bankininkystės santykiams su trečiųjų šalių gaunančiomis įstaigomis, kai verslo santykiai ar sandoriai vykdomi su politikoje dalyvaujančiais asmenimis arba kai egzistuoja didelė pinigų plovimo arba teroristų finansavimo grėsmė[495].

Minėtas įstatymas vienintelis taip detaliai ir griežtai reguliuoja tapatybės nustatymo klausimus finansų sektoriuje. Tačiau visi šie klausimai reguliuojami siekiant tinkamai įgyvendinti pinigų plovimo prevenciją, bet ne tapatybės vagystės, kuri savo ruožtu ne mažiau pavojinga finansų sektoriui, prevenciją.

[493] LR pinigų plovimo ir teroristų finansavimo prevencijos įstatymas. *Valstybės žinios*, 2008, Nr. 10-335, 15 str.
[494] *Ibid*., 10 str.
[495] *Ibid*., 11 str.

Lietuvoje nėra bendro dokumento, kuriame būtų įtvirtintos panašios taisyklės dėl tapatybės nustatymo, tapatybės vagystės prevencinių priemonių.

4.2.3. Tapatybės vagystės elektroninėje erdvėje prevencija neformalių socialinių junginių, darinių ir organizacijų lygmeniu

Neformalūs socialiniai junginiai, dariniai ir organizacijos gali būti įvairios, tad jų veikla vykdant tapatybės vagystės elektroninėje erdvėje prevenciją bus irgi labai įvairi. Jų veikla taip pat labai svarbi tapatybės vagystės elektroninėje erdvėje prevencijai. Šią svarbą pabrėžia ir Susan W. Brenner, akcentuodama civilinių žmonių įtraukimą į elektroninių nusikaltimų prevenciją[496]. Paminėtina, kad egzistuoja neformalios organizacijos, tiesiogiai susijusios su elektroninių nusikaltimų (tarp jų ir tapatybės vagystės elektroninėje erdvėje) prevencija. Viena iš tokių organizacijų yra „WiredSafety“[497], kuri yra ne pelno siekianti organizacija, įsikūrusi Vašingtone ir atstovaujanti vartotojams interneto saugumo klausimais[498]. Organizacija vienija savanorius, kurie stengiasi pagelbėti asmenims, susiduriantiems su pavojais elektroninėje erdvėje, tarp jų ir tapatybės vagystės elektroninėje erdvėje pavojumi.

Visgi aptariant neformalius socialinius junginius, darinius ir organizacijas elektroninėje erdvėje šioje monografijoje bus koncentruojamasi į virtualius socialinius tinklus. Tokie tinklai, kaip uždaros platformos, įgalina vartotojus pristatyti save, kurti ir jungtis į socialinius tinklus, tinkamai palaikyti ryšius tarpusavyje. Tokius virtualius tinklus galima apibrėžti kaip paslaugą Internete, kuri individams leidžia[499]:

- Socialiniame tinkle registruoti visiems prieinamą arba neviešą asmeninį profilį.
- Nustatyti asmenis, su kuriais palaikomas ryšys ir dalijamasi asmeninio profilio informacija.

[496] Brenner, S. W. *Cybercrime.* 2010.*Criminal Threats from Cyberspace*. Library of Congress Cataloging, p. 216.

[497] WiredSafety [interaktyvus, žiūrėta 2011-09-21]. <http://www.wiredsafety.org/>.

[498] Kshetri, N. 2010. *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives*. Springer-Verlag, p. 20

[499] Boyd, D. M.; Ellison, N. B. Social Network Sites: Definition, History, and Scholarship. [interaktyvus, žiūrėta 2011-09-21]. <http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html>.

- Peržiūrėti asmeninius ryšius su kitais asmenimis, juos naikinti ar apriboti.

Socialinių tinklų paskirtis vienyti tam tikrą bendrų interesų turinčią narių grupę, kuri ir kuria socialinio tinklalapio turinį, ir bendrauja tarpusavyje, automatizuotomis konkrečios socialinės svetainės internete priemonėmis[500]. Asmenys, kurdami ir plėtodami profilį socialiniame tinkle, atskleidžia daug asmeninės informacijos, kuri gali būti pasisavinta neteisėtai kitų asmenų ir panaudota nusikaltimams atlikti. Ankstesnėse šios monografijos dalyse buvo aptartos grėsmės, susijusios su netikrais ar pasisavintais profiliais socialiniuose tinkluose, tad šioje dalyje bus aprašomos tik konkrečių socialinių tinklų prevencinės priemonės kovoje su tapatybės vagystėmis ir asmens duomenų apsaugos pažeidimais. Autoriai pasirinko žinomiausius ir lankomiausius socialinius tinklus Lietuvoje – Facebook.com[501] ir one.lt[502].

Socialiniai tinklai elgesio taisykles apibrėžia sutartyse su vartotojais, kurios gali kisti priklausomai nuo vartotojų poreikių. Būtent savireguliacijos principas tampa pagrindine priemone apibrėžiant socialinių tinklų vartojimo taisykles, visos naujos taisyklės ir sąlygos pirmiausia būna aptariamos su vartotojais. Svarbią dalį šiuose rinkiniuose sudaro privatumo apsaugai skirtos taisyklės, kurios turi padėti vartotojui iki minimumo sumažinti asmeninių duomenų praradimą socialiniame tinkle. „Facebook“ siekia pasaulyje tapti atviru ir skaidriu socialiniu tinklu, tikisi sukurti didesnį tarpusavio supratimą ir ryšį. „Facebook“ skatina atvirumą ir skaidrumą suteikiant asmenims didesnę galią dalytis ir sujungti profilius. Šių principų siekimas turėtų būti apribotas tik teisės, technologijų ir kintančių socialinių normų. Kaip pagrindinės vertybės išskiriamos: laisvė dalytis ir prisijungti, informacijos nuosavybė ir kontrolė, laisvas informacijos srautas, lygybė, socialinė vertė, atvira platforma ir standartai, skaidrus procesas[503]. „Facebook“, be pagrindines sutarties su vartotojais, taip pat

[500] Social networking service [interaktyvus, žiūrėta 2011-09-21]. <http://en.wikipedia.org/wiki/Social_networking_service>.

[501] Registruota daugiau nei 750 milijonų vartotojų visame pasaulyje. Pusė iš jų naudojasi kiekvieną dieną.

[502] Registruota daugiau nei 700 tūkstančių vartotojų Lietuvoje. 260 tūkstančių iš jų naudojasi kiekvieną dieną.

[503] Facebook Principles [interaktyvus, žiūrėta 2011-09-21]. <http://www.facebook.com/principles.php>.

pateikia privatumo politiką, kurioje išdėstomos rekomendacijos vartotojams, kaip maksimaliai apsaugoti savo duomenis socialiniame tinkle. Toliau bus lyginami minėti du socialiniai tinklai, jų privatumo politikos nuostatos ir rekomendacines nuostatų dalis, kurių tikslas – duomenų saugumas ir prevencija.

4 lentelė. Privatumo politikos (*sudaryta autorių*)

„Facebook“ privatumo politika ir prevencija[505]	**„One.lt“ privatumo politika ir prevencija[506]**
Privatumo politikos pristatymas: • Galimybė užduoti klausimus pagalbos sistemoje ar paštu. • Priklausymas TRUSTe. Tai nepriklausoma ir ne pelno siekianti organizacija, kurios tikslas užtikrinti asmeninės informacijos privatumą internete. Ji sertifikuoja, stebi socialinių tinklų privatumo politiką, veiklą, sprendžia klientų nusiskundimus dėl privatumo pažeidimų. TRUSTe programos sudarytos pagal įvairių vyriausybinių institucijų ir pramonės sričių nustatytus reikalavimus ir rekomendacijas dėl asmeninės informacijos. • „Facebook“ vadovaujasi saugaus uosto duomenų apsaugos principu. • „Facebook“ privatumo taisyklėse nurodoma, kad asmenims iki 13 metų amžiaus negalima registruoti profilio, išaiškėjus tokiems atvėjams, „Facebook“ tokius profilius šalina automatiškai. • „Facebook“ rekomenduoja, kad nepilnamečiai vartotojai (13 metų ir vyresni) gautų tėvų sutikimą pateikti asmeninę informaciją socialiniame tinkle. Asmeninės informacijos pateikimas: • Rekomendacijos, kaip ir kokią informaciją pateikti apie save, reikalavimas pateikti tik tikrą informaciją, priešingu atveju vartotojo profilis bus panaikintas.	Nurodoma, kad vartotojai norėdami užtikrinti asmeninių duomenų saugumą, privalo vadovautis pateiktomis saugumo taisyklėmis. Taip pat perspėjama, kad jei vartotojai pateiktas rekomendacijas ignoruos, kitiems asmenims gali būti sudarytos sąlygos pasisavinti asmeninius duomenis. Taikomos šios rekomendacijos ir prevencinės priemonės: Rekomendacijos dėl slaptažodžių sudarymo, naudojimo, saugojimo. Rekomendacijos dėl telefono numerio nurodymo, jo pateikimo kitiems socialinio tinklo vartotojams. Rekomendacijos dėl tinkamo saugaus atsijungimo Privatumo apsaugos rekomendacijos • Rekomendacijos, kaip tinkamai pateikti informaciją apie save kitiems asmenims. Nurodoma, kokiu būdu „One.lt“ bendrauja su savo vartotojais, prevenciniais tikslais paaiškinta, į kokius pranešimus ir siūlymus nereikia reaguoti ir pranešti „One.lt“ administracijai. Moderatoriai • Tai tam tikras savireguliacijos būdas, kai socialinio tinklo vartotojai patys imasi priemonių nustatyti pažeidimus. Nurodoma, kad visi „One.lt“ vartotojai, vyresni nei 18 metų, gali tapti moderatoriais.

[504] Facebook's Privacy Policy [interaktyvus, žiūrėta 2011-09-21]. <http://www.facebook.com/policy.php>.

[505] Saugumo priemonės ONE.LT [interaktyvus, žiūrėta 2011-09-21]. <http://saugumas.one.lt/>.

Rekomendacijos dėl asmeninės informacijos dalijimosi su trečiosiomis šalimis: • Rekomendacijos, kaip tinkamai dalytis savo profilio informacija su kitais vartotojais, kaip maksimaliai sumažinti duomenų praradimo riziką. Kaip „Facebook“ naudoja vartotojų informaciją: • Pristatoma, kaip „Facebook“ naudoja vartotojų informaciją rinkodaros ir kitais įvardytais tikslais. Kaip „Facebook“ dalijasi vartotojų informacija: • Pristatoma, kaip „Facebook“ suteikia vartotojams galimybę rasti ir naudoti kitų asmenų informaciją. Kaip vartotojas gali pakeisti arba pašalinti asmeninę informaciją: • Rekomendacijos, kaip pašalinti informaciją, panaikinti ir ištrinti savo profilį. Kaip „Facebook“ apsaugo vartotojų informaciją: • „Facebook“ naudoja kriptografinius apsaugos protokolus ryšiui su vartotojais. Praneša atitinkamoms institucijos apie visus teisės pažeidimus socialiniame tinkle. Kitos „Facebook“ sąlygos: • Nurodoma, kad visos „Facebook“ privatumo politikos nuostatos bus keičiamos su socialinio tinklo vartotojų žinia.		Jie gali tikrinti naujai įkeliamų nuotraukų tinkamumą pagal atitinkamus kriterijus (ar tai tas pats žmogus, ar nuotraukos turinys neprieštarauja „One.lt“ sutarties nuostatoms). Rekomendacijos, kaip išvengti nepageidaujamo elektroninio pašto iš kitų „One.lt“ vartotojų • Kaip ir „Facebook“ socialinis tinklas, „One.lt“ nustatytas amžiaus cenzas. „One.lt“ vartotojų sutartyje[507] nurodoma, kad gali registruotis asmenys nuo 18 metų amžiaus, arba vyresni, kaip 14 metų, bet turėti tėvų sutikimą. Jaunesni asmenys neturi teisės lankytis „One.lt“ ir / ar naudotis esančia informacija (duomenimis). Tačiau mechanizmo ar procedūrų, kaip minėtas tėvų sutikimas turi būti pateikiamas, nėra numatyta. Nurodoma, kad tėvų pareiga užtikrinti savo vaikų apsaugą nuo informacijos, kuri gali būti nepageidaujama ar žalinga.

Kaip matyti iš privatumo taisyklių palyginimo, visos prevencinės priemonės skirtos vartotojų asmens duomenims apsaugoti, tačiau didesnė atsakomybė tinkamai juos saugoti tenka pačiam vartotojui. Nors ir nurodomas reikalavimas pateikti tik tikrus ir teisingus asmens duomenis, bet nėra pateikta jokio mechanizmo ar procedūrų, kaip socialiniai tinklai tai užtikrina („One.lt“ moderatoriai yra tik bandymas, tikintis, kad kiti asmenys atpažins netikrus vartotojus).

Būtent dėl netikrų duomenų pateikimo socialiniuose tinkluose ar profilių vagysčių vartotojai susiduria su kitu dalyku – reputacijos elektroninėje erdvėje problema. Netinkamai naudodami privatumo nustatymus sociali-

[506] „One.lt“ naudojimosi taisyklės. [interaktyvus, žiūrėta 2011-09-21]. <http://w27.one.lt/community/common/info/popup_Rules.jsp?language=lt>.

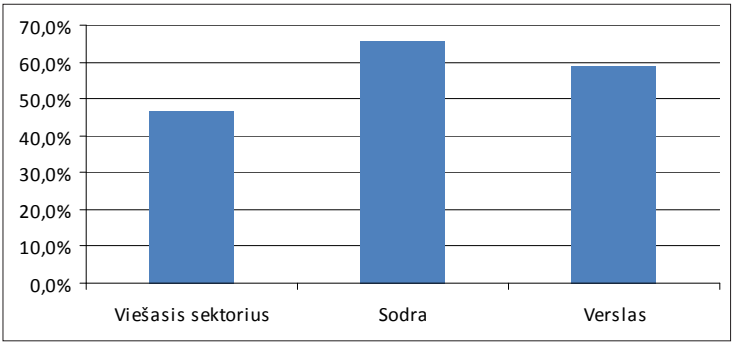
niame tinkle, asmenys rizikuoja, kad perteklinė asmeninė informacija bus pasiekiama plačiam ratui asmenų, neįtrauktų į jo artimų asmenų ratą. Tokiais asmenimis gali tapti darbdaviai, ieškantys socialiniuose tinkluose informacijos apie potencialų darbuotoją. Atskiros valstybės, suprasdamos šią problemą, teisiškai apribojo galimybę darbdaviams socialiniuose tinkluose ieškoti informacijos apie darbuotojus. Estijos duomenų apsaugos inspekcija uždraudė darbdaviams, priimantiems į darbą naujus žmones, tikrinti internete, taip pat socialiniuose tinkluose pareigas siekiančių užimti asmenų duomenis[507]. Panašių teisinių priemonių imamasi ir Vokietijoje[508]. Tačiau lieka neaišku, kaip tokius draudimus taikyti ir kontroliuoti.

Socialiniai tinklai susiduria su didėjančiomis grėsmėmis ir tinkamas vartotojų identifikavimas tampa prioritetine kryptimi. Šių tinklų vartotojai didžiąją dalį bendravimo būdų perkelia į elektroninę erdvę, todėl ypač svarbu garantuoti, kad tapatybės vagystės prevencinės priemonės tinkamai padėtų apsaugoti nuo netikrų ar suklastotų profilių naudojimo. Pirmieji valstybių mėginimai teisiškai sureguliuoti socialinių tinklų naudojimą jau yra (darbdavių galimybės ieškoti informacijos apie darbuotoją apribojimas), tačiau didėjantis tapatybės vagysčių skaičius socialiniuose tinkluose verčia susirūpinti, ar taikomos asmens duomenų apsaugos priemonės yra pakankamos, todėl prevencija turėtų būti plėtojama abiem kryptimis: ne tik vartotojui prisiimant atsakomybę pačiam rūpintis savo duomenų pateikimu ir saugumu, bet ir socialiniams tinklams dedant pastangas atidžiau peržvelgti asmens identifikavimo priemones (ankstesnėse monografijos dalyse minėta, kad dauguma didžiausių socialinių tinklų naudoja nevisiškai saugų „tai, ką vartotojas turi žinoti“ identifikavimo metodą) ir jas nuolatos tobulinti.

Dėl tapatybės vagystės elektroninėje erdvėje prevencijos organizacijų lygmeniu paminėtini autorių atliktų tyrimų apibendrinantys duomenys. Kiekybiniais metodais buvo ištirta, ar organizacija skiria lėšų pakankamai apsaugai nuo tapatybės vagystės elektroninėje erdvėje. Gauti tokie tyrimų rezultatai (atsakymai):

[507] Estijoje uždrausta internete tikrinti asmenų, ieškančių darbo, duomenis. *Delfi.lt* [interaktyvus]. 2011-01-30 [žiūrėta 2011-09-21]. <http://verslas.delfi.lt/law/estijoje-uzdrausta-internete-tikrinti-asmenu-ieskanciu-darbo-duomenis.d?id=41442117>.

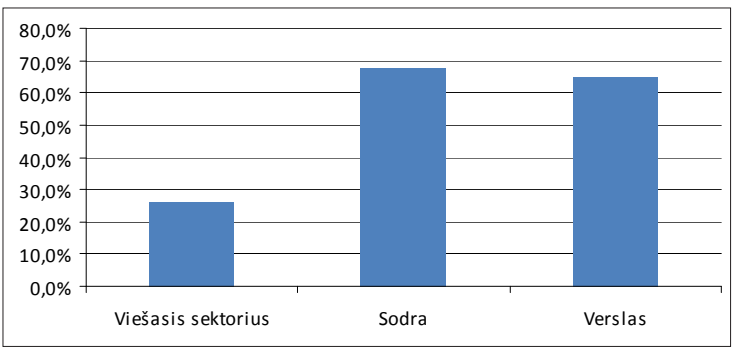
[508] Vokietijoje naujas įstatymas draus darbdaviams tikrinti „Facebook“ profilius. *Delfi.lt* [interaktyvus]. 2010-08-25 [žiūrėta 2011-09-21]. <http://gyvenimas.delfi.lt/career/article.php?id=35817883 >.



31 pav. Lėšų apsaugai nuo tapatybės vagystės elektroninėje erdvėje pakankamumas

Nors atsakymai santykinai panašūs, Sodros darbuotojai yra geriausios nuomonės apie jų organizacijos skiriamų lėšų pakankamumą apsaugai nuo tapatybės vagystės elektroninėje erdvėje, tačiau viešajame sektoriuje vyrauja nuomonė, kad apsaugai nuo tapatybės vagystės elektroninėje erdvėje lėšų skiriama nepakankamai. Todėl reikėtų svarstyti galimybę ypač šiame sektoriuje skirti daugiau lėšų apsaugai nuo tapatybės vagystės elektroninėje erdvėje.

Taip pat autoriai tyrė, ar pakankamai šiose organizacijoje imamasi priemonių kovai su tapatybės vagyste elektroninėje erdvėje ir jos prevencijai. Gauti (atsakymai) tokie rezultatai:



32 pav. Priemonių pakankamumas kovai su tapatybės vagyste elektroninėje erdvėje

Tyrimų rezultatai rodo, kad verslas ir Sodra panašiai, t. y. daug geriau vertina taikomų priemonių kovai su tapatybės vagyste elektroninėje erdvėje

ir jos prevencijai pakankamumą lyginant su viešuoju sektoriumi, kuriame šis rodiklis yra gana žemas. Todėl ypač viešajame sektoriuje reikėtų susirūpinti kovos su tapatybės vagyste elektroninėje erdvėje priemonėmis.

Detalesnė informacija apie autorių atliktų tyrimų rezultatus pateikiama monografijos 5. 2 dalyje.

Apibendrinančios išvados

• Tapatybės vagystės elektroninėje erdvėje prevencija organizacijų lygmeniu gali būti skirstoma į prevenciją viešajame ir privačiame sektoriuose bei neformalių socialinių junginių, darinių ir organizacijų lygmeniu.

• Vykdant tapatybės vagystės elektroninėje erdvėje prevenciją viešajame sektoriuje, į kurią įeina daug priemonių, labai svarbi organizacijos saugos politika, kuriai taikytini tam tikri reikalavimai. Viešajame sektoriuje turėtų būti skiriama daugiau lėšų ir imamasi daugiau priemonių apsaugai nuo tapatybės vagystės elektroninėje erdvėje. Šiam sektoriui taip pat turėtų būti pateikiama daugiau viešosios informacijos apie tapatybės vagystės pavojingumą ir apsisaugojimo būdus.

• Į tapatybės vagystės elektroninėje erdvėje prevenciją privačiame sektoriuje turi būti įtrauktos įvairios teisinės ir organizacinės techninės priemonės. Privatus sektorius taip pat turėtų skirti daugiau lėšų apsaugos priemonėms nuo tapatybės vagystės elektroninėje erdvėje plėtoti.

• Kaip prevencijos privačiame finansiniame sektoriuje gerosios praktikos pavyzdį galima panagrinėti JAV „Raudonosios vėliavos taisykles“. Literatūroje pabrėžiama šių taisyklių svarba, kadangi tai yra puikus netiesioginio JAV Federalinės Vyriausybės elektroninės erdvės reguliavimo pavyzdys. Lietuvoje kol kas tokia praktika netaikoma.

• Vertinant tapatybės vagystės elektroninėje erdvėje prevenciją neformalių socialinių junginių, darinių ir organizacijų lygmeniu, atkreiptinas dėmesys į socialinius tinklus. Didelę reikšmę turi socialinių tinklų privatumo politikos.

4.3. Tapatybės vagystės elektroninėje erdvėje prevencija valstybiniu lygmeniu

Viena iš pagrindinių prevencijos rūšių valstybės lygiu yra **teisinė prevencija**. Paminėtina, kad teisinės prevencijos svarbą pabrėžė 2-asis ir 8-asis

autorių apklausti ekspertai. Pasirinktos šios valstybės teisinio reguliavimo sritys, darančios įtaką tapatybės vagystės elektroninėje erdvėje prevencijai:

1) teisinė prevencija asmens duomenų teisinės apsaugos srityje, apibrėžta specialiuose teisės aktuose;
2) teisinė prevencija elektroninių duomenų saugos srityje;
3) teisinė prevencija asmens identifikavimo srityje.

Kiekviena iš šių teisinio reguliavimo sričių prevencijos aspektu bus aptariama detaliau.

Tapatybės vagystės elektroninėje erdvėje teisinė prevencija asmens duomenų apsaugos srityje

Asmens duomenų apsauga yra gana nauja teisės sritis, o pati asmens teisė į duomenų apsaugą, kaip savarankiška žmogaus teisė, susiformavo per pastaruosius tris dešimtmečius. Taigi, asmens duomenų apsaugos institutas skaičiuoja 30-uosius, o pats didžiausias iššūkis asmens duomenų apsaugai yra sparti elektroninių paslaugų plėtra ir interneto skvarba į visas žmogaus gyvenimo sritis.

Nuo 1981 m. priimtos Strasbūro konvencijos dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (toliau – Strasbūro konvencija) ir nuo 1995 m. spalio 24 d. priimtos Europos Parlamento ir Tarybos direktyvos Nr. 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo (toliau – Direktyva) sparčiai tobulėjo informacinės technologijos, plito internetas, didžiulė pažanga padaryta kasdienes paslaugas vis didesne apimtimi perkeliant į elektroninę erdvę, tačiau tobulėjant technologijoms, teisinis asmens duomenų apsaugos reguliavimas iš esmės nepasikeitė.

Asmens duomenų apsauga – vienas iš žmogaus teisės į privatų gyvenimą, įtvirtintos Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos 8 straipsnyje, aspektų. Lietuvoje asmens duomenų apsauga pradėta rūpintis jau 1992 m., priėmus Lietuvos Respublikos Konstituciją[509], tačiau realiai asmens duomenų teisinės apsaugos mechanizmas pradėjo veikti 1996 m. įsigaliojus Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymui, o 2001 m. sausio 1 d. įsigaliojus 2000 m. lie-

[509] Lietuvos Respublikos Konstitucija. *Valstybės Žinios*, 1992, Nr. 33-1014.

pos 17 d. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo pakeitimo įstatymui, buvo žengtas svarbus žingsnis derinant Lietuvos Respublikos teisę su Europos Sąjungos teise.

Monografijos 3.2.2 dalyje atlikta Lietuvos teisės aktų asmens duomenų teisinės apsaugos srityje analizė parodė, kad Lietuvoje asmens duomenų teisinis reguliavimas, kuris remiasi Europos Sąjungos teise, iš esmės yra pakankamas, išskyrus sankcijas už asmens duomenų teisinės apsaugos reikalavimų pažeidimus, kurios turėtų būti peržiūrėtos (t. y. sugriežtintos). Sparčiai tobulinamos technologijos ne tik palengvina ir supaprastina elektroninių paslaugų vartotojo santykius su kitais asmenimis, valdžios ir verslo institucijomis, bet ir kelia naujas grėsmes vienai iš pagrindinių Konstitucijoje įtvirtintų žmogaus teisių – teisei į privatumą, o kartu ir teisei į asmens duomenų apsaugą.

Strasbūro konvencijoje ir Direktyvoje yra įtvirtinti tik pagrindiniai asmens duomenų apsaugos principai, numatytas reguliavimas yra abstraktus ir įtvirtinantis technologiškai neutralią formą, todėl natūraliai kyla klausimas: ar pasikeitus technologijoms, neturėtų keistis ir teisinis reguliavimas?

2010 m. lapkričio 4 d. Europos Komisija (toliau – EK) paskelbė Komunikatą „Visapusiškas požiūris į asmens duomenų apsaugą Europos Sąjungoje“, (toliau – Komunikatas), skirtą Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų ir regionų komitetui. Komunikate teigiama, kad Direktyvoje 95/46/EB įtvirtinti principai pagrįsti, tačiau plėtojant technologijas ir vykstant globalizacijai pasaulis pasikeitė, o asmens duomenų apsaugos srityje kilo naujų uždavinių, todėl siūlomi esminiai Direktyvos 95/46/EB pakeitimai, susiję su naujųjų technologijų keliamomis problemomis, tarptautiniu duomenų perdavimu, institucinių priemonių stiprinimu, teisės sistemos suderinamumu, duomenų subjektų skaidrumu ir informuotumo didinimo veikla. Komunikate taip pat svarbus dėmesys skiriamas vaikų duomenų naudojimui ir neskelbtinų duomenų apsaugai stiprinti[510].

Pagrindiniai siūlomi pakeitimai:

1) Aiškiau ir konkrečiau reglamentuoti duomenų apsaugos principų taikymą naujoms technologijoms ir užtikrinti, kad asmenų duomenys būtų realiai saugomi, nepaisant, kokiomis technologijomis jie tvarkomi,

[510] Valstybinės duomenų apsaugos inspekcijos tinklapis [interaktyvus, žiūrėta 2011-09-21]. <http://www.ada.lt/index.php?lng=lt&action=page&id=20098>.

ir kad duomenų valdytojai būtų visapusiškai informuoti apie naujų technologijų poveikį duomenų apsaugai;

2) išspręsti su globalizacija susijusias problemas ir pagerinti tarptautinį duomenų perdavimą. Duomenų tvarkymo paslaugos vis dažniau užsakomos Europos Sąjungai nepriklausančiose šalyse, todėl kyla problemų dėl šiam procesui taikytinos teisės ir susijusios atsakomybės pasidalijimo, kadangi duomenų perdavimo sistemos turi būti supaprastintos, mažinama administracinė našta duomenų valdytojams;

3) sustiprinti institucines priemones, siekiant užtikrinti geresnį duomenų apsaugos taisyklių įgyvendinimą bei sustiprinti duomenų apsaugos institucijų įgaliojimus;

4) pagerinti duomenų apsaugos teisės sistemos suderinamumą. Europos Komisija turi pateikti nuoseklų požiūrį ir užtikrinti, kad asmenų teisės į duomenų apsaugą būtų visapusiškai laikomasi Europos Sąjungoje ir už jos ribų. Lisabonos sutartimi ES pripažįstama teisė į asmens duomenų apsaugą tapo teisiškai privaloma ir nustatytas naujas teisinis pagrindas, kuriuo sudarytos galimybės priimti nuoseklų Sąjungos teisės aktą dėl asmenų apsaugos tvarkant asmens duomenis ir laisvo duomenų judėjimo. Vadovaudamasi Lisabonos sutartimi Europos Sąjunga gali priimti bendras taisykles duomenų apsaugai reguliuoti policijos ir teisminio bendradarbiavimo baudžiamųjų bylų srityje. Užsienio ir saugumo politikos srities taisyklės turi būti nustatytos Tarybos sprendimu remiantis kitu teisiniu pagrindu;

5) didinti duomenų subjektų skaidrumą; būtina sąlyga, kad asmenys galėtų kontroliuoti savo duomenis, todėl svarbu, kad duomenų valdytojai aiškiai informuotų asmenis, kas ir kaip renka bei tvarko jų duomenis, kokiais tikslais ir kokiam laikotarpiui, taip pat kokios teisės, jei asmenys nori su duomenimis susipažinti, taisyti ar ištrinti, ypač jei šie duomenys buvo atsitiktinai ar neteisėtai sunaikinti, prarasti, pakeisti, su jais susipažino neįgalioti asmenys arba tie duomenys buvo jiems atskleisti;

6) ypač turi būti saugomi vaikai, nes jie gali nevisiškai suprasti su asmens duomenų tvarkymu susijusias grėsmes, padarinius, apsaugos priemones ir teises;

7) didinti duomenų subjektų galimybes kontroliuoti savo duomenis; siekiant užtikinti, kad asmenų duomenys būtų tinkamai saugomi, būtina įvykdyti šias sąlygas:

– duomenų valdytojai gali tvarkyti duomenis tik numatytais tikslais;

– duomenų subjektai turi veiksmingai kontroliuoti savo duomenis[511].

8) Komisija nagrinės, kaip aiškiau išdėstyti ir sugriežtinti sutikimu naudotis duomenimis taisykles, kad:

– būtų saugomi neskelbtini duomenys: dabar jau draudžiama tvarkyti ypatingus (neskelbtinus) duomenis, tačiau numatyta keletas išimčių[512].
– skatins standartų kūrimą ir taikymą;
– stiprins bendradarbiavimą su trečiosiomis šalimis ir tarptautinėmis organizacijomis, pvz., EBPO, Europos Taryba, Jungtinėmis Tautomis ir kt.

9) svarbus institucinių priemonių stiprinimas siekiant geriau įgyvendinti duomenų apsaugos taisykles, todėl atsižvelgiant į neseniai priimtą Europos Teisingumo Teismo sprendimą dėl jų nepriklausomumo suteikti būtinus įgaliojimus ir išteklius, kad institucijos galėtų tinkamai vykdyti užduotis nacionaliniu lygmeniu ir bendradarbiaudamos tarpusavyje. Taip pat būtina įtvirtinti duomenų apsaugos įgaliotinio statusą;

10) duomenų apsaugos institucijos turėtų glaudžiau bendradarbiauti ir geriau koordinuoti savo veiklą, svarbus vaidmuo gali tekti 29 str. Darbo grupei, kuriai jau priskirta užduotis pradėti vienodai taikyti Europos Sąjungos duomenų apsaugos taisykles nacionaliniu lygmeniu.

---

[511] Chartijos 8 str. 2 d. nustatyta, kad „kiekvienas turi teisę susipažinti su surinktais jo asmens duomenimis bei tai, kad jie būtų ištaisomi“. Ši teisė jau dabar įtvirtinta Direktyvoje 95/46/EB, bet tai ypač sudėtinga internete, nes duomenys dažnai išsaugomi nepranešus susijusiam asmeniui ir (arba) be jo sutikimo, todėl Komisija nagrinės, kaip sustiprinti duomenų kiekio mažinimo principą ir pagerinti galimybes faktiškai naudotis teisėmis susipažinti su duomenimis, juos ištaisyti, ištrinti ar sustabdyti jų tvarkymą (pvz., nustatyti atsakymų į asmenų prašymus terminą, leisti naudotis teisėmis elektroninėmis priemonėmis arba įtvirtinti principą, kad teisė susipažinti su duomenimis turėtų būti užtikrinama nemokamai).

[512] Atsižvelgiant į technologijų ir visuomenės raidą, būtina iš naujo apsvarstyti galiojančias neskelbtinų duomenų nuostatas, išnagrinėti, ar reikėtų įtraukti kitų duomenų kategorijų, ir aiškiau reglamentuoti jų tvarkymo sąlygas. Komisija svarstys, ar prie neskelbtinų duomenų reikėtų priskirti kitų kategorijų duomenis, pvz., genetinius; galimybes dar aiškiau reglamentuoti ir suderinti sąlygas, kurias įvykdžius leidžiama tvarkyti neskelbtinų duomenų kategorijų duomenis; perduoti duomenis į trečiąją šalį, kartais duomenų apsaugos priežiūros institucijai atliekant *ex post* priežiūrą, todėl Komisija nagrinės: teisėsaugos tikslais sudarytų Europos Sąjungos ir trečiųjų šalių susitarimų pagrindines duomenų apsaugos sudedamąsias dalis tam, kad nekiltų problemų dėl nevienodo duomenų apsaugos lygio vertinimo; galimybę įtvirtinti privalomas taisykles dėl duomenų perdavimo, pvz., duomenų valdytojams, priklausantiems tai pačiai įmonių grupei.

11) Komisija nagrinės, kaip stiprinti teisės sistemą, aiškiau išdėstyti ir suderinti nacionalinių duomenų apsaugos institucijų statusą ir įgaliojimus, įskaitant visapusišką visiško nepriklausomumo sąvokos įgyvendinimą; kaip pagerinti duomenų apsaugos institucijų bendradarbiavimą ir koordinavimą.

2011 m. sausio 18 d. Europos duomenų apsaugos priežiūros pareigūnas M. Peter Hustinx paskelbė Nuomonę dėl Komisijos komunikato, pažymėdamas, kad tai yra esminis naujos teisinės sistemos orientyras ir svarbiausias įvykis Europos Sąjungoje duomenų apsaugos srityje po 1995 m. spalio 24 d. Direktyvos 95/46/EB priėmimo prieš 16 metų.

Duomenų apsaugos priežiūros pareigūnas palankiai vertina Europos Komisijos ketinimus reformuoti teisinę sistemą, nes jo įsitikinimu, dabar galiojančios asmens duomenų apsaugą reglamentuojančių teisės aktų nuostatos nėra pakankamai veiksmingos šiuolaikinėje informacinėje visuomenėje. M. P. Hustinx pažymi, kad liekant galioti šalims narėms privalomiems 1981 m. sausio 28 d. Strasbūre sudarytoje Konvencijoje dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu įtvirtintiems bendriesiems privatumo ir asmens duomenų apsaugos principams informacinėje visuomenėje duomenų apsauga turi atitikti duomenų tvarkymo apimtis – kuo daugiau informacijos apie žmogų yra tvarkoma, tuo geresnė turi būti duomenų apsauga. Taip pat svarbu suteikti duomenų subjektui kuo daugiau teisių pačiam įgyvendinti teisę susipažinti su savo asmens duomenimis.

M. P. Hustinx pritaria pagrindiniams Komunikate nurodytiems klausimams ir iššūkiams, tačiau prašo ieškoti efektyvesnių sprendimų užtikrinant veiksmingesnę asmens duomenų apsaugos priežiūrą. Duomenų apsaugos priežiūros pareigūno nuomone, pagrindinį dėmesį reikia sutelkti galiojančio teisinio reguliavimo peržiūrai siekiant: stiprinti individo, atkreipiant ypatingą dėmesį į vaikų teisę į asmens duomenų apsaugą; didinti organizacijų duomenų valdytojų atsakomybę, skatinti juos laikytis duomenų proporcingumo principo, rūpintis privatumo apsauga nuo pat veiklos pradžios (angl. *privacy by design*); įtraukti asmens duomenų tvarkymo teisėsaugos institucijose klausimus į vieningą asmens duomenų apsaugos teisinio reglamentavimo sistemą; harmonizuoti asmens duomenų apsaugą reguliuojančius teisės aktus; užtikrinti technologiškai neutralų teisinį reguliavimą siekiant sukurti teisinį tikrumą ilgesniam laikui; suteikti daugiau

galių asmens duomenų apsaugos priežiūros institucijoms ir užtikrinti jų nepriklausomumą visose Europos Sąjungos šalyse narėse[513].

Teisinė prevencija, taikant specialiuosius teisės aktus

Išskiriant tapatybės vagystės elektroninėje erdvėje teisinę prevenciją specialiųjų teisės aktų aspektu, paminėtinos valstybės elektroninės informacijos saugos strategijos. Plačiau apie strategijas kaip teisinės prevencijos priemonę pateikta monografijos 3.2.3 dalyje.

Taip pat, paminėtina, kad Lietuvoje šiuo metu egzistuoja Lietuvos Respublikos Seimo 2003 m. kovo 20 d. nutarimu Nr. IX-1383 patvirtinta Nacionalinė nusikaltimų prevencijos ir kontrolės programa (toliau – Programa)[514], kuri parengta įgyvendinant Nacionalinio saugumo pagrindų įstatymo[515] 5 straipsnio nuostatas ir yra grindžiama Nacionalinio saugumo strategijos[516], patvirtintos Seimo 2002 m. gegužės 28 d. nutarimu Nr. IX-907, nuostatomis kaip specializuotas, nacionalinio saugumo užtikrinimą reglamentuojantis dokumentas.

Programos strateginis tikslas – sukurti naują nusikaltimų prevencijos ir kontrolės (principų, prioritetų, subjektų, organizavimo ir vadovavimo būdų) sistemos modelį, kurį panaudojus būtų sudarytos galimybės nuosekliai ir kompleksiškai šalinti esmines nusikalstamumo priežastis ir sąlygas, racionaliai naudoti finansinius bei žmogiškuosius išteklius ir padidinti nusikaltimų prevencijos bei kontrolės Lietuvoje veiksmingumą.

Pažymėtina, kad Programos VII skyriuje, įtvirtinančiame prioritetinių nusikaltimų prevencijos ir kontrolės krypčių sąrašą, nėra numatyta nusikaltimų elektroninėje erdvėje (taip pat ir tapatybės vagystės elektroninėje erdvėje) prevencijos ir kontrolės. Todėl reikėtų įvertinti tai, kad tiek elektroniniai nusikaltimai, tiek tapatybės vagystė elektroninėje erdvėje, kuri dažnai įvardijama kaip viena iš elektroninių nusikaltimų rūšių, gali sukelti pačių įvairiausių neigiamų pasekmių, pradedant nuo to, kad asmenys kurį

[513] Europos duomenų apsaugos pareigūnas išreiškė nuomonę dėl Komunikato apžvalgos. Valstybinės duomenų apsaugos inspekcijos tinklapis [interaktyvus]. 2011-01-24 [žiūrėta 2011-09-21]. <http://www.ada.lt/index.php?lng=lt&action=page&id=20120 >.

[514] Lietuvos Respublikos Seimo 2003 m. kovo 20 d. nutarimu Nr. IX-1383 patvirtinta Nacionalinė nusikaltimų prevencijos ir kontrolės programa. *Valstybės Žinios*, 2003, Nr. 32-1318.

[515] Nacionalinio saugumo pagrindų įstatymas. *Valstybės Žinios*, 1997, Nr. 2-16.

[516] Lietuvos Respublikos Seimo 2002 m. gegužės 28 d. nutarimu Nr. IX-907 patvirtinta Nacionalinio saugumo strategija. *Valstybės Žinios*, 2002, Nr. 56-2233.

laiką negali naudotis savo kompiuteriais, netikėtai internete susiduria su rasistinio ar pornografinio turinio informacija, tampa sukčiavimo aukomis ir patiria finansinių nuostolių, iki to, kad įmonės ar organizacijos vidinis tinklas tam tikrą laiką tampa nepasiekiamas ar sužinoma informacija, kuri yra komercinė paslaptimis. Dar daugiau – gali būti užblokuoti valstybės valdžios institucijų internetinių tinklalapių adresai arba internete paviešinta valstybės ir (ar) tarnybos paslaptį atskleidžianti informacija. Potenciali elektroninių nusikaltimų žala ir pasikėsinimo objektas lemia jų pavojingumą – nuo grėsmės privatumui ir asmens duomenų apsaugai iki pavojaus valstybės interesams ir nacionaliniam saugumui.

Pasikėsinus į elektroninius duomenis ir (ar) informacines sistemas, turinčius didelę strateginę reikšmę nacionaliniam saugumui, valstybės valdymui, ūkiui ar finansų sistemai, gali būti padaryta žala esminiams valstybės interesams – viešajam saugumui, valstybės valdymui, ekonominiams, finansiniams interesams ir kt. Tam tikrų valstybės informacinių infrastruktūrų nenutrūkstamą veiklą ir jų duomenų saugumą užtikrinti yra itin svarbu. Tokios infrastruktūros objektais laikytini energetikos sektorius, finansinės ir draudimo institucijos, telekomunikacijų operatoriai, sveikatos apsaugos institucijos, transporto sektorius, oro transporto kontrolė, karinės struktūros ir priemonės, valstybinės paslaugos, vandentiekio ir nuotekų šalinimo sistemos ir pan.[517].

Atsižvelgiant į tai, kad elektroniniai nusikaltimai (taip pat ir tapatybės vagystė elektroninėje erdvėje) yra labai pavojingi ir gali būti įvykdyti plačiu mastu, priklausomai nuo technologijų pažangos, siūlytina persvarstyti Programą ir į prioritetinių nusikaltimų prevencijos ir kontrolės krypčių sąrašą įtraukti elektroninių nusikaltimų (taip pat ir tapatybės vagystės elektroninėje erdvėje) prevenciją ir kontrolę.

Nagrinėjant teisinę tapatybės vagystės elektroninėje erdvėje prevenciją, reikia prisiminti ankstesnėje dalyje atliktą tapatybės vagystės elektroninėje erdvėje teisinio reguliavimo JAV ir Lietuvoje lyginamąją analizę: JAV, skirtingai nei Lietuvoje, tapatybės vagystė elektroninėje erdvėje yra kriminalizuota ir už ją numatyta griežta baudžiamoji atsakomybė, be to, JAV papildomai egzistuoja specialūs teisės aktai, nustatantys atsakomybę už tapatybės vagystę elektroninėje erdvėje. Toks

[517] *LR Baudžiamojo kodekso komentaras*, II dalis. 2009, p. 425.

JAV teisinis reguliavimas vertintinas kaip veiksminga kovos su tokio pobūdžio veikomis priemonė. Tuo tarpu Lietuvoje nėra specialių teisės aktų, reglamentuojančių tapatybės vagystę elektroninėje erdvėje, o Lietuvos Respublikos baudžiamojo kodekso normų sisteminė analizė rodo, kad tapatybės vagystės elektroninėje erdvėje vertinimas iš baudžiamosios teisės pozicijų yra pakankamai sudėtingas, todėl Lietuvos Respublikos baudžiamajame kodekse būtų tikslinga įtvirtinti tapatybės vagystės elektroninėje erdvėje kaip savarankiškos nusikalstamos veikos sudėtį – tai leistų panaikinti tapatybės vagystės elektroninėje erdvėje teisinio reguliavimo spragas, palengvintų minėtos veikos įrodinėjimą ir kvalifikavimą, be to, siekiant patraukti asmenį baudžiamojon atsakomybėn už tapatybės vagystę elektroninėje erdvėje padėtų išvengti gana sudėtingo nusikalstamų veikų daugeto įrodinėjimo.

Nepaisant to, kad tapatybės vagystė elektroninėje erdvėje JAV yra kriminalizuota, pati asmens duomenų apsaugos teisinė sistema JAV labai skiriasi nuo Lietuvos: JAV požiūris į asmens duomenų apsaugą remiasi sektoriniu reguliavimu ir savireguliacija, o Lietuvoje – visapusišku teisiniu reguliavimu. JAV nėra vieno bendro pagrindinio asmens duomenų apsaugą reglamentuojančio įstatymo, o duomenų tvarkymo atžvilgiu vadovaujamasi saugaus uosto sistema ir taikomi kitokie apsaugos standartai, kurie daugeliu požiūrių yra žemesnio lygio nei Lietuvoje. JAV, priešingai nei Lietuvoje, yra pakankamai silpnai reglamentuota asmens duomenų apsauga, ribotas įstatymų, reglamentuojančių asmens duomenų apsaugą, taikymas ir problemiškas jų įgyvendinimas, ir nepaisant to, kad, Europos Sąjungos nuomone, JAV užtikrina tinkamą asmens duomenų apsaugą, visos paminėtos problemos sudaro prielaidas įvykdyti tapatybės vagystę elektroninėje erdvėje ir už šią veiką išvengti atsakomybės. Tačiau reikėtų atkreipti dėmesį į sankcijas, taikomas už asmens duomenų apsaugos pažeidimus, kurios JAV yra keletą kartų didesnės nei Lietuvoje ir turėtų labiau atgrasinti potencialius pažeidėjus nuo galimų pažeidimų.

Taip pat, autorių nuomone, viena iš prevencijos, taikant specialiuosius teisės aktus prevencijos priemonių galėtų būti privalomas informavimas apie tapatybės vagystę elektroninėje erdvėje. Tai galėtų būti privalomo informavimo finansų srityje analoginė tvarka, kai tokio pobūdžio pranešimai apie įtartinas operacijas su pinigais yra stabdomi ir visa in-

formacija persiunčiama valstybės kompetentingoms institucijos[518], kuri galėtų būti pritaikyta ir tapatybės vagystės atveju. Apie tapatybės vagystę turėtų būti privalomai informuojama, atsižvelgiant į tam tikros žalos dydį arba grėsmės dydį. Lietuvoje įvykus tapatybės vagystės nusikaltimui finansų srityje, finansų įstaigos dažniausiai apie tokį nusikaltimą nepraneša dėl galimų grėsmių dalykinei reputacijai. Lietuvos baudžiamajame kodekse[519] numatyta atsakomybė dėl nepranešimo apie nusikaltimą, tačiau tik apie tokį, už kurį numatyta didesnė negu dešimt metų laisvės atėmimo bausmė. Reikėtų keisti nusistovėjusią praktiką ir finansų įstaigos privalėtų pranešti apie pastebėtus tapatybės vagystės atvejus, tokiu būdu būtų šalinamas veikos latentiškumas, didinamas finansų įstaigų veiklos skaidrumas.

Tapatybės vagystės elektroninėje erdvėje teisinė prevencija elektroninės informacijos saugos srityje

Kaip viena iš priemonių, paminėtinos teisės normos dėl privalomo informavimo apie elektroninės informacijos saugumo pažeidimus[520]. Tokios teisės normos jau įtvirtintos ir Lietuvos Respublikos elektroninių ryšių įstatyme. Šio įstatymo 62 straipsnio 4 dalyje nurodoma, kad *Asmens duomenų saugumo pažeidimo[521] atveju viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjas nedelsdamas privalo pranešti apie šį pažeidimą Valstybinei duomenų apsaugos inspekcijai. Tuo atveju, jeigu asmens duomenų saugumo pažeidimas gali turėti neigiamą poveikį abonento ar registruoto elektroninių ryšių paslaugų naudotojo arba kito asmens duomenų ar privatumo saugumui, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjas taip pat privalo apie tai pranešti abonentui ar registruotam elektroninių ryšių paslaugų naudotojui arba kitam asmeniui,*

[518] Pinigų plovimo prevencija Lietuvoje įgyvendinama vadovaujantis pagrindiniu įstatymu. Lietuvos Respublikos pinigų plovimo ir teroristų finansavimo prevencijos įstatymas Nr. X-1419. *Valstybės žinios,* 2008, Nr. 10-335.

[519] LR baudžiamasis kodeksas. Nr. VIII-1968, *Valstybės žinios*, 2000, Nr. 89-2741.

[520] Rannenberg, K.; Royer, D.; Deuker, A. 2009. *The Future of Identity in the Information Society*. Springer-Verlag, p. 328.

[521] Asmens duomenų saugumo pažeidimas Lietuvos Respublikos elektroninkiių ryšių įstatyme apibrėžiamas kaip *pažeidimas, dėl kurio atsitiktinai arba neteisėtai sunaikinami, prarandami, pakeičiami, be asmens sutikimo atskleidžiami asmens duomenys arba sudaroma galimybė naudotis tais duomenimis, kai jie buvo perduodami, saugomi arba kitaip tvarkomi teikiant viešąsias elektroninių ryšių paslaugas*.

išskyrus atvejus, kai viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjas Valstybinei duomenų apsaugos inspekcijai įrodo, kad įgyvendino tinkamas technines priemones, kurios buvo taikomos saugumo pažeidimo paveiktiems asmens duomenims. Šios priemonės turi užtikrinti, kad tam neįgalioti asmenys negalėtų susipažinti su asmens duomenimis[522]. Autoriai nori atkreipti dėmesį, kad toks teisinis reguliavimas taikomas tik elektroninių ryšių paslaugų teikėjų atžvilgiu. Jis gerokai susiaurina subjektų, kuriems taikomas atitinkamas teisinis reguliavimas, ratą. Manytina, kad tokia pareiga turėtų būti nustatyta ir informacinės visuomenės paslaugų teikėjams, kaip subjektams, veikiantiems elektroninėje erdvėje. Todėl minėtas reguliavimas, galbūt ir ne šiame teisės akte, bet turėtų būti praplėstas.

Nepaisant tokio sektorinio teisinio reguliavimo, atsižvelgiant į 3.2.3 dalyje išdėstytas išvadas dėl elektroninės informacijos saugos teisinio reguliavimo, susijusio su tapatybės vagyste elektroninėje erdvėje, Lietuvoje pageidautina, kad būtų taikomos aiškesnės ir sistemingesnės holistinio teisinio reguliavimo priemonės elektroninės informacijos saugos srityje. Pirmosios tokios reguliavimo iniciatyvos galėtų būti elektroninės informacijos saugos strategijos.

Valstybės elektroninės informacijos saugos strategija priskirtina informacijos saugos politikos dokumentams ir gali būti kaip vienas iš pagrindinių elektroninės informacijos saugos reguliavimo teisinių dokumentų: strategijoje ne tik įvardijamos pagrindinės elektroninės informacijos saugos problemos, bet ir numatomos svarbiausios elektroninės informacijos saugos užtikrinimo kryptys ir būdai.

Strategijos dažniausiai būna įtvirtinamos valstybių nacionaliniuose teisės aktuose ir turi tiesioginę įtaką kuriant naujus bei tobulinant jau priimtus elektroninės informacijos saugą reglamentuojančius teisės aktus. Remiantis strategijomis atskirose valstybėse įgyvendinama bendroji elektroninės informacijos saugos reguliavimo politika, kuri tampa vis svarbesnė šiuolaikinės informacinės visuomenės kontekste.

Elektroninės informacijos saugos reguliavimo srityje pažangiausiomis Europos valstybėmis galima laikyti Suomiją, Norvegiją, Čekiją. Jos visos turi patvirtintas elektroninės informacijos saugos valstybines

[522] Lietuvos Respublikos elektroninių ryšių įstatymas. *Valstybės žinios*, 2004, Nr. 69-2382, 62 str. 4 d.

strategijas, užtikrinančias elektroninės informacijos saugos reguliavimo tęstinumą. Šiose strategijose perimta Europos Sąjungos, Ekonominio bendradarbiavimo ir plėtros organizacijos (toliau – EBPO) ir kita informacijos saugos reguliavimo patirtis. Minėtų valstybių strategijos nacionaliniu lygiu įtvirtina pagrindinius tolesnės informacinių sistemų plėtros principus, numatytus 2002 m. EBPO Informacinių sistemų ir tinklų saugumo gairėse[523]; numato, kad būtina nacionaliniu lygiu kompleksiškai reguliuoti elektroninės informacijos saugos procesus; reguliavimo apimtis – visa nacionalinė elektroninės informacijos infrastruktūra, apimanti tiek privataus, tiek ir viešojo (taip pat ir valstybinio) sektorių elektroninę informaciją; išskirti du elektroninės informacijos saugos institucinės sistemos lygiai: elektroninės informacijos saugos politikos formavimo lygis ir elektroninės informacijos saugos kontrolės lygis; aiškiai įvardijamos institucijų kompetencijos informacijos saugos srityje ribos; daug dėmesio skiriama informacijos saugos informacinėse sistemose politikai bei kontrolei koordinuoti; privatus ir valstybinis sektoriai skatinami visapusiškai bendradarbiauti diegiant tam tikras elektroninės informacijos saugos reguliavimo priemones.

Paminėtina, kad valstybės institucijų sektoriuje tokia strategija kurį laiką egzistavo. Tai – Elektroninės informacijos saugos valstybės institucijų informacinėse sistemose valstybinė strategija iki 2008 metų[524]. Elektroninės informacijos saugos valstybės institucijų informacinėse sistemose valstybinė strategija iki 2008 metų, kaip jau minėta monografijos 3.2.3 dalyje, nustatė pagrindinius elektroninės informacijos saugos užtikrinimo principus, tikslus, uždavinius ir jų įgyvendinimą.

Strategija buvo skirta išimtinai valstybės institucijų sektoriui ir dėl to kritikuotina, nes informacijos saugumas negali būti veiksmingai užtikrinamas reguliuojant tik valstybės institucijų sektorių ir paliekant nuošalyje privatų sektorių, kadangi informacijos saugumą turi užtikrinti visos informacijos saugumo procese dalyvaujančios šalys. Pagrindiniai strategijos tikslai: tobulinti elektroninės informacijos saugos koordinavi-

[523] OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security [interaktyvus]. 2002 [žiūrėta 2011-05-30]. <http://www.oecd.org/dataoecd/16/22/15582260.pdf>.

[524] Elektroninės informacijos saugos valstybės institucijų informacinėse sistemose valstybinė strategija iki 2008 metų. *Valstybės žinios*, 2006, Nr. 70-2575.

mą ir priežiūrą; teisės aktais reguliuoti elektroninės informacijos saugą; kelti elektroninės informacijos saugos kultūrą; tobulinti elektroninės informacijos perdavimo infrastruktūros saugą; skatinti elektroninės informacijos saugos užtikrinimo projektų įgyvendinimą. Tačiau strategijoje nenumatyta svarbių elektroninės informacijos saugos užtikrinimo būdų ir priemonių, kurias galima aptikti šiuolaikinėse užsienio valstybių elektroninės informacijos saugos strategijose; nuostatos gana deklaratyvios, abstrakčios ir nekonkrečios; nėra išspręstas ryšio su kitais teisės aktais klausimas; priemonės pateikiamos atskirai patvirtintame strategijos įgyvendinimo priemonių plane, šių priemonių nekonkretinant; tam tikrais aspektais strategija neformuoja darnios elektroninės informacijos saugos politikos; reguliavimo sritis neapima valstybės ir žinybiniuose registruose tvarkomos elektroninės informacijos, apimančios didelę dalį valstybinio sektoriaus infrastruktūros.

Deja, po 2008 metų šios strategijos nepakeitė joks kitas strateginis dokumentas elektroninės informacijos saugos srityje, tad iš principo šiuo metu Lietuvoje nėra galiojančios elektroninės informacijos saugos valstybės informacinėse sistemose strategijos. Be to, Lietuvoje nėra priimta bendros elektroninės informacijos saugos strategijos, kuri apimtų ir privatų sektorių. Tokios strategijos buvimas leistų numatyti pagrindinius elektroninės informacijos saugos strateginius tikslus, uždavinius ir konkrečias įgyvendinimo priemones. Tokia strategija taip pat padėtų numatyti pagrindines elektroninės informacijos saugos teisinio reguliavimo kryptis ir priemones, formuoti aiškią valstybės viziją dėl šios labai svarbios srities teisinio reguliavimo.

Kadangi Lietuvoje šiuo metu nėra elektroninės informacijos saugos valstybinės strategijos, Lietuvos Respublikos Vyriausybė turėtų apsvarstyti tokio dokumento priėmimo galimybę, įvertindama jo svarbą informacijos saugos politikos srityje. Strategijoje neturėtų būti ankstesnėje strategijoje kritiškai vertintų aspektų, be to, ji turėtų būti skirta ne tik viešajam sektoriui, tačiau ir privačiam. Paminėtina, kad 2011 m. Lietuvos Respublikos Vyriausybės patvirtinta Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programa turi gana siaurą tikslą (plėtoti elektroninės informacijos saugą Lietuvoje, užtikrinti kibernetinį saugumą ir pasiekti, kad 2019 metais teisės aktų nustatytus elektroninės informacijos saugos (kibernetinio sau-

gumo) reikalavimus atitinkančių valstybės informacinių išteklių dalis pasiektų 98 procentus visų valstybės informacinių išteklių, vidutinis ypatingos svarbos informacinės infrastruktūros incidentų likvidavimo laikas sumažėtų iki 0,5 valandos, o Lietuvos gyventojų, kurie saugiai jaučiasi kibernetinėje erdvėje, dalis pasiektų 60 procentų[525]) ir negali atstoti elektroninės informacijos saugos strategijos, kuriai keltini visai kitokie tikslai.

Taip pat, išskyrus strategiją, keltinas klausimas dėl pamatinių teisės normų elektroninių duomenų saugos srityje. Diskutuotina, ar Lietuvai reikėtų elektroninių duomenų saugos klausimus reglamentuoti bendru holistiniu Elektroninių duomenų saugos įstatymu. Toks holistinis teisinis elektroninių duomenų saugos reguliavimas galėjo atsirasti prieš keletą metų, kai tarptinstituciniu lygiu buvo svarstomas Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugos įstatymo projektas. Šis projektas buvo parengtas vadovaujantis Lietuvos Respublikos Vyriausybės patvirtinta Elektroninių ryšių tinklų ir informacijos saugumo įstatymo koncepcija[526]. Deja, įstatymo projektas, įvykus daugeliui projekto rengimo darbo grupės svarstymų, taip ir nebuvo pateiktas Vyriausybei, ir, aišku, nebuvo registruotas Lietuvos Respublikos Seime.

Nors šiuo įstatymu buvo ketinta reglamentuoti tik elektroninės informacijos saugos klausimus elektroninių ryšių srityje, tačiau nepaisant to, tai galėjo būti kaip gera pamatinių teisės normų praktika reglamentuojant atitinkamus teisinius santykius elektroninės informacijos saugos srityje. Be abejo, tokia praktika, kai vienu holistiniu įstatymu reglamentuojama elektroninės informacijos sauga, nėra plačiai paplitusi pasaulyje. Pavyzdžiui, Suomijoje, tarp valstybės institucijų darbuotojų vyrauja nuomonė, kad vienu įstatymu labai sunku reglamentuoti visas elektroninės informacijos saugos sritis dėl jų skirtingumo. Pavyzdžiui, elektroninės informacijos sauga medicinos ir elektroniniuose ryšių srityse yra skirtinga. Tačiau tokia nuomonė kritikuotina. Įstatymu nebūtina detaliai sureguliuoti skirtingų sričių. Manytina, kad tokio holistinio įstatymo tikslas galėtų būti sąvokų elektroninės informacijos saugos srityje nustatymas, už elektroninės informacijos

[525] Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programa. *Valstybės žinios,* 2011, Nr. 83-4033; 3 punktas.

[526] Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymo koncepcija. *Valstybės* žinios, 2006, Nr. 134-5081.

saugą atsakingų institucijų funkcijų atskyrimas, pagrindinių elektroninės informacijos saugos kategorijų reglamentavimas ir kt.

Todėl autoriai siūlo svarstyti bendro holistinio įstatymo elektroninės informacijos saugos srityje priėmimo galimybę. Prieš tai turėtų būti apsvarstyta ir parengta atitinkamo įstatymo koncepcija.

Tapatybės vagystės elektroninėje erdvėje teisinė prevencija identifikavimo srityje

Kaip minėta ankstesniuose skyriuose, klientų tapatybė elektroninėje erdvėje nustatoma remiantis skirtingais metodais. Rekomenduotina reglamentuoti, kad nustatant tapatybę elektroninėje erdvėje, būtų remiamasi daugiau nei vienu asmens tapatybę nusakančiu rodikliu, kuris būtų saugesnis ir sunkiau pažeidžiamas. Dažniausiai šia rekomendacija naudojasi elektroninių atsiskaitymų sistemų kūrėjai, nes jiems būtina derinti saugumą, paprastumą ir patikimumą.

Vienas iš pagrindinių identifikacijos metodų, kurie dažniausiai taikomi elektroninėje erdvėje, yra informacija, kurią asmuo žino. Šį metodą taiko dauguma elektroninių paslaugų teikėjų. Be populiariausių PIN kodų, slaptažodžių, taip pat turi būti užduodami klausimai, reikalaujantys tikslaus atsakymo, kurį iš anksto suderina paslaugų teikėjas ir vartotojas. Kitas dažnas metodas – saugos paveikslėliai, kuriuos reikia atpažinti iš pateiktų daugybės kitų: vartotojas, matydamas savo parinktą paveikslėlį, yra užtikrintas, kad pateko ne pas falsifikuotą paslaugų teikėją. Slaptažodžius, PIN kodus, saugos klausimus, saugos paveikslėlius vartotojas gali rinktis pats, o sistemos kūrėjai gali numatyti, kad tokie saugumo elementai kas tam tikrą laiką būtų keičiami.

Kitas pažangesnis ir saugesnis metodas – tai, ką vartotojas turi. Tai gali būti tam tikros laikmenos, kurias būtina turėti, norint naudotis paslaugomis.

Tradiciškai visas identifikavimo priemones, kurios priskiriamos prie metodo tai, ką vartotojas turi, galima suskirstyti taip:

- mikroprocesorinės (*SmartCard*) kortelės;
- kodų generatoriai;
- kodų kortelės;
- USB kriptografiniai raktai;
- elektroninis parašas.

Mikroprocesorinės kortelės Europos Sąjungos šalyse turi standartizuotą EMV[527] [528] lustą, kuris užtikrina saugumą ir tinkamą identifikavimą. Kad būtų galima naudotis mikroprocesorine kortele, būtinas specialus skaitytuvas, kuriuo nuskaitoma kortelė, įvedami PIN kodai ir identifikuojamas vartotojas. Tokias korteles turime su savimi, jas paprasta ir saugu naudoti (EMV lustas eliminavo galimybę sukčiauti kortelei nesant, panaikino magnetinio takelio nesankcionuotą nuskaitymą, praktiškai padarė neįmanomą kortelės kopijavimą).

Kita svarbi technologija, kuri tik padidino saugumą ir atitolino tapatybės vagystės galimybę – EMUE technologija.[529] EMUE – tai VISA standarto kortelės, su įdiegta generuojamo vienkartinio kodo sistema bei integruotu ekranu, 12 mygtukų pagalbine klaviatūra. Tai visiškai nauja vartotojo tapatybės nustatymo galimybė, kurią VISA siūlo bankams. EMUE kortelėse yra baterija (veikimo garantija trejiems metams), elektroninio rašalo technologija paremtas ekranas. Kortelės su generuojamo vienkartinio kodo sistema – yra vartotojams siūlomas saugus būdas pirkti internetu, jungtis prie elektroninės bankininkystės paslaugų. Vartotojui nebūtina registruotis, kurti prisijungimo vardus, slaptažodžius, jam tereikia įrašyti PIN kodą pačia kortelės klaviatūra; kortelės generuojamas vienkartinio kodo algoritmas sukuria unikalų kodą, naudojamą konkrečiam atsiskaitymui ar atskiroms mokėjimo operacijoms. Kaip minėta, tokios kortelės mažina sukčiavimo galimybę ir eliminuoja sukčiavimą kortelės nesant. Kiekvienai konkrečiai operacijai atlikti generuojamas vienkartinis kodas, kurio nebus galima dar

[527] EMV – standartas, kuris apibrėžia bendrus reikalavimus, kuriuos turi atitikti įvairių gamintojų gaminama kreditinių ir debetinių kortelių bei mokėjimo terminalų programinė įranga. Šis standartas nurodo lustinės mokėjimo kortelės ir ją aptarnaujančio įrenginio keitimosi informacija eigą ir taisykles. Nuo 2011 sausio 1d. Remiantis mokėjimo sistemos SEPA reikalavimais, visos kortelinės operacijos atliekamos vedant PIN kodą. Taip pat visos Lietuvoje leidžiamos mokėjimų kortelės turi standartizuotą EMV lustą. EMV [interaktyvus, žiūrėta 2011-09-21]. <http://www.emvco.com/>.

[528] Nuo 2011 sausio 1d. Remiantis mokėjimo sistemos SEPA reikalavimais, visos kortelinės operacijos atliekamos vedant PIN kodą. Taip pat visos Lietuvoje leidžiamos mokėjimų kortelės turi standartizuotą EMV lustą.

[529] EMUE – finansinių paslaugų ir tinklo prieigos priemonių kūrėja, kompanija, kuri yra rinkos lyderė. Ji kuria novatoriškus autentiškumo patvirtinimo sprendimus. EMUE pagrindinis produktas - EMUE paprasto kortelės ir kreditinės kortelės su integruotą klaviatūra, ekranu ir mikroprocesoriumi. Šios kortelės naudojamos saugiai identifikuoti klientus elektroninėje erdvėje. EMUE [interaktyvus, žiūrėta 2011-09-21] <http://www.emue.com/site/home.htm>.

kartą panaudoti. Norint pasinaudoti tokia kortele, reikia ją pačią turėti ir žinoti kortelės savininko PIN kodą, o tai iki minimumo sumažina galimybę, kad vartotojas liks nepastebėjęs kortelės dingimo. Visas operacijos patvirtinimo procesas atliekamas tokia seka:

Pirmas žingsnis	**Antras žingsnis**	**Trečias žingsnis**
Naudojant kortelę atsiskaitymams internetu, jungiantis prie internetinės bankininkystės, pirmiausia inicijuojamas tapatybės nustatymas, spaudžiant atitinkamus mygtukus kortelės klaviatūroje.	Įrašomas mokėjimo kortelės PIN kodas, naudojant kortelės klaviatūrą.	Kortelės ekrane atsiranda unikalus vienkartinis kodas, kurį kortelės savininkas naudoja operacijai autorizuoti.

Kita technologija, padedanti išvengti sukčiavimo galimybių atsiskaitymo sistemose, yra bekontaktės mokėjimo priemonės. Kitaip, nei atsiskaitant įprastomis lustinėmis kortelėmis, bekontaktėms kortelėms nereikia vienalaikio fizinio kontakto su skaitytuvu, taip pat nereikia įrašyti ir PIN kodo, tokia kortelė tik priartinama prie atsiskaitymo įrenginio ir atsiskaitymo procesas radijo bangomis įvykdomas greičiau nei per sekundę, kortelei su nuskaitymo centru apsikeičiant visa reikalinga informacija. Tai mažos vertės mokėjimų priemonės ir jos labiausiai tinka kasdieniams smulkiems atsiskaitymams. Tokiose kortelėse taip pat naudojamas EMV standarto mikroprocesorinis lustas. Grynieji pinigai atsiskaitant vis dar dominuoja, nors vartotojai linkę vis dažniau naudoti mokėjimo korteles, minėtos bekontaktės atsiskaitymo priemonės skirtos smulkiems atsiskaitymams, užuot naudojus grynuosius pinigus. Tokie bekontakčiai mokėjimai greitesni, daug patogesni, saugesni (praradus kortelę nuostoliai minimalūs, nes yra nustatytos ribinės sumos). Jei mokama didesnė suma nei nustatytas limitas, kortelė naudojama kontaktiniu veikimo principu, įrašant PIN kodą. Pasaulyje populiariausios ir labiausiai paplitusios bekontaktės sistemos: *Visa PayWave*[530], *MasterCard PayPass*[531]. Tokios mo-

[530] Visa PayWave. [interaktyvus, žiūrėta 2011-09-21] <http://usa.visa.com/personal/cards/paywave/index.html>.

[531] Mastercard Paypass® [interaktyvus, žiūrėta 2011-09-21] <http://www.mastercard.us/paypass.html >.

kėjimo kortelės sparčiai skinasi kelią pasaulyje ir tampa populiaria atsiskaitymo priemone JAV ir Europoje.

Kitas populiarus elementas – kodų generatorius. Nedidelis įrenginys, generuojantis unikalų vienkartinį slaptažodį. Įrenginys garantuoja, kad tas pats slaptažodis būtų naudojamas tik vieną kartą. Vartotojas, identifikuodamas save, įrašo vardą, nuolatinį slaptažodį ir kodų generatoriaus sugeneruotą slaptažodį. Tapatybė patvirtinama, kai nuolatinis slaptažodis ir kodų generatoriaus sugeneruotas slaptažodis atitinka serveryje esančią informaciją. Generatorių naujas vienkartinis kodas yra generuojamas kas tam tikrą laiko tarpą. Tai saugus metodas, nes tikimybė naudoti jau sugeneruotą kodą atkrenta, o generatoriaus nebuvimas iš karto pastebimas, be to, jis negali būti naudojamas be slaptažodžio.

Pigesnis ir taip pat paprastesnis elementas yra kodų kortelė. Kodų kortelėje pateikiami iš skaičių ar raidžių sudaryti slaptažodžiai. Tokios kortelės naudojamas kartu su nuolatiniais tapatybės nustatymo duomenimis, vartotojo vardu ir slaptažodžiu, tik vietoje generatoriaus generuojamos reikšmės šiuo atveju kodas imamas iš kortelės įrašų. Tokiu būdu patvirtinama tapatybė ir prisijungiama prie norimos sistemos. Reikia pabrėžti, kad tai populiariausia elektroninės bankininkystės identifikavimo priemonė Lietuvoje, tačiau toli gražu ne saugiausia, nes žmonės per neapdairumą dažnai praranda dalį ar net visus kortelės kodus. Ateityje tokių sistemų neliks, atsižvelgiant į tai, kad pigesni tapo kodų generatoriai ir rinkoje vis populiaresnė tampa minėta EMUE technologija.

USB kriptografiniai raktai yra nedideli, patogūs, prijungiami prie kompiuterio, dažniausiai nereikalaujantys papildomos programinės įrangos įdiegimo. Tokios sistemos naudojamos siekiant sukurti saugų ryšio kanalą: į kurį, prijungtą prie kompiuterio ir atpažintą, įrašomas žinomas slaptažodis, patvirtinama tapatybė ir sistema identifikuoja vartotoją bei jo turimą kriptografinę laikmeną. Tokioms laikmenoms negali būti lengvai pritaikomi reversinės inžinerijos metodai, todėl dažniausiai jose saugomi elektroniniai parašai, jų sertifikatai, kurie suteikia galimybę identifikuoti vartotojus.

Viena iš sudėtingiausių ir brangiausių identifikavimo technologijų – biometrinis tapatybės nustatymas. Ji grindžiama asmens fiziologinėmis savybėmis: pirštų antspaudais, akies rainele, veido atvaizdu, balsu ir

kt. Vartotojo biometriniai duomenys konvertuojami į skaitmeninę formą ir taikant algoritmus gautas rezultatas registruojamas duomenų bazėje. Nuskaityti biometriniai vartotojo duomenys sulyginami su duomenų bazėje įregistruotais ir jei duomenų atitikmuo sutampa, vartotojo tapatybė patvirtinama.

Saugiausia, kai biometrinės technologijos naudojamos kartu su slaptažodžiais, elektroniniais parašais, taip panaikinant galimybę panaudoti asmens biometrinius duomenis prieš jo valią.

Galima paminėti, kad sparčiausiai plinta piršto atspaudų biometrinė technologija, grindžiama piršto linijų struktūros analize. Kadangi tai yra unikalūs fiziologiniai požymiai, todėl šis tapatybės nustatymo būdas labai patikimas, nes kiekvieno žmogus piršto atspaudai yra unikalūs. Tikrųjų pirštų antspaudų atvaizdų nesaugoma, saugomi tiktai matematiniai duomenys, gauti specialiais algoritmais apdorojus atspaudus ir jų struktūrą. Kaip vieną iš galimų trūkumų galima išskirti mobilumo stoką. Atpažinimo įrenginiai būtini kiekvienoje darbo vietoje, bet tai nėra priežastis, kuri turėtų slopinti plėtrą, nes minėtos technologijos kainos ir sąnaudos tampa vis mažesnės lyginant su akies rainelės nuskaitymu.

Kitas populiarus tapatybės patvirtinimo metodas – IP adresų sekimas. Priklausomai nuo to, ar naudojami statiniai, ar dinaminiai IP adresai, kompiuteris gauna interneto protokolo adresą, kurį jam priskiria interneto paslaugų teikėjas. Jei visi vartotojai naudotų statinius IP adresus, jiems būtų priskiriamas vienas unikalus IP numeris, kuriuos būtų galima saugoti oficialiame registre, o nustatant tapatybę reikėtų patikrinti, koks klientas turi atitinkamą IP. Tačiau Lietuvoje naudojami ir statiniai, ir dinaminiai IP adresai, kurie nėra susiejami su konkretaus vartotojo tapatybe, o tik su konkrečiu kompiuteriu ir interneto tiekimo paslauga. Kuriamos sistemos, kurios atpažįsta vietovę, iš kurios jungiasi vartotojas, ir jei ta vietovė nesutampa su vartotojo nurodyta vietove, sistemos blokuoja tokį jungimą, užkirsdamos kelią neteisėtam prisijungimui.

Kitas paplitęs būdas nustatyti tapatybę elektroninėje erdvėje – tapatybės nustatymas per patikimą trečiąją šalį, pasinaudojant mokėjimų kortelėmis. Mokėjimų kortelių didžiausi privalumai tie, kad jos veikia ne tik elektroninėje, bet ir fizinėje erdvėje. Vienintelė problema – negali-

ma tiksliai patvirtinti, kad kortele naudojasi jos savininkas. Atsiskaitant kortele elektroninėje erdvėje užtenka įrašyti kortelės numerį ir specialų triženklį kodą, kuris taip pat pateikiamas ant pačios kortelės, o tai leidžia net neturint kortelės atlikti mokėjimą, patvirtinus tapatybę įrašytais duomenimis, kaip tai darytų kortelės savininkas. Reikalaujama pateikti detalią informaciją, kuri pateikta ant pačios kortelės, tokią kaip kortelės galiojimo laikas, kortelės numeris, kortelės savininko vardas, pavardė. Taip pat prašoma pateikti informaciją, kurią žino tik savininkas: adresą, kuriuo registruota kortelė, ar vartotojas. Elektroninių mokėjimų sistemose kortelių naudojimas dažnai skirstomas:

- mokėjimai naudojant kortelių duomenis: paslaugų teikėjas kortelės duomenis gauna ir saugo pas save;
- mokėjimai naudojant užšifruotus kortelių duomenis: naudojama šifravimo technika, suvesti kortelės duomenys į sistemą koduojami taip, kad neįmanoma iššifruoti kitoms šalims. Šifruotus duomenis atpažįsta tik kortelės bankas emitentas, kuris patvirtina mokėjimą;
- mokėjimai pagrįsti trečiųjų šalių patvirtinimu: tai galima pavadinti aukščiausio lygio patikimumu. Kai naudojamasi kortele, paslaugų tiekėjas nesaugo kortelės duomenų savo sistemoje, o nukreipia juos į trečiosios šalies mokėjimo paslaugų tiekėjus. Tokiu būdu nereikia diegti savo serverių, trečiųjų šalių duomenų saugojimas užtikrinamas aukštesniu duomenų apsaugos lygiu.

Toks atsiskaitymo mechanizmas garantuoja vartotojui anonimiškumą paslaugų teikėjo atžvilgiu. Paslaugų teikėjas neturi galimybės matyti kortelės duomenų ir identifikuoti vartotoją, kadangi tapatybę patvirtina bankas trečiajai šaliai. Taip pat garantuojamas mokėtojo anonimiškumas banko atžvilgiu, bankas gauna informaciją apie finansinius rodiklius, bet nemato perkamos prekės ar paslaugos.

Tačiau visi minėti būdai pritaikyti atsiskaitymų būdams, nors ne ką mažiau svarbios sritys yra ir elektroninis paštas, socialiniai tinklai ir kitos paslaugos. Elektroninio pašto sistemos neretai tampa sukčių taikiniu, kurie turi tikslą gauti prieigas prie vartotojų pašto paskirų. Tai dažnai daroma siekiant išplatinti kuo daugiau nepageidaujamo turinio elektroninio pašto žinučių ar platinti kenkėjišką programinę įrangą. Vienas didžiausių elektroninio pašto paslaugų tiekėjų – *Google Gmail* – parengė naujovišką

tapatybės nustatymo būdą jungiantis prie pašto paskyros[532]. Vartotojai savo paskyrą pasiekia įvesdami vartotojo vardą ir slaptažodį bei kintamą raktą, kurį jie gauna į savo telefoną įdiegę būtiną *Google* programinę įrangą. Taigi, net praradę jungimosi duomenis, vartotojai lieka saugūs, nes turi telefoną, be kurio prisijungimas nebus įmanomas. Žinoma, tokios technologijos nemažai kainuoja, bet pamirštama, kad asmens susirašinėjimo slaptumas yra garantuojamas Konstitucijos, tad ir priemonės tokio susirašinėjimo apsaugai turėtų būti adekvačios saugomai teisei.

Lietuvoje veikiantys elektroninių paslaugų tiekėjai neskuba imti pavyzdžio iš valstybės institucijų teikiamų elektroninių paslaugų ir taikomų identifikavimo būdų, tikriausiai motyvuodami didele kaina ir sudėtingumu. Nors elektroninių parašų infrastruktūra Lietuvoje formuojasi sklandžiai, naujo pavyzdžio tapatybės kortelės su elektroniniais sertifikatais nėra plačiai naudojamos elektroninei identifikacijai verslo sektoriuje, taip pat kaip ir kitos e. parašų teikėjų technologijos. Tiesa, mobilusis parašas plačiai taikomas bankininkystės sektoriuje. Iš visų Lietuvoje veikiančių bankų, tik AB „ŪKIO BANKAS“ savo elektroninės bankininkystės sistemoje yra pritaikęs naudoti tiek tapatybės kortelėse saugomus elektroninius sertifikatus, tiek „Registrų centro“ išduodamuose USB raktuose saugomus elektroninius sertifikatus. Finansų sektoriui būtinos tokios priemonės, kurios tiksliai identifikuoja vartotojus, tačiau ir kitų pasaugų tiekėjai negali likti nuošalyje, šios priemonės tampa vis labiau prieinamos, vartotojai ateityje dažniau naudos elektroninius sertifikatus, kuriuos gaus su naujais tapatybės dokumentais, todėl nereikėtų eliminuoti galimybės plačiau taikyti šias priemones privačiame sektoriuje, kuriame taikomas tapatybės nustatymas per patikimą trečią šalį. Dalis paslaugų tiekėjų, norėdami patvirtinti pirmą kartą besijungiantį asmenį, naudoja bankus, kaip tapatybės garantus, įpareigodami vartotoją pervesti minimalią sumą paslaugų tiekėjui. Gavęs pavedimą, paslaugų teikėjas įsitikina, kad duomenys atitinka tikrą asmenį (bankas nurodo vardą, pavardę ir kt. duomenis). Taip galima bent minimaliai įsitikinti, ar kuriama nauja paskyra atitinka tikrąjį asmenį, o ir išlaidų prasme tai kainuoja minimaliai. Prie tokių pavyzdžių

[532] Pradedama naudoti patvirtinimą dviem veiksmais. Google žinynas [interaktyvus, žiūrėta 2011-09-21] <http://www.google.com/support/accounts/bin/static.py?hl=lt&page=guide.cs&guide=1056283&rd=1>.

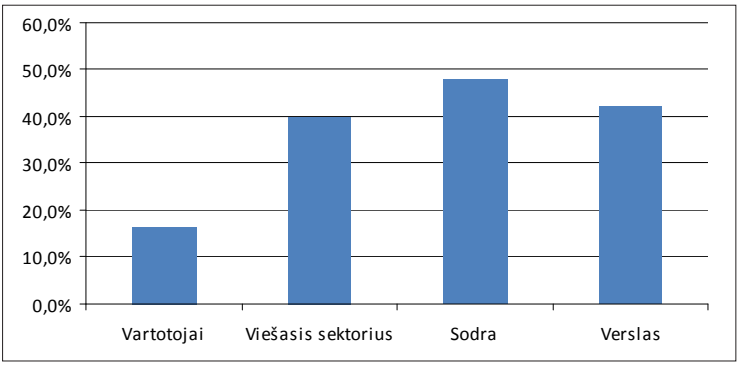
galima priskirti Kauno technologijos universiteto Informacinių technologijų plėtros institutą[533], kuris teikdamas .LT domenų registravimo paslaugas, asmenų tapatybę nustato remdamasis patikima šalimi – banku. Socialinių tinklų kūrėjai taip pat susiduria su tapatybės nustatymo būtinumu, todėl jiems taip pat būtų naudinga taikyti panašias tapatybės nustatymo procedūras. Ateityje jie susidurs su didėjančiu nepasitenkinimu dėl neteisėto atvaizdo naudojimo, fiktyvių, garbę ir orumą žeminančių anketų, o nustatyti pažeidėjus nebus lengva. Tinkama identifikacija padėtų sureguliuoti šias spragas, ir paslaugų teikėjai negalėtų naudotis privilegija teikti savo paslaugas elektroninėje erdvėje be jokios atsakomybės, kai už analogiškų paslaugų teikimą fizinėje erdvėje yra numatyta atsakomybė (nepilnamečių vaikų atvaizdų įdėjimas be tėvų sutikimo ir t. t).

Paminėtina, kad, be teisinės prevencijos valstybės lygmeniu, galimos ir kitos prevencijos priemonės. Vienos iš svarbesnių priemonių – prevencijos priemonės, skirtos viešajai informacijai apie tapatybės vagystę elektroninėje erdvėje platinti:

- vieši renginiai / akcijos tapatybės vagystės tema ir kitos visuomenės švietimo iniciatyvos;
- internetiniai tinklalapiai, kuriuose būtų viešinama pagrindinė informacija apie informacijos saugą ir kovos su elektroninėje erdvėje kylančiomis grėsmėmis, įskaitant tapatybės vagystę, pateikiami patarimai, kaip išvengti privatumo ir informacijos saugumo pažeidimų.
- lankstinukai;
- straipsniai spaudoje.

Paminėtina, kad pagal autorių atliktus kiekybinius tyrimus, viešosios informacijos apie tapatybės vagystę labiausiai stinga paprastiems vartotojams. Atitinkamoms respondentų grupėms buvo užduotas klausimas dėl viešosios informacijos apie tapatybės vagystę elektroninėje erdvėje pakankamumo. Gauti tokie rezultatai:

[533] .LT domeno procedūrinis reglamentas. VII skirsnis, Apmokėjimas. [interaktyvus, žiūrėta 2011-09-21]. <http://www.domreg.lt/static/doc/public/procedural_regulation-lt.pdf>.



33 pav. Viešosios informacijos apie tapatybės vagystę elektroninėje erdvėje pakankamumas

Taigi, vartotojai labiausiai pasigenda viešosios informacijos apie tapatybės vagystę elektroninėje erdvėje, kitos šiuo klausimu apklaustos respondentų grupės viešosios informacijos pakankamumą vertina žemiau negu vidutiniškai. Todėl ypatingai vartotojų kategorijai turėtų būti skiriamas didžiausias dėmesys platinant viešąją informaciją apie tapatybės vagystę elektroninėje erdvėje.

Viešosios informacijos apie tapatybės vagystę elektroninėje erdvėje mažėjimą rodo ir autorių atliktas elektroninės žiniasklaidos priemonių tyrimas. Šis tyrimas parodė, kad tokių publikacijų e. žiniasklaidos priemonėse mažėja, atitinkamai mažėja ir procentinė dalis publikacijų asmens privataus gyvenimo klausimais, susijusių su šiuo pavojingu reiškiniu. Taip pat mažėja e. žiniasklaidos priemonių, kuriose skelbiamos publikacijos apie tapatybės vagystę elektroninėje erdvėje atvejus, įvairovė. Tyrimo rezultatai taip pat patvirtino, kad tapatybės vagystės elektroninėje erdvėje atvejų bei informacijos apie šį reiškinį sklaida Lietuvos elektroninės žiniasklaidos priemonėse yra labai menka.

Detalesnė informacija apie autorių atliktus tyrimus pateikiama monografijos 5.2 dalyje.

Apibendrinančios išvados

• Tapatybės vagystės elektroninėje erdvėje prevencija asmens duomenų teisinės apsaugos srityje turi pasireikšti reformuojant esamą teisinį reguliavimą, atsižvelgiant į naujų technologijų keliamas grėsmes privatumui.

• Lietuvoje turėtų būti aktyvinama tapatybės vagystės elektroninėje erdvėje prevencija specialiaisiais teisės aktais.

• Tapatybės vagystės elektroninėje erdvėje prevencija elektroninių duomenų saugos srityje turėtų pasireikšti priimant strategiją šioje srityje numatančius dokumentus bei užtikrinant elektroninės informacijos saugos holistinį teisinį reguliavimą.

• Rekomenduotina reglamentuoti, kad nustatant tapatybę elektroninėje erdvėje, būtų remiamasi daugiau nei vienu asmens tapatybę nusakančiu rodikliu, kaip saugesniu ir sunkiau pažeidžiamu metodu.

• Be teisinės prevencijos valstybės lygmeniu, galimos ir kitos prevencijos priemonės. Vienos iš svarbesnių priemonių – prevencijos priemonės, skirtos viešajai informacijai apie tapatybės vagystę elektroninėje erdvėje platinti. Pastebimas viešosios informacijos apie tapatybės vagystę elektroninėje erdvėje trūkumas.

4.4. Tapatybės vagystės elektroninėje erdvėje prevencija tarptautiniu, dvišaliu (tarpvalstybiniu) ir (arba) regioniniu lygmeniu

Išskirtinos šios tarptautinės ir regioninės organizacijos, vykdančios tapatybės vagystės elektroninėje erdvėje prevenciją (šie veiksmai dažniausiai susiję su tam tikrų dokumentų priėmimu arba tam tikromis iniciatyvomis ir taikomi elektroninių duomenų saugumo, privatumo, vartotojų apsaugos ir pan. srityse):

– Ekonominio bendradarbiavimo ir plėtros organizacija (EBPO);
– APEC (angl. *Asia-Pacific Economic Cooperation*);
– Jungtinės tautos;
– Interpolas.

EBPO jau daugelį metų stengiasi didinti vartotojų pasitikėjimą elektronine erdve. Ši organizacija taip pat vysto įvairias gaires sukčiavimo vartotojų atžvilgiu srityse, taip pat, kiek tai susiję su brukalu (*spam*), saugumu ir privatumu[534]. Veikla vykdoma pasitelkiant šiuos pagrindinius instrumentus:

[534] Online Identity Theft. OECD, 2009, p. 81 [interaktyvus, žiūrėta 2011-09-21]. <http://www.keepeek.com/Digital-Asset-Management/oecd/science-and-technology/online-identity-theft_9789264056596-en>.

a) Elektroninės komercijos gairės (1999)[535]. Šiose gairėse pateikiami vartotojų teisinės apsaugos aspektai elektroninėje komercijoje. Paminėtina, kad vienas iš šių gairių tikslų – skatinti skaidrų elektroninio verslo tapatybės naudojimą elektroninėje erdvėje.
b) Tarptautinio sukčiavimo gairės (2003)[536]. Šios gairės skirtos vartotojams apsaugoti nuo sukčiavimo, vykdomo kertant valstybės sienas, įskaitant ir sukčiavimą elektroninėje erdvėje.
c) Vartotojų ginčų sprendimo gairės (2007)[537]. Gairės skirtos praktiniams ir juridiniams trukdžiams vartotojų bylose tiek lokaliame kontekste, tiek peržengiant valstybių sienas.
d) Informacinių sistemų ir tinklų saugumo gairės (2002)[538]. Šios gairės yra vienas iš pagrindinių dokumentų, nusakančių informacijos saugos principus. Nacionalinių valstybių įstatymų leidėjai, kurdami nacionalinius įstatymus informacijos saugos srityje, dažnai remiasi šiais principais ir inkorporuoja juos į nacionalinės teisės sistemą.
e) Privatumo apsaugos ir asmens duomenų judėjimo per sienas gairės (1980)[539]. Gairės nustato pagrindinius privatumo apsaugos principus.

APEC veikla daugiausia pasireiškė plėtojant atitinkamas strategijas, didinančias vartotojų pasitikėjimą elektronine erdve, pvz., Saugumo elektroninėje erdvėje strategija (angl. *Cyber Security Strategy*)[540], šalims narėms rekomenduojanti kriminalizuoti elektroninius nusikaltimus; Strategija dėl patikimos, saugios ir pastovios aplinkos elektroninėje erdvėje

[535] OECD Guidelines for Consumer Protection in the Context of Electronic Commerce, 1999 [interaktyvus, žiūrėta: 2011-09-21]. <http://browse.oecdbookshop.org/oecd/pdfs/free/9300023e.pdf>.

[536] OECD Guidelines for Protecting Consumer from Fraudulent and Deceptive Commercial Practices Across Borders [interaktyvus, žiūrėta 2011-09-21] <http://www.oecd.org/dataoecd/24/33/2956464.pdf>.

[537] OECD Recommendation on Consumer Dispute Resolution and Redress, 2007 [interaktyvus, žiūrėta 2011-09-21] <http://www.oecd.org/dataoecd/43/50/38960101.pdf>.

[538] OECD Guidelines for the Security of Information Systems and Networks, 2002. [interaktyvus, žiūrėta: 2011-09-21] <http://www.oecd.org/dataoecd/16/22/15582260.pdf>.

[539] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980 [interaktyvus, žiūrėta 2011-09-21]. <http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00.html>.

[540] APEC Cybersecyrity Strategy, 2002 [interaktyvus, žiūrėta 2011-09-21]. <http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan012298.pdf>.

užtikrinimo (angl. *Strategy to Ensure a Trusted, Secure and Sustainable Online Environment*)[541], akcentuojanti pavojingų veikų elektroninėje erdvėje grėsmę.

Jungtinės Tautos, kaip tarptautinė organizacija, taip pat prisideda prie tapatybės vagystės elektroninėje erdvėje prevencijos. 2005 metais ši organizacija subūrė ekspertų grupę parengti studiją dėl sukčiavimo ir tapatybės falsifikavimo. Ši grupė 2007 metais išleido ataskaitą, kurioje pateikta daugybė rekomendacijų dėl gerosios praktikos, galinti būti įdiegta valstybiniame ir privačiame sektoriuose[542].

Interpolas yra tarptautinė policijos organizacija, kurios tikslas – užkirsti kelią tarptautiniams nusikaltimams. Interpolas dažniausiai yra kaip pagrindas bendradarbiauti su nacionalinėmis policijos pajėgomis, vykdant tarpnacionalinius tyrimus dėl nusikaltimų, padarytų elektroninėje erdvėje. Interpolo elektroninių nusikaltimų ekspertai decentralizuotai dirba įvairiuose regionuose. Interpolas taip pat yra sudaręs darbo grupę, užsiimančią informacinių technologijų nusikaltimų klausimais, kuri, pavyzdžiui, parengė gerosios praktikos vadovą vykdant nusikaltimų tyrimus. Ši grupė taip pat įkūrė greito informacijos apsikeitimo tinklą, veikiantį 24/7 principu, be to, planuoja vykdyti bendradarbiavimo projektą, siekiant tirti *Botnet* tinklų veiklą Europoje bei keistis žiniomis ir geroja praktika, kovojant su šia pavojinga veika[543].

Kaip viena iš svarbių prevencijos priemonių paminėtini ir neformalūs tarptautiniai tinklai. Teisėsaugos institucijos jungiasi į neformalius tarptautinius tinklus, siekdamos pagerinti kovą su sukčiavimu ir brukalu (*spam*). Paminėtini šie tinklai:

– Tarptautinis vartotojų apsaugos tinklas (angl. *International Consumer Protection Network*). Jis dažniausiai naudojamas kaip priemonė apsikeisti informacija apie sukčiavimo metodus, nukreiptus

[541] APEC Strategy to Ensure Trusted, Secure and Sustainable Online Environment, 2005 [interaktyvus, žiūrėta: 2011-09-21]. <http://www.apec.org/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/~/media/Files/Groups/TEL/05_TEL_APECStrategy.ashx>.

[542] Online Identity Theft. OECD, 2009, p. 83 [interaktyvus, žiūrėta 2011-09-21]. <http://www.keepeek.com/Digital-Asset-Management/oecd/science-and-technology/online-identity-theft_9789264056596-en>.

[543] Online Identity Theft. OECD, 2009, p. 84 [interaktyvus, žiūrėta 2011-09-21]. <http://www.keepeek.com/Digital-Asset-Management/oecd/science-and-technology/online-identity-theft_9789264056596-en>.

prieš vartotojus. Tinklą sudaro 36 valstybių atitinkamų institucijų atstovai.

– Londono veiksmų planas (angl. *London Action Plan*). Šį globalų tinklą, skirtą kovoti su brukalu (*spam*), sudaro tiek valstybinių institucijų, tiek privataus verslo atstovai.
– G8 24/7 naujų technologijų nusikaltimų tinklas. Tinklas pateikia naujų technologijų ekspertų kontaktus, leidžiančius keistis informacija apie vykstančius elektroninių nusikaltimų tyrimus. Jis, sukurtas 1997 metais, šiuo metu apima 45 valstybių atstovus. Šio tinklo resursais buvo pasinaudota tiriant neteisėtos prieigos atakas prieš JAV, Vokietijos ir Meksikos bankus. Šio tinklo veikla taip pat susijusi su tapatybės nusikaltimų tyrimu.

Apibendrinančios išvados

• Tapatybės vagystės elektroninėje erdvėje prevencija tarptautiniu, dvišaliu (tarpvalstybiniu) ir (arba) regioniniu lygmeniu pasireiškia įvairių organizacijų veikla. Vienos iš svarbiausių tokių organizacijų yra Ekonominio bendradarbiavimo ir plėtros organizacija, APEC, Interpolas.

• Išskirtina neformalių tarptautinių tinklų reikšmė tapatybės vagystės elektroninėje erdvėje prevencijoje tarptautiniu, dvišaliu (tarpvalstybiniu) ir (arba) regioniniu lygmeniu.

5. Tyrimai

5.1. Elektroninės žiniasklaidos tyrimas

Problemos aprašymas, tyrimo būtinumo pagrindimas ir metodologija: tiriant tapatybės vagystę elektroninėje erdvėje, svarbus žiniasklaidos indėlis formuojant viešąją nuomonę apie tapatybės vagystę elektroninėje erdvėje, nušviečiant pagrindinius su šiuo reiškiniu susijusius įvykius. Todėl tikslinga ištirti tapatybės vagystės elektroninėje erdvėje atvejų ar informacijos apie šį reiškinį sklaidą žiniasklaidos priemonėse. Buvo pasirinktos elektroninės žiniasklaidos priemonės ir publikacijos jose 2009–2010 metais[544]. Analizuotos publikacijos šiose elektroninės žiniasklaidos priemonėse: www.delfi.lt, www.alfa.lt, www.ve.lt, www.atgimimas.lt, www.infolex.lt, www.kaunodiena.lt, www.lrytas.lt, www.lzinios.lt, www.balsas.lt, www.klaipeda.daily.lt, www.bernardinai.lt, www.bns.lt, www.lrt.lt, www.vilniausdiena.lt, www.skrastas.lt, www.vz.lt, www.respublika.lt, www.pareigunai.lt, www.politika.lt, www.kaveikiavaldzia.lt.

Taip pat analizuoti šie tinklalapiai: www.lat.lt (Lietuvos aukščiausiasis teismas), www.vat.lt (Vilniaus apygardos teismas), www.echr.coe.int (Europos Žmogaus teisių teismas), www.prokuraturos.lt (LR prokuratūra), www.lzlek.lt (Lietuvos žurnalistų ir leidėjų etikos komisija), www.lygybe.lt (Lygių galimybių kontrolieriaus tarnyba), www.3.lrs.lt/pls/inter/vaikai (Vaiko teisių apsaugos kontrolieriaus įstaiga), www.ada.lt (Valstybinė asmens duomenų apsaugos inspekcija), www.lzs.lt (Lietuvos žurnalistų sąjunga), www.viltis.lt (Lietuvos sutrikusio intelekto žmonių globos bendrija), www.gip-vilnius.lt (VšĮ „Globali iniciatyva psichiatrijoje“), www.inf.lt (Lietuvos neįgaliųjų forumas).

Pažymėtina, kad publikacijų kiekio ir kitų parametrų lyginimas gali būti sąlyginis. Tam turi reikšmės tas faktas, kad gerokai skiriasi tokių elektroninės žiniasklaidos priemonių, kaip www.delfi.lt ir www.lat.lt, publikacijų kiekis, be to, skiriasi specializacijos, taip pat dalis priemonių skirtos visai Lietuvos Respublikai, dalis yra regioninio pobūdžio[545].

[544] Publikacijos surinktos Žmogaus teisių stebėjimo instituto darbuotojų.

[545] Nors internetas regioninio pobūdžio elektroninę žiniasklaidos priemonę padaro prieinamą visoje Lietuvos Respublikoje, visgi auditorija ir nagrinėjamos temos yra daugiau regioninio pobūdžio.

Tyrimo tikslas: nustatyti tapatybės vagystės elektroninėje erdvėje atvejų ir informacijos apie šį reiškinį sklaidą Lietuvos elektroninės žiniasklaidos priemonėse.

Tyrimo uždaviniai:

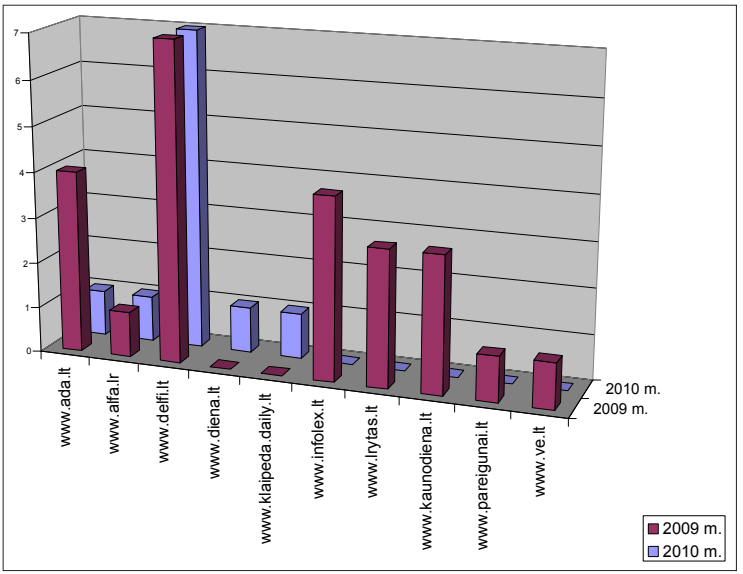
1) Aptarti publikacijų apie tapatybės vagystę elektroninėje erdvėje pasiskirstymą žiniasklaidos priemonėse;

2) Įvertinti publikacijų apie tapatybės vagystę elektroninėje erdvėje Lietuvos elektroninės žiniasklaidos priemonėse skaičiaus dinamiką 2009–2010 metais.

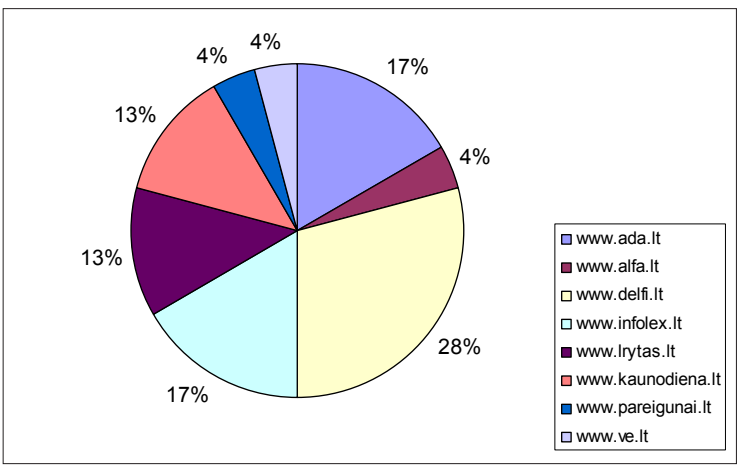
Tyrimo rezultatai:

Atliekant publikacijų apie tapatybės vagystę elektroninėje erdvėje pasiskirstymo e. žiniasklaidos priemonėse 2009–2010 m. analizę, nustatyta, kad 2009 m. publikacijos apie šio pavojingo reiškinio atvejus pasirodė tokiose e. žiniasklaidos priemonėse, kaip www.ada.lt, www.alfa.lt, www.delfi.lt, www.infolex.lt, www.lrytas.lt, www.kaunodiena.lt, www.pareigunai.lt, www.ve.lt. Daugiausia publikacijų buvo publikuota www.delfi.lt (7 publikacijos), www.ada.lt ir www.infolex.lt (po 4 publikacijas). Tačiau 2010 m. apie tapatybės vagystę elektroninėje erdvėje publikacijų pasirodė tik penkiose e. žiniasklaidos priemonėse: www.ada.lt, www.alfa.lt, www.delfi.lt, www.diena.lt ir www.klaipeda.daily.lt. 2010 m. kaip ir 2009 m. daugiausia publikacijų buvo www.delfi.lt (7 publikacijos), kitose e. žiniasklaidos priemonėse publikacijos pasiskirstė tolygiai (po vieną). Bendras publikacijų apie tapatybės vagystę elektroninėje erdvėje pasiskirstymas e. žiniasklaidos priemonėse 2009–2010 m. vaizduojamas 34 pav. pateiktoje diagramoje.

2009 m. e. žiniasklaidos priemonėse buvo paskelbta 24 publikacijų apie tapatybės vagystę elektroninėje erdvėje. Iš jų 28 proc. sudarė publikacijos, paskelbtos www.delfi.lt, po 17 proc. – www.ada.lt ir www.infolex.lt, po 13 proc. – www.lrytas.lt ir www.kaunodiena.lt, o kitose e. žiniasklaidos priemonėse – www.alfa.lt, www.pareigunai.lt ir www.ve.lt – publikacijos minėta tema sudarė po 4 proc. bendro publikacijų apie tapatybės vagystę elektroninėje erdvėje skaičiaus. Publikacijų apie tapatybės vagystę elektroninėje erdvėje pasiskirstymas e. žiniasklaidos priemonėse 2009 m. grafiškai vaizduojamas 35 pav. pateiktoje diagramoje.



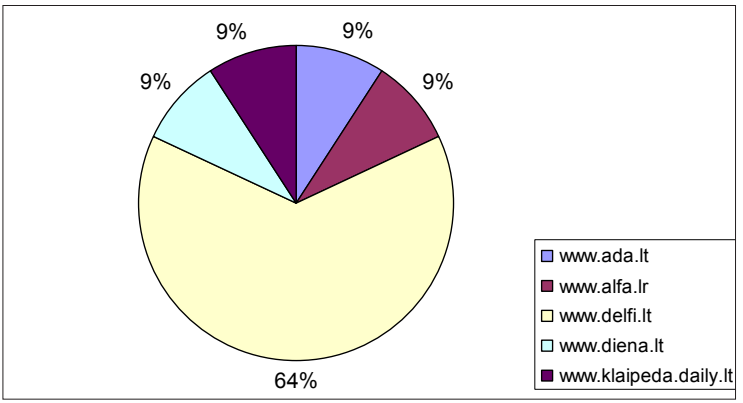
34 pav. Publikacijų apie tapatybės vagystę elektroninėje erdvėje pasiskirstymas e. žiniasklaidos priemonėse 2009–2010 m.



35 pav. Publikacijų apie tapatybės vagystę elektroninėje erdvėje pasiskirstymas e. žiniasklaidos priemonėse 2009 m.

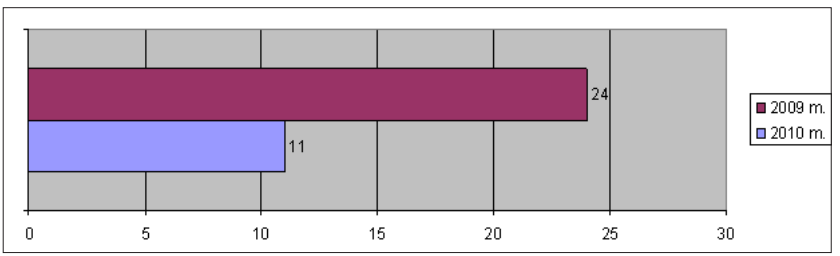
Tačiau 2010 m. e. žiniasklaidos priemonėse iš viso pasirodė 11 publikacijų apie tapatybės vagystę elektroninėje erdvėje, t. y. 2 kartais mažiau

nei 2009 m. Iš jų 64 proc. sudarė publikacijos, paskelbtos www.delfi.lt, kitose e. žiniasklaidos priemonėse – www.ada.lt, www.alfa.lt, www.diena.lt ir www.klaipeda.daily.lt – publikacijos minėta tema pasiskirstė po lygiai ir kiekvienoje iš šių e. žiniasklaidos priemonių sudarė po 9 proc. bendro publikacijų skaičiaus. Publikacijų apie tapatybės vagystę elektroninėje erdvėje pasiskirstymas e. žiniasklaidos priemonėse 2010 m. grafiškai pavaizduotas 36 pav. pateiktoje diagramoje.



36 pav. Publikacijų apie tapatybės vagystę elektroninėje erdvėje pasiskirstymas e. žiniasklaidos priemonėse 2010 m.

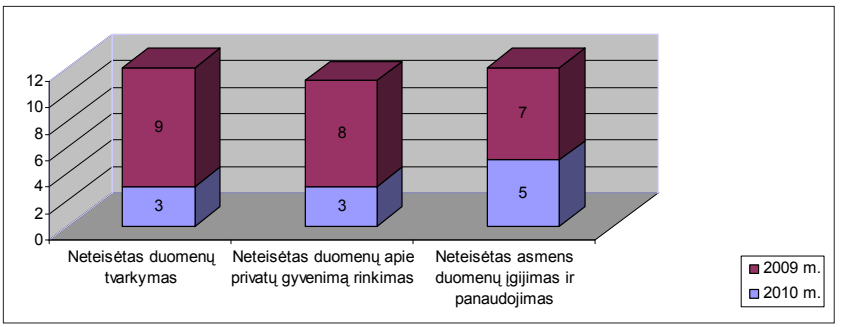
Bendra publikacijų apie tapatybės vagystę elektroninėje erdvėje e. žiniasklaidos priemonėse dinamika 2009–2010 m. grafiškai pavaizduota 37 pav.



37 pav. Publikacijų apie tapatybės vagystę elektroninėje erdvėje e. žiniasklaidos priemonėse dinamika 2009–2010 m.

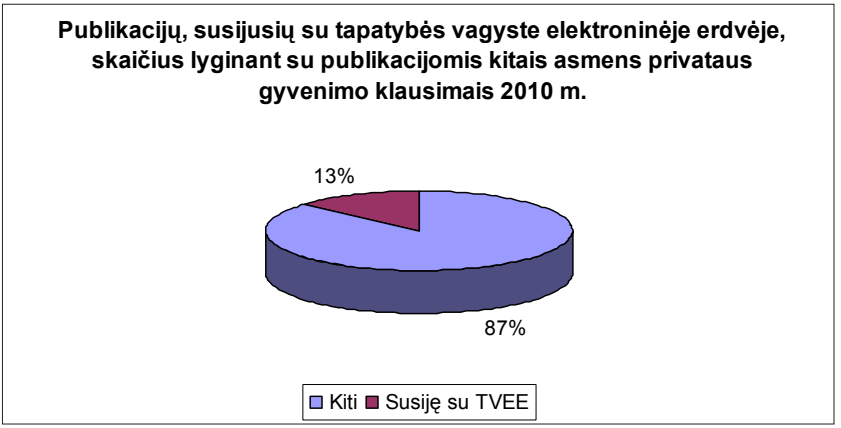
Pastebėta, kad e. žiniasklaidos priemonėse 2009–2010 m. paskelbtose publikacijose apie tapatybės vagystę elektroninėje erdvėje, visuome-

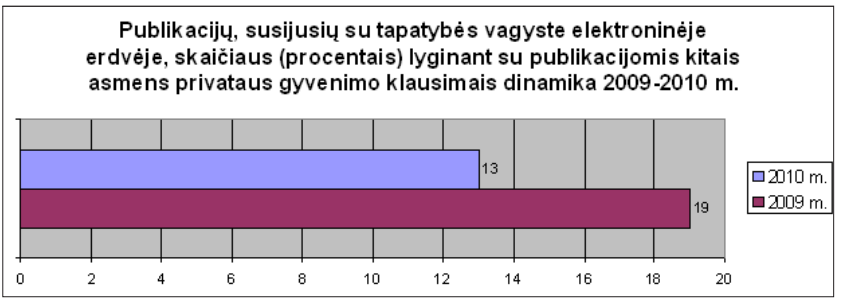
nė informuojama apie tris šio pavojingo reiškinio elementus – neteisėtą duomenų tvarkymą, neteisėtą duomenų apie privatų gyvenimą rinkimą ir neteisėtą asmens duomenų įgijimą bei panaudojimą. 2009 m. e. žiniasklaidos priemonėse pasirodė daugiau publikacijų apie kiekvieną minėtą tapatybės vagystės elektroninėje erdvėje elementą lyginant su publikacijų šia tema skaičiumi 2010 m. Pavyzdžiui, 2009 m. e. žiniasklaidos priemonėse publikacijų apie neteisėto duomenų tvarkymo atvejus pasirodė net 3 kartus daugiau nei 2010 m.; publikacijų, kuriose viešinamas neteisėtas duomenų apie privatų gyvenimą rinkimas, 2009 m. buvo 2,7 karto daugiau nei 2010 m., o publikacijų apie neteisėtą asmens duomenų įgijimą ir panaudojimą 2009 m. buvo 1,4 karto daugiau, lyginant su 2010 m. Tapatybės vagystės elektroninėje erdvėje elementų, aptariamų e. žiniasklaidos priemonėse, skaičius 2009–2010 m. pavaizduotas 38 pav. pateiktoje diagramoje.



38 pav. Tapatybės vagystės elektroninėje erdvėje elementų, aptariamų e. žiniasklaidos priemonėse, skaičius 2009–2010 m.

Pažymėtina, kad publikacijų, susijusių su tapatybės vagyste elektroninėje erdvėje, skaičius lyginant su publikacijomis kitais asmens privataus gyvenimo klausimais 2009 m. sudarė 19 proc., o 2010 m. – 13 proc., taigi pastebima, kad publikacijų apie tapatybės vagystę elektroninėje erdvėje e. žiniasklaidos priemonėse mažėja. Publikacijas, susijusias su tapatybės vagyste elektroninėje erdvėje, lyginimo su publikacijomis kitais asmens privataus gyvenimo klausimais dinamiką 2009–2010 m. galima pavaizduoti diagramomis (procentais) (39 pav.):





39 pav. Publikacijų skaičiaus palyginimo diagramos

Pastebėta, kad daugiausia publikacijų 2009–2010 m., lyginant su kitomis e. žiniasklaidos priemonėmis, buvo paskelbta www.delfi.lt. Pažymėtina, kad e. žiniasklaidos priemonėse, kuriose buvo paskelbtos publikacijos tapatybės vagystės elektroninėje erdvėje tema, buvo nurodyti tikrovę atitinkantys faktai, paviešinti tapatybės vagystės elektroninėje erdvėje atvejai, nepateikiant subjektyvios publikacijos rengėjo nuomonės, kadangi informacinių technologijų pažanga neišvengiamai sukelia daugybę grėsmių asmens privatumui elektroninėje erdvėje ir dėl to vartotojai gali pradėti mažiau naudotis elektroninėmis paslaugomis.

Apibendrinant e. žiniasklaidos tyrimo rezultatus, galima daryti išvadą, kad publikacijų apie tapatybės vagystę elektroninėje erdvėje e. žiniasklaidos priemonėse mažėja, atitinkamai mažėja ir procentinė dalis publi-

kacijų asmens privataus gyvenimo klausimais, susijusių su šiuo pavojingu reiškiniu. Taip pat mažėja e. žiniasklaidos priemonių, kuriose skelbiamos publikacijos apie tapatybės vagystę elektroninėje erdvėje atvejus, įvairovė. Tyrimo rezultatai taip pat patvirtino, kad tapatybės vagystės elektroninėje erdvėje atvejų bei informacijos apie šį reiškinį sklaida Lietuvos elektroninės žiniasklaidos priemonėse yra labai menka.

5.2. Kiekybiniai ir kokybiniai tyrimai

5.2.1. Metodologija

Kiekybinis tyrimo metodas buvo pasirinktas kaip pagrindinis (interneto vartotojų (toliau – vartotojai), viešojo sektoriaus darbuotojų, Valstybinio socialinio draudimo fondo administravimo įstaigųdarbuotojų (–Sodros) darbuotojų ir privataus sektoriaus darbuotojų (toliau – verslo darbuotojų) apklausos), kadangi juo gauti statistiniai skaitiniai duomenys yra tikslūs ir patikimi. Tyrimų tikslas – nustatyti, kaip atitinkamos respondentų grupės suvokia tapatybės vagystės elektroninėje erdvėje problemą, kaip vertina šios veikos pavojingumą ir paplitimą, kaip suvokia šios pavojingos veikos prevenciją.

Kiekybiniai tyrimai buvo atliekami apklausos tyrimo metodu[546]. Nors antrinių duomenų tyrimas turi daug privalumų (greitesnis ir lengvesnis, nedidelė kaina, trumpas duomenų rinkimo laikas[547]), visiems tyrimams buvo pasitelkti konkrečiai problemai spręsti naujai surinkti pirminiai duomenys[548] (lot. *ad hoc*), kadangi autoriai neaptiko pakankamai išsamių ir tinkamų apdoroti antrinių duomenų, kuriuos tiriant būtų galima gauti gana informatyvius atsakymus į keliamus probleminius klausimus.

Atsižvelgiant į tai, kad monografijoje aptariamas reiškinys Lietuvos moksle netyrinėtas, autoriai, pasitelkdami A. Bryman aprašytą induktyvųjį požiūrį (angl. *inductive approach* [549]), nekėlė išankstinių hipotezių, o rinko duomenis ir juos sistemino siekdami rasti atsakymus į mokslui rūpimus klausimus.

[546] Rudzkienė, V. 2010. *Parengta mokslinė-metodinė medžiaga*, p. 31.
[547] *Ibid*., p. 34.
[548] *Ibid*., p. 33.
[549] Bryman, A. 2008. *Social Research Methods*. Oxford University Press, p. 11.

Autoriai atliko kelis kiekybinius vienas kitą papildančius tyrimus, siekdami ištirti atskirų (svarbių tiriamam reiškiniui) grupių žinias, požiūrį ir šių grupių suvokimą apie reiškinio paplitimą, pavojingumą ir galimą prevenciją. Tokie paraleliniai atskirų susijusių grupių tyrimai sudaro galimybę palyginti rezultatus, ieškant sąsajų ir dėsningumų.

Prieš pateikiant respondentams anketos buvo patikrintos (aprobuotos), t. y. pateiktos užpildyti Mykolo Romerio universiteto studentams, siekiant įsitikinti, ar asmenys suvokia anketoje suformuluotus klausimus, ir atsižvelgti į jų pateiktas pastabas. Tokiu būdu patikrintos ir vėliau patikslintos anketos buvo pateiktos tyrimo vartotojų grupei.

Informacija apie bandomąjį tyrimą: iš viso apklaustas 131 Mykolo Romerio universiteto studentas. Studijų kryptis: Finansų ekonomika. Atliekant tyrimą dalyvavo 4 kurso abiejų lyčių studentai (tiek nuolatinių, tiek ištęstinių studijų). Amžius buvo nuo 20 iki 56 metų. Amžiaus vidurkis – 26 metai.

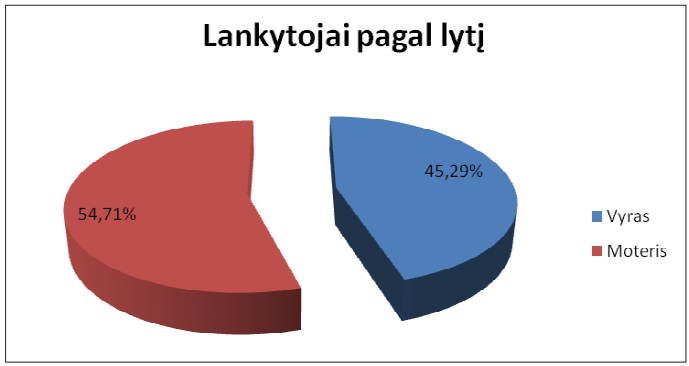
Pasirinktų tirti respondentų grupių ir metodų pagrindimas:
Vartotojai

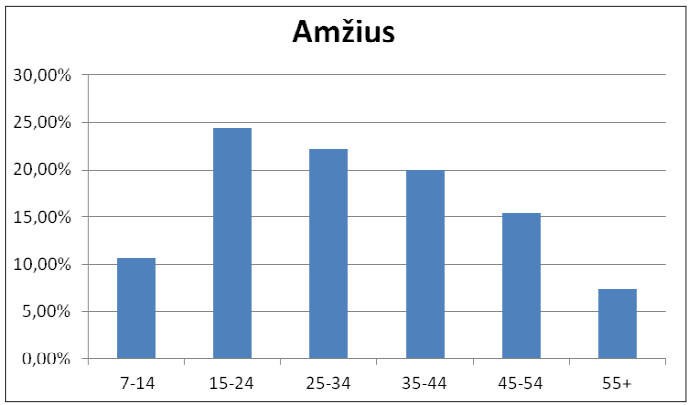
Tyrimo tikslas. Nustatyti, ar vartotojai suvokia tapatybės vagystės elektroninėje erdvėje problemą, kaip vertina šios veikos pavojingumą ir paplitimą.

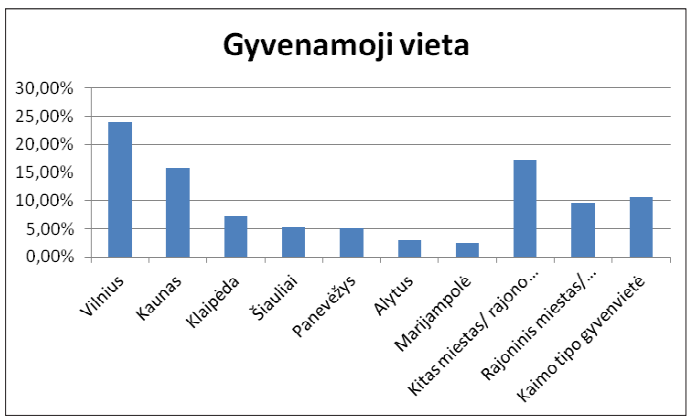
Problemos aprašymas ir tyrimo būtinumo pagrindimas. Tiriant tapatybės vagystę kaip reiškinį, svarbiausia tirtina grupė buvo asmenys, kurių duomenys gali būti pavogti. Atsižvelgdami į tai, autoriai tyrimo grupę parinko internetu besinaudojančius asmenis, kuriuos apklausė per laisvalaikio, pramogų ir informacinį (iš esmės ne verslui ar kitoms organizacijoms, o fiziniams asmenims skirtą) portalą www.zebra.lt, kuris respondentus per tiesioginę nuorodą nukreipdavo į www.manoapklausa.lt.[550]

Duomenys (pateikti paslaugos teikėjo) apie vartotojus www.zebra.lt (40 pav.):

[550] Sullivan, J. T. 2001. *Methods of Social research*. Northern Michigan University, p. 182 (rekomenduoja tyrimams pasitelkti profesionalius tyrimų internetinius puslapius).







40 pav. Duomenys apie vartotojus (pagal portalą www.zebra.lt)

Portalą per mėnesį aplanko daugiau kaip 400 000 vartotojų.

Autoriai nekėlė jokių papildomų išankstinių reikalavimų apklausiamų asmenų amžiui, lyčiai, išsilavinimui, net gyvenamai vietai, siekdami, kad klausimyną pildytų tokios sudėties vartotojai, kokia tyrimo metu yra interneto vartotojų sudėtis. Reikia atsižvelgti į tai, kad, nors autoriai siekė, kad respondentų sudėtis būtų kuo panašesnė į visų Lietuvoje internetu besinaudojančių asmenų sudėtį, tai nėra įmanoma atlikti apklausiant vieno portalo vartotojus, kadangi, nors portalas siekia subalansuotai atspindėti įvairių interneto vartotojų grupių interesus (yra atskiri skyreliai pagal interesų grupes, pvz.: pramogų, žinių, laisvalaikio skyriai ir pan.), tačiau neatitikimas Lietuvos interneto vartotojų vidurkio gali būti nulemtas atskirų interneto vartotojų skirtingų pomėgių (kadangi atskiros vartotojų grupės gali mėgti tik labai specializuotus puslapius, pvz.: vienų ar kitų internetinių žaidimų, diskusijų, socialinius tinklus, gal net draustino ar žalingo turinio, kurio aptariamas portalas neplatina), naudojimąsi portalo paslaugomis gali lemti internetinio raštingumo skirtumai (pvz., pradedantieji naudotis internetu arba mažesnio elektroninio raštingumo asmenys gali naudotis tik labai siauromis interneto galimybėmis (pvz., sužinoti labai konkrečią informaciją konkrečiame internetiniame puslapyje ir pan.). Minėtos aplinkybės nesumenkina gautų rezultatų svarbos, tačiau jie turi būti vertinami kompleksiškai su minėtomis išlygomis ir atsižvelgiant į taikomo metodo ir jo konkretaus taikymo specifiką. Aptariant vartotojams parengto klausimyno struktūrą, paminėtina, kad vartotojams pateiktoje anketoje vyrauja uždari klausimai, tačiau, siekiant gauti išsamesnių duomenų ir leisti vartotojams laisviau reikšti nuomonę, buvo ir dalis atvirų klausimų[551].

Vartotojų tyrimo imtis ir organizavimas. Anketinė apklausa buvo atlikta apklausiant Lietuvos gyventojus per www.manoapklausa.lt sistemą. Konkretaus tyrimo populiacija žinoma – Lietuvos gyventojai nuo 17 metų (ši imtis pasirinkta, nes LR Statistikos departamentas pateikia šio amžiaus diapazono duomenis). Remiantis LR Statistikos departamento duomenimis[552], 2011 m. liepos mėn. Lietuvoje gyventojų nuo 17 metų buvo 2 615 852. Norint nustatyti imtį buvo remiamasi Schwarze formule[553]:

[551] Tidikis, R. 2003. *Socialinių mokslų tyrimų metodologija*. Lietuvos Teisės Universitetas. p. 475.

[552] [interaktyvus, žiūrėta 2011-09-25] <http://www.stat.gov.lt/lt/pages/view/?id=1567>

[553] Rudzkienė V. 2005. *Socialinė statistika: vadovėlis*. Vilnius: Mykolo Romerio universiteto Leidybos centras. 260 p.

$$n = \frac{N \times 1{,}96^2 \times p \times q}{\varepsilon^2 \times (N-1) + 1{,}96^2 \times p \times q}$$

n – populiacijos dydis, reikšmė;

1,96 atitinka standartizuoto normaliojo skirstinio 95 proc. pasikliovimo lygmenį;

p – įvykio baigties tikimybė, kad nagrinėjamas požymis pasireikš tiriamoje populiacijoje (dažniausiai imama blogiausio varianto tikimybė – požymis būdingas pusei, t. y. 50 proc. populiacijos, todėl pasirenkama $p = 0{,}5$);

q – tikimybė, kad nagrinėjamas požymis nepasireikš tiriamoje populiacijoje ($q = 1 - p = 0{,}5$);

ε – pageidautinas tikslumas

Populiacija apima 2 615 852 respondentų. Tikimybė, kad nagrinėjamas požymis populiacijoje pasireikš, yra 0,5, kad nepasireikš – 0,5. Pageidautinas tikslumas yra 0,1. Viską apskaičiavę gauname:

$$\frac{2615852 \times 1{,}96^2 \times 0{,}5 \times 0{,}5}{0{,}1^2 \times (2615852-1) + 1{,}96^2 \times 0{,}5 \times 0{,}5} = 96{,}039$$

Remiantis formule, būtina apklausti bent 96 respondentus, kad būtų galima užtikrinti apsibrėžtą patikimumą.

Atliekant tyrimą – nuorodą portale www.zebra.lt vartotojai paspaudė 4 450 kartų, tačiau užpildė 359 respondentai, iš jų buvo 116 vyrų, 243 moterų. Vidutinis amžius – 31,1 m.

Viešojo sektorius darbuotojai ir Sodros darbuotojai

Tyrimo tikslas – ištirti, kaip tapatybės vagystės problemą ir prevenciją suvokia Sodros / viešojo sektoriaus darbuotojai, kurie yra sukaupę didelį kiekį asmens duomenų.

Problemos aprašymas ir tyrimo būtinumo pagrindimas. Kita tirti parinkta svarbi grupė asmenų, galinti būti tiesiogiai susijusi su tapatybės vagyste ir jos prevencija, tai asmenys, kurie dėl darbo specifikos disponuoja kitų asmenų asmens duomenimis. Tokius asmens duomenis dideliais kiekiais turi ir jais disponuoja atskiri viešojo sektoriaus subjektai. Dažnai tokiais duomenimis viešasis sektorius disponuoja be asmens noro ar sutikimo, o vadovaudamasis norminiais teisės aktais.

Viešasis sektorius ne tik disponuoja asmens duomenimis, bet ir teikia paslaugas internetu, o tokių paslaugų saugus ar nesaugus teikimas gali padidinti arba sumažinti tapatybės vagystės tikimybę. Autoriai ketino apklausti viešojo sektoriaus darbuotojus nedetalizuodami jų pagal darbo sritis, o detaliau apklausti – vieną profesionaliausiai su asmens duomenimis dirbantį viešojo sektoriaus subjektą. Kaip atskiras subjektas buvo pasirinkta Sodra, turinti itin dideles asmens duomenų bazes ir nuolat jas tvarkanti. Pažymėtina, kad Sodra yra institucija, skyrusi dideles investicijas diegiant kompiuterines darbdavių ir darbuotojų aptarnavimo sistemas, kuriose bendrauti pasitelkiamas elektroninis parašas ir kitos saugumą didinančios teisinės, organizacinės ir techninės priemonės. Ši institucija geranoriškai reagavo į autorių prašymą atlikti tyrimus apklausiant darbuotojus; darbuotojų aktyvumas buvo didelis ir, autorių nuomone, respondentai anketas pildė atvirai, kadangi taikytas kompiuterinis anketavimas, pasitelkiant kompiuterinį portalą www.manoapklausa.lt, neleido nei tyrėjams, nei darbdaviui nustatyti, kaip ir kuris darbuotojas užpildė anketą, todėl ir buvo galima tikėtis tikslesnių ir atviresnių duomenų. Bendras viešojo sektoriaus tyrimas buvo mažiau sėkmingas, kadangi į anketą, išplatintą per duomenų saugos įgaliotinius, esančius pagrindinėse viešojo sektoriaus įstaigose, buvo sulaukta tik 38 respondentų atsakymų, todėl apibendrinti visą Lietuvos viešąjį sektorių galima su tam tikra paklaida.

Sodros tyrimo imtis. Anketinė SODROS darbuotojų apklausa taip pat buvo atliekama per www.manoapklausa.lt sistemą. Konkretaus tyrimo galimų apklausti asmenų skaičius žinomas – 3700 darbuotojų[554]. Įrašę reikšmes į Schwarze formulę gauname:

$$\frac{3700 \times 1{,}96^2 \times 0{,}5 \times 0{,}5}{0{,}1^2 \times (3700 - 1) + 1{,}96^2 \times 0{,}5 \times 0{,}5} = 93{,}62$$

Siekiant užtikrinti apsibrėžtą patikimumą, remiantis formule būtina apklausti bent 94 respondentų. Atliekant tyrimą, Sodros darbuotojų apklausta 263 respondentai, iš jų buvo 30 vyrų, 233 – moterys. Vidutinis amžius – 45,1 m.

Viešojo sektoriaus imtis. Anketinė apklausa atlikta apklausiant asmenis, turinčius valstybės tarnautojo statusą, per www.manoapklausa.lt

[554] [interaktyvus, žiūrėta 2011-09-25] <http://www.sodra.lt/lt/veikla>.

sistemą. Konkretaus tyrimo populiacija žinoma – 53 279 valstybės tarnautojų[555]. Remdamiesi Schwarze formule ir įrašę reikšmes gauname:

$$\frac{53279 \times 1{,}96^2 \times 0{,}5 \times 0{,}5}{0{,}1^2 \times (53279 - 1) + 1{,}96^2 \times 0{,}5 \times 0{,}5} = 95{,}86$$

Remdamiesi formule gauname, kad norėdami turėti apsibrėžtą patikimumą turime apklausti apytikriai 96 valstybės tarnautojus. Atliekant tyrimą, viešojo sektoriaus darbuotojų apklausta: 38[556] respondentai, iš jų 27 vyrai, 11 moterų. Amžius buvo nuo 25 iki 65 metų, vidutinis amžius – 38 m. Kadangi apklaustas mažesnis nei minimalus skaičius respondentų, šio tyrimo duomenys turėtų būti vertinami kaip mažiau patikimi.

Verslo darbuotojai

Tyrimo tikslas – ištirti privataus sektoriaus (verslo) sektoriaus darbuotojų, sukaupiančių didelį kiekį asmens duomenų, tapatybės vagystės problemos ir prevencijos suvokimą.

Problemos aprašymas ir tyrimo būtinumo pagrindimas. Trečioji tirtina asmenų grupė – verslo subjektai, galbūt disponuojantys kitų asmenų asmens duomenimis ir teikiantys paslaugas elektroninėje erdvėje. Ji išskirta kaip atskira viešojo sektoriaus grupė, kadangi skiriasi prekių ir paslaugų pobūdis, o asmens duomenys beveik visais atvejais į verslo subjektų rankas patenka (arba nepatenka) pagal asmens duomenų savininko valią (su nedidelėmis įstatymuose numatytomis išimtimis, pvz., skolininkų sąrašai ir pan.). Pagrindinis asmens interesas pateikti asmens duomenis yra noras gauti privataus sektoriaus teikiamas paslaugas ir / ar pirkti prekių. Privatus verslas yra didelė terpė galimoms tapatybės vagystėms elektroninėje erdvėje, kadangi vartotojas dažnai negali susirinkti tiek duomenų apie prekių arba paslaugų teikėją, jo patikimumą, kad būtų visiškai užtikrintas, jog jo atiduoti asmens duomenys bus saugūs ir panaudoti tik tiems tikslams, kuriems jie perduoti. Taip pat pažymėtina, kad verslo subjektai nėra taip griežtai kontroliuojami, kaip viešasis sektorius, o atliekami sandoriai yra gana dideli ir kartais sudėtingi. Be to, kaip aptariama šioje monografijoje, nėra bendrų privačiam verslui taikomų techninio saugumo standartų ar imperatyvaus teisinio reguliavimo,

[555] [interaktyvus, žiūrėta 2011-09-25] <http://www.vtd.lt/index.php?1471208505>.

[556] Nors anketos tarp viešojo sektoriaus darbuotojų buvo platintos gana plačiai, viešojo sektoriaus darbuotojai labai vangiai pildė anketas.

kuris užtikrintų saugų asmens duomenų perdavimą. Anketa buvo paruošta vadovaujantis panašiais minėtais principais ir įkelta į www.manoapklausa.lt. Deja, verslo įmonių darbuotojai labai vangiai pildė anketas, teigdami, kad klausimai yra sudėtingi (nors anketos, pateiktos vartotojams, viešajam sektoriui ir verslo subjektų darbuotojams, buvo analogiškos, o klausimų sudėtingumas buvo patikrintas užduodant analogiškus klausimus M. Romerio universiteto studentams). Autoriai darė prielaidas, kad toks mažas respondentų dalyvavimas gali būti nulemtas ne tik anketos klausimų sudėtingumo, bet ir potencialių respondentų sąlyginio problemos nuvertinimo ar nenoro į ją gilintis, o tai rodo, kad verslo suinteresuotumas spręsti tapatybės vagystės elektroninėje erdvėje problemas gali būti nepakankamas.

Verslo sektoriaus imtis. Anketinė apklausa atlikta apklausiant Lietuvoje registruotas įmones (privataus kapitalo) per www.manoapklausa.lt sistemą. Konkretaus tyrimo populiacija žinoma – 159 979 įregistruotų įmonių[557]. Įrašę reikšmes į Schwarze formulę gauname:

$$\frac{159979 \times 1{,}96^2 \times 0{,}5 \times 0{,}5}{0{,}1^2 \times (159979 - 1) + 1{,}96^2 \times 0{,}5 \times 0{,}5} = 95{,}98$$

Remdamiesi formule gauname, kad siekiant apsibrėžto patikimumo, reikia apklausti apytikriai 96 įmones. Tyrimo metu apklausti 43[558] respondentai, iš jų buvo 26 vyrai, 17 moterų. Amžius buvo nuo 21 iki 52 metų, vidutinis amžius – 31,2 m. Kadangi apklausta mažiau nei minimalus kiekis respondentų, šio tyrimo duomenys turėtų būti vertinami kaip mažiau patikimi.

Ekspertai

Tyrimo tikslas: išsiaiškinti ekspertų nuomonę dėl svarbiausių tapatybės vagystės elektroninėje erdvėje kaip socialinio teisinio reiškinio aspektų.

Problemos aprašymas ir ekspertinio vertinimo būtinumo pagrindimas. Atsižvelgiant į tai, kad kiekybiniai ir kokybiniai tyrimo metodai ne prieštarauja tarpusavyje, bet papildo vieni kitus ir praplečia tyrimo galimybes[559], autoriai naudojo ir kokybinius tyrimus, kurie suteikia daug vertingos informa-

[557] [interaktyvus, žiūrėta 2011-09-25] <http://www.registrucentras.lt/jar/stat/sta.php>.

[558] Nors anketos tarp verslo sektoriaus darbuotojų buvo platintos gana plačiai, verslo sektoriaus darbuotojai labai vangiai pildė anketas.

[559] Rudzkienė, V. 2010. *Parengta mokslinė-metodinė medžiaga*, p. 39.

cijos, padedančios nustatyti ir tiksliai apibrėžti problemas. Tiriant santykinai naują ir sudėtingą reiškinį – tapatybės vagystę elektroninėje erdvėje – buvo svarbu atlikti ekspertų žinių ir vertinimų tyrimą, nes norint nuodugniau išanalizuoti reiškinį reikalingos respondentų specifinės žinios ir patirtis, kurių neturi (arba turi nepakankamai) kitos autorių apklaustos asmenų grupės. Kadangi tapatybės vagystė elektroninėje erdvėje yra santykinai naujas, kompleksinis ir sudėtingas reiškinys, tai atskirų šios srities specialistų faktiškai nėra, tačiau tiriamą reiškinį gerai išmano asmenys, dirbantys IT teisės, saugos technologijų, asmens duomenų teisinio reguliavimo ir kt. srityse. Taigi, autoriai pasirinko ekspertus, gerai išmanančius elektroninės erdvės specifiką, elektroninių duomenų saugumą, nusikaltimus elektroninėje erdvėje ir kitas su tapatybės vagyste elektroninėje erdvėje susijusias sritis. Atsižvelgiant į tai, kad tiriamasis reiškinys yra sudėtingas, dalis ekspertų geriau išmano tik tam tikrus reiškinio aspektus, tačiau kitų aspektų nėra atskirai tyrinėję, kai kurie ekspertai į tam tikrus klausimus atsakyti negalėjo.

Iš ekspertinio vertinimo metodų buvo pasirinktas aktyvus individualus anketavimo metodas. Ekspertams buvo pateikti atviri klausimai siekiant, kad jie vertintų laisvai, pasitelkdami sukauptas žinias ir intuiciją. Reikia atsižvelgti į tai, kad ekspertinio vertinimo atveju vieno mažesnio skaičiaus ekspertų ar net vieno iš ekspertų nuomonė gali būti svarbesnė ar santykinai teisingesnė negu didesnio kiekio ekspertų, todėl autoriai netaikė statistinių metodų, o vertinio ekspertų nuomones apibendrindami.

Autoriai parinko 9 ekspertus, turinčius žinių ir patirties tapatybės vagystės elektroninėje erdvėje srityje. Šis ekspertų skaičius tris kartus viršija minimalų rekomenduojamą[560], tačiau kadangi ekspertų – tos srities lyderių ir dar turinčių reikiamų specialių žinių kiekį, nėra daug, tyrime nebuvo siekiama dėl duomenų patikimumo apklausti daugiau ekspertų. Taip pat buvo atsižvelgta, kad vertinant agreguotus ekspertinius vertinimo modelius nustatyta, kad vienodų nedidelės ekspertų grupės sprendimų ir vertinimų tikslumas nenusileidžia didelės ekspertų grupės sprendimų ir vertinimų tikslumui[561]. Konkretus rekomenduojamų ekspertų skaičius skirtingoje mokslinėje literatūroje skiriasi[562].

[560] Rudzkienė, V. 2010. *Parengta mokslinė-metodinė medžiaga*, p. 55.

[561] *Ibid*., 56 p.

[562] Tidikis R. 2003. *Socialinių mokslų tyrimų metodologija*. Lietuvos Teisės Universitetas. p. 515, rekomenduoja apklausti 5–7 asmenis.

Ekspertų sąrašas:

1. **Dr. Algirdas Kunčinas**.

Dr. Algirdas Kunčinas (istorija, 05 H) yra Valstybinės duomenų apsaugos inspekcijos direktorius. Kadangi Valstybinė duomenų apsaugos inspekcijos kompetencija yra susijusi su privatumo ir asmens duomenų apsauga, todėl sąsajos su tapatybės vagyste elektroninėje erdvėje labai glaudžios, nes ši neteisėta veika vykdoma pasisavinant tam tikrus asmens duomenų elementus.

2. **Vitalijus Kirvaitis**.

Vitalijus Kirvaitis yra UAB „Omnitel" Juridinio skyriaus vadovas. Tapatybės vagystė elektroninėje erdvėje vykdoma elektroninių ryšių tinkluose. UAB „Omnitel" yra vienas iš didžiausių Lietuvoje elektroninių ryšių operatorių, tad tokios bendrovės Juridinio skyriaus vadovas, be abejo, yra kompetentingas išsakyti nuomonę apie tapatybės vagystę elektroninėje erdvėje.

3. **Dr. Irmantas Rotomskis**[563].

Dr. Irmantas Rotomskis (teisė, 01 S) yra Mykolo Romerio universiteto Ekonomikos ir finansų valdymo fakulteto prodekanas, docentas. Dr. Irmanto Rotomskio mokslinės veiklos sritys susijusios su elektronine komercija, interneto teise, todėl tapatybės vagystė, kuri pasireiškia internete ir dažnai būna susijusi su elektroninės komercijos procesais, yra artima sritis.

4. **Rytis Rainys**.

Rytis Rainys yra Lietuvos Respublikos ryšių reguliavimo tarnybos Tinklų ir informacijos saugumo departamento direktorius. Tapatybės vagystė elektroninėje erdvėje glaudžiai susijusi su duomenų sauga. Šios srities priežiūrą tam tikrais aspektais vykdo Lietuvos Respublikos ryšių reguliavimo tarnybos Informacijos saugos departamentas, kurio direktorius ir yra Rytis Rainys.

[563] Atsižvelgiant į tai, kad asmenų turinčių specialių žinių ir patirties tiriamoje srityje Lietuvoje yra nedaug, autoriai dr. Irmanto Rotomskio paprašė ne tik atsakyti į ekspertams pateiktus klausimus, bet ir recenzuoti monografiją. Šis asmuo atsakydamas į ekspertams pateiktus klausimus išsakė savo nuomonę, kuri monografijoje pagal pasirinktą metodiką buvo vertinama tik kaip viena iš ekspertų nuomonių, todėl recenzentas dr. Irmantas Rotomskis laikytinas nesuinteresuotu mokslininku.

5. **Dr. Rolandas Krikščiūnas**.

Dr. Rolandas Krikščiūnas (teisė, 01 S) yra Mykolo Romerio universiteto Administracinės teisės ir proceso katedros docentas. Už tapatybės vagystę elektroninėje erdvėje gali būti baudžiama ne tik kaip už nusikaltimą, bet ir kaip už administracinį teisės pažeidimą. Rolandas Krikščiūnas yra administracinės teisės specialistas, beje, išleidęs publikacijų ir apie elektroninius nusikaltimus.

6. **Renata Marcinauskaitė**.

Renata Marcinauskaitė yra Mykolo Romerio universiteto Baudžiamosios teisės ir kriminologijos katedros doktorantė. Viena iš tapatybės vagystės elektroninėje erdvėje problemų – atitinkamų vertybių apsaugojimo kriminalizuojant veikas problema, todėl būtinos baudžiamosios teisės žinios. Be to, Renata Marcinauskaitė rengia disertaciją iš elektroninių nusikaltimų srities: „Nusikalstamos veikos elektroninių duomenų ir informacinių sistemų saugumui".

7. **Dr. Skirmantas Bikelis**.

Dr. Skirmantas Bikelis (teisė, 01 S) yra Mykolo Romerio universiteto Baudžiamosios teisės ir kriminologijos katedros lektorius, Teisės instituto Baudžiamosios justicijos tyrimų skyriaus vedėjas, vyresnysis mokslo darbuotojas. Šio skyriaus veikla susijusi su moksliniais tyrimais baudžiamosios teisės, baudžiamojo proceso, bausmių vykdymo teisės srityse, teisės aktų ir jų projektų analize. Viena iš tapatybės vagystės elektroninėje erdvėje problemų – kriminalizavimo problema. Todėl būtinos baudžiamosios teisės specialistų žinios.

8. **Dr. Alfredas Kiškis**.

Dr. Alfredas Kiškis (teisė, 01 S) yra Mykolo Romerio universiteto Baudžiamosios teisės ir kriminologijos katedros docentas. Tapatybės vagystė elektroninėje erdvėje, kaip reiškinys, yra susijusi su kriminologija. Dr. Alfredo Kiškio specializacija yra kriminologijos mokslas, be to, jis ilgą laiką dirbo Lietuvos nusikaltimų prevencijos centre, kuris disponuoja elektroninių nusikaltimų statistika ir užsiima tokių nusikaltimų prevencijos klausimais.

9. **Žydrūnas Paškauskas**.

Žydrūnas Paškauskas tyrimo atlikimo metu buvo Lietuvos Respublikos vidaus reikalų ministerijos Saugos skyriaus vedėjas. Tapatybės vagystė elektroninėje erdvėje, kaip reiškinys, yra glaudžiai susijęs su duomenų sauga, o minimo skyriaus veikla ir susijusi su duomenų sauga.

Parenkant ekspertus buvo atsižvelgiama ir į formalius rodiklius (pareigas, mokslinius laipsnius ir vardus), tačiau tai nebuvo svarbiausias atrankos kriterijus. Autoriams svarbiausia buvo rasti tiesioginę tiriamo reiškinio ir eksperto lyderio kompetencijos bei patirties sąsają. Pasirenkant ekspertus atsižvelgta į tai, kad jie būtų ne vien teisės specialistai ar teisinį darbą dirbantys asmenys, nes tyrimo objektas apima platesnius socialinius ir net techninius problemos aspektus. Ekspertams anketa taip pat buvo suformuota pasitelkiant www.manoapklausa.lt portalą, tačiau klausimai buvo atviri.

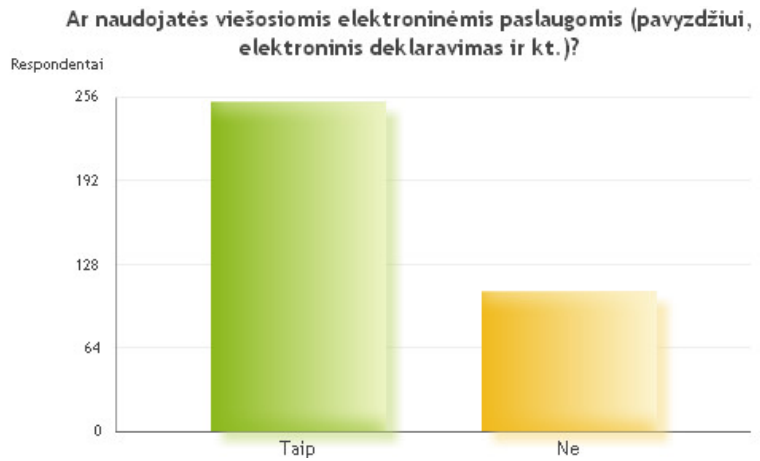
5.2.2. Vartotojų tyrimas

(vartotojų anketos pavyzdys pateikiamas 2 priede)

1. Ar naudojatės viešosiomis elektroninėmis paslaugomis (pavyzdžiui, elektroninis deklaravimas ir kt.)?

Taip	252	70,2 %
Ne	107	29,8 %
Iš viso atsakymų	359	

Iš 359 respondentų dažniausias atsakymas buvo „taip".

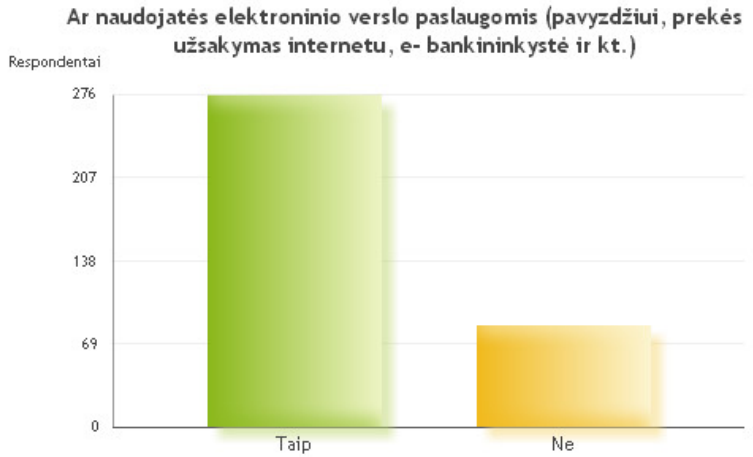


Atsižvelgiant į tai, kad respondentai yra asmenys, aktyviai besinaudojantys internetu (sugebėję užpildyti anketą, surandamą tik per internetinį portalą www.zebra.lt), buvo santykinai didelė dalis (29,8 proc.) asmenų,atsakiusių, kad nesinaudoja viešosiomis elektroninėmis paslaugomis.

2. Ar naudojatės elektroninio verslo paslaugomis (pavyzdžiui, prekės užsakymas internetu, e. bankininkystė ir kt.)?

Taip	275	76,6 %
Ne	84	23,4 %
Iš viso atsakymų	359	

Iš 359 respondentų dažniausias atsakymas buvo „taip".

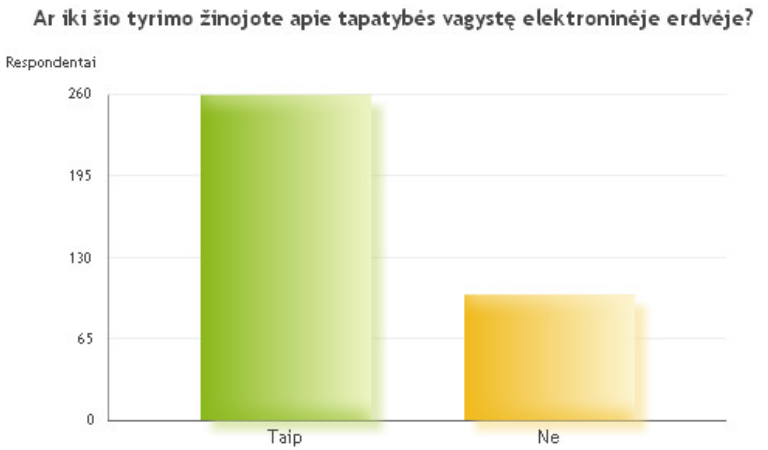


Elektroninio verslo paslaugomis naudojasi 6,4 proc. daugiau vartotojų negu viešosiomis paslaugomis. Tai rodo, kad tarp vartotojų privataus sektoriaus paslaugomis šiek tiek daugiau naudojamasi nei viešosiomis paslaugomis. Apibendrinant galima teigti, kad vis dar nemaža dalis asmenų, besinaudojančių internetu, nesinaudoja viešosiomis ir elektroninio verslo paslaugomis.

3. Ar iki šio tyrimo žinojote apie tapatybės vagystę elektroninėje erdvėje?

Taip	259	72,1 %
Ne	100	27,9 %
Iš viso atsakymų	359	

Iš 359 respondentų dažniausias atsakymas buvo „taip".

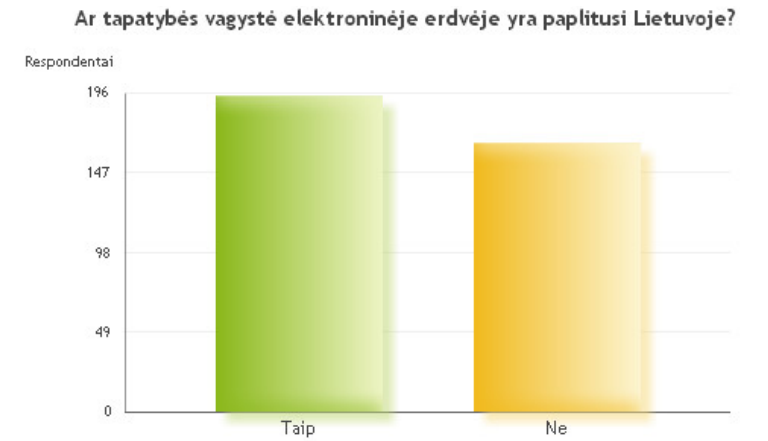


Didelė dalis vartotojų (72,1 proc.) teigia, kad tapatybės vagystės elektroninėje erdvėje problema jiems yra žinoma. Tačiau nemaža dalis (27,9 proc.) vartotojų iki šio tyrimo anketos pildymo nieko nežinojo apie tapatybės vagystę elektroninėje erdvėje.

4. Ar tapatybės vagystė elektroninėje erdvėje yra paplitusi Lietuvoje?

Taip	194	54 %
Ne	165	46 %
Iš viso atsakymų	359	

Iš 359 respondentų dažniausias atsakymas buvo „taip“

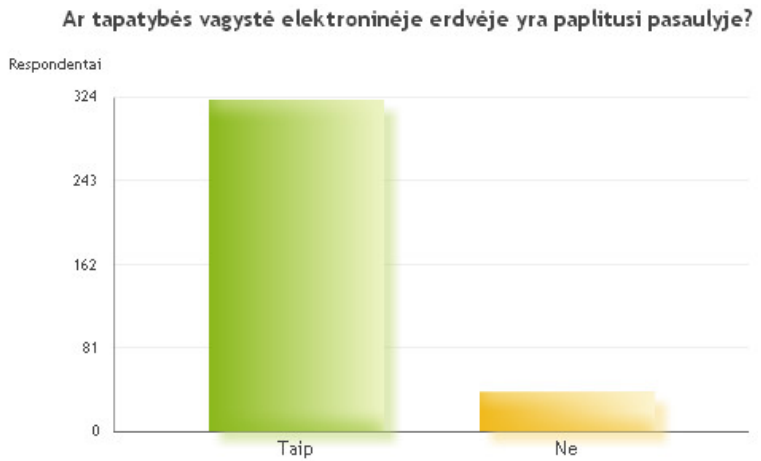


Respondentų nuomonės dėl tapatybės vagystės paplitimo Lietuvoje pasiskirstė beveik po lygiai. Keliais procentais daugiau buvo manančių, kad tapatybės vagystė elektroninėje erdvėje Lietuvoje yra palitusi. Atsižvelgiant į net 54 proc. respondentų teiginius, kad šis neigiamas reiškinys Lietuvoje yra paplitęs, galima teigti, kad problema egzistuoja ir turi būti detaliau tiriama.

5. Ar tapatybės vagystė elektroninėje erdvėje yra paplitusi pasaulyje?

Taip	321	89,4 %
Ne	38	10,6 %
Iš viso atsakymų	359	

Iš 359 respondentų dažniausias atsakymas buvo „taip“

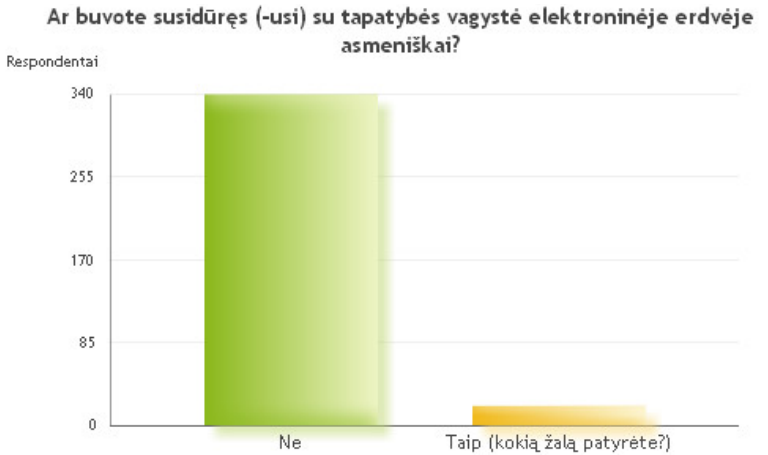


Respondentai, vertindami tiriamojo reiškinio palitimą pasaulyje, mano, kad tapatybės vagystė elektroninėje erdvėje yra paplitusi pasaulio mastu (89,4 proc.). Šie atsakymai rodo, kad respondentai atriboja Lietuvos elektroninę erdvę ir joje vykstančius reiškinius nuo globalios, manydami, kad Lietuvoje elektroninė erdvė yra saugesnė.

6. Ar teko susidurti su tapatybės vagyste elektroninėje erdvėje asmeniškai?

Ne	339	94,4 %
Taip (kokią žalą patyrėte?)	20	5,6 %
Iš viso atsakymų	359	

Iš 359 respondentų dažniausias atsakymas buvo „ne“.

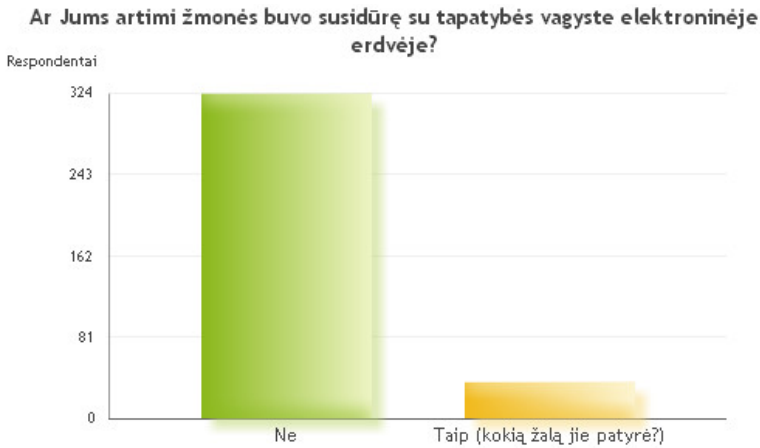


Didžioji dauguma (94,4 proc.) respondentų patys nebuvo susidūrę su tapatybės vagyste elektroninėje erdvėje, tačiau asmenų, susidūrusių su šiuo neigiamu reiškiniu, papildomi atsakymai rodo, kad daugeliu atvejų tai buvo tikrai tapatybės vagystė, t. y. asmenys gerai identifikuoja šį reiškinį (pvz.: mano elektroninį paštą pavogė ir apsimetė, kad esu žiauriai sužalota, pasinaudojo mano vardu, buvo naudotasi mano asmeninėmis nuotraukomis pažinčių svetainėse), tačiau dalis konkretesnių atsakymų leidžia abejoti (nors kategoriškai teigti nėra pagrindo), ar tikrai tai buvo tapatybės vagystė elektroninėje erdvėje (pvz., bankas apsiskaičiavo). Vertinant patirtą žalą respondentai vardijo sumas nuo 50 litų iki kelių tūkstančių (pvz.: 10 000£), nors vienas respondentas įvardijo ir itin didelę sumą 500 000 nežinomos valiutos. Respondentai kaip svarbią netektį taip pat įvardijo ir moralinę žalą.

7. Ar Jums artimi žmonės buvo susidūrę su tapatybės vagyste elektroninėje erdvėje?

Ne	323	90 %
Taip (kokią žalą jie patyrė?)	36	10 %
Iš viso atsakymų	359	

Iš 359 respondentų dažniausias atsakymas buvo „ne".



Respondentai pažymi, kad jų artimi žmonėsi susidūrė su tapatybės vagyste elektroninėje erdvėje beveik du kartus dažniau negu jie patys (5,6 proc. ir 10 proc.), tačiau dauguma respondentų nežinojo tokių atvejų, kad jų artimi žmonės būtų susidūrę su šiuo reiškiniu. Kaip ir savo tapatybės vagystės elektroninėje erdvėje atvejais, respondentai artimų žmonių susidūrimo su šiuo reiškiniu atvejais nurodydavo skirtingas prarastas sumas, tačiau didesnės sumos buvo nurodomos dažniau. Tapatybės vagystę elektroninėje erdvėje respondentai sieja su finansinėmis paslaugomis ir su kitais santykiais elektroninėje erdvėje (pvz.: suklastota interneto svetainė ir kt.).

8. Ar tapatybės vagystė elektroninėje erdvėje pavojingas reiškinys?

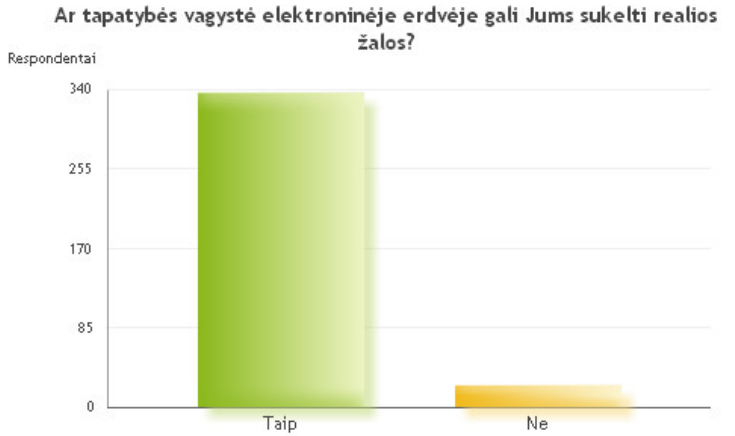
Iš 359 respondentų vidutinis atsakymas yra 8,47 (skalėje nuo 1 iki 10).
Mažiausias atsakymas yra 1, didžiausias – 10.

Vertindami reiškinio pavojingumą respondentų dešimties balų skalėje vidurkis buvo 8,47 balo. Nors didžioji dauguma respondentų reiškinį vertino 10 balų, tačiau buvo manančių, kad reiškinys nėra toks pavojingas.

9. Ar tapatybės vagystė elektroninėje erdvėje gali Jums sukelti realios žalos?

Taip	336	93,6 %
Ne	23	6,4 %
Iš viso atsakymų	359	

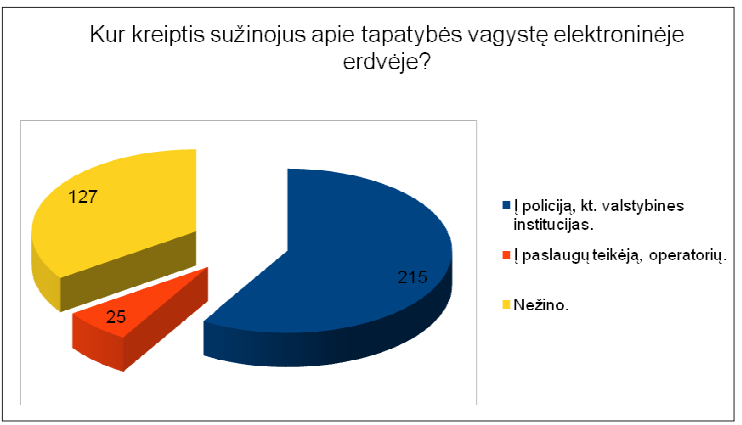
Iš 359 respondentų dažniausias atsakymas buvo „taip".



Vertindami, ar tapatybės vagystė elektroninėje erdvėje gali padaryti realios žalos, asmenys suvokia, kad reiškinys gali pakenkti ir jiems (93,6 proc.), nors nedidelė dalis (6,4 proc.) respondentų jautėsi saugūs ir nemanė, kad juos tai gali neigiamai paveikti.

10. Kur kreiptis sužinojus apie tapatybės vagystę elektroninėje erdvėje?

Vartotojų atsakymai pavaizduoti 41 pav. Atsakydami į atvirą klausimą, kur kreiptis sužinojus apie tapatybės vagystę elektroninėje erdvėje didžioji dauguma respondentų manė, kad į policiją ar kitas teisėsaugos institucijas (pvz., prokuratūra, FNTT), dalis nurodė, kad kreiptųsi į paslaugų teikėją / operatorių. Net 127 iš 359 vartotojų nežinojo, kur kreiptis, sužinojus apie tapatybės vagystę. Tai sudaro net 35,4 proc. visų apklaustų vartotojų.

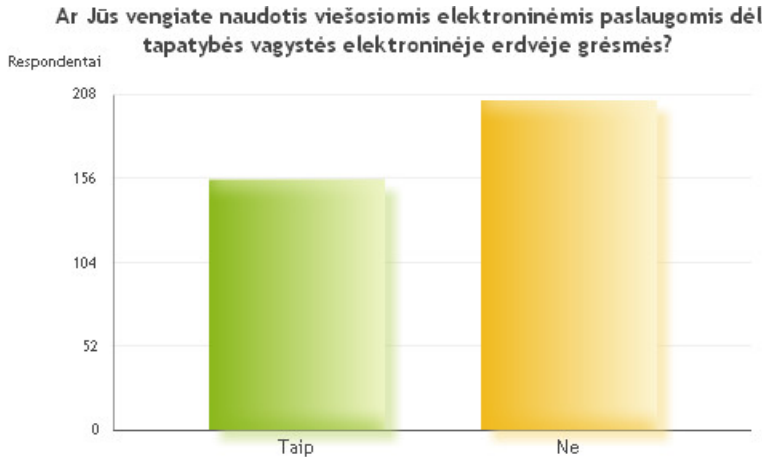


41 pav. Vartotojų atsakymai į klausimą: „Kur kreiptis sužinojus apie tapatybės vagystę elektroninėje erdvėje“?

11. Ar Jūs vengiate naudotis viešosiomis elektroninėmis paslaugomis dėl tapatybės vagystės elektroninėje erdvėje grėsmės?

Taip	155	43,2 %
Ne	204	56,8 %
Iš viso atsakymų	359	

Iš 359 respondentų dažniausias atsakymas buvo „ne".

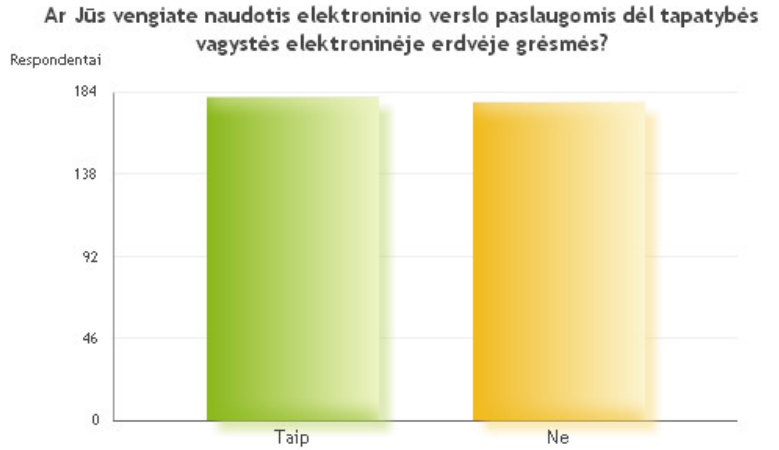


Beveik pusė respondentų (43,2 proc.) nurodė, kad vengia naudotis viešosiomis elektroninėmis paslaugomis, bes bijo tapatybės vagystės elektroninėje erdvėje.

12. Ar Jūs vengiate naudotis elektroninio verslo paslaugomis dėl tapatybės vagystės elektroninėje erdvėje grėsmės?

Taip	181	50,4 %
Ne	178	49,6 %
Iš viso atsakymų	359	

Iš 359 respondentų dažniausias atsakymas buvo „taip".



Truputį daugiau negu pusė respondentų (50,4 proc.) vengė naudotis privataus sektoriaus teikiamomis elektroninėmis paslaugomis, nes bijojo tapatybės vagystės elektroninėje erdvėje.

13. Ar naudodamiesi elektroninio verslo paslaugomis bijote, kad galite nukentėti nuo tapatybės vagystės elektroninėje erdvėje / tapti tapatybės vagystės elektroninėje erdvėje auka?

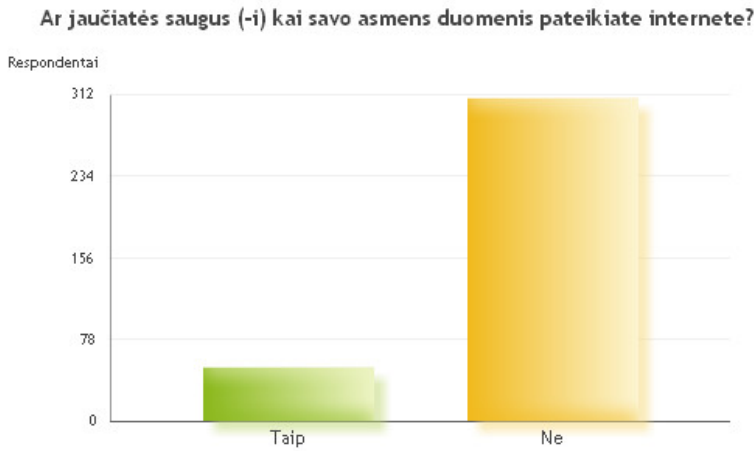
Iš 359 respondentų vidutinis atsakymas buvo 7,24 (skalėje nuo 1 iki 10).
Mažiausias atsakymas buvo 1, didžiausias – 10.

Respondentai, kurie naudojasi elektroninio verslo paslaugomis, baimę nukentėti nuo tapatybės vagystės dešimties balų sistemoje įvertino vidutiniškai 7,24 proc. Dažniausiai pasitaikantis atsakymas buvo 10 balų, nors nemažai respondentų savo baimę įvertino ir 5 balais.

14. Ar jaučiatės saugūs, kai asmens duomenis pateikiate internete?

Taip	51	14,2 %
Ne	308	85,8 %
Iš viso atsakymų	359	

Iš 359 respondentų dažniausias atsakymas buvo „ne".

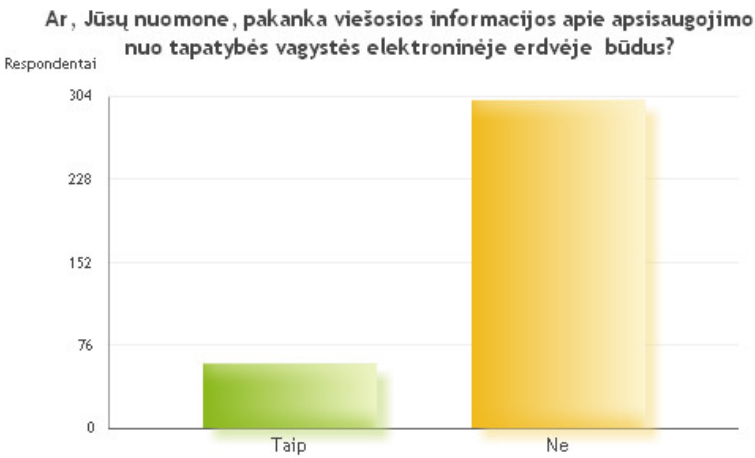


85,8 proc. apklaustųjų nesijautė saugūs atskleisdami savo duomenis internete, tačiau net 14,2 proc. respondentų nemanė, kad tai jiems gali sukelti nepatogumų.

15. Ar, Jūsų nuomone, pakanka viešosios informacijos apie apsisaugojimo nuo tapatybės vagystės elektroninėje erdvėje būdus?

Taip	59	16,4 %
Ne	300	83,6 %
Iš viso atsakymų	359	

Iš 359 respondentų dažniausias atsakymas buvo „ne".

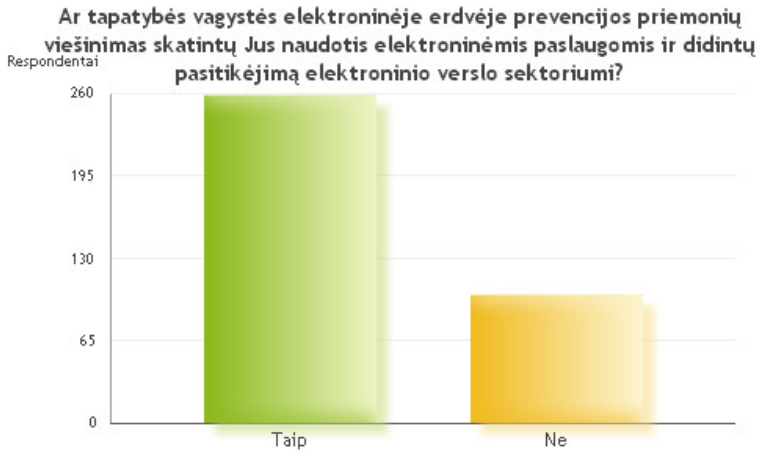


Dauguma vartotojų (83,6 proc.) mano, kad viešosios informacijos apie apsisaugojimo būdus nuo tapatybės vagystės elektroninėje erdvėje būdus nepakanka. Kita dalis apklaustųjų mano, kad tokios informacijos yra pakankamai.

16. Ar tapatybės vagystės elektroninėje erdvėje prevencijos priemonių viešinimas skatintų Jus naudotis elektroninėmis paslaugomis ir didintų pasitikėjimą elektroninio verslo sektoriumi?

Taip	258	71,9 %
Ne	101	28,1 %
Iš viso atsakymų	359	

Iš 359 respondentų dažniausias atsakymas buvo „taip".



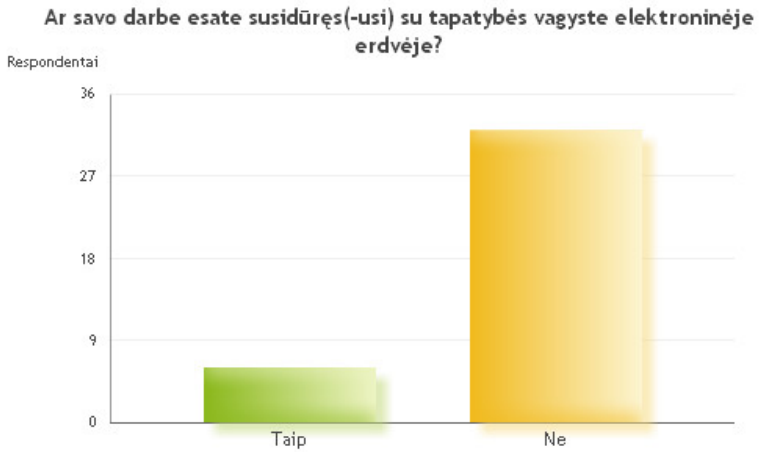
71,9 proc. respondentų nurodė, kad juos naudotis elektroninėmis paslaugomis skatintų ir pasitikėjimą elektroninio verslo sektoriumi didintų tapatybės vagystės elektroninėje erdvėje prevencijos priemonių viešinimas. 28,1 proc. apklaustųjų nemano, kad tai turėtų įtakos jų elgesiui.

5.2.3. **Viešojo sektoriaus tyrimas** (viešojo sektoriaus anketos pavyzdys pateiktas 2 priede)

1. Ar savo darbe esate susidūrę su tapatybės vagyste elektroninėje erdvėje?

Taip	6	15,8 %
Ne	32	84,2 %
Iš viso atsakymų	38	

Iš 38 respondentų dažniausias atsakymas buvo „ne".

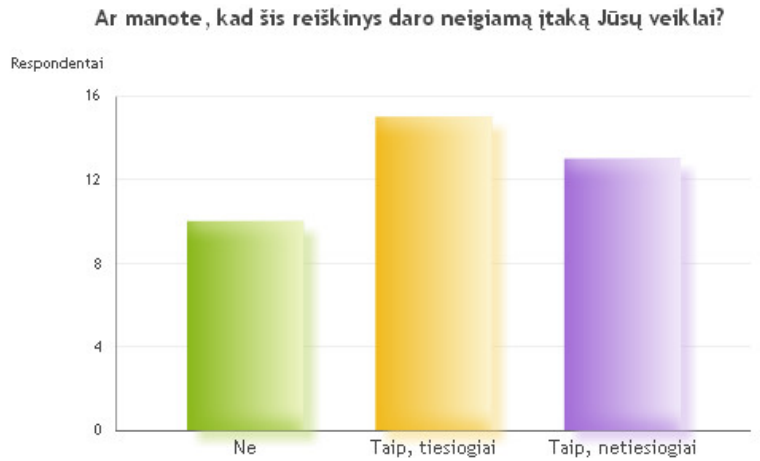


Skirtingai nuo Sodros darbuotojų, viešojo sektoriaus darbuotojai – respondentai apskritai dažniau (net 15,8 proc. viešojo sektoriaus, 4,9 proc. Sodros darbuotojų) savo darbe susidūrė su tapatybės vagyste elektroninėje erdvėje.

2. Ar manote, kad šis reiškinys daro neigiamą įtaką Jūsų veiklai?

Ne	10	26,3 %
Taip, tiesiogiai	15	39,5 %
Taip, netiesiogiai	13	34,2 %
Iš viso atsakymų	38	

Iš 38 respondentų dažniausias atsakymas buvo „taip, tiesiogiai".
Rečiausias atsakymas buvo „ne".



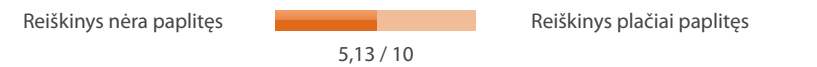
Viešojo sektoriaus darbuotojų – respondentų nuomonė apie neigiamą tiriamojo reiškinio įtaką jų darbinei veiklai buvo beveik identiška Sodros darbuotojų apklausos rezultatams: atsakiusiųjų, kad reiškinys apskritai nedaro įtakos, viešojo sektoriaus respondentų buvo 26,3 proc., Sodros darbuotojų – 25,9 proc.; manančiųjų, kad šis reiškinys daro tiesioginę neigiamą įtaką apskritai, iš viešojo sektoriaus buvo 39,5 proc., Sodros – 39,9 proc., o manančiųjų, kad daro netiesioginę neigiamą įtaką, iš viešojo sektoriaus buvo 34,2 proc., o Sodros – 34,2 proc.

3. Kaip vertinate šio reiškinio pavojingumą?

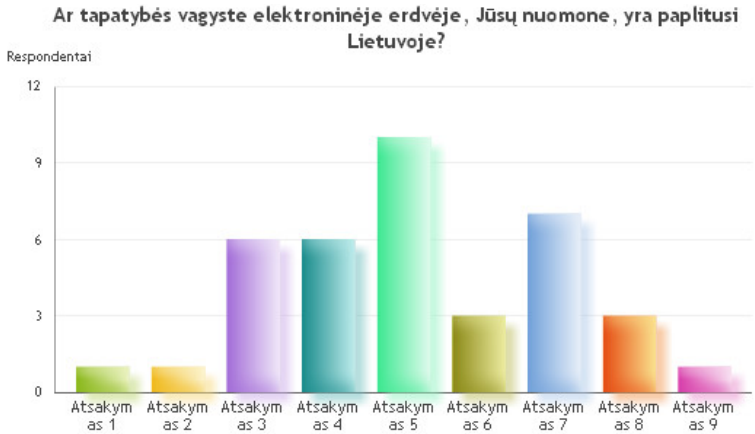
Iš 38 respondentų vidutinis atsakymas buvo 8,55 (skalėje nuo 1 iki 10).
Mažiausias atsakymas buvo 5, didžiausias – 10.

Vertinant reiškinio pavojingumą dešimtbalėje sistemoje viešojo sektoriaus darbuotojų respondentų vidurkio balas buvo labai panašus kaip Sodros (viešojo sektoriaus 8,55 balo, Sodros 8,34 balo), tačiau, skirtingai nuo Sodros darbuotojų, vertinusių 10 balų, viešojo sektoriaus buvo proporcingai mažiau.

4. Ar, Jūsų nuomone, tapatybės vagystė elektroninėje erdvėje yra paplitusi Lietuvoje?



Iš 38 respondentų vidutinis atsakymas buvo 5,13 (skalėje nuo 1 iki 10).
Mažiausias atsakymas buvo 1, didžiausias – 9.



Reiškinio paplitimą Lietuvoje viešojo sektoriaus darbuotojai (vidurkis 5,13 balai iš 10 galimų) vertino labai panašiai kaip Sodros darbuotojai (vidurkis 5,41 balai iš 10 galimų).

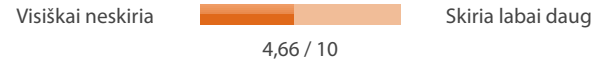
5. Ar tapatybės vagyste elektroninėje erdvėje gali sukelti neigiamų padarinių Jūsų organizacijos veiklai? (galite pasirinkti ne vieną atsakymą; yra daug galimų variantų)

Neigiamų padarinių sukelti negali;	1	0,7 %
Gali, institucijos reputacijai;	26	18,3 %
Gali, asmens garbei ir orumui;	20	14,1 %
Gali, finansinių (pvz., nuostoliai, negautos pajamos);	17	12 %
Gali, kitų turtinių;	10	7 %
Gali, privatumui;	23	16,2 %
Gali, duomenų saugumui;	30	21,1 %
Gali, vartotojų teisėms;	14	9,9 %
Gali, kita (nurodykite).	1	0,7 %
Iš viso atsakymų	142	

Iš 38 respondentų dažniausias atsakymas buvo „gali, duomenų saugumui".
Rečiausias atsakymai buvo „neigiamų padarinių sukelti negali"; „gali, kita (nurodykite)".

Vertindami galimus neigiamus padarinius darbovietei respondentai rinkosi labai panašius atsakymus; kad neigiamų padarinių šis reiškinys sukelti negali, vertino 0,7 proc. viešojo sektoriaus darbuotojų ir 0,4 proc. Sodros darbuotojų; kaip pagrindinę riziką – galimą poveikį duomenų saugumui atitinkamai įvertino 21,1 proc. ir 22,8 proc.

6. Ar pakankamai Jūsų organizacija skiria lėšų apsaugai nuo tapatybės vagystės elektroninėje erdvėje?



Iš 38 respondentų vidutinis atsakymas buvo 4,66 (skalėje nuo 1 iki 10). Mažiausias atsakymas buvo 1, didžiausias – 9.

Sodros darbuotojai mano, kad jų organizacijoje daugiau lėšų skiriama apsaugai nuo tiriamojo reiškinio, tad jie situaciją vertino 6,57 balo iš 10 galimų, o viešojo sektoriaus darbuotojai apskritai situaciją vertino 4,66 balo iš 10 galimų.

7. Ar pakankamai Jūsų organizacija imasi priemonių kovai su tapatybės vagyste elektroninėje erdvėje ir jos prevencijai?

Ne	28	73,7 %
Taip (nurodykite, kokių):	10	26,3 %
Iš viso atsakymų	38	

Iš 38 respondentų dažniausias atsakymas buvo „ne“.

Skirtingai nuo Sodros darbuotojų, viešojo sektoriaus darbuotojai apskritai mano, kad jų organizacijos nepakankamai imasi priemonių kovai su tapatybės vagyste ir jos prevencijai elektroninėje erdvėje, taip manė net 73,7 proc., o tuo pat metu Sodros darbuotojų, manančių, kad tokių priemonių nepakanka, buvo tik 31,9 proc. Apskritai viešojo sektoriaus laisvų kometarų buvo nedaug, tačiau respondentai paminėjo ir technines (pvz., antiviruisinė įranga) ir organizacines priemones (pvz., greitas reagavimas į incidentus).

8. Ar, Jūsų nuomone, pakanka viešosios informacijos apie tapatybės vagystės elektroninėje erdvėje pavojingumą ir apsisaugojimo nuo tapatybės vagystės elektroninėje erdvėje būdus?

Visiškai nėra informacijos — Yra labai daug informacijos

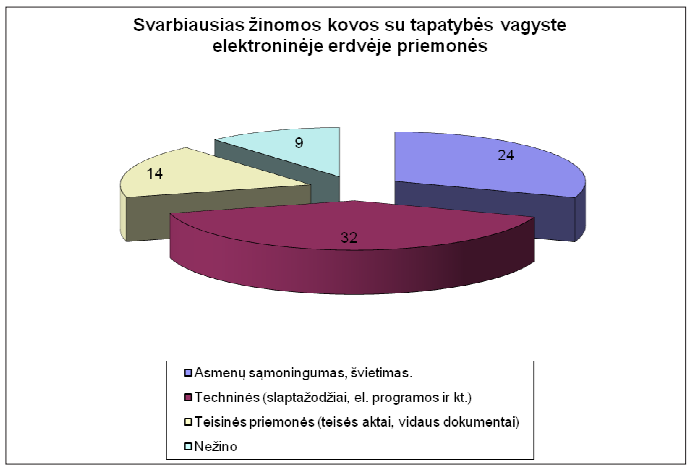
4 / 10

Iš 38 respondentų vidutinis atsakymas buvo 4 (skalėje nuo 1 iki 10).
Mažiausias atsakymas buvo 1, didžiausias – 9.

Viešosios informacijos pakankamumą apskritai viešojo sektoriaus darbuotojai vertino labai panašiai, t. y. 4 balais iš 10, o Sodros darbuotojai – 4,79 balais iš 10.

9. Nurodykite tris svarbiausias Jums žinomas kovos su tapatybės vagyste elektroninėje erdvėje priemones.

Viešojo sektoriaus darbuotojai (kaip ir Sodros darbuotojai), vardydami svarbiausias jiems žinomas kovos su tapatybės vagyste elektroninėje erdvėje priemones apskritai, pateikė gana profesionalių atsakymų iš esmės išvardydami beveik visas svarbesnes priemones. Šios priemonės apibendrintai pavaizduotinos 42 pav.



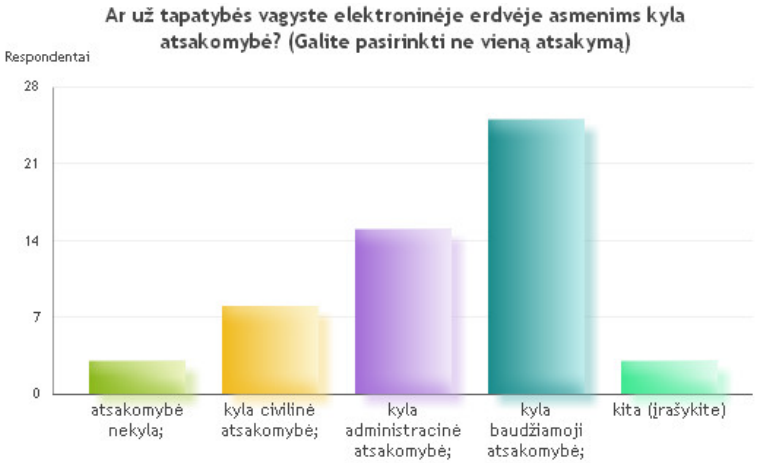
42 pav. Darbuotojų nurodytos kovos su tapatybės vagyste elektroninėje erdvėje priemonės

10. Ar už tapatybės vagyste elektroninėje erdvėje asmenims kyla atsakomybė? (Galite pasirinkti ne vieną atsakymą) (daug galimų variantų)

Atsakomybė nekyla;	3	5,6 %
Kyla civilinė atsakomybė;	8	14,8 %

Kyla administracinė atsakomybė;	15	27,8 %
Kyla baudžiamoji atsakomybė;	25	46,3 %
Kita (įrašykite)	3	5,6 %
Iš viso atsakymų	54	

Iš 38 respondentų dažniausias atsakymas buvo „kyla baudžiamoji atsakomybė“; Rečiausi atsakymai buvo „atsakomybė nekyla“, „kita (įrašykite)“.

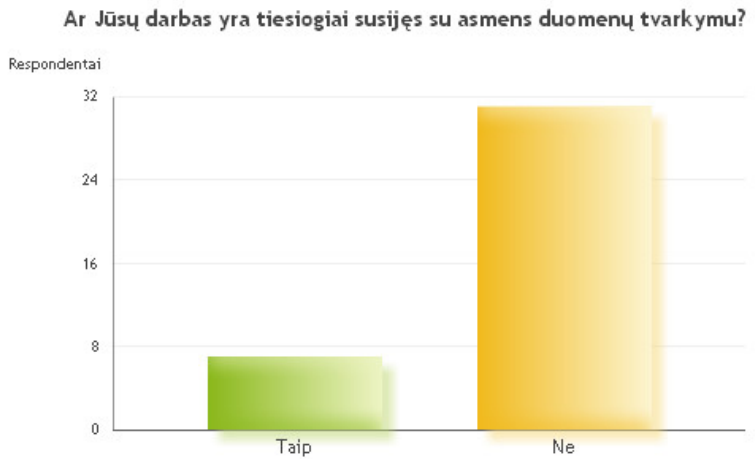


Apskritai viešojo sektoriaus darbuotojai dvigubai daugiau pasirinko atsakymą, kad atsakomybė nekyla (5,6 proc.) negu Sodros darbuotojai (2,1 proc.), nors kaip ir Sodros darbuotojai (43,1 proc.) dauguma viešojo sektoriaus darbuotojų (46,3 proc.) teigė, kad baudžiamoji atsakomybė kyla.

11. Ar Jūsų darbas yra tiesiogiai susijęs su asmens duomenų tvarkymu?

Taip	7	18,4 %
Ne	31	81,6 %
Iš viso atsakymų	38	

Iš 38 respondentų dažniausias atsakymas buvo „ne“.



Skirtingai nuo Sodros darbuotojų, apskritai viešojo sektoriaus darbuotojų (respondentai) darbas nebuvo dažniau tiesiogiai susijęs su asmens duomenų tvarkymu. Respondentų, viešajame sektoriuje tiesiogiai susijusių su asmens duomenų tvarkymu, buvo tik 18,4 proc., o Sodros darbuotojų (respondentų) – 78,3 proc.

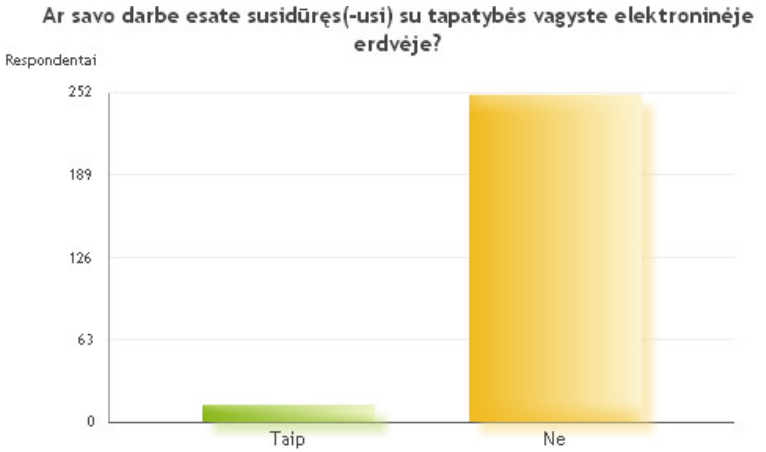
5.2.4. Sodros darbuotojų tyrimas

(Sodros darbuotojų anketos pavyzdys pateiktas 2 priede)

1. Ar savo darbe esate susidūręs(-usi) su tapatybės vagyste elektroninėje erdvėje?

Taip	13	4,9 %
Ne	250	95,1 %
Iš viso atsakymų	263	

Iš 263 respondentų dažniausias atsakymas buvo „ne".

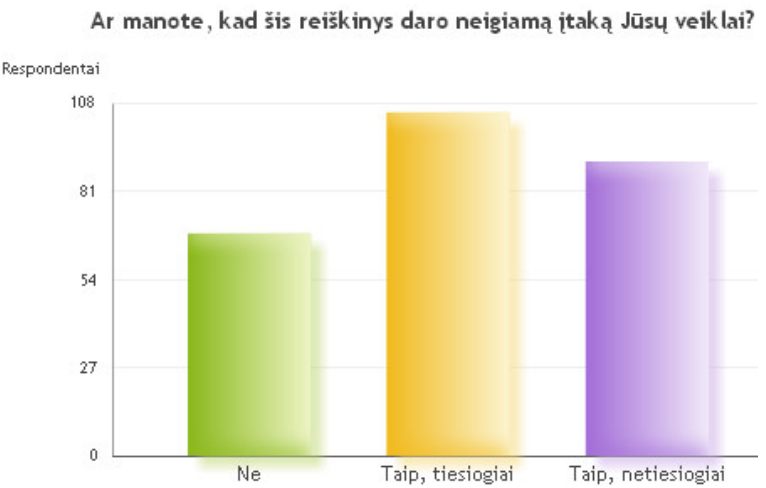


Didžioji dauguma (95,1 proc.) Sodros darbuotojų neigė, kad darbe buvo susidūrę su tapatybės vagyste elektroninėje erdvėje.

2. Ar manote, kad šis reiškinys daro neigiamą įtaką Jūsų veiklai?

Ne	68	25,9 %
Taip, tiesiogiai	105	39,9 %
Taip, netiesiogiai	90	34,2 %
Iš viso atsakymų	263	

Iš 263 respondentų dažniausias atsakymas buvo „taip, tiesiogiai".
Rečiausias atsakymas buvo „ne".



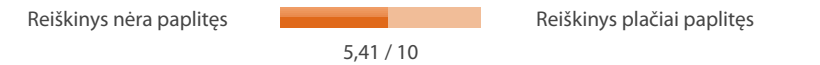
Vertindami tapatybės vagystės elektroninėje erdvėje įtaką veiklai didžioji dauguma respondentų (74,1 proc.) atsakė, kad tiesiogiai (39,9 proc.) arba netiesiogiai (34,2 proc.) šis reiškinys daro neigiamą įtaką. Ketvirtis (25,9 proc.) apklaustųjų nemanė, kad reiškinys daro neigiamą įtaką. Pažymėtina, kad su tapatybės vagyste buvo susidūrę tik 4,9 proc., bet manančiųjų, kad reiškinys daro neigiamą įtaką, buvo gerokai daugiau, tai rodo, kad net nesusidūrę su šiuo reiškiniu asmenys suvokia jo neigiamą poveikį savo veiklai.

3. Kaip vertinate šio reiškinio pavojingumą?

Iš 263 respondentų vidutinis atsakymas buvo 8,34 (skalėje nuo 1 iki 10).
Mažiausias atsakymas buvo 1, didžiausias buvo 10.

Reiškinio pavojingumą Sodros darbuotojai dešimties balų sistemoje įvertino panašiai kaip ir vartotojai (vartotojų vertinimo vidurkis – 8,47 proc.), Sodros darbuotojai pavojingumą įvertino vidutiniškai 8,34 balo, nors dauguma rinkosi 10 balų.

4. Ar, Jūsų nuomone, tapatybės vagystė elektroninėje erdvėje yra paplitusi Lietuvoje?



Iš 263 respondentų vidutinis atsakymas buvo 5,41 (skalėje nuo 1 iki 10).
Mažiausias atsakymas buvo 1, didžiausias – 10.

Reiškinio paplitimą Lietuvoje respondentai dešimties balų sistemoje vidutiniškai įvertino 5,41 balo. Dažniausiai buvo pasirenkami 5 balai, nors nemažai pasirinko 3–4 ir 6–8 balus.

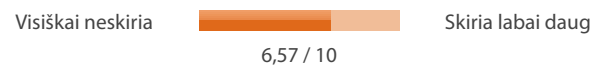
5. Ar tapatybės vagyste elektroninėje erdvėje gali sukelti neigiamų padarinių Jūsų organizacijos veiklai? (Galite pasirinkti ne vieną atsakymą) (daug galimų variantų)

Neigiamų padarinių sukelti negali;	4	0,4 %
Gali, institucijos reputacijai;	201	20,8 %
Gali, asmens garbei ir orumui;	120	12,4 %
Gali, finansinių (pvz., nuostoliai, negautos pajamos);	138	14,3 %
Gali, kitų turtinių;	54	5,6 %
Gali, privatumui;	153	15,9 %
Gali, duomenų saugumui;	220	22,8 %
Gali, vartotojų teisėms;	73	7,6 %
Gali, kita (nurodykite):	2	0,2 %
Iš viso atsakymų	965	

Iš 263 respondentų dažniausias atsakymas buvo „gali, duomenų saugumui“; Rečiausias atsakymas buvo „gali, kita (nurodykite)“.

Vertindami, ar gali tapatybės vagystė elektroninėje erdvėje sukelti neigiamų padarinių respondentų darbovietei, manančiųjų, kad gali sukelti neigiamų padarinių, buvo net 99,6 proc., manančiųjų, kad neigiami padariniai nėra galimi, buvo absoliuti mažuma (0,4 proc.). Respondentai, manantys, kad reiškinys gali sukelti neigiamų padarinių, dažniausiai pasirinko, kad gali nukentėti duomenų saugumas ir institucijos reputacija.

6. Ar pakankamai Jūsų organizacija skiria lėšų apsaugai nuo tapatybės vagystės elektroninėje erdvėje?



Iš 263 respondentų vidutinis atsakymas buvo 6,57 (skalėje nuo 1 iki 10). Mažiausias balas buvo 1, didžiausias – 10.

Savo organizacijos finansavimo, skiriamo apsaugai nuo tapatybės vagystės elektroninėje erdvėje, respondentų dešimties balų skalėje vertinimo vidurkis buvo 6,57 balo. Dažniausiai buvo vertinama 5 balais, bet nemažai ir 8–9 balais.

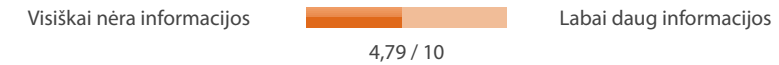
7. Ar pakankamai Jūsų organizacija imasi priemonių kovai su tapatybės vagyste elektroninėje erdvėje ir jos prevencijai?

Ne	84	31,9 %
Taip (nurodykite, kokių):	179	68,1 %
Iš viso atsakymų	263	

Vertindami organizacijoje taikomų priemonių kovai su tapatybės vagyste pakankamumą 31,9 proc. respondentų nurodė, kad tokių priemonių nepakanka, nors dauguma (68,1 proc.) manė, kad jų pakanka. Vardydami konkrečias kovos su tapatybės vagyste elektroninėje erdvėje priemones respondentai atskleidė, kad šios priemonės jiems žinomos, buvo išvardytos visos galimos prevencijos priemonės. Šie atsakymai pavaizduoti 43 pav.

43 pav. Respondentų nurodytos organizacijos prevencinės kovos su tapatybės vagyste elektroninėje erdvėje priemonės

8. Ar, Jūsų nuomone, pakanka viešosios informacijos apie tapatybės vagystės elektroninėje erdvėje pavojingumą ir apsisaugojimo nuo tapatybės vagystės elektroninėje erdvėje būdus?

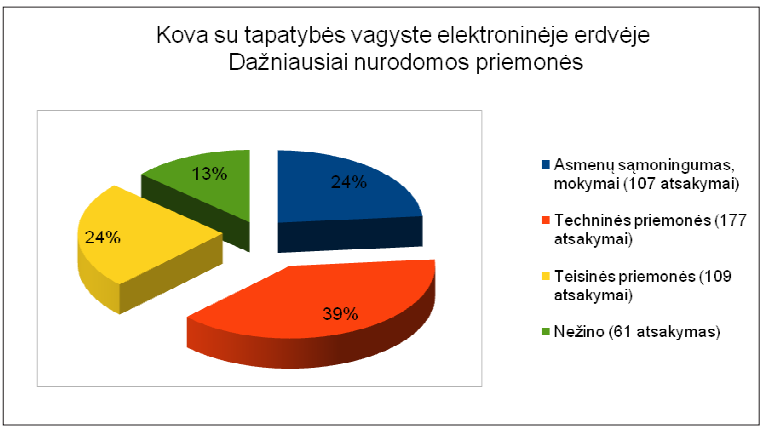


Iš 263 respondentų vidutinis atsakymas yra 4,79 (skalėje nuo 1 iki 10). Mažiausias balas buvo 1, didžiausias – 10.

Vertinant viešos informacijos pakankamumą apie tapatybės vagystės elektroninėje erdvėje pavojingumą ir apsisaugojimo nuo tapatybės vagystės elektroninėje erdvėje būdus dešimties balų skalėje respondentų vidurkis buvo 4,79 balo. Dažniausiai buvo pasirenkami 3 ir 5 balai.

9. Nurodykite tris svarbiausias Jums žinomas kovos su tapatybės vagyste elektroninėje erdvėje priemones.

Respondentai, vardydami tris svarbiausias jiems žinomas kovos su tapatybės vagyste elektroninėje erdvėje priemones, nurodė visas svarbiausias kovos su šiuo reiškiniu priemones. Atsakymai pavaizduoti 44 pav.



44 pav. Respondentų dažniausiai nurodytos trys svarbiausios kovos su tapatybės vagyste elektroninėje erdvėje priemonės

10. Ar už tapatybės vagystę elektroninėje erdvėje asmenims kyla atsakomybė? (Galite pasirinkti ne vieną atsakymą; daug galimų variantų)

Kyla administracinė atsakomybė;	138	32,7 %
Kyla baudžiamoji atsakomybė;	182	43,1 %
Kita (įrašykite)	22	5,2 %
Iš viso atsakymų	422	

•
•
• nežinau

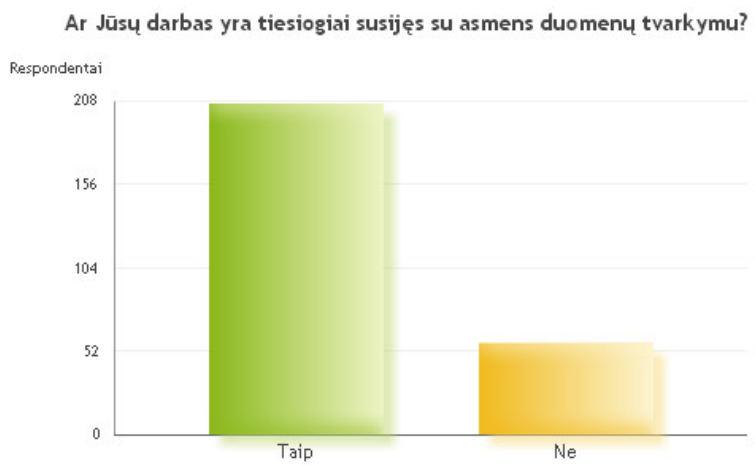
Iš 263 respondentų dažniausias atsakymas buvo „kyla baudžiamoji atsakomybė“; Rečiausias atsakymas buvo „atsakomybė nekyla“.

Tik 2,1 proc. respondentų manė, kad už tapatybės vagystę elektroninėje erdvėje atsakomybė nekyla. Dauguma manė, kad kyla baudžiamoji (43,1 proc.) arba administracinė (32,7 proc.) atsakomybė. Laisvai atsakydami dalis vartotojų prisipažino, kad nežino, tačiau buvo ir konkrečių atsakymų (pvz., ji nėra kriminalizuota, o yra kitų nusikalstamų veikų sudedamoji dalis, LR Baudžiamasis kodeksas to nenumato“).

11. Ar Jūsų darbas yra tiesiogiai susijęs su asmens duomenų tvarkymu?

Taip	206	78,3 %
Ne	57	21,7 %
Iš viso atsakymų	263	

Iš 263 respondentų dažniausias atsakymas buvo „taip“.



78,3 proc. respondentų nurodė, kad jų darbas tiesiogiai susijęs su asmens duomenų tvarkymu

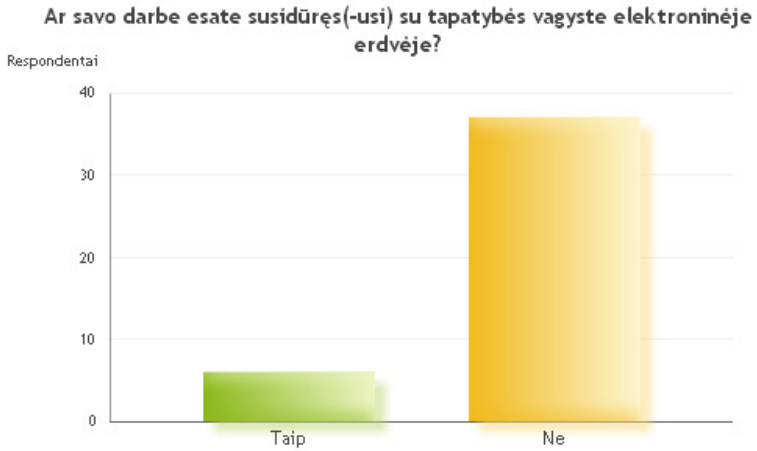
5.2.5. Verslo darbuotojų tyrimas

(verslo sektoriaus anketos pavyzdys pateiktas 2 priede)

1. Ar savo darbe esate susidūręs(-usi) su tapatybės vagyste elektroninėje erdvėje?

Taip	6	14 %
Ne	37	86 %
Iš viso atsakymų	43	

Iš 43 respondentų dažniausias atsakymas buvo „ne".

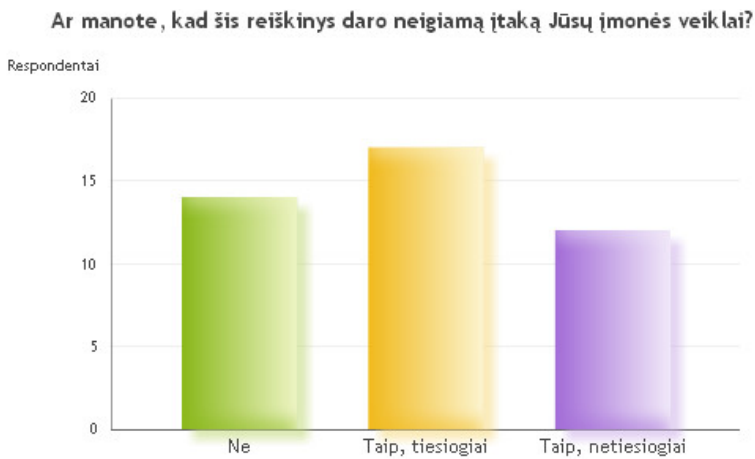


Net 14 proc. verslo atstovų nurodė, kad savo darbe yra susidūrę su tapatybes vagyste elektroninėje erdvėje. Tai didžiausias procentas iš visų apklaustų respondentų grupių.

2. Ar manote, kad šis reiškinys daro neigiamą įtaką Jūsų įmonės veiklai?

Ne	14	32,6 %
Taip, tiesiogiai	17	39,5 %
Taip, netiesiogiai	12	27,9 %
Iš viso atsakymų	43	

Iš 43 respondentų dažniausias atsakymas buvo „taip, tiesiogiai".
Rečiausias atsakymas buvo „taip, netiesiogiai".



32,6 proc. respondentų nemano, kad tapatybės vagystė elektroninėje erdvėje daro neigiamą įtaką jų įmonės veiklai. Manančiųjų, kad reiškinys daro tiesioginę neigiamą įtaką buvo daugiausia – 39,5 proc., o kartu su manančiais, kad reiškinys daro netiesioginę įtaką (27,9 proc.) jų įmonės veiklai iš viso buvo 67,4 proc.

3. Kaip vertinate šio reiškinio pavojingumą?

Reiškinys visiškai nepavojingas — Reiškinys labai pavojingas

8,4 / 10

Iš 43 respondentų vidutinis atsakymas buvo 8,4 (skalėje nuo 1 iki 10).
Mažiausias balas buvo 3, didžiausias – 10.

Dešimtbalėje sistemoje reiškinio pavojingumo vertinimo vidurkis buvo 8,4 balo. Dažniausiai respondentai pavojingumą vertino10 balų.

4. Ar tapatybės vagyste elektroninėje erdvėje, Jūsų nuomone, yra paplitusi Lietuvoje?

Reiškinys nėra paplitęs — Reiškinys plačiai paplitęs

4,98 / 10

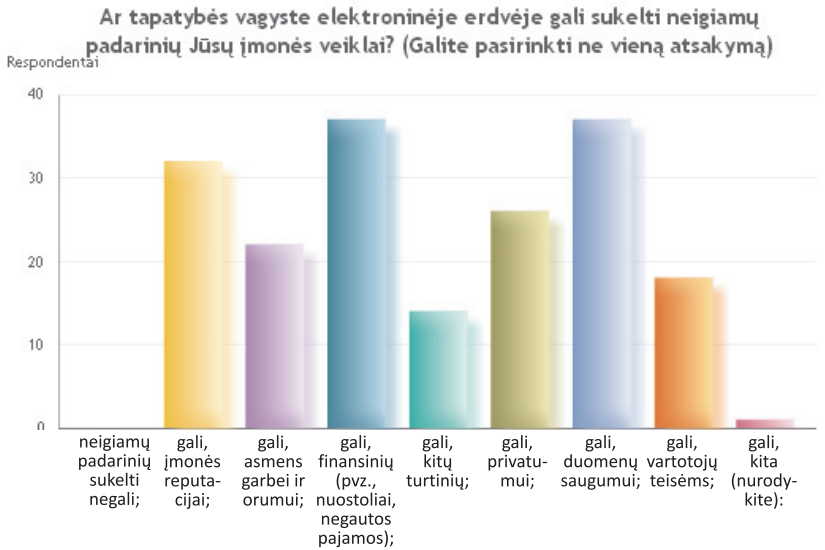
Mažiausias balas buvo 1, didžiausias – 10.

Iš 43 respondentų vidutinis atsakymas yra 4,98 (skalėje nuo 1 iki 10). Dažniausiai respondentai rinkosi 5 balus.

5. Ar tapatybės vagyste elektroninėje erdvėje gali sukelti neigiamų padarinių Jūsų įmonės veiklai? (Galite pasirinkti ne vieną atsakymą) (daug galimų variantų)

Neigiamų padarinių sukelti negali;	0	0%
Gali, įmonės reputacijai;	32	17,1 %
Gali, asmens garbei ir orumui;	22	11,8 %
Gali, finansinių (pvz., nuostoliai, negautos pajamos);	37	19,8 %
Gali, kitų turtinių;	14	7,5 %
Gali, privatumui;	26	13,9 %
Gali, duomenų saugumui;	37	19,8 %
Gali, vartotojų teisėms;	18	9,6 %
Gali, kita (nurodykite):	1	0,5 %
Iš viso atsakymų	187	

Iš 43 respondentų dažniausias atsakymai buvo „gali, finansinių (pvz., nuostoliai, negautos pajamos)“, gali, duomenų saugumui“, taigi, verslo sektorius neigiamus padarinius dažniausiai suvokia kaip finansinius.



Rečiausias atsakymas buvo „neigiamų padarinių sukelti negali“.

6. Ar pakankamai Jūsų įmonė skiria lėšų apsaugai nuo tapatybės vagystės elektroninėje erdvėje?

Visiškai neskiria — Skiria labai daug

5,88 / 10

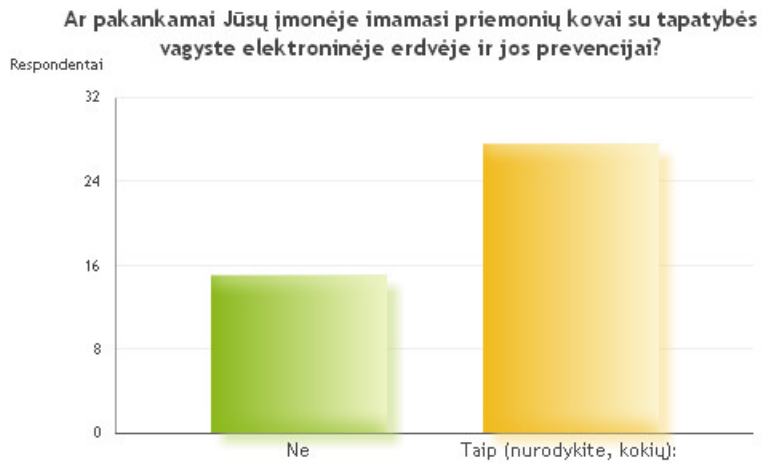
Iš 43 respondentų vidutinis atsakymas yra 5,88 (skalėje nuo 1 iki 10).
Mažiausias balas buvo 1, didžiausias – 10.

Vertinant, ar pakankamai įmonėje skiriama lėšų apsaugai nuo tapatybės vagystės elektroninėje erdvėje, dešimtbalėje skalėje daugiausia respondentų rinkosi 8 ir 5 balus, o vidurkis buvo 5,88 balo.

7. Ar pakankamai Jūsų įmonėje imamasi priemonių kovai su tapatybės vagyste elektroninėje erdvėje ir jos prevencijai?

Ne	15	34,9 %
Taip (nurodykite, kokių):	28	65,1 %
Iš viso atsakymų	43	

- nežinau arba negaliu atskleisti
- technologinių
- vienkartiniai prisijungimo kodai
- IT ir kitokia apsauga
- įvairios IT saugumo priemonės
- mums tokių nereikia



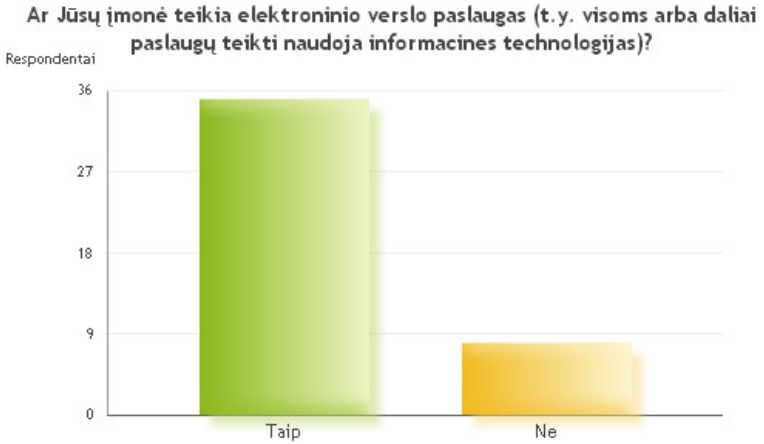
Vertindami prevencijos priemonių pakankamumą didžioji dalis respondentų mano, kad jų pakanka (65,1 proc.), tačiau net 34,9 proc. mano, kad tokių priemonių trūksta. Vardydami prevencijos priemones respondentai dažniausiai paminėjo slaptažodžių svarbą ir įvairias technines saugumo priemones, nors

dalis vartotojų paminėjo ir svarbias organizacines priemones (pvz.: mokymai, darbo procedūros).

8. Ar Jūsų įmonė teikia elektroninio verslo paslaugas (t. y. visoms arba daliai paslaugų teikti naudoja informacines technologijas)?

Taip	35	81,4 %
Ne	8	18,6 %
Iš viso atsakymų	43	

Iš 43 respondentų dažniausias atsakymas buvo „taip".



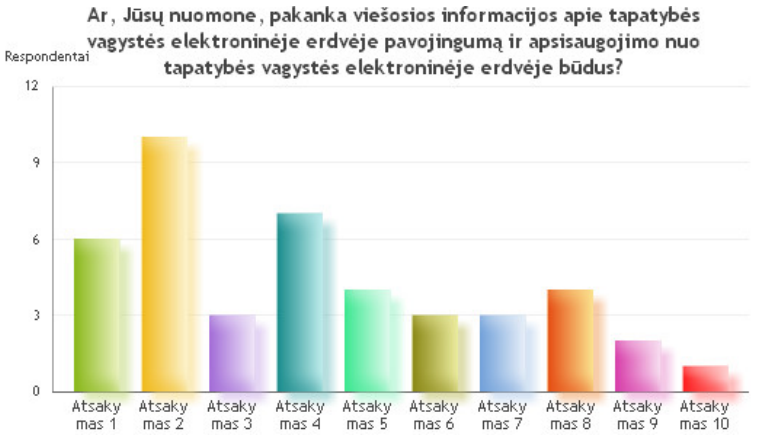
Didžioji dauguma (81,4 proc.) respondentų dirba įmonėse, kurios teikia elektroninio verslo paslaugas.

9. Ar, Jūsų nuomone, pakanka viešosios informacijos apie tapatybės vagystės elektroninėje erdvėje pavojingumą ir apsisaugojimo nuo tapatybės vagystės elektroninėje erdvėje būdus?

Visiškai nėra informacijos — Labai daug informacijos

4,23 / 10

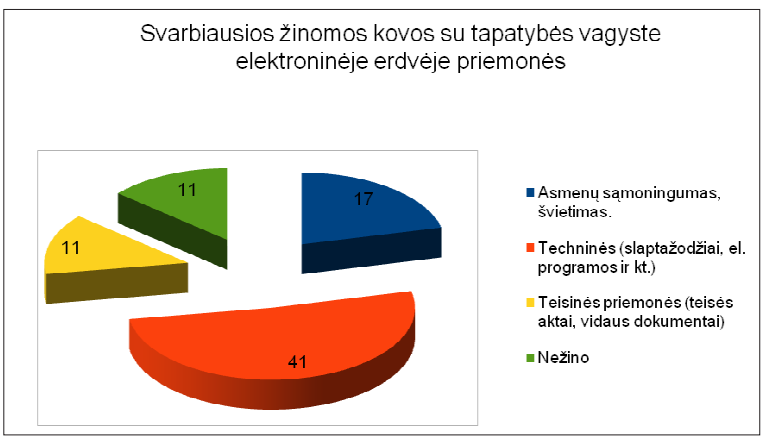
Iš 43 respondentų vidutinis atsakymas buvo 4,23 (skalėje nuo 1 iki 10). Mažiausias balas buvo 1, didžiausias – 10.



Vertindami dešimtbalėje sistemoje viešosios informacijos apie tapatybės vagystės elektroninėje erdvėje pavojingumą ir apsisaugojimo nuo šio reiškinio būdus pakankamumą respondentai dažniausiai pasirinko 2 balus, o vidurkis buvo 4,23 balo. Tai rodo, kad elektroninio verslo paslaugas teikiančių įmonių darbuotojai negauna pakankamai viešosios informacijos apie tapatybės vagystę elektroninėje erdvėje.

10. Nurodykite tris svarbiausias Jums žinomas kovos su tapatybės vagyste elektroninėje erdvėje priemones.

Gauti atsakymai pavaizduoti 45 pav.

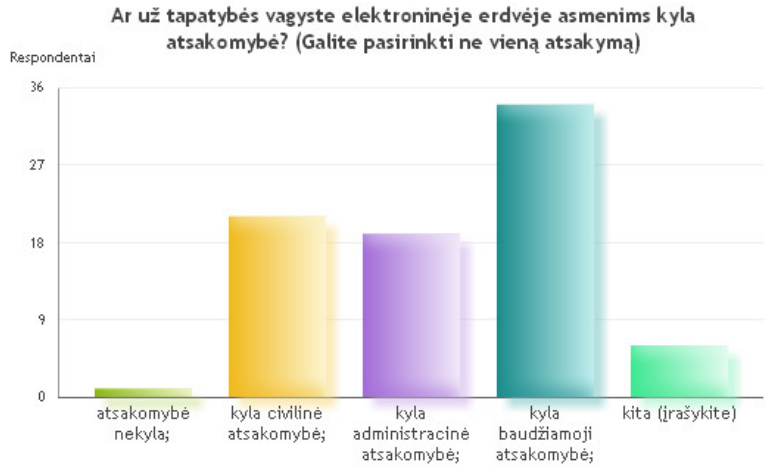


45 pav. Respondentų dažniausiai nurodytos trys svarbiausios kovos su tapatybės vagyste elektroninėje erdvėje priemonės

11. Ar už tapatybės vagystę elektroninėje erdvėje asmenims kyla atsakomybė? (Galite pasirinkti ne vieną atsakymą) (daug galimų variantų)

Atsakomybė nekyla;	1	1,2 %
Kyla civilinė atsakomybė;	21	25,9 %
Kyla administracinė atsakomybė;	19	23,5 %
Kyla baudžiamoji atsakomybė;	34	42 %
Kita (įrašykite)	6	7,4 %
Iš viso atsakymų	81	

Apibendrinant reikia nurodyti, kad visų grupių respondentai, neturėdami tikslios informacijos, manė, kad dėl tapatybės vagystės elektroninėje erdvėje turi kilti vienokia ar kitokia atsakomybė.



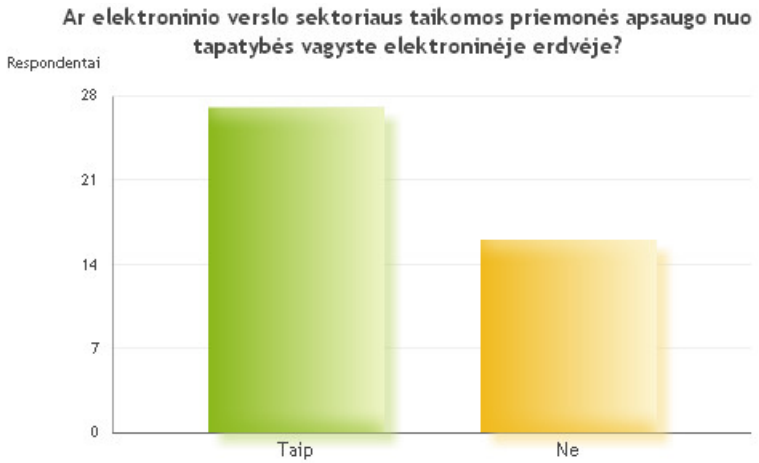
Iš 43 respondentų dažniausias atsakymas buvo „kyla baudžiamoji atsakomybė“. Rečiausias atsakymas buvo „atsakomybė nekyla“.

Respondentų, manančių, kad atsakomybė už tapatybės vagystę elektroninėje erdvėje nekyla, buvo tik 1,2 proc. Daugiausia buvo manančių, kad baudžiamoji atsakomybė kyla (42 proc.).

12. Ar elektroninio verslo sektoriaus taikomos priemonės apsaugo nuo tapatybės vagystės elektroninėje erdvėje?

Taip	27	62,8 %
Ne	16	37,2 %
Iš viso atsakymų	43	

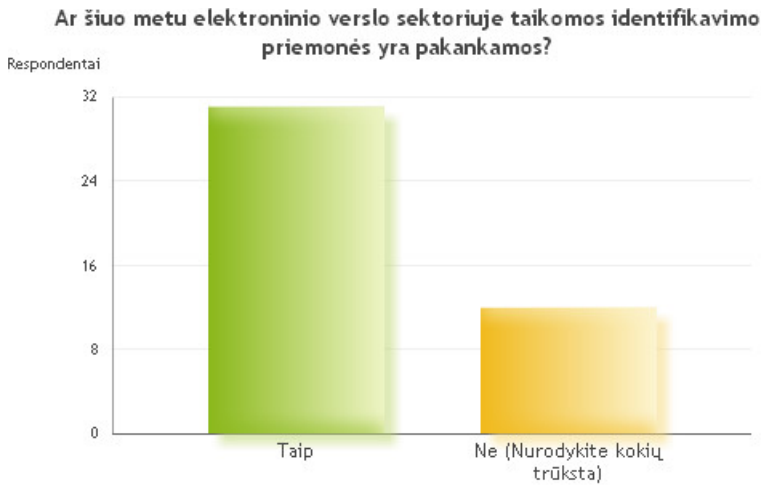
Iš 43 respondentų dažniausias atsakymas buvo „taip“.



Manančiųjų, kad dabar elektroninio verslo taikomos priemonės apsaugo nuo tapatybės vagystės elektroninėje erdvėje, buvo dauguma (62,8 proc.), tačiau net 37,2 proc. respondentų manė, kad šios priemonės yra nepakankamos.

13. Ar šiuo metu elektroninio verslo sektoriuje taikomos identifikavimo priemonės yra pakankamos?

Taip	31	72,1 %
Ne (nurodykite, kokių trūksta)	12	27,9 %
Iš viso atsakymų	43	



Dauguma (72,1 proc.) respondentų, dirbančių verslo įmonėse, manė, kad asmens indentifikavimo priemonės, taikomos elektroniniame versle, yra pakankamos ir tik 27,9 proc. manė, kad jos turėtų būti kitokios. Nurodydami trūkstamas asmens indentifikavimo priemones respondentai nebuvo aktyvūs, nors buvo paminėtos tokios priemonės, kaip elektroninio parašo platesnis taikymas, bankinių slaptažodžių kortelių privalomas keitimas į slaptažodžių generatorius.

14. Kurios iš elektroninio verslo sektoriaus naudojamų priemonių yra patikimos (nurodykite tris tokias patikimas identifikavimo priemones)?

Respondentai, vertindami, kurios iš elektroninio verslo sektoriaus naudojamų priemonių yra patikimos, dažniausiai nurodė kodus ir sudėtingus slaptažodžius, dažnai buvo minimas ir elektroninis parašas. Keli vartotojai nurodė pasitikintys bankų naudojamomis asmens indentifikavimo priemonėmis.

15. Ar elektroninio verslo sektoriaus naudojamos asmens identifikavimo priemonės turėtų būti privalomai reguliuojamos teisės normomis (argumentuokite)?

Didžioji dauguma respondentų pasisakė už tai, kad elektroninio verslo sektoriaus naudojamos asmens identifikavimo priemonės būtų privalomai reguliuojamos teisės normų. Tik nedidelė dalis bijojo, kad toks reguliavimas gali būti nelankstus ir apsunkintų veiklą. Atsižvelgiant į tai, turi būti ieškoma lankstaus ir subalansuoto teisinio reguliavimo priemonių, nes neigiantieji papildomo teisinio asmens indentifikavimo priemonių reguliavimo poreikį dažniau abejoja ne tokio reguliavimo reikalingumu, o dėl jo lankstumo, adekvatumo ir kt. Respondentų, pritariančių asmens indentifikavimo priemonių teisiniam reguliavimui, didelis skaičius rodo, kad versle yra tokio reguliavimo poreikis.

5.2.6. Ekspertų apklausa

(ekspertų anketos pavyzdys ir atitinkami atsakymai pateikti 2 priede).

Respondentų statistika:

Iš viso respondentų 9

Rezultatų santrauka

1. Kaip vertinate tapatybės vagystės elektroninėje erdvėje (toliau – TVEE) reiškinį?

Dėl tapatybės vagystės elektroninėje erdvėje visi ekspertai bendrai sutarė, kad tai neigiamai vertintinas reiškinys. Keturi ekspertai tapatybės vagystės neigiamą pasireiškimą glaudžiai siejo su galimomis pasekmėmis, iš jų trys nurodė, kad tapatybės vagystė elektroninėje erdvėje dažniausiai yra prielaida kitiems nusikaltimams daryti.

2. Ar TVEE, Jūsų nuomone, yra paplitusi? Argumentuokite.

Vertinant tapatybės vagystės elektroninėje erdvėje paplitimą, ekspertų nuomonės pasidalijo: 4 ekspertai (1-as, 5-as, 6-as ir 8-as) manė, kad Lietuvoje tai nėra paplitęs reiškinys, 3 ekspertai (2-as, 3-as, 9-as) manė, kad tai santykinai dažnas reiškinys, 2 ekspertai (4-as, 7-as) atsakė, kad tai latentinė veika, todėl nėra galimybės jos įvertinti.

3. Ar TVEE, Jūsų manymu, kelia pavojų? Jei taip, tai kam?

Ekspertai plačiai atskleidė tiriamojo reiškinio pavojingumą, dauguma ekspertų neapsiribojo siauru požiūriu, kad pavojus kyla tik konkrečiam asmeniui, kurio duomenys gauti ar panaudoti ne pagal jo norą, bet nurodė ir daugiau neigiamų pasekmių rūšių: pvz.: 1-asis ekspertas labai argumentuotai išdėstė, kad šis reiškinys kenkia verslui, vartotojams ir valstybei, 6-asis ekspertas teigė, kad nukenčia asmuo, kurio duomenys panaudojami, verslo subjektai ir visuomeninė tvarka, 9-asis ekspertas panašiai atskleidė požiūrį argumentuodamas, kad nukenčia vartotojas ir elektroninės komercijos vykdytojas, panašiai manė ir dalis kitų ekspertų (pvz.: 5-asis ekspertas teigė, kad nukenčia finansinės institucijos ir piliečiai), kiti ekspertai pavojų apibrėžė kiek siauriau (pvz., nurodė, kad nukenčia tik asmuo, kurio duomenys pavogti (8-asis ekspertas).

4. Nurodykite sritis (pagal sektorius: viešasis, privatus; pagal veiklos pobūdį: finansų, medicinos ir kt.), kuriose, Jūsų nuomone, tapatybės vagystės grėsmė yra didžiausia. Atsakymą pagrįskite.

Dauguma ekspertų (5 ekspertai: 1-as, 3-as, 5-as, 7-as, ir 8-as) teigė, kad rizikingiausias yra privatus sektorius. Taip pat ekspertai teigė, kad rizikingiausi sekto-

riai yra tie, kurie skiria mažiausiai dėmesio asmens indentifikavimo patikimumui (1-as, 2-as ekspertai). Kaip pagrindinį konkretų sektorių ekspertai įvardijo finansų sektorių, tačiau išskyrė ir specifinius, pvz.: SMS kreditų, elektroninės prekybos, socialinius tinklalapius, kritinės infrastruktūros objektus.

5. Ar, Jūsų nuomone, pakanka teisės normų ir teisinio reguliavimo priemonių, norint tinkamai sureguliuoti TVEE? Jei manote, kad nepakanka, tai kokių teisės normų trūksta?

1-asis, 2-asis, 4-asis ir 5-asis ekspertai teigė, kad reguliavimo pakanka; 7-asis, 8-asis ir 9-asis ekspertai teigė, kad reguliavimą reikėtų tobulinti; 3-asis ir 6-asis ekspertai negalėjo atsakyti į šį klausimą.

6. Ar Lietuvoje numatyta atsakomybė už TVEE? Jei taip, tai kokia?

Dalis ekspertų atsakydami apsiribojo baudžiamosios atsakomybės vertinimu, 4-asis, 5-asis ir 8-asis ekspertai nurodė, kad tokia veika nėra kriminalizuota. 2-asis ekspertas nurodė, kad jo paminėtais atvejais gali būti taikoma atsakomybė pagal LR Asmens duomenų teisinės apsaugos įstatymą. Dalis ekspertų teigė, kad atskirais atvejais kyla ir baudžiamoji atsakomybė (2-asis, 3-asis, 4-as, 6-as, 7-as ekspertai). 1-asis ekspertas teigė, kad kyla netiesioginė atsakomybė, priklausomai nuo veikos, atliktos pasitelkiant tapatybės vagystę elektroninėje erdvėje, tačiau nenurodė, kokia tai atsakomybė (civilinė, baudžiamoji ar kt.). 9-asis ekspertas negalėjo atsakyti į klausimą.

7. Ar manote, kad TVEE reikėtų kriminalizuoti kaip savarankišką nusikalstamą veiką? Kodėl?

Pritariančių tapatybės vagystės kriminalizavimui ekspertų skaičius (4 ekspertai: 2-as, 7-as, 8-as, 9-as) buvo vienodas jiems oponuojančių ekspertų skaičiui (4 ekspertai: 1-as, 3-as, 5-as, 6-as). 4-asis ekspertas neturėjo šiuo klausimu nuomonės. Pasisakantys už veikos kriminalizavimą ekspertai nuomonę grindė šiais argumentais: 2-asis ekspertas siūlė tapatybės vagystę elektroninėje erdvėje kriminalizuoti kaip savarankišką nusikalstamą veiką dėl jos specifikos, nes tai intelektinio pobūdžio veikos; jas paprasta išskaidyti į atskiras dalis, galima lygiagrečiai realizuoti, todėl labai sparčiai, kai kurie dalyviai gali net nesuprasti, kad yra įtraukti į nusikalstamą veiklą. Labai sudėtinga įvertinti, kokiems tolesniems nusikaltimams planuojami ir galimi panaudoti TVEE duomenys; 7-asis ekspertas atsakydamas į šeštą klausimą teigė, kad atsakomybė už tapatybės vagystę elektroninėje erdvėje yra fragmentiška ir tik dalis veikų kriminalizuota, todėl siūlė tapatybės vagystę kriminalizuoti; 8-asis ekspertas nurodė, kad kriminalizavimas drausmintų potencialius vagystės vykdytojus; 9-asis ekspertas nuomonę grindė didėjančia šio neigiamo reiškinio žala ir mastu.

Neigiantys veikos savarankiško kriminalizavimo poreikį ekspertai argumentavo taip: 1-asis ekspertas nurodė, kad tapatybės vagystė elektroninėje erdvėje gali apimti labai daug skirtingų veikų, už kurias gali grėsti labai skirtinga atsakomybė, todėl abejotina, ar galima nustatyti bendrą atsakomybę; 5-asis ekspertas teigė, kad tapatybės vagystė elektroninėje erdvėje pati savaime nepadaro žalos. Dažniausiai ji būna tik pasirengiamoji stadija atliekant nusikaltimą, t. y. jau krimanilzuotą nusikalstamą veiką.

8. Ar galiojančios teisės normos, reguliuojančios santykius, susijusius su TVEE, taikomos tinkamai?

Galiojančių normų, reguliuojančių tiriamą reiškinį, taikymą teigiamai vertino tik du ekspertai (8-as, 9-as), neigiamai vertino taip pat du ekspertai (1-as, 7-as). „Sunku pasakyti" arba „nėra pakankamai praktikos" paminėjo 2-asis ir 3-asis ekspertai. 4-asis ir 6-asis ekspertai negalėjo atsakyti į šį klausimą. 5-asis ekspertas teigė, kad nesant veikos kriminalizavimo normų taikymas neįmanomas.

9. Kokios problemos kyla dėl TVEE tyrimo?

Vardydami problemas, kylančias dėl tapatybės vagystės elektroninėje erdvėje tyrimo, keturi ekspertai negalėjo atsakyti į šį klausimą (3-as, 4-as, 5-as, 6-as). Kiti vardijo įvairias aktualias problemas: nepakankamą tyrėjų kompetenciją (1-as ekspertas); sudėtingumą įrodyti tapatybės vagystės elektroninėje erdvėje būdą ir tikslą (2-as ekspertas); dėl elektroninės erdvės specifikos sunku nustatyti padariusį veiką asmenį; tam trukdo ir tarptautinio bendradarbiavimo trūkumas (7-as ekspertas), žmogiškųjų išteklių trūkumas, nepakankamas duomenų pateikimas Ryšių reguliavimo tarnybai (9-as ekspertas). 8-asis ekspertas teigė, kad problemų nekyla, nes veika nėra kriminalizuota, problemos gali kilti, tik jei su duomenimis buvo kas nors daroma.

10. Ar pakankamai taikoma savireguliacijos TVEE mažinimo ir (arba) išvengimo priemonių? Kokios savireguliacijos priemonės galėtų mažinti TVEE?

Ekspertų, teigiančių, kad savireguliacijos priemonių pakanka, nebuvo. 2-asis, 4-asis ir 9-asis ekspertai teigė, kad savireguliacijos priemonių nepakanka. Keturi ekspertai (3-as, 5-as, 7-as, 8-as) negalėjo atsakyti į klausimą. 9-asis ekspertas teigė, kad savireguliacija kibernetinio saugumo srityje nėra veiksminga, todėl reikia daugiau reguliavimo priemonių, panašiai manė ir 2-asis ekspertas. 1-asis ekspertas paminėjo, kad reikalinga verslo subjektų atsakomybė. 1-asis ir 4-asis ekspertai nurodė, kad reikalingas informavimas ir švietimas. 6-asis ekspertas teigė, kad taikant priemones reikia atsižvelgti į siekiamo tikslo ir sąnaudų balansą.

11. Ar, Jūsų nuomone, valstybių tarpinstitucinis bendradarbiavimas yra pakankamas ir tinkamas? Jei ne, nurodykite, ko trūksta.

1-asis ir 2-asis ekspertai teigė, kad tarpinstitucinį bendradarbiavimą reikėtų gerinti. Kad bendradarbiavimas pakankamas, manė 8-asis ir 9-asis ekspertai. Neatsakė į klausimą 3-asis, 5-asis ir 6-asis ekspertai. 4-asis ir 7-asis ekspertai klausimą suprato netiksliai, t. y. tarpinstitucinį bendradarbiavimą sutapatino su tarptautiniu bendradarbiavimu.

12. Ar, Jūsų nuomone, bendradarbiavimas tarp valstybės ir privataus sektoriaus yra tinkamas? Jei ne, nurodykite, ko trūksta.

Kad bendradarbiavimas tarp valstybės ir privataus sektoriaus yra tinkamas nurodė tik 9-asis ekspertas. Ekspertai: 1-asis, 2-asis, 4-asis, 5-asis, 6-asis, 7-asis, 8-asis teigė, kad nėra geras arba galėtų būti geresnis. 3-asis ekspertas negalėjo atsakyti į klausimą. Ekspertai vardijo bendradarbiavimo trūkumus: 1-asis ekspertas sakė, kad trūksta pasitikėjimo verslu, ypač didelėmis įmonėmis, blogai, kad visiems verslo taikomi vienodi kriterijai; 2-asis ekspertas nurodė, kad trūksta vienos koordinuojančios institucijos, atsakingos už problemos sprendimą; 4-asis ekspertas nurodė, kad trūksta informacijos keitimosi, visuomenės sąmoningumo ir atsakingumo, 5-asis, 7-asis ir 8-asis ekspertai iškėlė panašią problemą, kad privatus sektorius nėra suinteresuotas pradėti tyrimus bei juos viešinti ir tai trukdo veiksmingai kovoti su šiuo reiškiniu.

13. Ar elektroninio verslo taikomos priemonės apsaugo nuo TVEE? Kokios priemonės yra pakankamos ir kokios neturėtų būti taikomos?

2-asis ir 8-asis ekspertai teigė, kad taikomos priemonės apsaugo nuo tapatybės vagystės elektroninėje erdvėje, tačiau 2-asis ekspertas patikslino, kad patikimesnės priemonės yra brangesnės ir mažina elektroninės erdvės patrauklumą. 5-asis ir 6-asis ekspertai teigė, kad nėra visiškai patikimų priemonių. Jiems nepritarė 9-asis ekspertas, kuris teigė, kad priemonių yra daug, bet taupymas, nežinojimas, rizikos nuvertinimas turi įtakos kompromisams, susijusiems su saugumo mažinimu. 1-asis, 3-asis, 4-asis, ir 7-asis ekspertai negalėjo atsakyti į klausimą.

14. Ar elektroninio verslo naudojamos asmens indentifikavimo priemonės turėtų būti privalomai reguliuojamos teisės normų? Argumentuokite.

2-asis, 6-asis, 7-asis, 8-asis ir 9-asis ekspertai pritarė, kad atitinkamas asmens indentifikavimo priemonių teisinis reguliavimas turi būti, dalis jų nurodė, kad ne visos indentifikavimo priemonės turi būti reguliuojamos normomis, pvz., 2-asis ekspertas teigė, kad indentifikavimo priemonės turi būti suskirstytos į lygmenis, vieni lygmenys turėtų būti reguliuojami teisės normomis, kiti tik re-

komendacijomis, o taikantis atitinkamą lygmenį asmuo turėtų nurodyti patikimumo lygmenį. 1-asis ir 5-asis ekspertai nemanė, kad asmens indentifikavimo priemones privalomai turėtų reguliuoti teisės normos.
3-asis ir 4-asis ekspertai negalėjo atsakyti į klausimą.

15. Kokias TVEE prevencijos priemones galėtumėte pasiūlyti?

Vieną ar kitą švietimo arba informavimo formą įvardijo 3 ekspertai: 1-asis, 2-asis ir 9-asis. Kiti ekspertai vardijo konkrečias technines ir organizacines priemones: 4-asis (nurodė daug konkrečių priemonių, kaip turi elgtis, asmuo siekiantis išvengti šio nepageidaujamo reiškinio), 5-asis (biometrinių indentifikavimo priemonių naudojimas), 7-asis (programinės įrangos tobulinimas). Teisinės bazės tobulinimą nurodė 2-asis ir 8-asis ekspertai. 3-asis ekspertas į klausimą neatsakė.

LITERATŪROS SĄRAŠAS:

1. .LT domeno procedūrinis reglamentas. VII skirsnis, Apmokėjimas [interaktyvus, žiūrėta 2011-09-21]. <http://www.domreg.lt/static/doc/public/procedural_regulation-lt.pdf>.
2. „One.lt“ naudojimosi taisyklės. [interaktyvus, žiūrėta 2011-09-21]. <http://w27.one.lt/community/common/info/popup_Rules.jsp?language=lt>.
3. „Saugaus uosto“ principai [interaktyvus, žiūrėta 2011-09-20]. <http://export.gov/safeharbor/eu/eg_main_018476.asp>.
4. 2005 m. birželio 23 d. Lietuvos Aukščiausiojo Teismo Senato nutarimas Nr. 52 „Dėl teismų praktikos vagystės ir plėšimo baudžiamosiose bylose“ [interaktyvus, žiūrėta 2011-09-19]. <http://www.lat.lt/4_tpbiuleteniai/senos/nutartis.aspx?id=29259>.
5. 2006 m. gegužės 31 d. Komisijos komunikatas Europos parlamentui, Tarybai ir Regionų komitetui saugios informacinės visuomenės strategija „Dialogas, partnerystė ir teisių suteikimas“ COM(2006)0251 galutinis [interaktyvus, žiūrėta 2011-09-19]. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0251:FIN:LT:HTML>.
6. 2006 m. gruodžio 13 d. Lietuvos Respublikos Vyriausybės nutarimas Nr. 1266 „Dėl elektroninės informacijos saugos koordinavimo komisijos sudarymo“. *Valstybės žinios*, 2006, Nr. 137-5224.
7. 2007 m. balandžio 25 d. Vyriausybės nutarimu Nr. 410 patvirtinti Bendrieji elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimai. *Valstybės žinios.* 2007, Nr. 49-1891.
8. 2008 m. gegužės 15 d. Lietuvos Banko valdybos nutarimas Nr. 82 „Dėl kredito įstaigoms skirtų nurodymų, kuriais siekiama užkirsti kelią pinigų plovimui ir (ar) teroristų finansavimui“. *Valstybės žinios.* 2008, Nr. 62-2374.
9. 2009 m. kovo 30 d. Komisijos komunikatas Europos parlamentui, Tarybai ir Regionų komitetui dėl ypatingos svarbos informacinės infrastruktūros apsaugos „Europos apsauga nuo didelio masto kibernetinių antpuolių ir veiklos sutrukdymo – geresnė parengtis, didesnis saugumas ir atsparumas“ COM(2009)149 galutinis [interaktyvus, žiūrėta 2011-09-19]. < http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:LT:PDF>.
10. 2009 m. kovo 30 d. Komisijos komunikatas Europos parlamentui, Tarybai ir Regionų komitetui dėl ypatingos svarbos informacinės infrastruktūros apsaugos „Europos apsauga nuo didelio masto kibernetinių antpuolių ir veiklos sutrukdymo – geresnė parengtis, didesnis saugumas ir atsparumas“ COM(2009)149 galutinis [interaktyvus, žiūrėta 2011-09-19]. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:LT:PDF>.
11. 42 Pa. Consol. Stat. Ann. [section] 8315. [interaktyvus, žiūrėta 2011-09-20]. <http://law.onecle.com/pennsylvania/judiciary-and-judicial-procedure/index.html>.

12. 8 požymiai, padedantys atpažinti tapatybės vagystės subjektą [interaktyvus, žiūrėta 2011-07-09]. <http://articles.moneycentral.msn.com/Banking/FinancialPrivacy/8SignsYouMayKnowAnIdentityThief.aspx>.
13. A. Sacharukas išsaugojo Seimo nario mandatą, L.Karalius neteko**.** *Lietuvos rytas* [interaktyvus]. 2010-11-11 [žiūrėta 2011-09-14]. <http://www.lrytas.lt/-12894613511288584418-a-sacharukas-i%C5%A1saugojo-seimo-nario-mandat%C4%85-l-karalius-neteko-nuotraukos-3-video.htm>.
14. Abagnale; F. W. *Stealing Your Life: The Ultimate Identity Theft prevention Act*. Broadway Books, 2007.
15. Access Device Fraud, Title 18, United States Code, Section 1029 [interaktyvus, žiūrėta 2011-09-15]. <http://www.law.cornell.edu/uscode/usc_sec_18_00001029----000-.html>.
16. Alcoff, L., Hames-Carcia, M.; Moya, P. M. L. 2006. *Identity Politics Reconsidered*. Palgrave Macmillan, Basingstoke.
17. APACS - the UK payments association in conjunction. Fraud The Facts 2009 [interaktyvus, žiūrėta 2011-09-15]. < http://www.eastscotlandfraudforum.org.uk/documents/Fraud%20the%20Facts%202009.pdf>.
18. APEC Strategy to Ensure Trusted, Secure and Sustainable Online Environment, 2005 [interaktyvus, žiūrėta: 2011-09-21]. <http://www.apec.org/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/~/media/Files/Groups/TEL/05_TEL_APECStrategy.ashx>.
19. Apsiperkančių internete padvigubėjo. *Delfi.lt* [interaktyvus]. 2011-05-18 [žiūrėta 2011-09-14]. <http://mokslas.delfi.lt/archive/print.php?id=45640243>.
20. APWG Phishing Activity Trends Report for the Month of December, 2007 [interaktyvus, žiūrėta 2011-09-19]. <http://www.antiphishing.org/reports/apwg_report_dec_2007.pdf>.
21. Babachinaitė, G. 2003. *Nusikalstamumo ir kitų nepageidautinų socialinių procesų prevencijos problemos bei jų sprendimo būdai Europos valstybėse*. LTU.
22. Bank Fraud Statute, Title 18, United States Code, Section 1344 [interaktyvus, žiūrėta 2011-09-15]. <http://www.law.cornell.edu/uscode/usc_sup_01_18_10_I_20_63.html>.
23. Bendrieji elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimai. *Valstybės žinios*, 1997, Nr. 83-2075.
24. Biegelman, M. T. 2009. *Identity Theft Handbook: Detection, Prevention, and Security*.
25. Biggest Identity Theft Case Ever: 11 Indicted For Stealing And Selling Over 40 Million Credit Card Numbers. [interaktyvus, žiūrėta 2011-09-18]. <http://www.huffingtonpost.com/2008/08/05/biggest-identity-theft-ca_n_117094.html>.
26. Blass, E. NEC falls victim to sophisticated "corporate identity theft" [interaktyvus]. 2006-04-27 [žiūrėta 2011-09-14]. <http://www.engadget.com/2006/04/27/nec-falls-victim-to-sophisticated-corporate-identity-theft/>.

27. Bluvšteinas J.; E. Bieliūnas, E; Justickis, V., *et al.* 2006. *Kriminologija*. Pradai.
28. Boyd, D. M.; Ellison, N. B. Social Network Sites: Definition, History, and Scholarship. [interaktyvus, žiūrėta 2011-09-21]. <http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html>.
29. Boulton, C. Google Apps for Government meets Federal Security Standart. *eWeek.com* [interaktyvus] 2010-07-06 [žiūrėta 2011-09-19]. <http://www.eweek.com/c/a/Cloud-Computing/Google-Apps-for-Government-Meets-Federal-Security-Standard-593503/>.
30. Brenner, S. W. 2010. *Cybercrime. Criminal Threats from Cyberspace*. Library of Congress Cataloging.
31. Bryman, A. 2008. *Social Research Methods*. Oxford University Press.
32. Burr, W. E.; Dodson, D. F.; Polk, W. T. Electronic Authentication Guideline. Recommendations of the National Institute of Standards and Technology [interaktyvus]. *Gaithersburg: NIST Special Publication* 800-63 Version 1.0.2., 2006 [žiūrėta 2011 09 19]. <http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf>.
33. Cal. Civ. Code [section] 1798.92-1798.97. [interaktyvus, žiūrėta 2011-09-20]. <http://www.leginfo.ca.gov/cgi-bin/calawquery?codesection=civ&codebody=&hits=20>.
34. California Data Security Breach Act Helps Protect Private Information. Buzzle.com [interaktyvus, žiūrėta 2011-09-19]. <http://www.buzzle.com/articles/california-data-security-breach-act-helps-protect-private-information.html>.
35. Camp, L. J. 2010. *Economics of Identity Theft*. Springer.
36. Cane P. and Conaghan J. 2006. *The New Oxford Companion to Law*. Oxford University Press Inc.
37. Children's Online Privacy Protection Act [interaktyvus, žiūrėta 2011-09-19]. <http://www.ftc.gov/ogc/coppa1.htm>.
38. CIFAS [interaktyvus, žiūrėta 2011 09 15]. <http://www.cifas.org.uk/default.asp?edit_id=561-56>.
39. Civil liability for identity theft: identity theft can cause catastrophic financial damage, but many victims also suffer emotional, psychological, and even physical injuries. Civil claims against the responsible parties can help repair the damage [interaktyvus]. 2007-02-01 [žiūrėta 2011-09-20]. <http://goliath.ecnext.com/coms2/gi_0199-6285492/Civil-liability-for-identity-theft.html>.
40. Civilka, M. Asmens duomenų teisinis reguliavimas interneto kontekste [interaktyvus, žiūrėta 2011-09-18]. <http://media.search.lt/GetFile.php?OID=92932&FID=269994>.
41. Clough, J. 2010. *Principles of Cybercrime*. Cambridge University Press. p. 209.
42. Codified in Fraud and Related Activity in Connection with Computers, Title 18, United States Code, Section 1030. [interaktyvus, žiūrėta 2011-09-15]. <http://www.panix.com/~eck/computer-fraud-act.html>.

43. Collins, M. J. 2006. *Investigating Identity Theft: A Guide for Businesses, law Enforcement, and Victims*. John Wiley & Sons, Inc.
44. Combating Identity Theft: A Strategic Plan. 2007 [interaktyvus, žiūrėta 2011-09-20]. <http://www.idtheft.gov/reports/StrategicPlan.pdf >.
45. Communication from the Commission to the Parliament, the Council and the Committee of Regions „Towards a general policy on the fight against cyber crime" COM(2007) 267 final [interaktyvus, žiūrėta 2011-09-19]. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF>.
46. Computer Misuse Act 1990 [interaktyvus, žiūrėta 2011-09-19]. <http://www.legislation.gov.uk/ukpga/1990/18/contents>.
47. Controlling the Assault of Non-Solicited Pornography and Marketing Act [interaktyvus, žiūrėta 2011-09-19]. <http://uscode.house.gov/download/pls/15C103.txt>.
48. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (entered into force on 1 October 1985) [interaktyvus]. CETS 108 [žiūrėta 2011-09-19]. <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=8&DF=26/04/2011&CL=ENG>.
49. Convention on Cybercrime CETS No.: 185 [interaktyvus, žiūrėta 2011-09-18]. <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm >.
50. Černišova V.O. Internet i prestupnost. Computer Crime Research Center [interaktyvus, žiūrėta 2011-09-20]. <http://www.crime-research.org/library/Chernish1.htm>.
51. Dabartinės lietuvių kalbos žodynas [interaktyvus, žiūrėta 2011-09-15]. <http://www.lki.lt/dlkz/>.
52. Dėl galimos duomenų vagystės bankai blokuoja korteles. *15 min* [interaktyvus]. 2009-10-13 [žiūrėta 2011-09-14]. <http://www.15min.lt/naujiena/aktualu/pinigai/58/59976/>.
53. Dingo kaip į vandenį. *Kauno diena*. [interaktyvus]. 2008-09-08 [žiūrėta 2011-09-18]. <http://kauno.diena.lt/dienrastis/pasaulis/dingo-kaip-i-vandeni-121179>.
54. Directive 2006/24/EC of the European parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communication services or of public communications networks and amending Directive 2002/58/EC [interaktyvus, žiūrėta 2011-09-18]. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF>.
55. Doctrine of the Information Security of the Russian Federation, 2000 [interaktyvus, žiūrėta 2011-09-19]. <http://www.medialaw.ru/e_pages/laws/project/d2-4.htm>.
56. *DoubleClick* kompanijos tinklapis [interaktyvus, žiūrėta 2011-09-18]. <http://www.doubleclick.com/privacy>.

57. Drivers Privacy Protection Act [interaktyvus, žiūrėta 2011-09-19]. <http://www.accessreports.com/statutes/DPPA1.htm>.
58. Duquenoy, P., *et al.* 2008. *Ethical, legal and professional issues in computing***.**
59. E-commerce sales rise 14.8% in 2010 [interaktyvus]. 2011-02-17 [žiūrėta 2011-09-24]. <http://www.internetretailer.com/2011/02/17/e-commerce-sales-rise-148-2010 >.
60. Electronic Authentication Guideline. Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-63 Version 1.0.2. [interaktyvus, [žiūrėta 2011-09-15]. <http://www.usda.gov/egov/egov_redesign/intranet/eauth/SP800-63V6.pdf>.
61. Electronic signatures in global and national commerce act. [interaktyvus, žiūrėta 2011-09-18]. <http://www.ftc.gov/os/2001/06/esign7.htm>.
62. Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programa. *Valstybės žinios.* 2011, Nr. 83-4033.
63. Elektroninės informacijos saugos valstybės institucijų informacinėse sistemose valstybinėje strategija iki 2008 metų. *Valstybės žinios.* 2006, Nr. 70-2575.
64. Elektroninių ryšių įstatymo 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 16, 17, 18, 21, 22, 23, 27, 28, 29, 30, 31, 32, 33, 34, 36, 37, 39, 40, 41, 48, 49, 50, 51, 52, 54, 56, 57, 58, 59, 61, 62, 63, 64, 66, 68, 69, 71, 72, 73, 74, 75, 77 straipsnių, antrojo skirsnio pavadinimo ir 2 priedo pakeitimo ir papildymo, Įstatymo papildymo 23(1), 23(2), 42(1) straipsniais ir 35 straipsnio pripažinimo netekusiu galios įstatymas. *Valstybės žinios*, 2011, Nr. 91-4327.
65. Elektroninių valdžios vartų portalas dėl saugumo spragų sustabdė savo veiklą neribotam laikui [interaktyvus]. 2010-07-12 [žiūrėta 2011-10-04]. <http://www.technologijos.lt/n/mtl/S-13875/straipsnis?name=S-13875&l=1&p=1>.
66. Eric Schmidt's Name Game Doesn't Make Sense. [interaktyvus, žiūrėta 2011-09-15]. <http://techcrunch.com/2010/08/16/eric-schmidt-change-name/>.
67. Estijoje uždrausta internete tikrinti asmenų, ieškančių darbo, duomenis. *Delfi.lt* [interaktyvus]. 2011-01-30 [žiūrėta 2011-09-21]. <http://verslas.delfi.lt/law/estijoje-uzdrausta-internete-tikrinti-asmenu-ieskanciu-darbo-duomenis.d?id=41442117>.
68. Estijos baudžiamasis kodeksas**.** [interaktyvus, žiūrėta 2011-09-19]. <http://www.legislationline.org/download/action/download/id/1280/file/4d16963509db70c09d23e52cb8df.htm/preview>.
69. European Network and Information Security Agency [interaktyvus, žiūrėta: 2011-09-21] <http://www.enisa.europa.eu/>.
70. Europos duomenų apsaugos pareigūnas išreiškė nuomonę dėl Komunikato apžvalgos. Valstybinės duomenų apsaugos inspekcijos tinklapis [interaktyvus]. 2011-01-24 [žiūrėta 2011-09-21]. <http://www.ada.lt/index.php?lng=lt&action=page&id=20120 >.

71. Europos Parlamento ir Tarybos 1995 m. spalio 24 d. direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo [interaktyvus]. [1995] *OL L281/31*. [žiūrėta 2011-09-19]. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1995L0046:20031120:LT:PDF>.
72. Europos Parlamento ir Tarybos direktyva dėl atakų prieš informacines sistemas ir dėl tarybos pamatinio sprendimo 2005/222/TVR panaikinimo KOM(2010)517 galutinis (siūlymas) [interaktyvus, žiūrėta 2011-09-19]. <http://www.europarl.europa.eu/meetdocs/2009_2014/documents/com/com_com(2010)0517_/com_com(2010)0517_lt.pdf >.
73. Europos Parlamento ir Tarybos direktyva Nr. 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo [interaktyvus, žiūrėta 2011-09-19]. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1995L0046:20031120:LT:PDF>.
74. Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija. *Valstybės žinios*, 1995, Nr. 40-987.
75. Explanatory Report of Convention on Cybercrime [interaktyvus, žiūrėta 2011-09-20] <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>.
76. Facebook banga šluoja konkurentus [interaktyvus]. 2010-07-22 [žiūrėta 2011-09-18]. <http://www.lrytas.lt/-12797981811279127001-facebook-banga-%C5%A1luoja-konkurentus-jo-nari%C5%B3-skai%C4%8Dius-pasiek%C4%97-500-milijon%C5%B3-video.htm >.
77. Facebook Principles [interaktyvus, žiūrėta 2011-09-21]. <http://www.facebook.com/principles.php>.
78. Facebook's Privacy Policy [interaktyvus, žiūrėta 2011-09-21]. <http://www.facebook.com/policy.php>.
79. Fair and Accurate Credit Transactions Act [interaktyvus, žiūrėta 2011-09-19]. <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ159.108>.
80. Fair Credit Reporting Act [interaktyvus, žiūrėta 2011-09-19]. <http://www.ftc.gov/os/statutes/031224fcra.pdf>.
81. False Statements Act (18 U.S.C. § 1001). [interaktyvus]. [žiūrėta 2011-09-19]. <http://www.law.cornell.edu/uscode/18/usc_sec_18_00001001----000-.html>.
82. Family Educational Rights and Privacy Act of 1974 [interaktyvus, žiūrėta 2011-09-19]. <www.ed.gov/policy/gen/guid/fpco/ferpa/index.html>.
83. FBI [interaktyvus, žiūrėta 2011-09-15]. <http://www.fbi.gov/about-us/investigate/cyber/identity_theft>.
84. Federal Act No. 149-FZ of the Russian Federation on Information, Information Technologies and Information Protection [interaktyvus]. 14 July, 2006 [žiūrėta 2011-09-19]. <http://www.medialaw.ru/e_pages/laws/russian/information-en.htm>.

85. Federal Act No. 152-FZ on Personal Data. 27 July, 2006 [interaktyvus, žiūrėta 2011-09-19]. <http://www.mofo.com/docs/mofoprivacy/Federal%20Law%20of%2027%20July%202006%20N152-FZ%20on%20Personal%20Data%20%20(English).pdf>.
86. Federal Act No. 24-FZ of the Russian Federation on Information, Informatization and Protection of Information [interaktyvus]. 20 February, 1995 [žiūrėta 2011-09-19]. <http://www.medialaw.ru/e_pages/laws/russian/iipi-en.htm>.
87. Federal Bureu of Investigation. Identity Theft [interaktyvus, žiūrėta 2011 09-20]. <http://www.fbi.gov/about-us/investigate/cyber/identity_theft>.
88. Federal Information Security Management Act, 2002. US code, Title 44, Chapter 35, Subchapter III [interaktyvus]. [žiūrėta, 2011-09-19]. < http://www.law.cornell.edu/uscode/44/usc_sup_01_44_10_35_20_III.html >.
89. Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications (ROSKOMNADZOR) [interaktyvus, žiūrėta 2011-09-19]. <http://www.rsoc.ru/eng/>.
90. Federalinės prekybos komisijos tinklapis, skirtas kovai su tapatybės vagyste [interaktyvus, žiūrėta 2011-09-15]. <http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html>.
91. Financial Modernization Act, Gramm-Leach-Bliley Act [interaktyvus,žiūrėta 2011-09-19]. <http://www.ftc.gov/privacy/glbact/glbsub1.htm>.
92. FIPS 200 "Minimum Security Requirements for Federal Information and Information Systems"[interaktyvus]. 2006 [žiūrėta 2011-09-19]. <http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf >.
93. FIPS PUB 199 "Standards for Security Categorization of Federal Information and Information Systems" [interaktyvus]. 2004 [žiūrėta 2011-09-19]. < http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf>.
94. First INTERPOL information security conference to provide global platform for preventing and detecting high-tech crimes [interaktyvus]. 2010-09-15 [žiūrėta 2011-09-18].
95. Fraud Act 2006 [interaktyvus, žiūrėta 2011-09-15]. <http://www.legislation.gov.uk/ukpga/2006/35/contents>.
96. FTC FACT Act Red Flags Rule Template [interaktyvus, žiūrėta 2011-09-19]. <http://www.finra.org/web/idcplg?IdcService=GET_FILE&dDocName=p119095&RevisionSelectionMethod=LatestReleased&Rendition=primary&allowInterrupt=1>.
97. Gercke, M. Internet-related identity thef. Project on Cybercrime [interaktyvus]. 2007 [žiūrėta 2011-09-19] <http://www.coe.int/T/DG1/LegalCooperation/Economiccrime/cybercrime/cy%20activity_events_on_identity_theft/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf>.
98. Ghosh, S.; Turrini, E. 2010. *Cybercrimes: A Multidisciplinary Analysis*. Springer-Verlag.

99. Gmail.com siaubas – jaunuoliai iš Elektrėnų. *Kauno diena* [interaktyvus] 2010-06-03 [žiūrėta 2011-09-19] <http://kauno.diena.lt/naujienos/kriminalai/-gmail-com-siaubas-jaunuoliai-is-elektrenu-281729>.
100. Google targeted in e-mail scam [interaktyvus]. 2009-10-06 [žiūrėta 2011-09-18]. <http://news.bbc.co.uk/2/hi/technology/8292928.stm>.
101. Graham, J. 2009. *Cyber Fraud: Tactics, Techniques and Procedures*. Taylor&Francis Group.
102. Graždanskij kodeks Rosisjoj Federaciji. [interaktyvus,žiūrėta 2011-09-19]. <http://base.garant.ru/10164072/>.
103. Guide for the Security Certification and Accreditation of Federal Information Systems [interaktyvus]. 2008 [žiūrėta 2011-09-19]. <http://csrc.nist.gov/publications/nistpubs/800-53A/SP800-53A-final-sz.pdf>.
104. Guide to Authentication Standards for Online Services. State Services Commission, June 2006, Version 1.0. ISBN 0–478–24461–4. Crown Copyright [interaktyvus, žiūrėta 2011-09-15]. <http://www.e.govt.nz/library/egif-guide-to-authentication-standards-june-2006.pdf >.
105. Hack Pack The biggest identity theft case ever. Right here in Miami [interaktyvus, žiūrėta 2011-09-18]. <http://www.miaminewtimes.com/content/printVersion/2270696/>.
106. Health Insurance Portability and Accountability Act [interaktyvus, žiūrėta 2011-09-19]. <http://www.cms.gov/HIPAAGenInfo/Downloads/HIPAALaw.pdf>.
107. Heath, N. Brits living in fear of identity fraud [interaktyvus]. 2008-05-20 [žiūrėta 2011-09-15]. <http://www.silicon.com/legacy/research/specialreports/fulldisclosure/0,3800014102,39225528,00.htm>.
108. Heiman, B. J. 2003. Cybersecurity regulation is here. *RSA security conference*. Washington, D.C. Retrieved October 17, 2005.
109. Higgins, G. E. 2010. *Cybercrime: An Introduction to an Emerging Phenomenon*. McGraw-Hill.
110. Hoffman, S. K.; 2010. Mccinley T., G. *Identity theft*. Greenwood publishing group.
111. Hoikkanen A.; Bacigalupo, M., *et al.* New Challenges and Possible Policy Options for the Regulation of Electronic Identity. *Journal of International Commercial Law and Technology.* 2010, 5(1) [interaktyvus, žiūrėta 2011-09-15]. <http://www.jiclt.com/index.php/jiclt/index>.
112. How Does Identity Theft Impact Human Society? *eHow.com* [interaktyvus, žiūrėta 2011-07-14] <http://www.ehow.com/about_6293396_identity-theft-impact-human-society_.html>.
113. How to clean up your online reputation. IT Business.ca. [interaktyvus, žiūrėta 201-09-15]. <http://www.itbusiness.ca/it/client/en/home/News.asp?id=60843&PageMem=2>.

114. ID burglary risk ignored [interaktyvus]. 2008-04-22 [žiūrėta 2011-09-15]. <http://www.myfinances.co.uk/savings/news//bank-account-fraud/id-burglary-risk-ignored-$1219804.htm>.
115. Identity Cards Act 2006 [interaktyvus, žiūrėta 2011-09-19]. <http://www.legislation.gov.uk/ukpga/2006/15/introduction>.
116. Identity Theft and Assumption Deterrence Act, 1998 [interaktyvus, žiūrėta 2011-09-19]. <http://www.ftc.gov/os/statutes/itada/itadact.htm >.
117. Identity Theft Enforcement and Restitution Act of 2008 [interaktyvus, žiūrėta 2011-09-20]. <http://www.govtrack.us/congress/billtext.xpd?bill=h110-5938>.
118. Identity Theft Enhancement Penalty Act [interaktyvus, žiūrėta 2011-09-19]. <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ275.108.pdf>.
119. Identity Theft on the Rise: Survey [interaktyvus, žiūrėta 2011-09-18]. <http://gigaom.com/2010/02/10/identity-theft-on-the-rise-survey/>.
120. Identity Theft Resource Center [interaktyvus, žiūrėta 2011-09-14]. <http://www.idtheftcenter.org/>.
121. Informacijos technologijų saugos valstybinė strategija. *Valstybės žinios*, 2001, Nr. 110-4006.
122. Informacinės visuomenės plėtros komiteto prie Lietuvos Respublikos Vyriausybės direktoriaus 2008 m. gruodžio 1 d. įsakymas „Dėl viešojo administravimo institucijų informacinių sistemų interoperabilumo sistemos funkcionavimo taisyklių patvirtinimo“ Nr. T-228. *Valstybės žinios*. 2008, Nr. 145-5850.
123. Informacinių technologijų naudojimas namų ūkiuose [interaktyvus,žiūrėta 2011-09-15] <http://www.stat.gov.lt/lt/news/view/?id=7963 >.
124. Informacinių technologijų saugos atitikties vertinimo metodika, *Valstybės žinios*, 2004, Nr. 80-2855.
125. Internet Crime Report, 2010. Internet Crime Complaint Center [interaktyvus, žiūrėta 2011-09-19] <http://www.ic3.gov/media/annualreport/2010_ic3report.pdf>.
126. Internet usage in 2010 – Households and Individuals [interaktyvus, žiūrėta 2011-09-15]. <http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/KS-QA-10-050/EN/KS-QA-10-050-EN.PDF >
127. Interneto tarnybinių stočių apsaugos rekomendacijos. *Valstybės žinios*, 2004, Nr. 85-3095.
128. Interneto tinklapis „Tapatybės vagystė; netapk auka“, sukurtas bendradarbiaujant Jungtinės Karalystės vyriausybei ir privačiam sektoriui [interaktyvus, žiūrėta 2011-09-19]. <https://www.identitytheft.org.uk/criminal-offences.asp>.
129. Internetu plinta pavojingi pranešimai [interaktyvus]. 2011-07-18 [žiūrėta: 2011-09-18]. <http://www.rrt.lt/lt/pranesimai-spaudai/internetu-plinta-pavojingi-pranesimai.html>.

130. Interpol chief has Facebook identity stolen [interaktyvus]. 2010-09-19 [žiūrėta 2011-09-18]. <http://www.networkworld.com/news/2010/091910-interpol-chief-has-facebook-identity.html>.
131. Interpolo vadas: kibernetiniai nusikaltimai – didžiausia grėsmė [interaktyvus]. 2010-09-22 [žiūrėta 2011 09 18]. <http://www.elektronika.lt/naujienos/kompiuterija/25373/interpolo-vadas-kibernetiniai-nusikaltimai-didziausia-gresme>.
132. Iowa Code [section] 714.16B [interaktyvus, žiūrėta 2011-09-20]. <http://coolice.legis.state.ia.us/coolice/default.asp?category=billinfo&service=iowacode&ga=83&input=714>.
133. ISO/IEC 27001 [interaktyvus, žiūrėta 2011-09-20]. <http://en.wikipedia.org/wiki/ISO/IEC_27001>.
134. Įsilaužėliai pavogė „Citibank" klientų duomenis. *Delfi.lt* [interaktyvus]. 2011-06-09 [žiūrėta: 2011-09-18]. <http://verslas.delfi.lt/archive/print.php?id=46440885>.
135. Įsilaužėlis pralobti nespėjo. *Lietuvos rytas*, 2011-08-25.
136. Jakovlev, A. M. 1985. Teorija kriminologiji ir socialnaja praktika. Moskva: Nauka.
137. Javelin Study Finds Identity Fraud Reached New High in 2009, but Consumers are Fighting Back [interaktyvus, žiūrėta 2011-09-14]. <http://www.prnewswire.com/news-releases/javelin-study-finds-identity-fraud-reached-new-high-in-2009-but-consumers-are-fighting-back-83987287.html>.
138. Johannes, R. 2006 Identity Fraud Survey Report (abridged) (Javelin Strategy Research Jan. 2006) [interaktyvus, žiūrėta 2011-09-19]. <www.javelinstrategy.com/products/ 99DEBA/27/delivery.pdf>.
139. John M. Last. 2007. *A Dictionary of Public Health*. Oxford University Press, Inc.
140. Day, J. 2008. Red Flag Rules Require Companies to Take Identity Theft Seriously. *Venulex Legal Summaries*. Q4.
141. Judge Rules Facebook Trolling = Identity Theft. *Techmento* [interaktyvus, žiūrėta 2011-09-20]. <http://techmento.com/2011/08/03/judge-rules-facebook-trolling-identity-theft>.
142. Kanados teisingumo departamento oficialus tinklapis [interaktyvus, žiūrėta 2011-09-15]. <http://www.justice.gc.ca/>.
143. Kinijos baudžiamasis kodeksas [interaktyvus, žiūrėta 2011-09-19]. <http://www.cecc.gov/pages/newLaws/criminalLawENG.php>.
144. Kiškis, M.; Petrauskas, R.; Rotomskis, I.; Štitilis, D. 2006. *Teisės informatika ir informatikos teisė*. Vilnius: Mykolo Romerio universitetas.
145. Klein Aguilar, M. Red Flags Rule Enforcement Goes Into Effect. *Compliance Week*, 888.519.9200 JANUARY 2011.
146. Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui „Europos skaitmeninė

darbotvarkė“ KOM(2010) 245 galutinis [interaktyvus, žiūrėta 2011-09-14]. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:LT:PDF>.

147. Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui „Europos skaitmeninė darbotvarkė“ KOM(2010) 245 galutinis [interaktyvus, žiūrėta 2011-09-19]. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:LT:PDF>.
148. Komisijos sprendimas 2000 m. liepos 26 d. dėl Europos Parlamento ir Tarybos direktyvos 95/46/EB dėl „saugaus uosto“ privatumo principų teikiamos apsaugos pakankamumo ir su tuo susijusių JAV komercijos departamento pateiktų „Dažnai užduodamų klausimų“. [2000] OL L 215.
149. Konstitucinio Teismo 1999 m. spalio 21 d. nutarimas „Dėl vardų ir pavardžių rašymo Lietuvos Respublikos piliečio pase“. *Valstybės žinios.* 1999, Nr. 90-2662.
150. Konstitucinio Teismo 2002 m. rugsėjo 19 d. nutarimas „Dėl Telekomunikacijų, Operatyvinės veiklos įstatymų ir Baudžiamojo proceso kodekso“. *Valstybės žinios.* 2002, Nr. 93-4000.
151. Konvencija „Dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu“ ETS Nr. 108. *Valstybės žinios*. 2001, Nr. 32-1059.
152. Konvencija dėl elektroninių nusikaltimų. *Valstybėsžinios*, 2004, Nr. 36-1188.
153. Kshetri, N. 2010. *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives*. Springer-Verlag.
154. Kuner, C. *European Data Privacy law and Online Business*. Oxford: Oxford University Press, 2003.
155. La. Stat. Ann. [section] 9:3568. [interaktyvus, žiūrėta 2011-09-20] <http://www.legis.state.la.us/lss/lss.asp?folder=83>.
156. Latviją supurtė amžiaus vagystė. *Respublika* [interaktyvus]. 2010-02-17 [žiūrėta 2011-09-18]. <http://www.respublika.lt/lt/naujienos/pasaulis/nusikaltimai_ir_nelaimes/latvija_supurte_amziaus_vagyste/>.
157. Leenes, R. FIDIS, D5.2b: ID-related crime: towards a common ground for interdisciplinary research [interaktyvus]. 2006 [žiūrėta 2011-09-14]. <http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp5-del5.2b.ID-related_crime.pdf>.
158. Lietuviai tuštino JAV bankus neiškeldami kojos iš namų**.** *Lietuvos rytas* [interaktyvus]. 2010-01-28 [žiūrėta 2011-09-14]. <http://m.lrytas.lt/?data=20100128&id=akt28_a4100128&view=2>.
159. *Lietuvių kalbos žodynas*. Vilnius: Lietuvių kalbos institutas, 2005.
160. Lietuvos bankai masiškai blokuoja mokėjimo korteles dėl galimos duomenų vagystės. *Lietuvos rytas* [interaktyvus]. Vilnius, 2009-10-13 [žiūrėta 2011-09-14]. <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>.

161. Lietuvos informacinės visuomenės plėtros 2010-2015 m. strategijos projektas. [interaktyvus, žiūrėta 2011-09-15], <http://www.transp.lt>.
162. Lietuvos Respublikos administracinių teisės pažeidimų kodeksas. *Valstybės žinios*. 1985, Nr. 1-1.
163. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas. *Valstybės žinios.* 2008, Nr. 22-804.
164. Lietuvos Respublikos asmens tapatybės kortelės įstatymas. *Valstybės žinios*. 2001, Nr. 97-3417.
165. Lietuvos Respublikos baudžiamasis kodeksas. *Valstybės žinios*, 2000, Nr. 89-2741.
166. Lietuvos Respublikos civilinis kodeksas. *Valstybės žinios.* 2000, Nr. 74-2262.
167. Lietuvos Respublikos elektroninio parašo įstatymas. Valstybės žinios. 2000, Nr. 61-1827.
168. Lietuvos Respublikos elektroninių ryšių įstatymas, *Valstybės žinios.* 2004, Nr. 69-2382.
169. Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymo koncepcija. *Valstybės žinios*, 2006, Nr. 134-5081.
170. Lietuvos Respublikos Konstitucija. *Valstybės Žinios.* 1992, Nr. 33-1014.
171. Lietuvos Respublikos operatyvinės veiklos įstatymo Nr. XI-1374 3, 7, 9, 10, 11, 12, 13, 21, 23 straipsnių pakeitimo ir papildymo įstatymas. *Valstybės žinios.* 2011, Nr. 653047.
172. Lietuvos Respublikos ryšių reguliavimo tarnybos nuostatai, *Valstybės žinios.* 2004, Nr. 131-4743.
173. Lietuvos Respublikos ryšių reguliavimo tarnybos Tinklų ir informacijos saugumo skyriaus interneto tinklapis, skirtas informacijos saugai elektroninėje erdvėje [interaktyvus, žiūrėta 2011-09-18]. <http://www.esaugumas.lt/index.php?-229839978>.
174. Lietuvos Respublikos Seimo 2002 m. gegužės 28 d. nutarimu Nr. IX-907 patvirtinta Nacionalinio saugumo strategija. *Valstybės Žinios*. 2002, Nr. 56-2233.
175. Lietuvos Respublikos Seimo 2003 m. kovo 20 d. nutarimu Nr. IX-1383 patvirtinta Nacionalinė nusikaltimų prevencijos ir kontrolės programa. *Valstybės Žinios*. 2003, Nr. 32-1318.
176. Lietuvos Respublikos vidaus reikalų ministerijos nuostatai, *Valstybės* žinios. 2001, Nr. 27-794.
177. Lietuvos Respublikos vidaus reikalų ministro įsakymu Nr. 1V-247 patvirtintos Valstybės institucijų ir įstaigų informacinių sistemų klasifikavimo pagal jose tvarkomą elektroninę informaciją gairės ir Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos saugos reikalavimai. *Valstybės žinios.* 2007, Nr. 78-3160.
178. Lietuvos vartotojų instituto interneto tinklapis [interaktyvus, žiūrėta 2011-09-19]. <http://www.vartotojai.lt/index.php?id=7324>.

179. *LR Baudžiamojo kodekso komentaras*, II dalis, 2009.
180. LR pinigų plovimo ir teroristų finansavimo prevencijos įstatymas. *Valstybės žinios*. 2008, Nr. 10-335.
181. LR Statistikos departamentas. 16–74 m. amžiaus asmenys, kurie naudojosi kompiuteriu, internetu. [interaktyvus, žiūrėta 2011-09-15]. <http://db1.stat.gov.lt/statbank/selectvarval/saveselections.asp?MainTable=M9020201&PLanguage=0&TableStyle=&Buttons=&PXSId=9492&IQY=&TC=&ST=ST&rvar0=&rvar1=&rvar2=&rvar3=&rvar4=&rvar5=&rvar6=&rvar7=&rvar8=&rvar9=&rvar10=&rvar11=&rvar12=&rvar13=&rvar14=>.
182. LR vidaus reikalų ministro įsakymas „Dėl saugos dokumentų turinio gairių patvirtinimo“ 2007 m. gegužės 8 d. Nr. 1V-172. *Valstybės žinios.* 2007-05-15, Nr. 53-2070.
183. Mail Fraud Statute, Title 18, United States Code, Section 1341. [interaktyvus, žiūrėta 2011-09-15]. < http://www.law.cornell.edu/uscode/usc_sup_01_18_10_I_20_63.html>.
184. Mastercard Paypass® [interaktyvus, žiūrėta 2011-09-21] <http://www.mastercard.us/paypass.html >.
185. McCue, A. $350,000 Citibank theft victims 'gullible and careless [interaktyvus]. 2005-04-12 [žiūrėta 2011-09-15]. <http://www.silicon.com/legacy/research/specialreports/offshoring/0,3800003026,39129475,00.htm>.
186. Medvedev poruchil do 1 maja izdat akty dlja vypuska i premenenija UehK [interaktyvus]. 2011-03-16 [žiūrėta 2011-09-18]. <http://www.rian.ru/economy/20110316/354390288.html>.
187. Minimum Security Requirements for Federal Information and Information Systems [interaktyvus]. 2006 [žiūrėta 2011-09-19]. <http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf>.
188. Morrison & Foerster LLP. Identity Theft Red Flags Rule and Address Discrepancy Rule Frequently Asked Questions. Venulex Legal Summaries. 2008 Q3.
189. Murray V. Bank of America, N. A. [interaktyvus, žiūrėta 2011-09-20]. <http://www.judicial.state.sc.us/opinions/displayOpinion.cfm?caseNo=3634>.
190. MVD RF soobshhaet o kiberprestupnosti. [interaktyvus}. 2011-07-01 [žiūrėta 2011-09-15]. <http://www.crime-research.ru/news/01.07.2011/7251/>.
191. N.J. Stat. Ann. [section] 56:11-50. [interaktyvus, žiūrėta 2011-09-20]. <http://www.njleg.state.nj.us/2004/bills/pl05/226_.htm>.
192. Nacionalinio elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinio veiklos nuostatai. *Valstybės žinios.* 2009, Nr. 36-1419.
193. Nacionalinio saugumo pagrindų įstatymas. *Valstybės Žinios*. 1997, Nr. 2-16.
194. Nigerijos baudžiamasis kodeksas [interaktyvus, žiūrėta 2011-09-19]. <http://www.nigeria-law.org/Criminal%20Code%20Act-Tables.htm>.
195. Nir Kshetri. 2010. *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives*. Springer-Verlag.

196. No Ordinary Case of Identity Theft [interaktyvus]. October 18, 2004. [žiūrėta 2011-09-14]. <http://www.fbi.gov/news/stories/2004/october/uncoveridt_101504>.
197. Ob elektronnoj cifrovoj podpisi [interaktyvus, žiūrėta 2011-09-18]. <http://www.obki.ru/DOCS/zakonECP.rtf>.
198. OECD Guidelines for Consumer Protection in the Context of Electronic Commerce, 1999 [interaktyvus, žiūrėta 2011-09-21]. <http://browse.oecdbookshop.org/oecd/pdfs/free/9300023e.pdf>.
199. OECD Guidelines for Protecting Consumer from Fraudulent and Deceptive Commercial Practices Across Borders [interaktyvus, žiūrėta 2011-09-21] <http://www.oecd.org/dataoecd/24/33/2956464.pdf>.
200. OECD Guidelines for the Security of Information Systems and Networks, 2002 [interaktyvus, žiūrėta: 2011-09-21] <http://www.oecd.org/dataoecd/16/22/15582260.pdf>.
201. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980 [interaktyvus, žiūrėta 2011-09-21]. <http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00.html>.
202. OECD Policy Guidance on Online Indentity Theft. OECD Ministerial Meeting on the Future of the Internet Economy. Seoul, Korea, 17-18 June 2008.
203. OECD Recommendation on Consumer Dispute Resolution and Redress, 2007 [interaktyvus, žiūrėta 2011-09-21] <http://www.oecd.org/dataoecd/43/50/38960101.pdf>.
204. Oficialus Lietuvos Respublikos Konstitucinio Teismo tinklapis [interaktyvus, žiūrėta 2011-09-14]. <http://www.lrkt.lt/Pranesimai/txt_2010/L20100929c.htm>.
205. Oficialus Lietuvos Respublikos Seimo tinklapis [interaktyvus, žiūrėta 2011-09-14]. <http://www3.lrs.lt/pls/inter/w5_show?p_r=618&p_k=1&p_d=98673>.
206. Online Identity Theft [interaktyvus]. OECD, 2009 [žiūrėta 2011-09-14], <http://browse.oecdbookshop.org/oecd/pdfs/browseit/9309021E.PDF >.
207. Personal Data Is Pirated From Russian Phone Files. *The New York Times* [interaktyvus]. 2003-01-23 [žiūrėta 2011 09 19]. <http://www.nytimes.com/2003/01/23/business/personal-data-is-pirated-from-russian-phone-files.html>.
208. Petkevičius, P. 1996. *Administracinė atsakomybė*. Vilnius: Justitia.
209. Petrauskas, R.; Štitilis, D.; Rotomskis, I.; Paškauskas, Ž. 2006. International legislative Regulation Provisions Concerning the Security of Informations Systems and Information. Implementation of the Provisions in Lithuania. *Databases and Information Systems: seventh International baltic Conference on Databases and Information Systems.* Vilnius: Technika.
210. Phishing kits banned by new Fraud Act. *Out-Law news* [interaktyvus]. 2006-11-13 [žiūrėta 2011-09-15]. <www.out-law.com/page-7469>.

211. Piesliakas, V. 1993. Ekonominiai nusikaltimai Europos valstybių bei JAV teisėje. *Lietuvos policijos akademijos mokslo darbai* 1.
212. Piesliakas, V. 2009. *Lietuvos baudžiamoji teisė.* Antra pataisyta ir papildyta laida. Vilnius: Justitia, Kn. 1.
213. Piesliakas, V. 1996. *Mokymas apie nusikaltimą ir nusikaltimo sudėtį*. Vilnius: Lietuvos policijos akademija.
214. Piesliakas,V. 2008. *Lietuvos baudžiamoji teisė*. Vilnius: Justitia, Kn. 2.
215. Police and Justice Act 2006. [interaktyvus, žiūrėta 2011-09-19]. <http://www.legislation.gov.uk/ukpga/2006/48/contents>.
216. Pradedama naudoti patvirtinimą dviem veiksmais. Google žinynas [interaktyvus, žiūrėta 2011-09-21] <http://www.google.com/support/accounts/bin/static.py?hl=lt&page=guide.cs&guide=1056283&rd=1>.
217. Prancūzijos baudžiamasis kodeksas [interaktyvus, žiūrėta 2011-09-19]. <http://www.legislationline.org/documents/section/criminal-codes>.
218. Privacy Act of 1974 [interaktyvus, žiūrėta 2011-09-19]. <http://www.justice.gov/opcl/privstat.htm>.
219. Rai, S. Indian outsourcers move to fix security. *The New York Times* [interaktyvus]. 2005-06-17. [žiūrėta 2011-09-15]. <http://www.nytimes.com/2005/06/16/technology/16iht-security.html?_r=1>.
220. Rannenberg, K.; Royer, D.; Deuker, A. 2009. *The Future of Identity in the Information Society: Challenges and Opportunities*. Berlin: Springer.
221. Real ID Act [interaktyvus, žiūrėta 2011-09-19]. <http://www.ncsl.org/default.aspx?tabid=13582>.
222. Reed, C.; Angel, J. 2007. *Computer Law: the law and regulation of information technology*.
223. Reidenberg, J.R.; Schwartz. P. M. Data protection law and on-line services: regulatory responses. ARETE Study [interaktyvus, žiūrėta 2011-09-18]. <http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/regul_en.pdf >.
224. Remsburg, V. Docusearch, Inc. [interaktyvus, žiūrėta 2011-09-20]. <http://www.courts.state.nh.us/supreme/opinions/2003/remsb017.htm>.
225. Report on Identity Theft/Fraud. Fraud Prevention Expert Group. Brussels, 22 October 2007. [ineraktyvus, žiūrėta 2011-09-18]. <http://ec.europa.eu/internal_market/fpeg/docs/id-theft-report_en.pdf>.
226. Respublikos asmens tapatybės kortelės įstatymas. *Valstybės žinios*. 2001, Nr. 97-3418.
227. Review 2005 of the Data Protection Ombudsman [interaktyvus, žiūrėta 2011-09-19]. <www.tietosuoja.fi/uploads/q0vw1ft5.rtf>.
228. Rudzkienė V. 2005. *Socialinė statistika: vadovėlis*. Vilnius: Mykolo Romerio universiteto Leidybos centras.
229. Rudzkienė, V. 2010. *Parengta mokslinė-metodinė medžiaga*.

230. Rusijos Federacijos baudžiamasis kodeksas**.** [interaktyvus, žiūrėta 2011-09-19] <http://www.legislationline.org/download/action/download/id/1697/file/0cc1acff8241216090943e97d5b4.htm/preview>.
231. Russia accused of unleashing cyberwar to disable Estonia. G*uardian.co.uk.* [interaktyvus]. 2007-05-17 [žiūrėta 2011-09-18]. <http://www.guardian.co.uk/world/2007/may/17/topstories3.russia>.
232. Saugaus elektroninės informacijos teikimo sutartis. *Valstybės žinios*. 2007, Nr. 75-2980.
233. Saugos dokumentų turinio gairės. *Valstybės žinios*. 2007, Nr. 53-2070.
234. Saugumo priemonės ONE.LT [interaktyvus, žiūrėta 2011-09-21]. <http://saugumas.one.lt/ >.
235. Segalis, B. Russia Postpones Enforcement of Data Protection Law; Considers Revision [interaktyvus]. 2011-01-13 [žiūrėta 2011-09-19]. <http://www.infolawgroup.com/2011/01/articles/enforcement/russia-postpones-enforcement-of-data-protection-law-considers-revisions/>.
236. Sieber U. Legal Aspects of Computer-Related Crime in the Information Society. Comcrime study, prepared for European Commission [interaktyvus]. 1998 [žiūrėta 2011-09-20]. <http://www.archividelnovecento.it/archivinovecento/CAPPATO/Cappato/Faldone64-12Dirittiumanipaesiextracom/DonneAfghanistan/Desktop/sieber.pdf >.
237. Sileo, J. D. 2005. *Stolen lives: identity theft prevention made simple.*
238. Smith, A. The Red Flag Rules: A Closer Look. *Health Care Registration: The Newsletter for Health Care Registration Professionals*. Mar 2009, Vol. 18 Issue 6.
239. Social networking service [interaktyvus, žiūrėta 2011-09-21]. <http://en.wikipedia.org/wiki/Social_networking_service>.
240. Stan Z. Li, Anil K. Jain. 2009. *Encyclopedia of Biometrics*. Springer Science Business Media, LLC.
241. *Standardisation of definitions of identity crime terms: A step towards consistency*. Australasian Centre fo Policing research, 2006.
242. Standards for Security Categorization of Federal Information and Information Systems [interaktyvus]. 2004 [žiūrėta 2011-09-19]. <http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf>.
243. Starkus S.; Kiškis, A. 2008. Kam reikalingos prevencinės programos ir projektai? Kodėl prevencija, kodėl turime rengti prevencines programas ir/ar projektus? *Kriminologijos paskaitų konspektas*.
244. Sukčiai pakišo jauką – kalėdines nuolaidas. *Lietuvos rytas* [inetraktyvus]. 2010-12-10 [žiūrėta 2011 09 18]. <http://m.lrytas.lt/?data=20101210&id=akt10_a1101210&view=2>.
245. Sullivan, B. 2004.*Your evil twin: behind the identity theft epidemic.*
246. Sullivan, J. T. 2001. *Methods of Social research*. Northern Michigan University.

247. Suomijos baudžiamasis kodeksas**.** [interaktyvus, žiūrėta 2011-09-19]. <http://www.legislationline.org/documents/section/criminal-codes>.
248. Swartz, N. 2009. Will Red Flags Detour ID Theft? *Information Management* 43(1).
249. Štitilis D. 2002. *Teisinės atsakomybės už neteisėtas veikas elektroninėje erdvėje nustatymo problemos*. Daktaro disertacija, socialiniai mokslai, teisė 01 S.
250. Štitilis, D. 2003. Prekių ženklų naudojimas elektroninėje erdvėje: teisiniai aspektai. *Jurisprudencija* 41(33).
251. Štitilis, D.; Pakutinskas, P.; Dauparaitė, I.; Laurinaitis, M. 2011. Teisinė aplinka siekiant išvengti tapatybės vagystės elektroninėje erdvėje: JAV ir Lietuvos teisės aktų lyginamoji analizė, *Socialinės technologijos* 1(1).
252. Štitilis, D.; Pakutinskas, P.; Dauparaitė, I.; Laurinaitis, M. 2011. Preconditions for Legal Regulation of Personal Identification in Cyberspacem, *Jurisprudence* 18(2).
253. Štitilis, D.; Pakutinskas, P.; Dauparaitė, I.; Laurinaitis, M. 2011. Tapatybės vagystės elektroninėje erdvėje kriminalizavimas: lyginamieji aspektai, *Socialinių mokslų studijos* 3(1).
254. Štitilis, D.; Laurinaitis M. Tapatybės vagystė elektroninėje erdvėje. *Informacijos mokslai.* 2009, Nr. 50.
255. Štitilis, D.; Paškauskas, Ž. 2007. Valstybės elektroninės informacijos saugos strategija – vienas iš pagrindinių elektroninės informacijos saugos reguliavimo instrumentų: lyginamoji analizė, *Jurisprudencija* 92(2).
256. Tapatybės vagystė; netapk auka [interaktyvus, žiūrėta 2011-09-15]. <http://www.identitytheft.org.uk/identity-crime-definitions.asp>.
257. Testimony of Dennis Lormel, Chief, Terrorist Financing Operations Section, Counterterrorism Division, FBI Before the Senate Judiciary Committee, Subcommittee on Technology, Terrorism, and Government Information [interaktyvus]. 2002 [žiūrėta 2011-09-15]. <http://www.investigativeproject.org/documents/testimony/234.pdf>.
258. The Constitution of the Russian Federation of 25.12.1993 [interaktyvus, žiūrėta 2011-10-01] <http://www.constitution.ru/en/10003000-01.htm>.
259. The Cost of Cybercime, A Detica Report [interaktyvus]. 2011 [žiūrėta 2011-09-15]. <http://www.detica.com/uploads/resources/THE_COST_OF_CYBER_CRIME_SUMMARY_FINAL_14_February_2011.pdf>.
260. The Fair Credit Billing Act [interaktyvus, žiūrėta 2011-09-19]. <http://www.ftc.gov/os/statutes/fcb/fcb.pdf>.
261. The Following Countries Are in the Process of developing laws to Prosecute Cyber Crime [interaktyvus, žiūrėta 2011-09-20]. <http://www.mcconnellinternational.com>.
262. The President's Identity Theft Task Force, Combating Identity Theft: A Strategic Plan. [interaktyvus] April 2007, 13 [žiūrėta 2011-09-14]. <www.idtheft.gov/reports/StrategicPlan.pdf>.

263. Tidikis, R. 2003. *Socialinių mokslų tyrimų metodologija*. Lietuvos teisės universitetas.
264. Twitter lankomumas per metus išaugo 109 proc. [interaktyvus]. 2010-08-18–22 [žiūrėta2011-09-18]. <http://www.elektronika.lt/news/computers/24804/>.
265. Ugolovnij kodeks Rosiskoj Federaciji. [interaktyvus, žiūrėta 2011-09-19]. <http://www.interlaw.ru/law/docs/10008000/>.
266. *Understanding and Mitigating Identity Theft*. 2009. Thomson Reuters.
267. United Kingdom Cabinet Office, Economic and Domestic Secretariat. Identity Fraud: A Study [interaktyvus]. London, 2002 [žiūrėta 2011-09-14]. <http://www.statewatch.org/news/2004/may/id-fraud-report.pdf>.
268. United Nations Manual on Computer-Related Crime. *International Review of Criminal Policy* Nos. 43/44, 1994 [interaktyvus, žiūrėta 2011-09-20]. <http://www.uncjin.org/Documents/EighthCongress.html>.
269. United Nations Manual on the prevention and control of computer-related crime. 2001 [interaktyvus, žiūrėta 2011-09-25]. < http://www.bcbkuwait.com/english/int_regulations/UN/CompCrims_UN_Guide.pdf>.
270. United States Code („U. S. C"), [interaktyvus, žiūrėta 2011-09-19]. < http://www.law.cornell.edu/uscode/>.
271. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act [interaktyvus,žiūrėta 2011-09-19]. <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107.pdf >.
272. US FTC (2007a), Report on Consumer Fraud and Identity Theft Complaint Data [interaktyvus, žiūrėta 2011-07-14] <http://www.ftc.gov/opa/2008/02/fraud.pdf>.
273. Using Someone Else's Facebook Is ID Theft: CA Judge. *Findlaw* [interaktyvus]. 2011-08-05 [žiūrėta 2011-09-20]. <http://blogs.findlaw.com/blotter/2011/08/using-someone-elses-facebook-is-id-theft-ca-judge.html>.
274. Vaišvila, A. 1998. Baudžiamoji justicija – juridinė asmens teisinio statuso identifikacija, *Teisės problemos* 3–4 (21, 22).
275. Vaišvila, A. *Teisės teorija*. 2009. Vilnius: Mykolo Romerio universitetas, 3-asis eid.
276. Valstybės informacinių sistemų steigimo ir įteisinimo taisyklės. *Valstybės žinios*. 2004, Nr. 58-2061.
277. Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos techniniuose saugos reikalavimuose. *Valstybės žinios*. 2008, Nr. 127-4866.
278. Valstybės institucijų ir įstaigų informacinių sistemų klasifikavimo pagal jose tvarkomą elektroninę informaciją gairės. *Valstybės žinios*. 2007, Nr. 78-3160.
279. *Valstybės ir teisės teorija*. 1989. Vilnius: Mintis.
280. Valstybinė duomenų apsaugos inspekcija [interaktyvus]. Vilnius, [žiūrėta 2011-09-03]. < http://www.ada.lt>.

281. Visa PayWave [interaktyvus, žiūrėta 2011-09-21] <http://usa.visa.com/personal/cards/paywave/index.html>.
282. Vokietijoje naujas įstatymas draus darbdaviams tikrinti „Facebook“ profilius. *Delfi.lt* [interaktyvus]. 2010-08-25 [žiūrėta 2011-09-21]. <http://gyvenimas.delfi.lt/career/article.php?id=35817883 >.
283. Walden, I. 2007. *Computer Crimes and Digital Investigations*.
284. Williams, M. *Virtually criminal: Crime, deviance and regulation online*. New York: Routledge, 2006.
285. Winston & Strawn LLP. 2010. FTC Red Flags Rule Reminder to Financial Institutions and Creditors. *Financial Services*.
286. Wire Fraud Statute, Title 18, United States Code, Section 1343 [interaktyvus, žiūrėta 2011-09-15]. < http://www.law.cornell.edu/uscode/usc_sup_01_18_10_I_20_63.html>.
287. WiredSafety [interaktyvus, žiūrėta 2011-09-21]. <http://www.wiredsafety.org/>.
288. Wold, Ch. *A Practical Guide to the Red Flag Rules: Identifying and Addressing Indentity Theft Risks*. Practising Law Institute; 1st edition, 2008.
289. Wu Nanlan. Police crack down on Internet identity theft [interaktyvus]. 2008-01-11 [žiūrėta 2011-09-15]. <http://www.china.org.cn/english/China/239068.htm>.
290. Žurnalas „Veidas“, 2011-08-08.

PRIEDAI

1 priedas. Konvencija dėl elektroninių nusikaltimų

KONVENCIJA DĖL ELEKTRONINIŲ NUSIKALTIMŲ

2001 11 23, Budapeštas

PREAMBULĖ

Europos Tarybos valstybės narės ir kitos šią Konvenciją pasirašiusios valstybės,

TURĖDAMOS omenyje, kad Europos Tarybos tikslas – siekti didesnės savo narių vienybės;

PRIPAŽINDAMOS skatinimo bendradarbiauti su kitomis šios Konvencijos šalimis svarbą;

ĮSITIKINUSIOS, kad būtina pirmenybę teikti bendros baudžiamosios politikos, kuria siekiama apsaugoti visuomenę nuo elektroninių nusikaltimų, *inter alia* priimant tinkamus teisės aktus ir skatinant tarptautinį bendradarbiavimą, vykdymui;

MATYDAMOS dideles permainas, vykstančias dėl kompiuterių tinklų skaitmeninio keitimo, susiliejimo ir nuolatinės globalizacijos;

SUSIRŪPINUSIOS, kad kompiuteriniai tinklai ir elektroninė informacija taip pat gali būti naudojami daryti nusikaltimams ir kad tokių nusikaltimų įrodymai gali būti saugomi šiuose tinkluose ir jais perduodami;

PRIPAŽINDAMOS, kad valstybėms ir privačiam verslui būtina bendradarbiauti kovojant su elektroniniais nusikaltimais ir būtinybę ginti teisėtus interesus naudojant bei plėtojant informacines technologijas;

MANYDAMOS, kad norint sėkmingai kovoti su elektroniniais nusikaltimais reikia tarptautiniu mastu daugiau, greičiau ir sklandžiau bendradarbiauti baudžiamosiose bylose;

ĮSITIKINUSIOS, kad ši Konvencija, nustatydama joje apibūdintų veikų baudžiamumą, suteikdama pakankamai įgaliojimų veiksmingai kovoti su tokiais nusikaltimais, palengvindama jų susekimą, tyrimą bei baudžiamąjį persekiojimą nacionaliniu bei tarptautiniu lygiu ir pateikdama greito bei patikimo tarptautinio bendradarbiavimo gaires, yra reikalinga, kad būtų sustabdyti veiksmai, nukreipti prieš kompiuterinių sistemų, tinklų ir kompiu-

terinių duomenų konfidencialumą, vientisumą ir prieinamumą, taip pat kad nebūtų leista netinkamai naudoti tokių sistemų, tinklų ir duomenų;

SUPRASDAMOS poreikį užtikrinti tinkamą balansą tarp teisėsaugos interesų ir pagarbos pagrindinėms žmogaus teisėms, įtvirtintoms 1950 m. Europos Tarybos Žmogaus teisių ir pagrindinių laisvių apsaugos konvencijoje, 1966 m. Jungtinių Tautų tarptautiniame pilietinių ir politinių teisių pakte ir kitose taikytinose tarptautinėse žmogaus teisių sutartyse, kurios dar kartą patvirtina kiekvieno asmens teisę laisvai laikytis savo nuomonės, taip pat laisvai reikšti savo mintis ir įsitikinimus, nepaisant valstybių sienų, gauti bei perduoti visokią informaciją ir idėjas ir teisę į tai, kad būtų gerbiamas jo asmeninis gyvenimas;

SUPRASDAMOS, be kita ko, būtinybę apsaugoti asmens duomenis, kaip nustatyta 1981 m. Europos Tarybos konvencijoje dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu;

ATSIŽVELGDAMOS į 1989 m. Jungtinių Tautų vaiko teisių konvenciją ir 1999 m. Tarptautinės darbo organizacijos blogiausių vaikų darbo formų konvenciją;

ATSIŽVELGDAMOS į galiojančias Europos Tarybos konvencijas dėl bendradarbiavimo baudžiamojoje srityje, taip pat į panašias sutartis, sudarytas tarp Europos Tarybos valstybių narių ir kitų valstybių, ir PAŽYMĖDAMOS, jog šios Konvencijos tikslas – papildyti šias konvencijas, kad nusikaltimų, susijusių su kompiuterinėmis sistemomis ir duomenimis, tyrimas ir nagrinėjimas būtų atliekami veiksmingiau ir kad šių nusikaltimų įrodymus būtų galima rinkti elektroniniu pavidalu;

PRITARDAMOS naujausiems poslinkiams, skatinantiems tarptautinį supratimą ir bendradarbiavimą kovojant su elektroniniais nusikaltimais, tarp jų Jungtinių Tautų, OECD, Europos Sąjungos ir G8 veiksmus;

ATSIMINDAMOS Rekomendaciją Nr. R(85) 10, skirtą praktiniam Europos konvencijos dėl savitarpio pagalbos baudžiamosiose bylose taikymui vykdant teismo pavedimus dėl telekomunikacinių priemonių pasiklausymo, Rekomendaciją Nr. R(88) 2 dėl autorių teisių ir gretutinių teisių pažeidimų, Rekomendaciją Nr. R(87) 15, reglamentuojančią asmens duomenų naudojimą policijos pajėgose, Rekomendaciją Nr. R(95) 4 dėl asmens duomenų apsaugos telekomunikacijų paslaugų srityje, ypač telefono ryšio paslaugų srityje, taip pat Rekomendaciją Nr. R(89) 9 dėl kompiuterinių nusikaltimų, kurioje pateikiamos rekomendacijos valstybių įstatymų leidybos institucijoms dėl kai kurių kompiuterinių nusikaltimų apibrėžimų, ir Rekomendaciją Nr. R(95) 13 dėl baudžiamojo proceso teisės problemų, susijusių su informacijos technologijomis;

ATSIŽVELGDAMOS į Rezoliuciją Nr. 1, priimtą Europos valstybių teisingumo ministrų 21-ojoje konferencijoje (1997 m. birželis, Praha), rekomendavusią Ministrų Komitetui paremti darbą, kurį Europos nusikalstamumo problemų komitetas (CDPC) atlieka elektroninių nusikaltimų srityje siekdamas vienodinti nacionalinės baudžiamosios teisės nuostatas ir tokių nusikaltimų tyrimui taikyti veiksmingas priemones, taip pat Rezoliuciją Nr. 3, priimtą Europos valstybių teisingumo ministrų 23-iojoje konferencijoje (2000 m. birželis, Londonas), kurioje besiderančios šalys raginamos toliau ieškoti tinkamų sprendimų, kad kuo daugiau valstybių galėtų tapti šios Konvencijos Šalimis, ir pripažįstamas reikalas turėti greitai ir gerai veikiančią tarptautinio bendradarbiavimo sistemą, kurioje būtų deramai atsižvelgiama į kovos su elektroniniais nusikaltimais ypatumus;

ATSIŽVELGDAMOS, be to, į Europos Tarybos valstybių ir jų vyriausybių vadovų veiksmų planą, priimtą antrajame viršūnių susitikime (1997 m. spalio 10–11 d., Strasbūras), kuriuo siekiama bendro atsako į naujų informacinių technologijų plėtrą, pagrįsto Europos Tarybos kriterijais ir vertybėmis,

s u s i t a r ė:

I SKYRIUS. SĄVOKŲ VARTOJIMAS

1 straipsnis. Sąvokų apibrėžimai

Šioje Konvencijoje:

a) „kompiuterinė sistema“ – tai įtaisas arba tarpusavyje sujungtų ar susijusių įtaisų grupė, iš kurių vienas ar daugiau pagal programą automatiškai apdoroja duomenis;

b) „kompiuteriniai duomenys“ – tai bet kokia faktų, informacijos arba sąvokų pateiktis tokiu pavidalu, kad juos būtų galima apdoroti kompiuterine sistema, taip pat programa, pagal kurią kompiuterinė sistema gali vykdyti tam tikrą funkciją;

c) „paslaugos teikėjas“ – tai:

i) bet kuris viešasis ar privatus subjektas, teikiantis savo paslaugos vartotojams galimybę bendrauti pasinaudojant kompiuterine sistema;

ii) bet kuris kitas subjektas, apdorojantis arba saugantis tokios ryšio paslaugos arba tokios paslaugos vartotojų kompiuterinius duomenis;

d) „srauto duomenys“ – tai visi kompiuteriniai duomenys, perduodami kompiuterine sistema, suformuoti kompiuterinės sistemos, kuri sudaro ryšio grandinės dalį, ir rodantys perduotos informacijos kilmę, paskirtį, perdavimo kelią, laiką, datą, dydį, trukmę arba pagrindinės paslaugos rūšį.

II SKYRIUS. PRIEMONĖS, KURIŲ REIKIA IMTIS NACIONALINIU LYGIU

1 skirsnis. Materialioji baudžiamoji teisė

1 dalis. Nusikaltimai kompiuterinių duomenų ir sistemų konfidencialumui, vientisumui ir prieinamumui

2 straipsnis. Neteisėta prieiga

Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti pagal jos vidaus teisę nustatyti baudžiamajai atsakomybei už sąmoningą ir neteisėtą prieigą prie visos kompiuterinės sistemos arba jos dalies. Šalis gali reikalauti, kad toks nusikaltimas būtų padarytas pažeidžiant apsaugos priemones, ketinant gauti kompiuterinius duomenis ar turint kitą nesąžiningą ketinimą, arba kad jis būtų susijęs su kompiuterine sistema, sujungta su kita kompiuterine sistema.

3 straipsnis. Neteisėta perimtis

Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti pagal jos vidaus teisę nustatyti baudžiamajai atsakomybei už sąmoningą ir neteisėtą neviešo kompiuterinių duomenų perdavimo į kompiuterinę sistemą, iš jos ir jos viduje perimtį techninėmis priemonėmis, taip pat už elektromagnetinės emisijos iš kompiuterinės sistemos, perduodančios tokius kompiuterinius duomenis, perimtį. Šalis gali reikalauti, kad toks nusikaltimas būtų padarytas turint nesąžiningą ketinimą arba susijęs su kompiuterine sistema, sujungta su kita kompiuterine sistema.

4 straipsnis. Poveikis duomenims

1. Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti pagal jos vidaus teisę nustatyti baudžiamajai atsakomybei už sąmoningą ir neteisėtą kompiuterinių duomenų sugadinimą, sunaikinimą, apgadinimą, pakeitimą arba galimybės naudotis tokiais duomenimis panaikinimą.

2. Šalis gali pasilikti teisę reikalauti, kad veika, apibūdinta šio straipsnio 1 dalyje, turi padaryti didelę žalą.

5 straipsnis. Poveikis sistemai

Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti pagal jos vidaus teisę nustatyti baudžiamajai atsakomybei už sąmo-

ningą ir neteisėtą didelį kompiuterinės sistemos darbo trukdymą įvedant, perduodant, sugadinant, sunaikinant, apgadinant, pakeičiant kompiuterinius duomenis arba panaikinant galimybę naudotis tokiais duomenimis.

6 straipsnis. Netinkamas įtaisų naudojimas

1. Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti pagal jos vidaus teisę nustatyti baudžiamajai atsakomybei už sąmoningą ir neteisėtą:

a) gaminimą, pardavimą, įsigijimą naudoti, įvežimą, platinimą arba kitokį galimybės naudotis suteikimą:

i) įtaiso, įskaitant kompiuterinę programą, sukurto ar pritaikyto pirmiausia 2–5 straipsniuose apibūdintiems nusikaltimams daryti;

ii) kompiuterio slaptažodžio, prieigos kodo arba panašių duomenų, kuriais galima prieiti prie visos kompiuterinės sistemos arba jos dalies,

kai ketinama juos panaudoti 2–5 straipsniuose apibūdintiems nusikaltimams daryti, ir

b) a punkto i ir ii papunkčiuose minimo dalyko turėjimą ketinant jį panaudoti 2–5 straipsniuose apibūdintiems nusikaltimams daryti. Šalis, vadovaudamasi savo teise, gali reikalauti, kad baudžiamoji atsakomybė būtų užtraukiama tik turint keletą tokių dalykų.

2. Šis straipsnis negali būti aiškinamas kaip užtraukiantis baudžiamąją atsakomybę kai šio straipsnio 1 dalyje minimas gaminimas, pardavimas, įsigijimas naudoti, įvežimas, platinimas ir kitoks galimybės naudotis suteikimas arba turėjimas nėra skirtas daryti nusikaltimui, apibūdintam šios Konvencijos 2–5 straipsniuose, o tik sankcionuotam kompiuterinės sistemos tikrinimui arba jos apsaugai.

3. Kiekviena Šalis gali pasilikti teisę netaikyti šio straipsnio 1 dalies, jei ši išlyga nesiejama su pardavimu, platinimu arba kitokiu galimybės naudoti šio straipsnio 1 dalies a punkto ii papunktyje nurodytas priemones sudarymą.

2 dalis. Kompiuteriniai nusikaltimai

7 straipsnis. Kompiuterinės klastotės

Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti pagal jos vidaus teisę nustatyti baudžiamajai atsakomybei už sąmoningą ir neteisėtą kompiuterių duomenų įvedimą, pakeitimą, sunaikinimą arba galimybės naudotis tokia informacija panaikinimą, kurių pasekmė yra

neautentiški duomenys, su tikslu, kad jie būtų laikomi autentiškais, ar jais būtų naudojamasi teisėtiems tikslams, nepriklausomai nuo to, ar šie duomenys yra tiesiogiai skaitomi ir suprantami. Šalis gali reikalauti, kad baudžiamoji atsakomybė užtraukiama tik esant ketinimui apgauti ar panašiam nesąžiningam ketinimui.

8 straipsnis. Kompiuterinis sukčiavimas

Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti pagal jos vidaus teisę nustatyti baudžiamajai atsakomybei už sąmoningus ir neteisėtus veiksmus, sąlygojusius kito asmens nuosavybės praradimą:

a) įvedant, pakeičiant, sunaikinant kompiuterinius duomenis arba panaikinant galimybę naudotis tokiais duomenimis;

b) paveikiant kompiuterinės sistemos darbą,

nesąžiningai arba nedorai ketinant gauti neteisėtos ekonominės naudos sau arba kitam asmeniui.

3 dalis. Turinio nusikaltimai

9 straipsnis. Nusikaltimai, susiję su vaikų pornografija

1. Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti pagal jos vidaus teisę nustatyti baudžiamajai atsakomybei už tokią sąmoningą ir neteisėtą veiką:

a) pornografinio turinio produkcijos, kurioje atvaizduotas vaikas, gaminimą turint tikslą platinti per kompiuterinę sistemą;

b) pornografinio turinio produkcijos, kurioje atvaizduotas vaikas, siūlymą arba pateikimą per kompiuterinę sistemą;

c) pornografinio turinio produkcijos, kurioje atvaizduotas vaikas, platinimą arba perdavimą per kompiuterinę sistemą;

d) pornografinio turinio produkcijos, kurioje atvaizduotas vaikas, įsigijimą per kompiuterinę sistemą sau arba kitam asmeniui;

e) pornografinio turinio produkcijos, kurioje atvaizduotas vaikas, laikymą kompiuterinėje sistemoje arba kokioje nors kompiuterinių duomenų atmeniojoje terpėje.

2. Šio straipsnio 1 dalyje „pornografinio turinio produkcija, kurioje atvaizduotas vaikas“ – tai pornografinė medžiaga, vizualiai vaizduojanti:

a) aiškiai seksualų nepilnamečio elgesį;

b) aiškiai seksualų asmens, atrodančio kaip nepilnametis, elgesį;

c) tikroviškus nepilnamečio aiškiai seksualaus elgesio vaizdus.

3. Šio straipsnio 2 dalyje sąvoka „nepilnametis“ reiškia visus asmenis iki 18 metų. Tačiau bet kuri Šalis gali nustatyti žemesnę amžiaus ribą, ir tas amžius negali būti mažiau nei 16 metų.

4. Kiekviena Šalis gali pasilikti teisę netaikyti visų arba kai kurių šio straipsnio 1 dalies d bei e punktų ir 2 dalies b bei c punktų.

4 dalis. Nusikaltimai, susiję su autorių teisių ir gretutinių teisių pažeidimais

10 straipsnis. Nusikaltimai, susiję su autorių teisių ir gretutinių teisių pažeidimais

1. Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti pagal jos vidaus teisę nustatyti baudžiamajai atsakomybei už autorių teisių pažeidimus, kaip apibrėžta tos Šalies teisėje laikantis įsipareigojimų, kuriuos ji prisiėmė pagal Berno konvencijos dėl literatūros ir meno kūrinių apsaugos Paryžiaus aktą, priimtą 1971 m. liepos 24 d., Sutartį dėl intelektinės nuosavybės teisių prekyboje aspektų ir WIPO autorių teisių sutartį, išskyrus moralines teises, suteikiamas tokių konvencijų, kai tokie veiksmai atliekami sąmoningai, komerciniais tikslais ir naudojantis kompiuterių sistema.

2. Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti pagal jos vidaus teisę nustatyti baudžiamajai atsakomybei už gretutinių teisių pažeidimus, kaip apibrėžta tos Šalies teisėje laikantis įsipareigojimų, kuriuos ji prisiėmė pagal Romoje sudarytą Tarptautinę konvenciją dėl atlikėjų, fonogramų gamintojų ir transliuojančiųjų organizacijų apsaugos (Romos konvencija), Sutartį dėl intelektinės nuosavybės teisių prekyboje aspektų ir WIPO atlikimų ir fonogramų sutartį, išskyrus moralines teises, suteikiamas tokių konvencijų, kai tokie veiksmai atliekami sąmoningai, komerciniais tikslais ir naudojantis kompiuterių sistema.

3. Šalis gali pasilikti teisę ribotomis aplinkybėmis nenustatyti baudžiamosios atsakomybės, užtraukiamos pagal šio straipsnio 1 ir 2 dalis, jeigu esama kitų veiksmingų priemonių ir jeigu tokia išlyga nepažeidžia Šalies tarptautinių įsipareigojimų, išvardytų tarptautiniuose dokumentuose, minimuose šio straipsnio 1 ir 2 dalyse.

5 dalis. Papildoma atsakomybė ir sankcijos

11 straipsnis. Pasikėsinimas ir bendrininkavimas arba kurstymas

1. Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti pagal jos teisės aktus nustatyti baudžiamajai atsakomybei už

sąmoningą bendrininkavimą arba kurstymą daryti nusikaltimus, išvardytus šios Konvencijos 2–10 straipsniuose, ketinant tuos nusikaltimus padaryti.

2. Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti pagal jos teisės aktus nustatyti baudžiamajai atsakomybei už sąmoningą pasikėsinimą daryti nusikaltimus, išvardytus šios Konvencijos 3–5, 7, 8 straipsniuose, 9 straipsnio 1 dalies a ir c punktuose.

3. Kiekviena Šalis pasilieka teisę netaikyti visos šio straipsnio 2 dalies arba kai kurių jos nuostatų.

12 straipsnis. Juridinio asmens atsakomybė

1. Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti užtikrinant, kad juridinis asmuo galėtų būti patrauktas atsakomybėn už nusikaltimus, minimus šioje Konvencijoje ir padarytus jo naudai fizinio asmens, veikiančio individualiai arba kaip juridinio asmens organo dalis ir einančio vadovaujančias pareigas juridiniame asmenyje, paremtas teise:

a) atstovauti šiam juridiniam asmeniui;

b) priimti sprendimus šio juridinio asmens vardu;

c) kontroliuoti juridinio asmens veiklą.

2. Be jau minėtų 1 dalyje atvejų, kiekviena Šalis imasi priemonių, reikalingų užtikrinti, kad juridinis asmuo galėtų būti patrauktas atsakomybėn, kai dėl šio straipsnio 1 dalyje minimo fizinio asmens nepakankamos priežiūros arba kontrolės jurinio asmens įgaliotam fiziniam asmeniui buvo galima juridinio asmens naudai padaryti šioje Konvencijoje nustatytą nusikaltimą.

3. Atsižvelgiant į Šalies teisės principus, juridinio asmens atsakomybė gali būti baudžiamoji, civilinė arba administracinė.

4. Tokia atsakomybė nepašalina fizinių asmenų, padariusių nusikaltimą, baudžiamosios atsakomybės.

13 straipsnis. Sankcijos ir priemonės

1. Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti užtikrinti, kad už 2–11 straipsniuose minimus nusikaltimus būtų taikomos veiksmingos, proporcingos ir atgrasančios sankcijos, įskaitant laisvės atėmimą.

2. Kiekviena Šalis užtikrina, kad juridiniams asmenims, traukiamiems atsakomybėn pagal 12 straipsnį, būtų taikomos veiksmingos, proporcingos ir atgrasančios baudžiamosios arba nebaudžiamosios sankcijos arba priemonės, įskaitant pinigines baudas.

2 skirsnis. Proceso teisė

1 dalis. Bendrosios nuostatos

14 straipsnis. Procesinių nuostatų taikymo sritis

1. Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti nustatyti šiame skirsnyje numatytiems įgaliojimams ir procedūroms konkretiems nusikaltimams tirti ar nagrinėti.

2. Išskyrus 21 straipsnyje konkrečiai nustatytus atvejus, kiekviena Šalis šio straipsnio 1 dalyje minimus įgaliojimus ir procedūras taiko:

a) nusikaltimams, nustatytiems šios Konvencijos 2–11 straipsniuose;

b) kitiems nusikaltimams, padarytiems naudojantis kompiuterine sistema,

c) nusikaltimo įrodymų rinkimui elektroniniu pavidalu.

3. a) Kiekviena Šalis gali pasilikti teisę 20 straipsnyje minimas priemones taikyti tiktai išlygoje nurodytiems nusikaltimams arba nusikaltimų kategorijoms, jeigu tokių nusikaltimų arba nusikaltimų kategorijų apimtis nėra siauresnė nei nusikaltimų, kuriems ji taiko 21 straipsnyje minimas priemones. Kiekviena Šalis apsvarsto, kaip apriboti tokią išlygą, kad būtų galima kuo plačiau taikyti 20 straipsnyje minimas priemones.

b) Jeigu Šalis dėl jos teisės aktuose, galiojančiuose šios Konvencijos priėmimo metu, esančių apribojimų negali 20 ir 21 straipsniuose minimų priemonių taikyti informacijai, perduodamai paslaugos teikėjo kompiuterinėje sistemoje, kuri:

i) veikia uždaros vartotojų grupės naudai,

ii) nenaudoja viešųjų ryšių tinklų ir nėra sujungta su kita vieša ar privačia kompiuterine sistema,

ta Šalis gali pasilikti teisę netaikyti šių priemonių tokiai informacijai. Kiekviena Šalis apsvarsto, kaip apriboti tokią išlygą, kad būtų galima kuo plačiau taikyti 20 ir 21 straipsniuose minimas priemones.

15 straipsnis. Sąlygos ir garantijos

1. Kiekviena Šalis užtikrina, kad šiame skirsnyje numatytų įgaliojimų ir procedūrų nustatymas, vykdymas ir taikymas priklausytų nuo sąlygų ir garantijų, numatytų tos valstybės vidaus teisėje, kurios laiduoja tinkamą žmogaus teisių ir laisvių apsaugą, įskaitant teises, kylančias iš įsipareigojimų, prisiimtų pagal 1950 m. Europos Tarybos žmogaus teisių ir pagrindinių laisvių apsaugos konvenciją, 1966 m. Jungtinių Tautų tarptautinį pilietinių ir

politinių teisių paktą bei kitus taikytinus tarptautinius žmogaus teisių dokumentus, ir pagal kurias laikomasi proporcingumo principo.

2. Prie tokių sąlygų ir garantijų, tinkamai atsižvelgiant į įgaliojimo arba procedūros pobūdį, *inter alia* yra priskiriama teisminė arba kitokia nepriklausoma priežiūra, jų taikymą pateisinantys pagrindai ir tokio įgaliojimo arba tokios procedūros taikymo srities bei trukmės apribojimas.

3. Tiek, kiek tai neprieštarauja visuomenės interesams, ypač tinkamam teisingumo vykdymui, kiekviena Šalis apsvarsto šiame skirsnyje minimų įgaliojimų ir procedūrų poveikį trečiųjų šalių teisėms, įsipareigojimams ir teisėtiems interesams.

2 dalis. Operatyvus laikomųjų kompiuterinių duomenų išsaugojimas

16 straipsnis. Operatyvus laikomųjų kompiuterinių duomenų išsaugojimas

1. Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti įgalinant jos kompetentingas institucijas nurodyti arba panašiai pasirūpinti operatyviu konkrečių kompiuterinių duomenų, įskaitant srauto duomenis, laikomus kompiuterinėje sistemoje, išsaugojimu, ypač kai yra pagrindo manyti, jog tie kompiuteriniai duomenys gali būti nesunkiai prarasti arba pakeisti.

2. Kai vykdydama šio straipsnio 1 dalį Šalis kuriam nors asmeniui nurodo išsaugoti tam tikrus to asmens turimus ir valdomus kompiuterinius duomenis, Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti, kad tas asmuo būtų įpareigotas išsaugoti ir išlaikyti tokių kompiuterių duomenų vientisumą tiek laiko, kiek tai yra reikalinga, ne ilgiau kaip 90 dienų, kad kompetentingos institucijos galėtų pareikalauti juos atskleisti. Šalis gali numatyti, kad toks nurodymas vėliau gali būti kartojamas.

3. Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti, kad kompiuterinių duomenų saugotojas arba kitas juos saugantis asmuo būtų įpareigotas išlaikyti tokių procedūrų slaptumą tiek laiko, kiek numatyta pagal tos Šalies vidaus teisę.

4. Šiame straipsnyje minimiems įgaliojimams ir procedūroms taikomi 14 ir 15 straipsniai.

17 straipsnis. Operatyvus srauto duomenų išsaugojimas ir dalinis atskleidimas

1. Pagal 16 straipsnį būtinų išsaugoti srauto duomenų atžvilgiu kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti:

a) užtikrinti, kad toks operatyvus srauto duomenų išsaugojimas yra galimas, nepaisant to, ar tokią informaciją perdavė vienas ar daugiau paslaugos teikėjų;

b) užtikrinti, kad kompetentingai Šalies institucijai arba jos paskirtam asmeniui būtų operatyviai atskleista pakankamai srauto duomenų, leidžiančių Šaliai nustatyti paslaugos teikėjus ir tos informacijos perdavimo kelią.

3. Šiame straipsnyje minimiems įgaliojimams ir procedūroms taikomi 14 ir 15 straipsniai.

3 dalis. Nurodymas dėl duomenų pateikimo

18 straipsnis. Nurodymas dėl duomenų pateikimo

1. Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti, įgalinant jos kompetentingas institucijas nurodyti:

a) jos teritorijoje esančiam asmeniui pateikti konkrečiai nurodytus to asmens turimus arba valdomus kompiuterinius duomenis, laikomus kompiuterinėje sistemoje arba kompiuterinių duomenų atmeniojoje terpėje;

b) paslaugos teikėjui, tos Šalies teritorijoje siūlančiam savo paslaugas, pateikti jo turimą arba valdomą abonentinę informaciją, susijusią su tokiomis paslaugomis.

2. Šiame straipsnyje minimiems įgaliojimams ir procedūroms taikomi 14 ir 15 straipsniai.

3. Šiame straipsnyje „abonentinė informacija“ – tai bet kuri kompiuterinių duomenų ar kitokio pavidalo (išskyrus srauto arba turinio duomenis) informacija, turima paslaugos teikėjo ir susijusi su jo paslaugų abonentais, iš kurios galima nustatyti:

a) naudotos ryšio paslaugos tipą, taikytas technines priemones ir naudojimo laiką;

b) abonento tapatybę, pašto ar geografinės padėties adresą, telefono ir bet kokį kitą prieigos numerį, informaciją apie sąskaitas ir mokėjimus, gaunamą paslaugos sutarties arba susitarimo pagrindu;

c) bet kurią kitą informaciją ryšių aparatūros įrengimo vietoje, turimą pagal paslaugos sutartį arba susitarimą.

4 dalis. Laikomųjų kompiuterinių duomenų paieška ir poėmis

19 straipsnis. Laikomųjų kompiuterinių duomenų paieška ir poėmis

1. Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti, įgalinant jos kompetentingas institucijas apieškoti ar panašiai ištirti:

a) kompiuterinę sistemą arba jos dalį ir joje laikomus kompiuterinius duomenis;

b) kompiuterinių duomenų atmeniąją terpę, kurioje tos Šalies teritorijoje gali būti laikomi kompiuteriniai duomenys.

2. Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti užtikrinti, kad jos institucijoms pagal šio straipsnio 1 dalies a punktą apieškant ar panašiai tiriant konkrečią kompiuterinę sistemą arba jos dalį ir turint priežasčių manyti, kad ieškomi duomenys laikomi tos Šalies teritorijoje esančioje kitoje kompiuterinėje sistemoje arba jos dalyje ir kad tokie duomenys yra teisėtai prieinami naudojant pirmąją sistemą, tokios institucijos galėtų operatyviai išplėsti paiešką ar panašų tyrimą į kitą sistemą.

3. Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti įgalinant jos kompetentingas institucijas areštuoti arba panašiai išsaugoti kompiuterinius duomenis, gautus pagal šio straipsnio 1 arba 2 dalį. Prie šių priemonių priskiriami įgaliojimai:

a) areštuoti arba panašiai išsaugoti kompiuterinę sistemą arba jos dalį, arba kompiuterių duomenų atmeniąją terpę;

b) pasidaryti ir pasilaikyti tokių kompiuterinių duomenų kopiją;

c) išsaugoti atitinkamų kompiuterinių duomenų vientisumą;

d) padaryti tokius kompiuterių duomenis neprieinamus arba pašalinti juos iš apieškotos kompiuterinės sistemos.

4. Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti, įgalinant jos kompetentingas institucijas nurodyti bet kuriam asmeniui, žinančiam apie tokios kompiuterinės sistemos veikimą arba apie priemones, kurių buvo imtasi joje esantiems kompiuteriniams duomenims apsaugoti, pateikti, kiek tai pagrįsta, informaciją, reikalingą, kad būtų galima taikyti šio straipsnio 1 ir 2 dalyse minimas priemones.

5. Šiame straipsnyje minimiems įgaliojimams ir procedūroms taikomi 14 ir 15 straipsniai.

5 dalis. Kompiuterinių duomenų surinkimas realiuoju laiku

20 straipsnis. Srauto duomenų surinkimas realiuoju laiku

1. Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti, įgalinant jos kompetentingas institucijas:

a) tos Šalies teritorijoje surinkti arba techninėmis priemonėmis įrašyti;

b) priversti paslaugos teikėją pagal jo technines galimybes:

i) tos Šalies teritorijoje surinkti arba techninėmis priemonėmis įrašyti arba

ii) bendradarbiauti su kompetentinga institucija ir padėti jai surinkti arba įrašyti

realiuoju laiku srauto duomenis, susijusius su konkrečia informacija, jos teritorijoje perduodama naudojantis kompiuterine sistema.

2. Jeigu Šalis dėl savo teisinės sistemos principų negali taikyti šio straipsnio 1 dalies a punkte minimų priemonių, ji gali priimti tokius teisės aktus ir kitas priemones, kurių gali prireikti, kad jos teritorijoje realiuoju laiku, naudojant technines priemones, būtų surinkti ir įrašyti srauto duomenys, susiję su konkrečia toje teritorijoje perduodama informacija.

3. Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti įpareigoti paslaugos teikėją laikyti paslaptyje bet kurių šiame straipsnyje minimų įgaliojimų vykdymą ir bet kurią informaciją apie jų vykdymą.

4. Šiame straipsnyje minimiems įgaliojimams ir procedūroms taikomi 14 ir 15 straipsniai.

21 straipsnis. Turinio duomenų perimtis

1. Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti, kad dėl sunkių nusikaltimų, apibrėžtų tos Šalies vidaus teisėje, kompetentingos institucijos būtų įgalintos:

a) tos Šalies teritorijoje surinkti arba techninėmis priemonėmis įrašyti

b) priversti paslaugos teikėją pagal jo turimas technines galimybes:

i) tos Šalies teritorijoje surinkti arba techninėmis priemonėmis įrašyti arba

ii) bendradarbiauti su kompetentingomis institucijomis ir padėti jai surinkti arba įrašyti

realiuoju laiku turinio duomenis, susijusius su konkrečia informacija, jos teritorijoje perduodamus naudojantis kompiuterine sistema.

2. Jeigu Šalis dėl savo teisinės sistemos principų negali taikyti šio straipsnio 1 dalies a punkte minimų priemonių, ji gali priimti tokius teisės aktus ir kitas priemones, kurių gali prireikti, kad jos teritorijoje realiuoju laiku, naudojant technines priemones būtų surinkti ir įrašyti turinio duomenys, susiję su konkrečia toje teritorijoje perduodama informacija.

3. Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti įpareigojant paslaugos teikėją laikyti paslaptyje bet kurių šiame straipsnyje minimų įgaliojimų vykdymą ir bet kurią informaciją apie jų vykdymą.

4. Šiame straipsnyje minimiems įgaliojimams ir procedūroms taikomi 14 ir 15 straipsniai.

3 skirsnis. Jurisdikcija

22 straipsnis. Jurisdikcija

1. Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti nustatyti jurisdikciją šios Konvencijos 2–11 straipsniuose nurodytiems nusikaltimams, kai nusikaltimas padarytas:

a) jos teritorijoje;

b) laive, plaukiojančiame su tos Šalies vėliava;

c) orlaivyje, įregistruotame pagal tos Šalies įstatymus;

d) tos Šalies piliečio, jeigu padarius nusikaltimą yra baudžiama pagal baudžiamuosius įstatymus arba jeigu toks nusikaltimas yra padarytas už bet kurios valstybės teritorinės jurisdikcijos.

2. Kiekviena Šalis gali pasilikti teisę netaikyti arba tik tam tikrais atvejais arba tam tikromis aplinkybėmis taikyti jurisdikcijos taisykles, nustatytas šio straipsnio 1 dalies b–d punktuose, arba dalį šių taisyklių.

3. Kiekviena Šalis priima tokias priemones, kurių gali prireikti nustatyti jurisdikciją šios Konvencijos 24 straipsnio 1 dalyje nurodytiems nusikaltimams, kai įtariamasis yra jos teritorijoje ir ji, gavusi prašymą jį išduoti, kitai Šaliai jo neišduoda vien dėl jo pilietybės.

4. Ši Konvencija nepašalina jokios baudžiamosios jurisdikcijos, vykdomos pagal vidaus teisę.

5. Kai dėl tariamo nusikaltimo, nustatyto pagal šią Konvenciją, teisę į jurisdikciją pareiškia daugiau nei viena Šalis, tos Šalys prireikus tarpusavyje konsultuojasi siekdamos nustatyti labiausiai persekiojimui tinkamą jurisdikciją.

III SKYRIUS. TARPTAUTINIS BENDRADARBIAVIMAS

1 skirsnis. Bendrieji principai

1 dalis. Bendrieji tarptautinio bendradarbiavimo principai

23 straipsnis. Bendrieji tarptautinio bendradarbiavimo principai

Tirdamos nusikaltimus, susijusius su kompiuterinėmis sistemomis ir duomenimis, arba persekiodamos, arba rinkdamos nusikaltimo įrodymus elektroniniu pavidalu, Šalys kuo didesniu mastu bendradarbiauja tarpusavyje, vadovaudamosi šio skyriaus nuostatomis, taikydamos atitinkamus tarptautinius dokumentus dėl tarptautinio bendradarbiavimo baudžiamosiose bylose, susitarimus, pagrįstus vienodais ar abipusiais teisės aktais, ir vidaus teisę.

2 dalis. Ekstradicijos principai

24 straipsnis. Ekstradicija

1. a) Šis straipsnis taikomas ekstradicijai tarp Šalių už nusikaltimus, nurodytus šios Konvencijos 2–11 straipsniuose, jeigu pagal abiejų susijusių Šalių įstatymus už tokius nusikaltimus baudžiama maksimalia, mažiausiai vienerių metų, laisvės atėmimo bausme arba griežtesne bausme.

b) Kai pagal susitarimą, pagrįstą vienodais ar abipusiais teisės aktais, arba pagal ekstradicijos sutartį, taip pat pagal Europos konvenciją dėl ekstradicijos (ETS Nr. 24), taikomą tarp dviejų ar daugiau šalių, kitokia mažiausia bausmė būtų taikoma, tokia pagal tokį susitarimą ar sutartį mažiausia bausmė ir taikoma.

2. Šio straipsnio 1 dalyje apibūdinti nusikaltimai laikomi nusikaltimais, už kuriuos išduodama, visose sutartyse dėl ekstradicijos tarp dviejų ar daugiau Šalių. Šalys įsipareigoja tokius nusikaltimus kaip nusikaltimus, už kuriuos išduodama, įtraukti į visas sutartis dėl ekstradicijos, sudaromas tarp dviejų ar daugiau Šalių.

3. Jeigu Šalis, siejanti ekstradiciją su sutartimi, gauna prašymą dėl ekstradicijos iš kitos Šalies, su kuria nėra sudariusi sutarties dėl ekstradicijos, ji gali šią Konvenciją laikyti teisiniu pagrindu ekstradicijai už bet kurį nusikaltimą, nurodytą šio straipsnio 1 dalyje.

4. Šalys, nesiejančios ekstradicijos su sutartimi, šio straipsnio 1 dalyje minimus nusikaltimus tarpusavyje pripažįsta nusikaltimais, už kuriuos išduodama.

5. Ekstradicija vykdoma pagal prašomosios Šalies teisėje arba taikytinose ekstradicijos sutartyse nustatytas sąlygas, įskaitant pagrindus, kuriems esant prašomoji Šalis gali atsisakyti vykdyti ekstradiciją.

6. Jeigu asmenį, padariusį šio straipsnio 1 dalyje minimą nusikaltimą, atsisakoma išduoti vien dėl jo pilietybės arba dėl to, kad prašomoji Šalis mano, jog tas nusikaltimas priklauso jos jurisdikcijai, prašomoji Šalis prašančiosios Šalies prašymu perduoda bylą savo kompetentingoms institucijoms, kad jos vykdytų baudžiamąjį persekiojimą ir tinkamu laiku praneša prašančiajai Šaliai galutinį jo rezultatą. Šios institucijos priima sprendimą ir atlieka tyrimą bei bylos nagrinėjimą tokiu pat būdu, kaip ir panašiose baudžiamosiose bylose, sprendžiamose pagal tos Šalies teisę.

7. a) Nesant sutarties Šalys, pasirašydamos arba deponuodamos šios Konvencijos ratifikavimo, priėmimo, patvirtinimo arba prisijungimo prie jos dokumentus, Europos Tarybos Generaliniam Sekretoriui praneša kiekvienos institucijos, atsakingos už prašymo išduoti arba laikinai suimti asmenį pateikimą arba gavimą, pavadinimą ir adresus.

b) Europos Tarybos Generalinis Sekretorius sudaro ir atnaujina Šalių nurodytą institucijų registrą. Kiekviena Šalis pasirūpina, kad informacija registre visuomet būtų teisinga.

3 dalis. Bendrieji savitarpio pagalbos principai

25 straipsnis. Bendrieji savitarpio pagalbos principai

1. Atlikdamos tyrimą arba nagrinėdamos bylas dėl nusikaltimų, susijusių su kompiuterinėmis sistemomis ir duomenimis, arba rinkdamos nusikaltimo įrodymus elektroniniu pavidalu, Šalys teikia viena kitai didžiausią įmanomą pagalbą.

2. Kiekviena Šalis taip pat priima tokius teisės aktus ir tokias priemones, kurių gali prireikti 27–35 straipsniuose nustatytiems įsipareigojimams vykdyti.

3. Skubiais atvejais kiekviena Šalis gali perduoti savitarpio pagalbos arba su tuo susijusios informacijos prašymus operatyviomis ryšio priemonėmis, tarp jų faksimiliniu ryšiu arba elektroniniu paštu, jeigu tomis priemonėmis galima užtikrinti tinkamą informacijos saugumą bei autentiškumą (naudojant, kai tai reikalinga, šifravimą), ir prašomosios Šalies prašymu tokią informaciją oficialiai patvirtina. Prašomoji Šalis prašymą priima ir į jį atsako bet kuria tokia operatyvia ryšio priemone.

4. Jeigu šio skyriaus straipsniuose kitaip nenurodyta, savitarpio pagalba teikiama pagal prašomosios Šalies teisėje arba taikytinose savitarpio pagalbos sutartyse nustatytas sąlygas, įskaitant pagrindus, kuriems esant prašomoji Šalis gali atsisakyti bendradarbiauti. Prašomoji Šalis nesinaudoja teise atsisakyti teikti savitarpio pagalbą dėl 2–11 straipsniuose minimų nusikaltimų, remdamasi tiktai tuo, kad prašymas susijęs su nusikaltimu, kurį ji laiko finansiniu nusikaltimu.

5. Kai pagal šio skyriaus nuostatas prašomajai Šaliai leidžiama savitarpio pagalbos teikimą sieti su dvigubo baudžiamumo buvimu, tokia sąlyga laikoma įvykdyta, neatsižvelgiant į tai, ar jos įstatymai priskiria tą nusikaltimą tai pačiai nusikaltimų kategorijai ir vadina tais pačiais terminais, kaip ir prašančioji Šalis, jeigu sudarantis nusikaltimo pagrindą elgesys, dėl kurio prašoma pagalbos, pagal jos įstatymus yra nusikaltimas.

26 straipsnis. Savanoriškas informavimas

1. Kiekviena Šalis, kiek tai leidžia jos vidaus teisė, gali be ankstesnio prašymo perduoti kitai Šaliai informaciją, gautą per savo pačios atliekamus tyrimus, jeigu ji mano, kad tokios informacijos atskleidimas padėtų ją gavusiai Šaliai pradėti arba atlikti tyrimą ar nagrinėti bylas dėl pagal šią Konvenciją

nustatytų nusikaltimų, arba paskatintų tą Šalį pagal šį skyrių pateikti prašymą bendradarbiauti.

2. Prieš teikdama tokią informaciją, teikiančioji Šalis gali prašyti, kad būtų išsaugotas jos konfidencialumas arba kad ji būtų naudojama tik nurodytomis sąlygomis. Jeigu informaciją gaunanti Šalis negali įvykdyti tokio prašymo, ji apie tai praneša teikiančiajai Šaliai, kuri tada sprendžia, ar, nepaisant to, tokią informaciją teikti. Jeigu informaciją gaunanti Šalis sutinka, kad informacija būtų naudojama nurodytomis sąlygomis, ji privalo laikytis tų sąlygų.

4 dalis. Savitarpio pagalbos prašymų pateikimo tvarka, kai nėra taikytinų tarptautinių susitarimų

27 straipsnis. Savitarpio pagalbos prašymų pateikimo tvarka, kai nėra taikytinų tarptautinių susitarimų

1. Jeigu tarp prašančiosios ir prašomosios Šalių nėra savitarpio pagalbos sutarties arba susitarimo, pagrįsto vienodais ar abipusiais teisės aktais, taikomos šio straipsnio 2–9 dalių nuostatos. Jeigu tokia sutartis, susitarimas arba teisės aktai yra, šio straipsnio nuostatos netaikomos, nebent susijusios Šalys susitartų vietoj jų taikyti kurią nors arba visą likusią šio straipsnio dalį.

2. a) Kiekviena Šalis paskiria centrinę instituciją arba institucijas, atsakingas už savitarpio pagalbos prašymų ir atsakymų į juos siuntimą, tokių prašymų vykdymą arba jų perdavimą vykdyti kompetentingoms institucijoms.

b) Centrinės institucijos vienos su kitomis bendradarbiauja tiesiogiai.

c) Kiekviena Šalis, pasirašydama arba deponuodama šios Konvencijos ratifikavimo, priėmimo, patvirtinimo ar prisijungimo dokumentą, Europos Tarybos Generaliniam Sekretoriui praneša institucijų, paskirtų pagal šią straipsnio dalį, pavadinimus ir adresus.

d) Europos Tarybos Generalinis Sekretorius sudaro ir atnaujina Šalių nurodytų centrinių institucijų registrą. Kiekviena Šalis pasirūpina, kad informacija registre visuomet būtų teisinga.

3. Pagal šį straipsnį siunčiami savitarpio pagalbos prašymai vykdomi prašančiosios Šalies nurodyta tvarka, išskyrus atvejus, kai ji nesuderinama su prašomosios Šalies teise.

4. Be 25 straipsnio 4 dalyje išvardytų atsisakymo pagrindų, prašomoji Šalis gali atsisakyti teikti pagalbą, jeigu:

a) prašymas susijęs su nusikaltimu, kurį prašomoji Šalis laiko politiniu nusikaltimu arba nusikaltimu, susijusiu su politiniu nusikaltimu;

b) ta Šalis mano, kad prašymo vykdymas pakenktų jos suverenumui, saugumui, viešajai tvarkai arba kitiems svarbiems interesams.

5. Prašomoji Šalis gali atidėti prašymo vykdymą, jeigu jį vykdant būtų pakenkta jos institucijų atliekamam nusikaltimų tyrimui arba bylų nagrinėjimui.

6. Prieš atsakydama teikti pagalbą arba atidėdama jos teikimą prašomoji Šalis, kai reikia, pasitarusi su prašančiąja Šalimi, apsvarsto galimybę patenkinti prašymą iš dalies arba tokiomis sąlygomis, kokias ji laiko reikalingomis.

7. Prašomoji Šalis nedelsdama informuoja prašančiąją Šalį apie pagalbos prašymo vykdymo rezultatą. Jeigu prašymą atsisakoma vykdyti arba jo vykdymas atidedamas, nurodomos to nevykdymo arba atidėjimo priežastys. Prašomoji Šalis taip pat informuoja prašančiąją Šalį apie priežastis, dėl kurių neįmanoma įvykdyti prašymo arba dėl kurių jo vykdymas gali būti labai uždelstas.

8. Prašančioji Šalis gali prašyti, kad prašomoji Šalis išsaugotų pagal šio skyriaus nuostatas pateikto prašymo ir jo turinio konfidencialumą tiek, kiek to reikia prašymui vykdyti. Jeigu prašomoji Šalis negali patenkinti konfidencialumo sąlygos, ji nedelsdama apie tai praneša prašančiajai Šaliai, kuri tada sprendžia, ar prašymą vis dėlto reikėtų vykdyti.

9. a) Skubiu atveju savitarpio pagalbos ar su ja susijusios informacijos prašymus prašančiosios Šalies teisminės institucijos gali siųsti tiesiogiai tokioms prašomosios Šalies institucijoms. Tokiais atvejais kopija tuo pačiu metu per prašančiosios Šalies centrinę instituciją yra siunčiama prašomosios Šalies centrinei institucijai.

b) Šioje straipsnio dalyje minimi prašymai arba pranešimai gali būti perduodami per Tarptautinę kriminalinės policijos organizaciją (Interpolą).

c) Kai prašymas pateikiamas pagal šios straipsnio dalies a punktą, o institucija neturi įgaliojimų jį nagrinėti, ji perduoda prašymą kompetentingai nacionalinei institucijai ir apie tai tiesiogiai informuoja prašančiąją Šalį.

d) Jeigu šioje straipsnio dalyje minimi prašymai arba pranešimai nėra susiję su prievartos priemonėmis, juos kompetentinga prašančiosios Šalies institucija tiesiogiai perduoda kompetentingai prašomosios Šalies institucijai.

e) Kiekviena Šalis, pasirašydama arba deponuodama šios Konvencijos ratifikavimo, priėmimo, patvirtinimo arba prisijungimo dokumentus, Europos Tarybos Generaliniam Sekretoriui gali pranešti, kad, siekiant didesnio veiksmingumo, šioje straipsnio dalyje minimi prašymai turi būti siunčiami jos centrinei institucijai.

28 straipsnis. Konfidencialumas ir informacijos naudojimo apribojimas

1. Jeigu tarp prašančiosios ir prašomosios Šalių nėra savitarpio pagalbos sutarties arba susitarimo, pagrįsto vienodais ir abipusiais teisės aktais, taikomos šio straipsnio nuostatos. Jeigu tokia sutartis, susitarimas arba teisės

aktai yra, šio straipsnio nuostatos netaikomos, nebent Šalys susitartų vietoj jų taikyti kurią nors arba visą likusią šio straipsnio dalį.

2. Atsakydama į prašymą suteikti informaciją arba medžiagą, prašomoji Šalis gali nustatyti sąlygą, kad:

a) būtų išsaugomas jos konfidencialumas tais atvejais, kai savitarpio teisinės pagalbos prašymas negalėtų būti vykdomas nesant tokios sąlygos;

b) ji būtų naudojama tik prašyme nurodytam tyrimui arba bylų nagrinėjimui.

3. Jeigu prašančioji Šalis negali įvykdyti šio straipsnio 2 dalyje minimos sąlygos, ji apie tai nedelsdama praneša kitai Šaliai, kuri tada sprendžia, ar, nepaisant to, teikti tokią informaciją. Jeigu prašančioji Šalis sutinka su tokia sąlyga, ji privalo jos laikytis.

4. Kiekviena Šalis, kuri teikia informaciją arba medžiagą laikydamasi šio straipsnio 2 dalyje minimos sąlygos, gali, remdamasi ta sąlyga, paprašyti kitą Šalį paaiškinti, kam tokia informacija arba medžiaga reikalinga.

2 skirsnis. Specialiosios nuostatos

1 dalis. Savitarpio pagalba dėl laikinųjų priemonių

29 straipsnis. Operatyvus laikomųjų kompiuterinių duomenų išsaugojimas

1. Šalis gali prašyti kitą Šalį nurodyti operatyviai išsaugoti duomenis, laikomus kompiuterinėje sistemoje, kuri yra tos kitos Šalies teritorijoje ir dėl kurios prašančioji Šalis ketina pateikti savitarpio pagalbos prašymą, susijusį su tokių duomenų paieška arba panašia prieiga, areštu ar panašiu poėmiu arba su jų atskleidimu, arba prašyti kitaip pasirūpinti tokių duomenų išsaugojimu.

2. Pagal šio straipsnio 1 dalį pateikiamame prašyme išsaugoti duomenis nurodoma:

a) išsaugoti duomenis prašanti institucija;

b) nusikaltimas, dėl kurio atliekamas tyrimas arba vyksta procesas, ir trumpas susijusių faktų apibendrinimas;

c) išsaugotini laikomieji kompiuteriniai duomenys ir jų sąsaja su nusikaltimu;

d) bet kuri turima informacija, leidžianti nustatyti laikomųjų kompiuterinių duomenų saugotoją arba kompiuterinės sistemos vietą;

e) būtinybė išsaugoti duomenis;

f) Šalies ketinimas pateikti savitarpio pagalbos prašymą, susijusį su laikomųjų kompiuterinių duomenų paieška arba panašia prieiga, areštu ar panašiu poėmiu arba su jų atskleidimu.

3. Gavusi kitos Šalies prašymą, prašomoji Šalis imasi visų reikalingų priemonių, kad, vadovaudamasi savo vidaus teise, operatyviai išsaugotų nurodytus duomenis. Atsakant į prašymą, nereikalaujama dvigubo baudžiamumo, kaip tokio išsaugojimo sąlygos.

4. Šalis, kuri atsakymą į savitarpio pagalbos prašymą, susijusį su duomenų paieška arba panašia prieiga, areštu ar panašiu poėmiu arba su jų atskleidimu, sieja su dvigubo baudžiamumo sąlyga, gali nusikaltimų, išskyrus nurodytuosius šios Konvencijos 2–11 straipsniuose, atžvilgiu pasilikti teisę atmesti pagal šį straipsnį pateiktą prašymą išsaugoti duomenis, kai ji turi pagrindo manyti, kad atskleidimo metu dvigubo baudžiamumo sąlyga negali būti įvykdyta.

5. Be to, prašymas dėl išsaugojimo gali būti atmestas, tik jeigu:

a) prašymas pateiktas dėl nusikaltimo, kurį prašomoji Šalis laiko politiniu nusikaltimu arba nusikaltimu, susijusiu su politiniu nusikaltimu;

b) prašomoji Šalis mano, kad prašymo vykdymas galėtų pakenkti jos suverenumui, saugumui, viešajai tvarkai arba kitiems svarbiems interesams.

6. Jeigu prašomoji Šalis mano, kad išsaugojimas neužtikrins duomenų prieinamumo ateityje arba sukels pavojų prašančiosios Šalies tyrimo konfidencialumui ar kitaip jam pakenks, ji nedelsdama apie tai praneša prašančiajai Šaliai, kuri tada sprendžia, ar prašymą vis dėlto reikėtų vykdyti.

7. Atsakant į šio straipsnio 1 dalyje minimą prašymą, duomenys išsaugojami ne mažiau kaip 60 dienų, kad prašančioji Šalis galėtų pateikti prašymą dėl duomenų paieškos arba panašios prieigos, arešto ar panašaus poėmio arba dėl jų atskleidimo. Gavus tokį prašymą, tokie duomenys saugojami iki sprendimo dėl prašymo priėmimo.

30 straipsnis. Operatyvus išsaugotų srauto duomenų atskleidimas

1. Jeigu vykdydama pagal 29 straipsnį pateiktą prašymą išsaugoti srauto duomenis, susijusius su tam tikra informacija, prašomoji Šalis sužino, kad su šios informacijos perdavimu yra susijęs kitoje valstybėje esantis paslaugos teikėjas, ji operatyviai atskleidžia prašančiajai Šaliai pakankamai srauto duomenų, leidžiančių nustatyti paslaugos teikėją ir tos informacijos perdavimo kelią.

2. Atsisakyti atskleisti srauto duomenis pagal šio straipsnio 1 dalį galima tik tais atvejais, kai:

a) prašymas pateiktas dėl nusikaltimo, kurį prašomoji Šalis laiko politiniu nusikaltimu arba nusikaltimu, susijusiu su politiniu nusikaltimu;

b) prašomoji Šalis mano, kad prašymo vykdymas galėtų pakenkti jos suverenumui, saugumui, viešajai tvarkai arba kitiems svarbiems interesams.

2 dalis. Savitarpio pagalba atliekant tyrimą

31 straipsnis. Savitarpio pagalba dėl laikomųjų kompiuterių duomenų prieigos

1. Šalis gali pateikti kitai Šaliai prašymą dėl duomenų, laikomų kompiuterinėje sistemoje, kuri yra prašomosios Šalies teritorijoje, paieškos arba panašios prieigos, arešto ar panašaus poėmio ir atskleidimo, taip pat ir dėl duomenų, kurie buvo išsaugoti pagal 29 straipsnį.

2. Atsakydama į prašymą, prašomoji Šalis vadovaujasi tarptautiniais dokumentais, susitarimais ir įstatymais, nurodytais 23 straipsnyje, ir atitinkamomis šio skyriaus nuostatomis.

3. Į prašymą operatyviai atsakoma tais atvejais, kai:

a) yra pagrindo manyti, kad reikalingi duomenys gali būti nesunkiai prarasti arba pakeisti;

b) operatyvus bendradarbiavimas yra numatytas šio straipsnio 2 dalyje nurodytuose dokumentuose, susitarimuose ir įstatymuose.

32 straipsnis. Tarptautinė laikomųjų kompiuterių duomenų prieiga gavus sutikimą arba esant viešajai prieigai

Kiekviena Šalis be oficialaus kitos Šalies leidimo gali:

a) prieiti prie viešai prieinamų (atviras šaltinis) laikomųjų kompiuterinių duomenų, kad ir kokioje geografinėje vietoje jie būtų;

b) per savo teritorijoje esančią kompiuterinę sistemą prieiti prie laikomųjų kompiuterių duomenų, esančių kitoje Šalyje, arba gauti tuos duomenis, jeigu ta Šalis gauna asmens, teisiškai įgalioto per tokią kompiuterių sistemą atskleisti tai Šaliai tokius duomenis, teisėtą ir sąmoningą sutikimą.

33 straipsnis. Savitarpio pagalba, teikiama dėl srauto duomenų rinkimo realiuoju laiku

1. Šalys teikia savitarpio pagalbą realiuoju laiku renkant srauto duomenis, susijusius su konkrečia informacija, jos teritorijoje perduodama naudojantis kompiuterine sistema. Atsižvelgiant į šio straipsnio 2 dalies nuostatas, pagalba teikiama laikantis šalies vidaus teisėje nustatytos tvarkos ir sąlygų.

2. Kiekviena Šalis tokią pagalbą teikia bent tų baudžiamųjų nusikaltimų atvejais, kai srauto duomenys realiuoju laiku būtų renkami toje valstybėje nagrinėjamose panašiose bylose.

34 straipsnis. Savitarpio pagalba, teikiama dėl turinio duomenų perimties

Šalys teikia savitarpio pagalbą realiuoju laiku renkant arba įrašant turinio duomenis, susijusius su konkrečia informacija, perduodama kompiuterine sistema, kiek tai leidžia jų taikytinos sutartys ir vidaus įstatymai.

3 dalis. 24/7 tinklas

35 straipsnis. 24/7 tinklas

1. Kad būtų galima teikti skubią pagalbą tyrimui ar bylų nagrinėjimui, susijusiems su nusikaltimais kompiuterinėms sistemoms ir duomenims, arba nusikaltimo įrodymų rinkimui elektroniniu pavidalu, kiekviena Šalis paskiria ryšio punktą, veikiantį visą parą 7 dienas per savaitę. Be kita ko, tokia pagalba apima toliau išvardytų dalykų palengvinimą arba, jeigu tai leidžia valstybės vidaus teisė ir praktika, tiesiogiai:

a) techninių konsultacijų teikimą;

b) duomenų išsaugojimą pagal 29 ir 30 straipsnius;

c) įrodymų rinkimą, teisinės informacijos teikimą ir įtariamųjų buvimo vietos nustatymą.

2. a) Šalies ryšio punktas turi galimybę palaikyti operatyvų ryšį su kitos Šalies ryšio punktu.

b) Jeigu Šalies paskirtas ryšio punktas nėra tos Šalies institucijos arba institucijų, atsakingų už tarptautinę savitarpio pagalbą arba ekstradiciją, dalis, toks ryšio punktas pasirūpina, kad galėtų operatyviai bendradarbiauti su tokia institucija arba institucijomis.

3. Kad palengvintų tinklo darbą, kiekviena Šalis parūpina apmokytą personalą ir įrangą jam.

IV SKYRIUS. BAIGIAMOSIOS NUOSTATOS

36 straipsnis. Pasirašymas ir įsigaliojimas

1. Šią Konvenciją gali pasirašyti Europos Tarybos valstybės narės ir prie jos rengimo prisidėjusios valstybės, kurios nėra narės.

2. Ši Konvencija turi būti ratifikuojama, priimama arba patvirtinama. Ratifikavimo, priėmimo arba patvirtinimo dokumentai deponuojami Europos Tarybos Generaliniam Sekretoriui.

3. Ši Konvencija įsigalioja kito mėnesio pirmą dieną, praėjus trims mėnesiams nuo tos dienos, kai penkios valstybės, tarp jų ne mažiau kaip trys

Europos Tarybos narės, pagal šio straipsnio 1 ir 2 dalis pareiškė sutikimą įsipareigoti pagal šią Konvenciją.

4. Kiekvienai šią Konvenciją pasirašiusiai valstybei, kuri vėliau pareiškė sutikimą įsipareigoti pagal ją, Konvencija įsigalioja kito mėnesio pirmą dieną, praėjus trims mėnesiams nuo tos dienos, kai ji pagal šio straipsnio 1 ir 2 dalis pareiškia sutikimą įsipareigoti pagal šią Konvenciją.

37 straipsnis. Prisijungimas prie Konvencijos

1. Šiai Konvencijai įsigaliojus, Europos Tarybos Ministrų Komitetas, pasikonsultavęs su šios Konvencijos Susitariančiosiomis Šalimis ir gavęs vieningą jų sutikimą, gali pakviesti bet kurią valstybę, kuri nėra Tarybos narė ir neprisidėjo prie šios Konvencijos rengimo, prisijungti prie jos. Sprendimas priimamas pritarus Europos Tarybos statuto 20 straipsnio d punkte nustatytai daugumai ir vieningai balsavus Susitariančiųjų Šalių atstovams, kurie yra teisėti Ministrų Komiteto nariai.

2. Ši Konvencija prie jos pagal šio straipsnio 1 dalį prisijungusiai valstybei įsigalioja kito mėnesio pirmą dieną, praėjus trims mėnesiams nuo tos dienos, kai Europos Tarybos Generaliniam Sekretoriui deponuojamas prisijungimo dokumentas.

38 straipsnis. Teritorinis taikymas

1. Kiekviena valstybė pasirašymo metu arba deponuodama savo ratifikavimo, priėmimo, patvirtinimo arba prisijungimo dokumentą, gali nurodyti teritoriją arba teritorijas, kurioms ši Konvencija taikoma.

2. Kiekviena valstybė bet kada vėliau gali Europos Tarybos Generaliniam Sekretoriui adresuotu pareiškimu išplėsti šios Konvencijos taikymą bet kuriai kitai tame pareiškime nurodytai teritorijai. Tokiai teritorijai Konvencija įsigalioja kito mėnesio pirmą dieną, praėjus trims mėnesiams nuo tos dienos, kai Generalinis Sekretorius gauna tokį pareiškimą.

3. Kiekvienas pareiškimas pagal dvi pirmesnes šio straipsnio dalis kiekvienai tokiame pareiškime nurodytai teritorijai gali būti atšauktas Europos Tarybos Generaliniam Sekretoriui adresuotu pranešimu. Atšaukimas įsigalioja kito mėnesio pirmą dieną, praėjus trims mėnesiams nuo tos dienos, kai Generalinis Sekretorius gauna tokį pranešimą.

39 straipsnis. Konvencijos galiojimas

1. Šios Konvencijos tikslas – papildyti taikytinas daugiašales ir dvišales Šalių sutartis bei susitarimus, tarp jų:

– Europos konvenciją dėl ekstradicijos, pateiktą pasirašyti 1957 m. gruodžio 13 d. Paryžiuje (ETS Nr. 24);

– Europos konvenciją dėl savitarpio pagalbos baudžiamosiose bylose, pateiktą pasirašyti 1959 m. balandžio 20 d. Strasbūre (ETS Nr. 30);

– Europos konvencijos dėl savitarpio pagalbos baudžiamosiose bylose papildomą protokolą, pateiktą pasirašyti 1978 m. kovo 17 d. Strasbūre (ETS Nr. 99).

2. Jeigu dvi ar daugiau Šalių jau yra sudariusios susitarimą arba sutartį šios Konvencijos reglamentuojamais klausimais arba kitaip nustačiusios savo santykius šioje srityje, arba tai padarytų ateityje, jos taip pat turi teisę taikyti tą susitarimą arba sutartį ir pagal juos reglamentuoti savo santykius. Tačiau jeigu šios Konvencijos reglamentuojamais klausimais Šalys nustato savo santykius kitaip, nei jie reglamentuojami šioje Konvencijoje, jos privalo juos tvarkyti taip, kad jie neprieštarautų šios Konvencijos tikslams ir nuostatoms.

3. Ši Konvencija niekaip nekeičia kitų Šalies teisių, apribojimų, pareigų ir įsipareigojimų.

40 straipsnis. Pareiškimai

Kiekviena valstybė pasirašydama šią Konvenciją arba deponuodama savo ratifikavimo, priėmimo, patvirtinimo arba prisijungimo dokumentą gali Europos Tarybos Generaliniam Sekretoriui adresuotu rašytiniu pranešimu pareikšti, kad ji pasilieka teisę reikalauti papildomų sąlygų, kaip nustatyta 2 ir 3 straipsniuose, 6 straipsnio 1 dalies b punkte, 7 straipsnyje, 9 straipsnio 3 dalyje ir 27 straipsnio 9 dalies e punkte.

41 straipsnis. Konvencijos galiojimas federacinėje valstybėje

1. Federacinė valstybė gali pasilikti teisę prisiimti įsipareigojimus pagal šios Konvencijos II skyrių, neprieštaraujančius pagrindiniams principams, kuriais grindžiami santykiai tarp jos centrinės vyriausybės ir ją sudarančių valstybių ar kitų panašių teritorinių vienetų, jeigu ji tebėra pasirengusi bendradarbiauti pagal III skyrių.

2. Darydama šio straipsnio 1 dalyje nurodytą išlygą, federacinė valstybė gali netaikyti tokių šios išlygos sąlygų, kurios atmeta arba iš esmės sumažina jos įsipareigojimus imtis II skyriuje nurodytų priemonių. Apskritai ji plačiai ir veiksmingai užtikrina šių priemonių vykdymą.

3. Apie tas Konvencijos nuostatas, kurių taikymas priklauso federaciją sudarančių valstybių arba panašių teritorinių vienetų, pagal jos konstituciją neįpareigotų vykdyti įstatymų leidybos funkcijų, jurisdikcijai, federacijos vy-

riausybė informuoja kompetentingas tokių valstybių institucijas, palankiai vertindama tokias nuostatas ir skatindama tokias valstybes imtis tinkamų veiksmų joms įgyvendinti.

42 straipsnis. Išlygos

Kiekviena valstybė pasirašydama šią Konvenciją arba deponuodama savo ratifikavimo, priėmimo, patvirtinimo arba prisijungimo dokumentą, gali Europos Tarybos Generaliniam Sekretoriui adresuotu rašytiniu pranešimu pareikšti, kad ji pasilieka teisę daryti 4 straipsnio 2 dalyje, 6 straipsnio 3 dalyje, 9 straipsnio 4 dalyje, 10 straipsnio 3 dalyje, 11 straipsnio 3 dalyje, 14 straipsnio 3 dalyje, 22 straipsnio 2 dalyje, 29 straipsnio 4 dalyje ir 41 straipsnio 1 dalyje nurodytas išlygas. Jokių kitų išlygų daryti negalima.

43 straipsnis. Išlygų statusas ir atšaukimas

1. Šalis, padariusi 42 straipsnyje nurodytą išlygą, gali Generaliniam Sekretoriui adresuotu pranešimu visai arba iš dalies ją atšaukti. Toks atšaukimas įsigalioja nuo tos dienos, kai Generalinis Sekretorius gauna tokį pranešimą. Jeigu pranešime nurodoma, jog išlyga atšaukiama nuo jame nustatytos datos ir tokia data yra vėlesnė nei ta, kai pranešimą gauna Generalinis Sekretorius, išlygos atšaukimas įsigalioja vėlesnę dieną.

2. Kai tik leidžia aplinkybės, Šalis, padariusi 42 straipsnyje nurodytą išlygą, visai arba iš dalies ją atšaukia.

3. Europos Tarybos Generalinis Sekretorius periodiškai klausia Šalių, padariusių vieną ar daugiau 42 straipsnyje nurodytų išlygų, apie galimybę tokią išlygą arba išlygas atšaukti.

44 straipsnis. Pakeitimai

1. Kiekviena Šalis gali siūlyti šios Konvencijos pakeitimus, apie kuriuos Europos Tarybos Generalinis Sekretorius praneša Europos Tarybos valstybėms narėms, prie šios Konvencijos rengimo prisidėjusioms valstybėms, kurios nėra narės, ir valstybėms, pagal šios Konvencijos 37 straipsnį prisijungusioms arba pakviestoms prisijungti prie jos.

2. Apie kiekvieną Šalies siūlomą pakeitimą pranešama Europos nusikalstamumo problemų komitetui (CDPC), kuris savo nuomonę dėl siūlomo pakeitimo perduoda Ministrų Komitetui.

3. Ministrų Komitetas apsvarsto siūlomą pakeitimą bei Europos nusikalstamumo problemų komiteto (CDPC) pateiktą nuomonę ir, pasikonsul-

tavęs su nepriklausančioms Europos Tarybai Konvencijos Šalimis, gali tokį pakeitimą priimti.

4. Kiekvieno pakeitimo tekstas, Ministrų Komiteto priimtas pagal šio straipsnio 3 dalį, perduodamas Šalims, kad jos pareikštų sutikimą.

5. Kiekvienas pakeitimas, priimtas pagal šio straipsnio 3 dalį, įsigalioja praėjus trisdešimčiai dienų nuo tos dienos, kai visos Šalys Generaliniam Sekretoriui pareiškia savo sutikimą.

45 straipsnis. Ginčų sprendimas

1. Europos nusikalstamumo problemų komitetas (CDPC) yra nuolat informuojamas apie šios Konvencijos aiškinimą ir taikymą.

2. Tarp Šalių kilus ginčui dėl šios Konvencijos aiškinimo arba taikymo, jos stengiasi ginčą išspręsti derybomis arba kitomis taikiomis joms priimtinomis ginčų sprendimo priemonėmis, be kita ko, pateikdamos ginčą Europos nusikalstamumo problemų komitetui (CDPC), arbitražiniam teismui, kurio sprendimai Šalims privalomi, arba Tarptautiniam Teisingumo Teismui, jei Šalys taip susitarė.

46 straipsnis. Šalių konsultacijos

1. Prireikus Šalys periodiškai konsultuojasi, kad palengvintų:

a) veiksmingą šios Konvencijos taikymą ir vykdymą, taip pat dėl to kylančių problemų ir pagal šia Konvenciją padarytų pareiškimų arba išlygų poveikio nustatymą;

b) keitimąsi informacija apie svarbius teisės, politikos arba technikos pokyčius, susijusius su elektroniniais nusikaltimais ir įrodymų rinkimu elektroniniu pavidalu;

c) galimų Konvencijos papildymų arba pakeitimų svarstymą.

2. Europos nusikalstamumo problemų komitetas (CDPC) periodiškai informuojamas apie šio straipsnio 1 dalyje minimų konsultacijų rezultatus.

3. Europos nusikalstamumo problemų komitetas (CDPC) prireikus tarpininkauja šio straipsnio 1 dalyje minimose konsultacijose ir imasi reikalingų priemonių, kad padėtų Šalims papildyti arba iš dalies pakeisti šią Konvenciją. Ne vėliau kaip praėjus trejiems metams nuo šios Konvencijos įsigaliojimo Europos nusikalstamumo problemų komitetas (CDPC), bendradarbiaudamas su Šalimis, persvarsto visas Konvencijos nuostatas ir, jei būtina, siūlo atitinkamus pakeitimus.

4. Išskyrus atvejus, kai išlaidas padengia Europos Tarybos, šio straipsnio 1 dalies nuostatų vykdymo išlaidas Šalys padengia jų sutartu būdu.

5. Vykdyti pagal šį straipsnį nustatytas funkcijas Šalims padeda Europos Tarybos Sekretoriatas.

47 straipsnis. Denonsavimas

1. Kiekviena Šalis bet kada Europos Tarybos Generaliniam Sekretoriui adresuotu pranešimu gali denonsuoti šią Konvenciją.

2. Toks denonsavimas įsigalioja kito mėnesio pirmą dieną, praėjus trims mėnesiams nuo tos dienos, kai Generalinis Sekretorius gauna pranešimą.

48 straipsnis. Pranešimas

Europos Tarybos Generalinis Sekretorius Europos Tarybos valstybėms narėms, valstybėms, prisidėjusioms prie šios Konvencijos rengimo, kurios nėra narės, ir visoms valstybėms, prisijungusioms arba pakviestoms prie jos prisijungti, praneša apie:

a) kiekvieną pasirašymą;

b) kiekvieno ratifikavimo, priėmimo, patvirtinimo arba prisijungimo dokumento deponavimą;

c) kiekvieną šios Konvencijos įsigaliojimo pagal 36 ir 37 straipsnius datą;

d) kiekvieną pagal 40 straipsnį padarytą pareiškimą arba pagal 42 straipsnį padarytą išlygą;

e) bet kurį kitą veiksmą, pranešimą arba informaciją, susijusią su šia Konvencija.

Tai paliudydami, toliau nurodyti tinkamai įgalioti asmenys pasirašė šią Konvenciją.

Priimta 2001 m. lapkričio 23 d. Budapešte anglų ir prancūzų kalbomis, abu tekstai yra autentiški, vienu egzemplioriumi, kuris deponuojamas Europos Tarybos archyvuose. Europos Tarybos Generalinis Sekretorius patvirtintas kopijas siunčia kiekvienai Europos Tarybos valstybei narei, prie šios Konvencijos rengimo prisidėjusioms valstybėms, kurios nėra valstybės narės, ir kiekvienai prie šios Konvencijos prisijungti pakviestai valstybei.

2 priedas. Anketos

Tapatybės vagystė elektroninėje erdvėje – VARTOTOJAI

Tapatybės vagystė elektroninėje erdvėje – tai neteisėti veiksmai su asmens duomenimis , turint tikslą apsimesti kitu asmeniu.

Tyrimo tikslas: Nustatyti ar vartotojai suvokia tapatybės vagystės problemą, kaip vertina jos pavojingumą bei paplitimą.

Prašome įvesti informaciją apie save:

Lytis

Amžius

Gyvenamoji vieta

Išsilavinimas

Užsiėmimas

1. Ar naudojatės viešosiomis elektroninėmis paslaugomis (pavyzdžiui, elektroninis deklaravimas ir kt.)?
☐ Taip
☐ Ne

2. Ar naudojatės elektroninio verslo paslaugomis (pavyzdžiui, prekės užsakymas internetu, e- bankininkystė ir kt.)
☐ Taip
☐ Ne

3. Ar iki šio tyrimo žinojote apie tapatybės vagystę elektroninėje erdvėje?
☐ Taip
☐ Ne

4. Ar tapatybės vagystė elektroninėje erdvėje yra paplitusi Lietuvoje?
☐ Taip
☐ Ne

5. Ar tapatybės vagystė elektroninėje erdvėje yra paplitusi pasaulyje?
☐ Taip
☐ Ne

6. Ar buvote susidūręs (-usi) su tapatybės vagystė elektroninėje erdvėje asmeniškai?
☐ Ne
☐ Taip (kokią žalą patyrėte?) _____

7. Ar Jums artimi žmonės buvo susidūrę su tapatybės vagyste elektroninėje erdvėje?
☐ Ne
☐ Taip (kokią žalą jie patyrė?) _____

8. Ar tapatybės vagystė elektroninėje erdvėje pavojingas reiškinys?

Reiškinys visiškai nepavojingas	1	2	3	4	5	6	7	8	9	10	Reiškinys labai pavojingas
	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	

9. Ar tapatybės vagystė elektroninėje erdvėje gali Jums sukelti realios žalos?
☐ Taip
☐ Ne

10. Kur kreiptis sužinojus apie tapatybės vagystę elektroninėje erdvėje?

_____

11. Ar Jūs vengiate naudotis viešosiomis elektroninėmis paslaugomis dėl tapatybės vagystės elektroninėje erdvėje grėsmės?
☐ Taip
☐ Ne

12. Ar Jūs vengiate naudotis elektroninio verslo paslaugomis dėl tapatybės vagystės elektroninėje erdvėje grėsmės?
☐ Taip
☐ Ne

13. Ar naudodamiesi elektroninio verslo paslaugomis bijote, kad galite nukentėti nuo tapatybės vagystės elektroninėje erdvėje /tapti tapatybės vagystės elektroninėje erdvėje auka?

Ne, nesibaiminu 1 2 3 4 5 6 7 8 9 10 Taip, baiminuosi

14. Ar jaučiatės saugus (-i) kai savo asmens duomenis pateikiate internete?
☐ Taip
☐ Ne

15. Ar, Jūsų nuomone, pakanka viešosios informacijos apie apsisaugojimo nuo tapatybės vagystės elektroninėje erdvėje būdus?
☐ Taip
☐ Ne

16. Ar tapatybės vagystės elektroninėje erdvėje prevencijos priemonių viešinimas skatintų Jus naudotis elektroninėmis paslaugomis ir didintų pasitikėjimą elektroninio verslo sektoriumi?
☐ Taip
☐ Ne

Tapatybės vagystė elektroninėje erdvėje – VIEŠAS SEKTORIUS

Tapatybės vagystė elektroninėje erdvėje – tai neteisėti veiksmai su asmens duomenimis, turint tikslą apsimesti kitu asmeniu.

Tyrimo tikslas: Ištirti dviejų skirtingų sričių asmenų, sukaupiančių didelį kiekį asmens duomenų, tapatybės vagystės problemos ir prevencijos suvokimą.

Prašome įvesti informaciją apie save:

Lytis

Amžius

Išsilavinimas

Kokia Jūsų profesija?

Kokį darbą Jūs dirbate?

Kokios Jūsų pareigos?

1. Ar savo darbe esate susidūręs(-usi) su tapatybės vagyste elektroninėje erdvėje?

☐ Taip
☐ Ne

2. Ar manote, kad šis reiškinys daro neigiamą įtaką Jūsų veiklai?

☐ Ne
☐ Taip, tiesiogiai
☐ Taip, netiesiogiai

3. Kaip vertinate šio reiškinio pavojingumą?

Reiškinys visiškai nepavojingas ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 Reiškinys labai pavojingas

4. Ar tapatybės vagyste elektroninėje erdvėje, Jūsų nuomone, yra paplitusi Lietuvoje?

Reiškinys nėra paplitęs ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 Reiškinys plačiai paplitęs

5. Ar tapatybės vagyste elektroninėje erdvėje gali sukelti neigiamų padarinių Jūsų organizacijos veiklai? (Galite pasirinkti ne vieną atsakymą) (daug galimų atsakymų)

☐ neigiamų padarinių sukelti negali;
☐ gali, institucijos reputacijai;
☐ gali, asmens garbei ir orumui;
☐ gali, finansinių (pvz., nuostoliai, negautos pajamos);
☐ gali, kitų turtinių;
☐ gali, privatumui;
☐ gali, duomenų saugumui;
☐ gali, vartotojų teisėms;
☐ gali, kita (nurodykite): _____

6. Ar pakankamai Jūsų organizacija skiria lėšų apsaugai nuo tapatybės vagystės elektroninėje erdvėje?

Visiškai neskiriama ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 Skiriama labai daug

7. Ar pakankamai Jūsų organizacija imasi priemonių kovai su tapatybės vagyste elektroninėje erdvėje ir jos prevencijai?

☐ Ne
☐ Taip (nurodykite, kokių): _____

8. Ar, Jūsų nuomone, pakanka viešosios informacijos apie tapatybės vagystės elektroninėje erdvėje pavojingumą ir apsisaugojimo nuo tapatybės vagystės elektroninėje erdvėje būdus?

Visiškai nėra informacijos ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 Labai daug informacijos

9. Nurodykite tris svarbiausias Jums žinomas kovos su tapatybės vagyste elektroninėje erdvėje priemones.

10. Ar už tapatybės vagyste elektroninėje erdvėje asmenims kyla atsakomybė? (Galite pasirinkti ne vieną atsakymą) (daug galimų atsakymų)
☐ atsakomybė nekyla;
☐ kyla civilinė atsakomybė;
☐ kyla administracinė atsakomybė;
☐ kyla baudžiamoji atsakomybė;
☐ kita (įrašykite) _____

11. Ar Jūsų darbas yra tiesiogiai susijęs su asmens duomenų tvarkymu?
☐ Taip
☐ Ne

Tapatybės vagystė elektroninėje erdvėje – (VIEŠAS SEKTORIUS – SODRA)

Tapatybės vagystė elektroninėje erdvėje – tai neteisėti veiksmai su asmens duomenimis , turint tikslą apsimesti kitu asmeniu.

Tyrimo tikslas: Ištirti dviejų skirtingų sričių asmenų, sukaupiančių didelį kiekį asmens duomenų, tapatybės vagystės problemos ir prevencijos suvokimą.

Prašome įvesti informaciją apie save:

Lytis

Amžius

Išsilavinimas

Kokia Jūsų profesija?

Kokį darbą Jūs dirbate?

Kokios Jūsų pareigos?

1. Ar savo darbe esate susidūręs(-usi) su tapatybės vagyste elektroninėje erdvėje?

☐ Taip
☐ Ne

2. Ar manote, kad šis reiškinys daro neigiamą įtaką Jūsų veiklai?

☐ Ne
☐ Taip, tiesiogiai
☐ Taip, netiesiogiai

3. Kaip vertinate šio reiškinio pavojingumą?

Reiškinys visiškai nepavojingas ☐1 ☐2 ☐3 ☐4 ☐5 ☐6 ☐7 ☐8 ☐9 ☐10 Reiškinys labai pavojingas

4. Ar tapatybės vagyste elektroninėje erdvėje, Jūsų nuomone, yra paplitusi Lietuvoje?

Reiškinys nėra paplitęs ☐1 ☐2 ☐3 ☐4 ☐5 ☐6 ☐7 ☐8 ☐9 ☐10 Reiškinys plačiai paplitęs

5. Ar tapatybės vagyste elektroninėje erdvėje gali sukelti neigiamų padarinių Jūsų organizacijos veiklai? (Galite pasirinkti ne vieną atsakymą) (daug galimų atsakymų)

☐ neigiamų padarinių sukelti negali;
☐ gali, institucijos reputacijai;
☐ gali, asmens garbei ir orumui;
☐ gali, finansinių (pvz., nuostoliai, negautos pajamos);
☐ gali, kitų turtinių;
☐ gali, privatumui;
☐ gali, duomenų saugumui;
☐ gali, vartotojų teisėms;
☐ gali, kita (nurodykite): _____

6. Ar pakankamai Jūsų organizacija skiria lėšų apsaugai nuo tapatybės vagystės elektroninėje erdvėje?

Visiškai neskiriama	1	2	3	4	5	6	7	8	9	10	Skiriama labai daug
	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	

7. Ar pakankamai Jūsų organizacija imasi priemonių kovai su tapatybės vagyste elektroninėje erdvėje ir jos prevencijai?

☐ Ne
☐ Taip (nurodykite, kokių): _____

8. Ar, Jūsų nuomone, pakanka viešosios informacijos apie tapatybės vagystės elektroninėje erdvėje pavojingumą ir apsisaugojimo nuo tapatybės vagystės elektroninėje erdvėje būdus?

Visiškai nėra informacijos	1	2	3	4	5	6	7	8	9	10	Labai daug informacijos
	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	

9. Nurodykite tris svarbiausias Jums žinomas kovos su tapatybės vagyste elektroninėje erdvėje priemones.

10. Ar už tapatybės vagyste elektroninėje erdvėje asmenims kyla atsakomybė? (Galite pasirinkti ne vieną atsakymą) (daug galimų atsakymų)
☐ atsakomybė nekyla;
☐ kyla civilinė atsakomybė;
☐ kyla administracinė atsakomybė;
☐ kyla baudžiamoji atsakomybė;
☐ kita (įrašykite) _____

11. Ar Jūsų darbas yra tiesiogiai susijęs su asmens duomenų tvarkymu?
☐ Taip
☐ Ne

Tapatybės vagystė elektroninėje erdvėje – VERSLO ATSTOVAI

Tapatybės vagystė elektroninėje erdvėje – tai neteisėti veiksmai su asmens duomenimis , turint tikslą apsimesti kitu asmeniu.

Tyrimo tikslas: Ištirti dviejų skirtingų sričių asmenų, sukaupiančių didelį kiekį asmens duomenų, tapatybės vagystės problemos ir prevencijos suvokimą.

Prašome įvesti informaciją apie save:

Lytis

Amžius

Išsilavinimas

Kokia Jūsų profesija?

Kokį darbą Jūs dirbate?

Kokios Jūsų pareigos?

Kokia Jūsų įmonės veiklos sritis?

1. Ar savo darbe esate susidūręs(-usi) su tapatybės vagyste elektroninėje erdvėje?

☐ Taip
☐ Ne

2. Ar manote, kad šis reiškinys daro neigiamą įtaką Jūsų įmonės veiklai?

☐ Ne
☐ Taip, tiesiogiai
☐ Taip, netiesiogiai

3. Kaip vertinate šio reiškinio pavojingumą?

Reiškinys visiškai nepavojingas ☐1 ☐2 ☐3 ☐4 ☐5 ☐6 ☐7 ☐8 ☐9 ☐10 Reiškinys labai pavojingas

4. Ar tapatybės vagyste elektroninėje erdvėje, Jūsų nuomone, yra paplitusi Lietuvoje?

Reiškinys nėra paplitęs ☐1 ☐2 ☐3 ☐4 ☐5 ☐6 ☐7 ☐8 ☐9 ☐10 Reiškinys plačiai paplitęs

5. Ar tapatybės vagyste elektroninėje erdvėje gali sukelti neigiamų padarinių Jūsų įmonės veiklai? (Galite pasirinkti ne vieną atsakymą) (daug galimų atsakymų)

☐ neigiamų padarinių sukelti negali;
☐ gali, įmonės reputacijai;
☐ gali, asmens garbei ir orumui;
☐ gali, finansinių (pvz., nuostoliai, negautos pajamos);
☐ gali, kitų turtinių;
☐ gali, privatumui;
☐ gali, duomenų saugumui;
☐ gali, vartotojų teisėms;
☐ gali, kita (nurodykite): _____

6. Ar pakankamai Jūsų įmonė skiria lėšų apsaugai nuo tapatybės vagystės elektroninėje erdvėje?

Visiškai neskiriama ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 Skiriama labai daug

7. Ar pakankamai Jūsų įmonėje imamasi priemonių kovai su tapatybės vagyste elektroninėje erdvėje ir jos prevencijai?

☐ Ne
☐ Taip (nurodykite, kokių): _____

8. Ar Jūsų įmonė teikia elektroninio verslo paslaugas (t.y. visoms arba daliai paslaugų teikti naudoja informacines technologijas)?

☐ Taip
☐ Ne

9. Ar, Jūsų nuomone, pakanka viešosios informacijos apie tapatybės vagystės elektroninėje erdvėje pavojingumą ir apsisaugojimo nuo tapatybės vagystės elektroninėje erdvėje būdus?

Visiškai nėra informacijos ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 Labai daug informacijos

10. Nurodykite tris svarbiausias Jums žinomas kovos su tapatybės vagyste elektroninėje erdvėje priemones.

_____

11. Ar už tapatybės vagyste elektroninėje erdvėje asmenims kyla atsakomybė? (Galite pasirinkti ne vieną atsakymą) (daug galimų atsakymų)
☐ atsakomybė nekyla;
☐ kyla civilinė atsakomybė;
☐ kyla administracinė atsakomybė;
☐ kyla baudžiamoji atsakomybė;
☐ kita (įrašykite)

12. Ar elektroninio verslo sektoriaus taikomos priemonės apsaugo nuo tapatybės vagyste elektroninėje erdvėje?
☐ Taip
☐ Ne

13. Ar šiuo metu elektroninio verslo sektoriuje taikomos identifikavimo priemonės yra pakankamos?
☐ Taip
☐ Ne (Nurodykite kokių trūksta)

14. Kurios iš elektroninio verslo sektoriaus naudojamų priemonių yra patikimos (nurodykite tris tokias patikimas identifikavimo priemones)?

15. Ar elektroninio verslo sektoriaus naudojamos asmens identifikavimo priemonės turėtų būti privalomai reguliuojamos teisės normomis (argumentuokite)?

Tapatybės vagystė elektroninėje erdvėje – EKSPERTAI

Tapatybės vagystė elektroninėje erdvėje – tai neteisėti veiksmai su asmens duomenimis , turint tikslą apsimesti kitu asmeniu.

Tyrimo tikslas: Ištirti dviejų skirtingų sričių asmenų, sukaupiančių didelį kiekį asmens duomenų, tapatybės vagystės problemos ir prevencijos suvokimą.

1. Kaip vertinate tapatybės vagystės elektroninėje erdvėje (toliau – TVEE) reiškinį?

2. Ar TVEE, Jūsų nuomone, yra paplitusi? Argumentuokite.

3. Ar TVEE, Jūsų manymu, kelia pavojų? Jei taip, tai kam?

4. Nurodykite sritis (pagal sektorius: viešasis, privatusis ir pagal veiklos pobūdį: finansų, medicinos ir kt.), kuriose, Jūsų nuomone, tapatybės vagystės grėsmė yra didžiausia. Savo atsakymą pagrįskite.

5. Ar, Jūsų nuomone, pakanka teisės normų ir teisinio reguliavimo tinkamai sureguliuoti TVEE? Jei manote, kad nepakanka, tai kokių teisės normų trūksta?

6. Ar Lietuvoje numatyta atsakomybė už TVEE? Jei taip, tai kokia?

7. Ar manote, kad TVEE reikėtų kriminalizuoti kaip savarankišką nusikalstamą veiką? Kodėl?

8. Ar galiojančios teisės normos, reguliuojančios santykius, susijusius su TVEE, taikomos tinkamai?

9. Kokios problemos kyla dėl TVEE tyrimo?

10. Ar pakankamai taikoma savireguliacinių TVEE sumažinimo ir (arba) išvengimo priemonių? Kokios savireguliacinės priemonės galėtų sumažinti TVEE?

11. Ar, Jūsų nuomone, valstybių tarpinstitucinis bendradarbiavimas yra pakankamas ir tinkamas? Jei ne, nurodykite, ko trūksta.

12. Ar, Jūsų nuomone, bendradarbiavimas tarp valstybės ir privataus sektoriaus yra tinkamas? Jei ne, nurodykite, ko trūksta.

13. Ar elektroninio verslo taikomos priemonės apsaugo nuo TVEE? Kokios priemonės yra pakankamos ir kokios neturėtų būti taikomos?

14. Ar elektroninio verslo naudojamos asmens indentifikavimo priemonės turėtų būti privalomai reguliuojamos teisės normomis? Argumentuokite.

15. Kokias TVEE prevencijos priemones galėtumėte pasiūlyti?

Apklausa Tapatybės vagystė elektroninėje erdvėje (Ekspertai)

Respondentas #1

1. Kaip vertinate tapatybės vagystės elektroninėje erdvėje (toliau – TVEE) reiškinį?

Šį reiškinį reikia vienareikšmiškai vertinti negiamai.

2. Ar TVEE, Jūsų nuomone, yra paplitusi? Argumentuokite.

Masiškai tai nėra paplitę, tačiau toliau vystantis technologinei pažangai tokių reiškinių bei jų formų daugės.

3. Ar TVEE, Jūsų manymu, kelia pavojų? Jei taip, tai kam?

Tai kelia pavojų visoms suiteresuotosm šalims – verslui, vartotojams ir pačiai valstybei. Verslas dėl TVEE praranda pajamas, vartotojų pasitikėjimą. Vartotojai gali nukentėti pačiais įvairiausiais būdais – pradedant reputacija, baigiant finansiniais nuostoliais. Vasltybei tai ta pati vartotoju pasitikejimo problema vystant valstybes e.paslaugas, taip pat tai papildoma problema teisėsaugai, kurią reikia spręsti.

4. Nurodykite sritis (pagal sektorius: viešasis, privatusis ir pagal veiklos pobūdį: finansų, medicinos ir kt.), kuriose, Jūsų nuomone, tapatybės vagystės grėsmė yra didžiausia. Savo atsakymą pagrįskite.

Rizikingiausias ko gero mažos privataus sektoriaus įmonės, kurios šiai problemai neskiriamas pakankamas dėmesys. Pagal verslo šaką išskirti būtų sunkoka, pvz galėtų būti SMS kreditus teikiančios nedidelės įmonės.

5. Ar, Jūsų nuomone, pakanka teisės normų ir teisinio reguliavimo tinkamai sureguliuoti TVEE? Jei manote, kad nepakanka, tai kokių teisės normų trūksta?

Manau, kad sureguliuota pakankamai, reikėtų tik efektyviau taikyti.

6. Ar Lietuvoje numatyta atsakomybė už TVEE? Jei taip, tai kokia?

Netiesioginė, priklauso nuo veikos, atliktos pasitelkiant TVEE.

7. Ar manote, kad TVEE reikėtų kriminalizuoti kaip savarankišką nusikalstamą veiką? Kodėl?

Ne. TVEE gali apimti labai daug skirtingų veikų už kurias gali grėsti labai skirtinga atsakomybė, todėl vieningos atsakomybės įvedimas abejotinas.

8. Ar galiojančios teisės normos, reguliuojančios santykius, susijusius su TVEE, taikomos tinkamai?

Manau, kad kartais pristinga efektyvesnio esamų normų taikymo.

9. Kokios problemos kyla dėl TVEE tyrimo?

Nepakankama tyrėjų kompetencija

10. Ar pakankamai taikoma savireguliacinių TVEE sumažinimo ir (arba) išvengimo priemonių? Kokios savireguliacinės priemonės galėtų sumažinti TVEE?

Daugiau atsakingumo iš verslo subjektų pusės, proaktyvus vartotojų informavimas ir švietimas.

11. Ar, Jūsų nuomone, valstybių tarpinstitucinis bendradarbiavimas yra pakankamas ir tinkamas? Jei ne, nurodykite, ko trūksta.

Yra kelios institucijos šioje srityje formuojančios praktiką, kartais jų pozicijos išsiskiria.

12. Ar, Jūsų nuomone, bendradarbiavimas tarp valstybės ir privataus sektoriaus yra tinkamas? Jei ne, nurodykite, ko trūksta.

Daugiau pasitikėjimo verslu, ypač didelėmis, patikimomis įmonėms, visiems taikomi vienodi kriterijai.

13. Ar elektroninio verslo taikomos priemonės apsaugo nuo TVEE? Kokios priemonės yra pakankamos ir kokios neturėtų būti taikomos?

Sunku pasakyti.

14. Ar elektroninio verslo naudojamos asmens indentifikavimo priemonės turėtų būti privalomai reguliuojamos teisės normomis? Argumentuokite.

Ne, tai turėtų būti atsakingo verslo savireguliacijos sritis.

15. Kokias TVEE prevencijos priemones galėtumėte pasiūlyti?

Vartotojų švietimas.

Apklausa Tapatybės vagystė elektroninėje erdvėje (Ekspertai)

Respondentas #2

1. Kaip vertinate tapatybės vagystės elektroninėje erdvėje (toliau – TVEE) reiškinį?

TVEE yra naujas reiškinys, kuris atsirado daugelį veiksmų, visų pirma identifikavimą, perkėlus į elektroninę vertę. Kaip ir bet kuri kita vagystė tai yra nusikaltimas, kita vertus, ji sudaro prielaidas tolimesniems nusikaltimams. Be to, TVEE ilgą laiką gali būti nepastebėta ir užfiksuota tik jos pagalba įvykdžius kitą nusikaltimą.

2. Ar TVEE, Jūsų nuomone, yra paplitusi? Argumentuokite.

TVEE yra paplitusios tuo labiau, kuo plačiau naudojamas identifikavimas elektroninėje erdvėje įvairiose srityse. Lietuvoje TVEE kol kas dar nėra plačiai paplitę, tačiau ateityje jos gali paplisti gana staigiai, tuo labiau, kad jas galima daryti savo darbo vietoje, jų nevaržo nei valstybių sienos, nei laikas.

3. Ar TVEE, Jūsų manymu, kelia pavojų? Jei taip, tai kam?

Be abejonės, jei nebus imamasi papildomų priemonių, TVEE keliamas pavojus nuolat didės, visų pirma, tiems asmenims, kurie vis plačiau naudos identifikavimą elektroninėje erdvėje.

4. Nurodykite sritis (pagal sektorius: viešasis, privatusis ir pagal veiklos pobūdį: finansų, medicinos ir kt.), kuriose, Jūsų nuomone, tapatybės vagystės grėsmė yra didžiausia. Savo atsakymą pagrįskite.

Manyčiau, kad tapatybės vagystės grėsmė didesnė bus tame sektoriuje, kuriame bus mažiau kreipiama dėmesio į asmenybės identifikavimo patikimumą, griežtesnį identifikavimo reglamentavimą. Tapatybės vagystės yra galimos visose veiklos srityse, žmonės dažniausia skaudžiausiai pajunta šių vagysčių pasekmes finansų sferoje, tačiau nė kiek ne mažesnė žala gali būti padaryta sveikatos apsaugos sferoje, tapatybės vagystės pagalba yra galimas šantažavimas visose veiklos srityse.

5. Ar, Jūsų nuomone, pakanka teisės normų ir teisinio reguliavimo tinkamai sureguliuoti TVEE? Jei manote, kad nepakanka, tai kokių teisės normų trūksta?

Dabartinėje situacijoje tinkamai sureguliuoti TVEE teisės normų ir teisinio reguliavimo gal ir užtenka, tačiau, prognozuojant spartų TVEE plitimą, būtinai reikia įvertinti šių vagysčių specifiką ir įvesti specialius straipsnius TVEE reguliavimui.

6. Ar Lietuvoje numatyta atsakomybė už TVEE? Jei taip, tai kokia?

TVEE yra gana ilgas ir sudėtingas procesas. Lietuvoje pradinius veiksmus galima vertinti pagal Asmens duomenų teisinės apsaugos įstatymą, tačiau čia numatomos baudos yra gana mažos (500–1000 Lt), vėliau veiksmus jau galima vertinti kaip kriminalinį nusikaltimą ir taikyti Baudžiamojo Kodekso numatytą atsakomybę.

7. Ar manote, kad TVEE reikėtų kriminalizuoti kaip savarankišką nusikalstamą veiką? Kodėl?

Pritarčiau, kad TVEE reikėtų kriminalizuoti kaip savarankišką nusikalstamą veiką, nes šios vagystės yra intelektinio pobūdžio, jas paprasta išskaidyti į atskiras dalis, kurias galima realizuoti lygiagrečiai, todėl jas galima realizuoti labai sparčiai, kai kurie jų dalyviai gali net nesuprasti, kad jie dalyvauja nusikalstamoje veikloje. Labai sudėtinga įvertinti, kokiems tolimesniems nusikaltimams planuojami ir galimi panaudoti TVEE duomenys.

8. Ar galiojančios teisės normos, reguliuojančios santykius, susijusius su TVEE, taikomos tinkamai?

Galiojančios teisės normos, reguliuojančios santykius, susijusius su TVEE yra taikomos palyginti neseniai, dar nėra nusistovėjusios teisinės praktikos,

ne visi ikiteisminio tyrimo vykdytojai bei teisėjai yra pasirengę nagrinėti tokio pobūdžio bylas, todėl būtų reikalingi specialiai parengti apibendrinimai ir rekomendacijos tokių bylų tyrimui.

9. Kokios problemos kyla dėl TVEE tyrimo?

Gana sudėtinga nustatyti, kokiu būdu buvo įvykdyta TVEE, kartais ji gali būti atlikta ne vienu veiksmu, o keliais tarpusavyje nesusijusiais veiksmais, sudėtingą įrodyti kokiu tikslu yra įvykdyta tapatybės vagystė.

10. Ar pakankamai taikoma savireguliacinių TVEE sumažinimo ir (arba) išvengimo priemonių? Kokios savireguliacinės priemonės galėtų sumažinti TVEE?

Savireguliacinių TVEE sumažinimo ir (arba) išvengimo priemonių Lietuvoje yra nepakankamai, kadangi kol kas dar nepakankamai suvokiama tokių vagysčių grėsmė. Pirmiausia, reikia apibrėžti, kas norėtų, galėtų ar net privalėtų dalyvauti tokioje savireguliacinėje veikloje bei savireguliacijos principus ir priemones įteisinti atitinkamais teisės aktais.

11. Ar, Jūsų nuomone, valstybių tarpinstitucinis bendradarbiavimas yra pakankamas ir tinkamas? Jei ne, nurodykite, ko trūksta.

Valstybių tarpinstitucinis bendradarbiavimas vyksta, tačiau jis yra nepakankamas, nes TVEE gali būti vykdomos vienoje valstybėje, o pasekmės patiriamos kitoje. Todėl būtų tikslinga suvienodinti teisinę atsakomybę už TVEE, kita vertus, tikslinga sutelkti visų valstybių mokslines pajėgas kurti priemones, kurių pagalba butų galima užkirsti kelią TVEE ir jų operatyviam atskleidimui.

12. Ar, Jūsų nuomone, bendradarbiavimas tarp valstybės ir privataus sektoriaus yra tinkamas? Jei ne, nurodykite, ko trūksta.

Bendravimas tarp valstybės ir privataus sektoriaus šioje srityje vyksta, kadangi suvokiama TVEE grėsmė ir galimos tolimesnės pasekmės. Tačiau ši problema yra aktuali beveik visam privačiam sektoriui ir skirtingo pavaldumo valstybės institucijoms, todėl trūksta vienos koordinuojančios institucijos, atsakingos už šios problemos sprendimą.

13. Ar elektroninio verslo taikomos priemonės apsaugo nuo TVEE? Kokios priemonės yra pakankamos ir kokios neturėtų būti taikomos?

Elektroninio verslo taikomos priemonės, suprantama, apsaugo nuo TVEE. Tačiau, viena vertus, kuo patikimesnės apsaugos priemonės tuo jos brangesnės, kita vertus, kuo patikimesnės apsaugos priemonės tuo jos labiau mažina elektroninės erdvės teikiamus privalumus. Tad visuomet reikia konkrečiai įvertinti koks apsaugos lygis yra reikalingas ir kokias priemones reikia taikyti, kad jos pasiteisintų.

14. Ar elektroninio verslo naudojamos asmens indentifikavimo priemonės turėtų būti privalomai reguliuojamos teisės normomis? Argumentuokite.

Elektroninio verslo naudojamos identifikavimo priemonės turėtų būti suskirstytos į kelis patikimumo lygmenis. Kai kuriose srityse identifikavimo priemonės gali būti privalomai reguliuojamos teisės normomis, kitoms gali būti rekomenduojamas atitinkamas identifikavimo patikimumo lygmuo, o visur turėtų būti nurodytas identifikavimo patikimumo lygmuo.

15. Kokias TVEE prevencijos priemones galėtumėte pasiūlyti?

TVEE prevencijos pagrindinės krytys yra trys – 1)asmens identifikavimo patikimumo teisinis reglamentavimas, 2) asmens duomenų valdytojų teisinės atsakomybės už asmens duomenų apsaugą didinimas (bausmių didinimas), 3) žymiai platesnis visuomenės švietimas apie duomenų apsauga pradedant nuo vaikų, įvedant specialias temas apie duomenų apsaugą mokyklose, kolegijose universitetuose.

Apklausa Tapatybės vagystė elektroninėje erdvėje (Ekspertai)

Respondentas #3

1. Kaip vertinate tapatybės vagystės elektroninėje erdvėje (toliau – TVEE) reiškinį?

Neigiamai, kaip galintį padaryti didelės žalos tapatybės turėtojui.

2. Ar TVEE, Jūsų nuomone, yra paplitusi? Argumentuokite.

Atsižvelgiant į platų interneto vartojimą, intrnetinių tapatybių gausą, manytina, paplitusi.

3. Ar TVEE, Jūsų manymu, kelia pavojų? Jei taip, tai kam?

Visų pirma finansiniams asmenų interesams, jo reputacijai.

4. Nurodykite sritis (pagal sektorius: viešasis, privatusis ir pagal veiklos pobūdį: finansų, medicinos ir kt.), kuriose, Jūsų nuomone, tapatybės vagystės grėsmė yra didžiausia. Savo atsakymą pagrįskite.

Finansų, perkant internetu, socialiniuose tinklapiuose.

5. Ar, Jūsų nuomone, pakanka teisės normų ir teisinio reguliavimo tinkamai sureguliuoti TVEE? Jei manote, kad nepakanka, tai kokių teisės normų trūksta?

Sunku pasakyti.

6. Ar Lietuvoje numatyta atsakomybė už TVEE? Jei taip, tai kokia?

Baudžiamoji atsakomybė už kai kuriuos TVEE numatyta BK 215 str., taip pat manytina, TVEE galėtų apimti BK 300 str. dokumento klastojimas.

7. Ar manote, kad TVEE reikėtų kriminalizuoti kaip savarankišką nusikalstamą veiką? Kodėl?

Galiojančio BK normos apima TVEE.

8. Ar galiojančios teisės normos, reguliuojančios santykius, susijusius su TVEE, taikomos tinkamai?

Sunku pasakyti.

9. Kokios problemos kyla dėl TVEE tyrimo?

Sunku pasakyti.

10. Ar pakankamai taikoma savireguliacinių TVEE sumažinimo ir (arba) išvengimo priemonių? Kokios savireguliacinės priemonės galėtų sumažinti TVEE?

Sunku pasakyti.

11. Ar, Jūsų nuomone, valstybių tarpinstitucinis bendradarbiavimas yra pakankamas ir tinkamas? Jei ne, nurodykite, ko trūksta.

Sunku pasakyti.

12. Ar, Jūsų nuomone, bendradarbiavimas tarp valstybės ir privataus sektoriaus yra tinkamas? Jei ne, nurodykite, ko trūksta.

Sunku pasakyti.

13. Ar elektroninio verslo taikomos priemonės apsaugo nuo TVEE? Kokios priemonės yra pakankamos ir kokios neturėtų būti taikomos?

Sunku pasakyti.

14. Ar elektroninio verslo naudojamos asmens indentifikavimo priemonės turėtų būti privalomai reguliuojamos teisės normomis? Argumentuokite.

Sunku pasakyti.

15. Kokias TVEE prevencijos priemones galėtumėte pasiūlyti?

Sunku pasakyti.

Apklausa Tapatybės vagystė elektroninėje erdvėje (Ekspertai)

Respondentas #4

1. Kaip vertinate tapatybės vagystės elektroninėje erdvėje (toliau – TVEE) reiškinį?

Tapatybės vagystėmis yra siekiama gauti prieigą prie finansinės informacijos, materialinių vertybių pasisavinimo. Kito asmens tapatybe taip pat gali būti pasinaudojama tolimesnėms tapatybės vagystėms: gauti informaciją

apie kitus asmenis, jų kontaktinę informaciją, pajamas, turtą, sveikatos būklę ar slaptažodžius. Apsimetant kitu asmeniu gali būti siekiama prieigos prie konfidencialios informacijos. Jei yra norima patekti į apsaugotą teritoriją ar patalpas, darbuotojų pažymėjimai, įeigos kontrolės kortelės ir apsauginės signalizacijos atjungimo kodai taip pat gali tapti nusikaltėlių taikiniu. Be abejo šį reiškinį vertinu neigiamai.

2. Ar TVEE, Jūsų nuomone, yra paplitusi? Argumentuokite.

Tapatybės vagystę dažniausiai yra sunku nustatyti prieš prasidedant neigiamoms pasekmėms. Teisėsaugos institucijų reikalavimai pasiaiškinti už nusikalstamą jūsų vardu atliktą veiklą vienareikšmiškai reiškia, kad jūsų tapatybe pasinaudojo kiti.

3. Ar TVEE, Jūsų manymu, kelia pavojų? Jei taip, tai kam?

Tapatybės vagystės pasekmės yra neigiamos ir dažniausiai susijusios su didesniais ar mažesniais nuostoliai. Dažniausiai tapatybės vagytės tikslas yra finansinis pasipelnymas. Kreditinių kortelių numeriai, PIN kodai, mobiliųjų paslaugų papildymo kodai – visa tai yra nusikaltėlių taikinys. Naudojantis internetinės bankininkystės paslaugoms, savo sąskaitą galima valdyti iš bet kurio prie interneto prijungto kompiuterio, tereikia įvesti teisingą naudotojo identifikatorių ir slaptažodžius. Jei tokie naudotojų identifikatoriai ir slaptažodžiai patektų į svetimas rankas, vieną dieną galite sužinoti, kad jūsų sąskaita yra tuščia arba net su neigiamu balansu.

Taip pat yra galimybė, kad pasinaudojus jūsų tapatybės duomenimis gali būti suteršta reputacija: paviešinta asmeninės informacija, jūsų vardu išplatinta tikrovės neatitinkanti informacija, sugadinta gera kreditinė istorija. Gavus prieigą prie jūsų sąskaitos valdymo, atsiranda galimybė vykdyti neteisėtas finansines operacijas, pvz., pinigų plovimą. Pavogtas pasas gali būti panaudotas neteisėtam kitų asmenų valstybės sienos kirtimui arba paskolų, kurių net nesirengiama gražinti, pasiėmimui. Jūsų vairavimo teisių pažymėjimu gali būti parduotas asmeniui, kuriam yra atimta teisė vairuoti.

Jei neįgalioti asmenys turės jūsų elektroninio pašto naudotojo vardą ir slaptažodį, jie ne tik galės skaityti jūsų asmenines paslaptis, siųsti elektroninius laiškus jūsų vardu, bet ir šantažuoti jus, grasindami paskelbti asmeninio susirašinėjimo detales ir taip siekdami finansinės naudos.

Bet kuriuo tapatybės vagystės atveju bus sugaišta daug brangaus laiko įrodymams, kad neteisėtus veiksmus atliko kitas asmuo. Ne visais atvejais pavyksta susigražinti pavogtas finansines lėšas, sugadintos reputacijos atstatymui reikia daug laiko arba jos iš viso nepavyksta atstatyti.

4. Nurodykite sritis (pagal sektorius: viešasis, privatusis ir pagal veiklos pobūdį: finansų, medicinos ir kt.), kuriose, Jūsų nuomone, tapatybės vagystės grėsmė yra didžiausia. Savo atsakymą pagrįskite.

TVEE ypač aktuali kritinės infrastruktūros objektų apsaugai: elektros ir vandentiekio tiekimo sistemoms, traukinių ir lėktuvų valdymo įrangai.

5. Ar, Jūsų nuomone, pakanka teisės normų ir teisinio reguliavimo tinkamai sureguliuoti TVEE? Jei manote, kad nepakanka, tai kokių teisės normų trūksta?

Manau, kad pakanka.

6. Ar Lietuvoje numatyta atsakomybė už TVEE? Jei taip, tai kokia?

TVEE kaip savarankiška nusikalstama veika nėra kriminalizuota. Dažniausiai veksmai TVEE atveju bus kvalifikuojami kaip sukčiavimas.

7. Ar manote, kad TVEE reikėtų kriminalizuoti kaip savarankišką nusikalstamą veiką? Kodėl?

Neturiu nuomonės.

8. Ar galiojančios teisės normos, reguliuojančios santykius, susijusius su TVEE, taikomos tinkamai?

Neturiu nuomonės Nesusijęs su normų taikymu.

9. Kokios problemos kyla dėl TVEE tyrimo?

Neturiu nuomonės Nesusijęs su tyrimu.

10. Ar pakankamai taikoma savireguliacinių TVEE sumažinimo ir (arba) išvengimo priemonių? Kokios savireguliacinės priemonės galėtų sumažinti TVEE?

Manau nepakanka. Pirmoji pagalba šioje srityje yra visuomenės, subjektų teisinis švietimas ir auklėjimas.

11. Ar, Jūsų nuomone, valstybių tarpinstitucinis bendradarbiavimas yra pakankamas ir tinkamas? Jei ne, nurodykite, ko trūksta.

Reiškinys neturintis sienų, ko nepasakysi apie valstybių jurisdikciją. Tarpvalstybinis bendradarbiavimas prevencijos, nusikaltėlių išdavimo srityje ir kitais aspektais.

12. Ar, Jūsų nuomone, bendradarbiavimas tarp valstybės ir privataus sektoriaus yra tinkamas? Jei ne, nurodykite, ko trūksta.

Bendradarbiavimo trūksta, visų pirma informacijos keitimosi, visuomenės samoningumo ir atsakingumo didinimo srityje.

13. Ar elektroninio verslo taikomos priemonės apsaugo nuo TVEE? Kokios priemonės yra pakankamos ir kokios neturėtų būti taikomos?

Neturiu nuomonės. Nesusijęs su e-verslu.

14. Ar elektroninio verslo naudojamos asmens indentifikavimo priemonės turėtų būti privalomai reguliuojamos teisės normomis? Argumentuokite.

Neturiu nuomonės. Nesusijęs su e-verslu.

15. Kokias TVEE prevencijos priemones galėtumėte pasiūlyti?

Tapatybės vagystės galima išvengti, jei laikomasi paprastų saugumo principų. Visų pirma reikia užtikrinti deramą pasų, kortelių ir kitokių pažymėjimų saugą, siekiant išvengti vagystės: laikyti saugioje vietoje ir nešiotis kartu su savimi tik tada, kai rengiatės jau pasinaudoti. Rekomenduojama laikytis „švaraus stalo" politikos: neužsirašyti ir nesakyti kitiems slaptažodžių ir PIN kodų; perskambinti asmenims ar organizacijoms, prašančioms jūsų konfidencialios informacijos, žinomais numeriais; naudotis slaptažodžiu apsaugota kompiuterio ekrano užsklanda; svarbius dokumentus saugoti užrakintus stalčiuose arba seife; nereikalingus arba išmetimui skirtus svarbius dokumentus sunaikinti dokumentų naikikliu; išeinant iš kabineto uždaryti langus ir užrakinti duris; baigus darbą nepamiršti įjungti signalizaciją. Taip pat reikėtų nesakyti svarbios asmeninės informacijos jos prašantiems asmenims, prieš tai neįsitikinus jų tapatybe ir įgaliojimais.

Apklausa Tapatybės vagystė elektroninėje erdvėje (Ekspertai)

Respondentas #5

1. Kaip vertinate tapatybės vagystės elektroninėje erdvėje (toliau – TVEE) reiškinį?

TVEE turi būti priskiriama nusikalstamai veikai, jei dėl to kyla kokių nors neigiamų pasekmių (materialinė žala, nukenčia subjekto garbė ir orumas ir pan.)

2. Ar TVEE, Jūsų nuomone, yra paplitusi? Argumentuokite.

Mano nuomone, TVEE nėra labai paplitęs reiškinys (bent jau Lietuvoje). Deja, neturiu duomenų, kuriais galėčiau pagrįsti šį teiginį. Tai subjektyvus vertinimas remiantis bendra informacija.

3. Ar TVEE, Jūsų manymu, kelia pavojų? Jei taip, tai kam?

TVEE kelia pavojų tuo atveju, jei šia veika padaroma žala. Subjektai, kuriems kyla didžiausia grėsmė būtų finansinės institucijos bei piliečiai besinaudojantys elektroninėmis atsiskaitymo priemonėmis.

4. Nurodykite sritis (pagal sektorius: viešasis, privatusis ir pagal veiklos pobūdį: finansų, medicinos ir kt.), kuriose, Jūsų nuomone, tapatybės vagystės grėsmė yra didžiausia. Savo atsakymą pagrįskite.

Privačiame sektoriuje tapatybės vagystės grėsmė turėtų būti didesnė, kadangi viešasis sektorius gali naudotis duomenų bazėmis, ne visada prieinamomis

privataus sektoriaus subjektams, kurių saugumas valstybės mastu yra labiau užtikrinamas. Taip pat viešajame sektoriuje yra daug aiškesnis teisinis reguliavimas dėl informacijos saugumo užtikrinimo, o tai leidžia daryti prielaidą, kad turėtų būti mažesnė rizika TVEE.
Pagal veiklos pobūdį išskirčiau finansų sritį kap pagrindinę, kurioje gali pasireikšti TVEE. Finansinės naudos gavimas būtų kaip pagrindinis tikslas, o šiam tikslui pasiekti finansų sektorius būtų palankiausias, ypač turint omeny, kad šis sektorius vienas iš pirmųjų ir sparčiausiai vystantis veiklą elektroninėje erdvėje. Taip pat ir elektroninėje komercijoje įvykdyti TVEE atveai būtų susiję su apmokėjimu, t.y. finansinėmis operacijomis, todėl irgi priskirtinos finansinei sričiai.

5. Ar, Jūsų nuomone, pakanka teisės normų ir teisinio reguliavimo tinkamai sureguliuoti TVEE? Jei manote, kad nepakanka, tai kokių teisės normų trūksta?

Kadangi manau, kad TVEE neturi būti kvalifikuojamas kaip atskiras nusikaltimas, tai šiuo metu esamų teisės normų pakanka, kad būtų galima tinkamai sureguliuoti TVEE.

6. Ar Lietuvoje numatyta atsakomybė už TVEE? Jei taip, tai kokia?

Vien tik už TVEE Lietuvoje atsakomybė nenumatyta.

7. Ar manote, kad TVEE reikėtų kriminalizuoti kaip savarankišką nusikalstamą veiką? Kodėl?

Nemanau, kad TVEE reikia kriminalizuoti kaip savarankišką nusikalstamą veiką. TVEE pati savaime nepadaro žalos. Dažniausia tai tik pasirengiamoji stadija atliekant nusikaltimą, t.y. jau krimanilzuotą nusikalstamą veiką.

8. Ar galiojančios teisės normos, reguliuojančios santykius, susijusius su TVEE, taikomos tinkamai?

Nesant teisės normų atskirai kriminalizuojančių TVEE, jų taikymo negali ir būti.

9. Kokios problemos kyla dėl TVEE tyrimo?

Negaliu atsakyti į šį klausimą.

10. Ar pakankamai taikoma savireguliacinių TVEE sumažinimo ir (arba) išvengimo priemonių? Kokios savireguliacinės priemonės galėtų sumažinti TVEE?

Neturiu duomenų.

11. Ar, Jūsų nuomone, valstybių tarpinstitucinis bendradarbiavimas yra pakankamas ir tinkamas? Jei ne, nurodykite, ko trūksta.

Neturiu duomenų.

12. Ar, Jūsų nuomone, bendradarbiavimas tarp valstybės ir privataus sektoriaus yra tinkamas? Jei ne, nurodykite, ko trūksta.

TVEE esant tik kaip pasirengiamajai stadijai kitai kriminalizuotai veikai, svarbu, kad būtų mažinamas tokio pobūdžio veiklos latentiškumas. Privataus sektoriaus nesuinteresuotumas pradėti tyrimus (ne vidaus) dėl priežasčių, kuomet pats tyrimas verslui labiau pakenktų nei žalos atlyginimas nukentėjusiajam, neleidžia efektyviai kovoti su tokio pobūdžio nusikaltimais. Neturiu duomenų ar privatus sektorius dažnai nutyli tokio pobūdžio nusikalstamas veikas, kurių metu taip pat buvo įvykdyta TVEE. Tačiau, turint omeny, didelį elektroninių nusikaltimų latentiškumą, tikėtina, kad ir TVEE atvejų įvykusių privačiame sektoriuje valstybės institucijos dažnai nesužino.

13. Ar elektroninio verslo taikomos priemonės apsaugo nuo TVEE? Kokios priemonės yra pakankamos ir kokios neturėtų būti taikomos?

Šiai dienai nėra tokių priemonių, kurios būtų pakankamos apsaugant nuo TVEE elektroniniame versle.

14. Ar elektroninio verslo naudojamos asmens indentifikavimo priemonės turėtų būti privalomai reguliuojamos teisės normomis? Argumentuokite.

Asmens identifikavimo priemonės neturi būti reguliuojamos teisės normomis.

15. Kokias TVEE prevencijos priemones galėtumėte pasiūlyti?

Biometrinės priemonės būtų tinkamos tik ypač svarbiose valstybinio sektoriaus srityse. Tačiau atsižvelgiant į tai, kad šiose srityse nėra didelio pavojaus dėl TVEE, šios priemonės nėra tokios svarbios. Elektroninėje komercijoje šios priemonės gali būti naudingos tik tuo atveju, jei jų naudojimas nestabdys elektroninės komercijos vystymosi. Tokios priemonės turi būti priimtinos visoms sandorio šalims. Atsižvelgiant į tai, kad šiai dienai nėra tokių priemonių, reikalingas tokių technologijų tobulinimas bei pritaikomumas elektroninės komercijos poreikiams.

Apklausa Tapatybės vagystė elektroninėje erdvėje (Ekspertai)

Respondentas #6

1. Kaip vertinate tapatybės vagystės elektroninėje erdvėje (toliau – TVEE) reiškinį?

Neigiamai vertinu. Tai pavojingas reiškinys.

2. Ar TVEE, Jūsų nuomone, yra paplitusi? Argumentuokite.

Mano žiniomis, tai nėra labai palitęs reiškinys Lietuvoje. Pasitaiko atvejų, bet jie yra reti.

3. Ar TVEE, Jūsų manymu, kelia pavojų? Jei taip, tai kam?

Taip, kelia pavojų pirmiausia tam asmeniui, kurio tapatybės duomenimis pasinaudojama. Kelia pavojų ir verslo subjektams, nes gali kilti dėl to problemų su atsiskaitymu už prekes ir palaugas, gali būti patiriama žala. Kelia pavojų ir visuomeninei tvarkai, pavyzdžiui, teisinio poveikio priemonės gali būti nukreiptos į tikrąjį tų duomenų savininką, kuris yra niekuo dėtas.

4. Nurodykite sritis (pagal sektorius: viešasis, privatusis ir pagal veiklos pobūdį: finansų, medicinos ir kt.), kuriose, Jūsų nuomone, tapatybės vagystės grėsmė yra didžiausia. Savo atsakymą pagrįskite.

Tokios statistikos ir tyrimų neteko matyti. Sunku pasakyti.

5. Ar, Jūsų nuomone, pakanka teisės normų ir teisinio reguliavimo tinkamai sureguliuoti TVEE? Jei manote, kad nepakanka, tai kokių teisės normų trūksta?

Nesu įsigilinęs į šiuos aspektus.

6. Ar Lietuvoje numatyta atsakomybė už TVEE? Jei taip, tai kokia?

Taip numatyta. Tam tikrais atvejais ir baudžiamoji atsakomybė.

7. Ar manote, kad TVEE reikėtų kriminalizuoti kaip savarankišką nusikalstamą veiką? Kodėl?

Kaip savarankiškos veikos TVEE kriminalizacijos būtinybę reiktų įrodyti.

8. Ar galiojančios teisės normos, reguliuojančios santykius, susijusius su TVEE, taikomos tinkamai?

Nesusipažinęs su šia praktika.

9. Kokios problemos kyla dėl TVEE tyrimo?

Nesu susipažinęs.

10. Ar pakankamai taikoma savireguliacinių TVEE sumažinimo ir (arba) išvengimo priemonių? Kokios savireguliacinės priemonės galėtų sumažinti TVEE?

Visiškai to išvengti negalima. Reikalingas protingas balansas tarp sąnaudų irr siekiamų tikslų.

11. Ar, Jūsų nuomone, valstybių tarpinstitucinis bendradarbiavimas yra pakankamas ir tinkamas? Jei ne, nurodykite, ko trūksta.

Neturiu informacijos.

12. Ar, Jūsų nuomone, bendradarbiavimas tarp valstybės ir privataus sektoriaus yra tinkamas? Jei ne, nurodykite, ko trūksta.

Tarp valstybės ir privataus sektoriaus bendradarbiavimas kažin ar kokioje nors sferoje Lietuvoje yra tinkamas.

13. Ar elektroninio verslo taikomos priemonės apsaugo nuo TVEE? Kokios priemonės yra pakankamos ir kokios neturėtų būti taikomos?

Nėra visiškai apsaugančių priemonių, kad ir kokios tobulos būtų.

14. Ar elektroninio verslo naudojamos asmens indentifikavimo priemonės turėtų būti privalomai reguliuojamos teisės normomis? Argumentuokite.

Minimalūs standartai taip.

15. Kokias TVEE prevencijos priemones galėtumėte pasiūlyti?

Papildomi saugikliai tikrinant, ar asmuo yra tas, kuo jis save laiko.

Apklausa Tapatybės vagystė elektroninėje erdvėje (Ekspertai)

Respondentas #7

1. Kaip vertinate tapatybės vagystės elektroninėje erdvėje (toliau – TVEE) reiškinį?

Neigiamai. Tai vienas iš konfidencialumo pažeidimų elektroninėje erdvėje.

2. Ar TVEE, Jūsų nuomone, yra paplitusi? Argumentuokite.

Tikruosius šio reiškinio mastus dėl jo latentiškumo yra sunku nustatyti.

3. Ar TVEE, Jūsų manymu, kelia pavojų? Jei taip, tai kam?

Manyčiau, kad kelia. Pirmiausia pavojus yra susijęs su įvairiais asmens privataus gyvenimo neliečiamumo pažeidimais, taip pat tokio pobūdžio veikos sudaro sąlygas kitų nusikalstamų veikų padarymui (pavyzdžiui, sukčiavimui elektroninėje erdvėje).

4. Nurodykite sritis (pagal sektorius: viešasis, privatusis ir pagal veiklos pobūdį: finansų, medicinos ir kt.), kuriose, Jūsų nuomone, tapatybės vagystės grėsmė yra didžiausia. Savo atsakymą pagrįskite.

Privatus sektorius, veiklos pobūdis – finansų. Manyčiau, kad įvairūs asmens tapatybės vagystės atvejai yra susiję su turtinės naudos siekiu, kai asmens tapatybę patvirtinantys duomenys yra panaudojami įvykdant turtines nusikalstamas veikas, nusikalstamas veikas ekonomikai, finansų sistemai.

5. Ar, Jūsų nuomone, pakanka teisės normų ir teisinio reguliavimo tinkamai sureguliuoti TVEE? Jei manote, kad nepakanka, tai kokių teisės normų trūksta?

Manyčiau, kad su TVEE prevencija susijusios teisės normos turėtų būti peržiūrimos. Galėtų būti svarstomos administracinės ir baudžiamosios atsakomybės už TVEE tobulinimo galimybės.

6. Ar Lietuvoje numatyta atsakomybė už TVEE? Jei taip, tai kokia?

Atsakomybė už TVEE padarymą yra fragmentiška. Tik dalis TVEE atvejų yra kriminalizuota Baudžiamajame kodekse.

7. Ar manote, kad TVEE reikėtų kriminalizuoti kaip savarankišką nusikalstamą veiką? Kodėl?

Iš esmės pritarčiau TVEE kriminalizavimui kaip savarankiškai nusikalstamai veikai, tačiau į tokius siūlymus reiktų žiūrėti kompleksiškai – nustatyti, kokia apimtimi ji yra kriminalizuota šiuo metu, kokiuose Baudžiamojo kodekso straipsniuose tai yra padaryta.

8. Ar galiojančios teisės normos, reguliuojančios santykius, susijusius su TVEE, taikomos tinkamai?

Atsižvelgiant į tai, kad nusikalstamos veikos elektroninėje erdvėje kol kas yra sunkiai tiriamos, taip pat nesant vieningos nuomonės kaip spręsti šių nusikalstamų veikų daugeto problemas, Baudžiamojo kodekso normos ne visais atvejais gali būti taikomos tinkamai.

9. Kokios problemos kyla dėl TVEE tyrimo?

Galima būtų teigti, kad viena pagrindinių problemų ta, kad dėl elektroninės erdvės suteiktų galimybių TVEE padaręs asmuo nenustatomas. O ir nustačius dėl tarptautinio bendradarbiavimo trūkumų tolimesnių veiksmų atlikimas nėra galimas ar operatyvus.

10. Ar pakankamai taikoma savireguliacinių TVEE sumažinimo ir (arba) išvengimo priemonių? Kokios savireguliacinės priemonės galėtų sumažinti TVEE?

–

11. Ar, Jūsų nuomone, valstybių tarpinstitucinis bendradarbiavimas yra pakankamas ir tinkamas? Jei ne, nurodykite, ko trūksta.

Nors bandoma vystyti tarptautinį bendradarbiavimą, tačiau jam trūksta operatyvumo. Taip pat tarptautiniame bendradarbiavime dalyvauja ne visos užsienio valstybės.

12. Ar, Jūsų nuomone, bendradarbiavimas tarp valstybės ir privataus sektoriaus yra tinkamas? Jei ne, nurodykite, ko trūksta.

Bendradarbiavimas ne visais atvejais yra tinkamas. Šį bendradarbiavimą gali gerinti pačio privataus sektoriaus suinteresuotumas, kurį skatintų ir tinkamas viešojo sektoriaus reagavimas į tas problemas, kurias nurodo privataus sektoriaus atstovai (pavyzdžiui, atlikti tyrimo veiksmus, jei pranešama apie galimus pažeidimus).

13. Ar elektroninio verslo taikomos priemonės apsaugo nuo TVEE? Kokios priemonės yra pakankamos ir kokios neturėtų būti taikomos?

–

14. Ar elektroninio verslo naudojamos asmens indentifikavimo priemonės turėtų būti privalomai reguliuojamos teisės normomis? Argumentuokite.

Bet kokios tokio pobūdžio priemonės turėtų būti reguliuojamos teisės normomis, nes susijusios su atitinkamų teisių ir pareigų nustatymu.

15. Kokias TVEE prevencijos priemones galėtumėte pasiūlyti?

Manyčiau, kad pirmiausia tokios priemonės turėtų būti skirtos pirminei prevencijai – informavimui apie TVEE (pavyzdžiui, tinkama phishing atveju). Taip pat svarbi prevencinė priemonė būtų – programinės įrangos tobulinimas (pavyzdžiui, gerinant apsaugą nuo neteisėtų prisijungimų prie informacinės sistemos).

Apklausa Tapatybės vagystė elektroninėje erdvėje (Ekspertai)

Respondentas #8

1. Kaip vertinate tapatybės vagystės elektroninėje erdvėje (toliau – TVEE) reiškinį?

Žinoma, kad neigiamai.

2. Ar TVEE, Jūsų nuomone, yra paplitusi? Argumentuokite.

Netikslus klausimas. Lietuvoje nėra paplitusi nes net veika nėra kriminalizuota, Pasaulyje, esu tikras, kad taip, paplitus.

3. Ar TVEE, Jūsų manymu, kelia pavojų? Jei taip, tai kam?

Kelia pavojų asmeniui kieno asmens duomenys pavogti.

4. Nurodykite sritis (pagal sektorius: viešasis, privatusis ir pagal veiklos pobūdį: finansų, medicinos ir kt.), kuriose, Jūsų nuomone, tapatybės vagystės grėsmė yra didžiausia. Savo atsakymą pagrįskite.

Privatus – finansai nes tai esminis vagysciu pagrindas, – nauda.

5. Ar, Jūsų nuomone, pakanka teisės normų ir teisinio reguliavimo tinkamai sureguliuoti TVEE? Jei manote, kad nepakanka, tai kokių teisės normų trūksta?

Sunku pasakyti ar pakanka , neatlikus atskiro išsamaus tyrimo. Manau, kad nepakanka , nes BK nėra straipsnio kuris konkrečiai būtų skirtas TVEE problemai.

6. Ar Lietuvoje numatyta atsakomybė už TVEE? Jei taip, tai kokia?

Konkrečiai BK tokio str., nėra.

7. Ar manote, kad TVEE reikėtų kriminalizuoti kaip savarankišką nusikalstamą veiką? Kodėl?

Manau, kad taip nes tikėtinas bausmės sulaukimas gal kiek drausmintų potencialius tapatybės vagystės vykdytojus.

8. Ar galiojančios teisės normos, reguliuojančios santykius, susijusius su TVEE, taikomos tinkamai?

Manau, kad taip.

9. Kokios problemos kyla dėl TVEE tyrimo?

Problemų nekyla nes nesant konkrečiam straipsniui negali būt pradėtas ikiteisminis tyrimas dėl TVEE, problemos gali kilti jei tapatybės vagystes atveju su tais duomenimis kas buvo daroma...

10. Ar pakankamai taikoma savireguliacinių TVEE sumažinimo ir (arba) išvengimo priemonių? Kokios savireguliacinės priemonės galėtų sumažinti TVEE?

Nežinau.

11. Ar, Jūsų nuomone, valstybių tarpinstitucinis bendradarbiavimas yra pakankamas ir tinkamas? Jei ne, nurodykite, ko trūksta.

Manau, kad pakankamas.

12. Ar, Jūsų nuomone, bendradarbiavimas tarp valstybės ir privataus sektoriaus yra tinkamas? Jei ne, nurodykite, ko trūksta.

Manau, kad nėra grįžtamojo ryšio tarp privataus sektoriaus ir valstybės. Taip sakau dėl to, kad nepakankamai privatus sektorius kelia problemas valstybiniu lygiu.

13. Ar elektroninio verslo taikomos priemonės apsaugo nuo TVEE? Kokios priemonės yra pakankamos ir kokios neturėtų būti taikomos?

Manau , kad yra pakankamos. Neturiu nuomonės kokios neturėtų būti taikomos, sakyčiau, kad visos turi būti taikomos.

14. Ar elektroninio verslo naudojamos asmens indentifikavimo priemonės turėtų būti privalomai reguliuojamos teisės normomis? Argumentuokite.

Manau, kad taip nes tai veiktų kaip prevencinė priemonė išvengiant tapatybės vagysčių elektroninėje erdvėje.

15. Kokias TVEE prevencijos priemones galėtumėte pasiūlyti?

Kad pasiūlyti priemones, reikėtų nustatyti rizikas. Atlikti rizikos analizę, kurią sudarytų grėsmių analizė ir t.t. Šiaip, prevencinės priemonės turėtų būti teisinės (teisės aktai, taisyklės, rekomendacijos) ir techninės (kortelės su mikroschemomis ir t.t.).

Apklausa Tapatybės vagystė elektroninėje erdvėje (Ekspertai)

Respondentas #9

1. Kaip vertinate tapatybės vagystės elektroninėje erdvėje (toliau – TVEE) reiškinį?

Lietuvos Respublikoje tai neteisėta veikla.

2. Ar TVEE, Jūsų nuomone, yra paplitusi? Argumentuokite.

Reiškinys salyginai dažnas. Iš esmės tai priklauso nuo IT integracijos visuomenėje. Augant IT ir vykstant Interneto plėtrai (tas šiuo metu Lietuvoje labai ryškiai pastebima) TVEE auga proporcingai.

3. Ar TVEE, Jūsų manymu, kelia pavojų? Jei taip, tai kam?

Pavojus IT vartotojui. Pažeidimai programinėje įrangoje, saugumo spragos informacinėse sistemose ir t. t. gali lemti duomenų vagystes iš trečiųjų asmenų. „Socialinės inžinerijos" tipo atakos prieš vartotojus tas pats.

Pavojus e. komercijos vykdytojams. Dėl tų pačių saugumo priežasčių, yra faktų kai įmonės praranda sukauptus duomenis apie vartotojų asmens tapatybes, kai įvyksta nesankcionuoti prisijungimai prie duomenų bazių. Išaiškėję tokie faktai pakenkia tokių įmonių komercinei veiklai, nes nukenčia reputacija, pasitikėjimas ir pan.

4. Nurodykite sritis (pagal sektorius: viešasis, privatusis ir pagal veiklos pobūdį: finansų, medicinos ir kt.), kuriose, Jūsų nuomone, tapatybės vagystės grėsmė yra didžiausia. Savo atsakymą pagrįskite.

Visi sektoriai. Tai nepriklauso nuo sektoriaus, tai priklauso nuo IT, saugumo spragų, duomenų valdymo politikos. Finansų sektorius labiausiai. Pagal RRT tyrimų statistiką www.cert.lt, dauguma saugumo incidentų susiję su finansine kibernetinių nusikaltėlių motyvacija.

5. Ar, Jūsų nuomone, pakanka teisės normų ir teisinio reguliavimo tinkamai sureguliuoti TVEE? Jei manote, kad nepakanka, tai kokių teisės normų trūksta?

Trūksta sistemingo teisinio reguliavimo visoje kibernetinio saugumo srityje, tame tarpe ir TVEE. Pavyzdžiui, situacija pasikeitus priėmus atskirą įstatymą http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=2883 04&p_query=&p_tr2=

6. Ar Lietuvoje numatyta atsakomybė už TVEE? Jei taip, tai kokia?

BK manau geriau pakomentuotų ir problemas identifikuotų policija.

7. Ar manote, kad TVEE reikėtų kriminalizuoti kaip savarankišką nusikalstamą veiką? Kodėl?

Taip. Dėl augančios žalos ir masto.

8. Ar galiojančios teisės normos, reguliuojančios santykius, susijusius su TVEE, taikomos tinkamai?

Taip, bet pačios teisinės normos yra labai ribotos ir turi būti tobulinamos

9. Kokios problemos kyla dėl TVEE tyrimo?

Žmogiškųjų išteklių trūkumas, nepakankamas duomenų pateikimas RRT

10. Ar pakankamai taikoma savireguliacinių TVEE sumažinimo ir (arba) išvengimo priemonių? Kokios savireguliacinės priemonės galėtų sumažinti TVEE?

Nepakankamai. Duomenų valdytojų atsakingesnis požiūris į IT saumą ir platesnis saugumo standartų taikymas yra būtinas. Deja savireguliacijos principai kibernetinio saugumo srityje yra neefektyvūs. Reikalingas didesnis reguliavimas kas ir turėtų įvykti ES direktyvų pagalba.

11. Ar, Jūsų nuomone, valstybių tarpinstitucinis bendradarbiavimas yra pakankamas ir tinkamas? Jei ne, nurodykite, ko trūksta.

Pakankamas

12. Ar, Jūsų nuomone, bendradarbiavimas tarp valstybės ir privataus sektoriaus yra tinkamas? Jei ne, nurodykite, ko trūksta.

Pakankamas, bet galėtų būti platesnis

13. Ar elektroninio verslo taikomos priemonės apsaugo nuo TVEE? Kokios priemonės yra pakankamos ir kokios neturėtų būti taikomos?

Priemonių išties yra daug, tiek organizacinių tiek techninių. Nuo jų taikymo masto priklauso apsauga nuo TVEE. Deja taupymas, nežinojimas, rizikų nuvertinimas įtakoja tam tikrus kompromisus dėl ko nukenčia saugumas.

14. Ar elektroninio verslo naudojamos asmens identifikavimo priemonės turėtų būti privalomai reguliuojamos teisės normomis? Argumentuokite.

Taip, bet neabsoliučiai. Reguliavimas reikalingas iki tam tikro lygio. Šiuo metu RRT vykdo e. parašo priežiūrą, kurio reglamentavimas turi gilias šaknis ir vis dar tobulinamas. Praktika yra,galima ja pasiremti taikant nuo aukšto lygio tapatybės identifikavimo (t.y. e. parašas) vertikaliai žemyn.

15. Kokias TVEE prevencijos priemones galėtumėte pasiūlyti?

Visų pirma informavimas www.esaugumas.lt

Darius Štitilis, Paulius Pakutinskas, Marius Laurinaitis, Inga Dauparaitė

Ta-113 TAPATYBĖS VAGYSTĖ ELEKTRONINĖJE ERDVĖJE: SOCIALINIAI, ELEKTRONINIO VERSLO IR TEISINIO REGULIAVIMO ASPEKTAI. Monografija. – Vilnius: Mykolo Romerio universitetas, 2011. 508 p.

ISBN 978-9955-19-374-6

Monografijoje autoriai išsamiai nagrinėja tapatybės vagystę elektroninėje erdvėje kaip naujo tipo pavojingą veiką, jos požymius ir keliamą grėsmę visuomeniniams santykiams (t.y. įvertina teisinio reguliavimo pakankamumą, įskaitant teisinės atsakomybės už šią veiką aspektą) bei galimas prevencijos priemones. Monografijoje apžvelgiama tapatybės vagystė elektroninėje erdvėje kaip socialinis-teisinis reiškinys, pateikiamos šio reiškinio vystymosi tendencijos; aptariami tapatybės vagystės elektroninėje erdvėje atlikimo būdai, jų specifika ir šios veikos padariniai. Monografijoje taip pat nagrinėjami teisinio reguliavimo, įskaitant teisinės atsakomybės, susijusios su tapatybės vagyste elektroninėje erdvėje, aspektai; pateikiamos rekomendacijos dėl teisinio reguliavimo tobulinimo ir tapatybės vagystės elektroninėje erdvėje kriminalizavimo; tiriami ir pateikiami tapatybės vagystės elektroninėje erdvėje prevencijos priemonės ir būdai.

Monografija skirta visiems, kas domisi ne tik elektroninės erdvės teikiamais privalumais, bet ir joje vykdomomis pavojingomis veikomis, susijusiomis su neteisėtu asmens duomenų ir tapatybės panaudojimu, bei tokių veikų prevencija.

UDK 342.7

Darius Štitilis, Paulius Pakutinskas, Marius Laurinaitis, Inga Dauparaitė

TAPATYBĖS VAGYSTĖ ELEKTRONINĖJE ERDVĖJE:
SOCIALINIAI, ELEKTRONINIO VERSLO IR TEISINIO REGULIAVIMO ASPEKTAI

Kolektyvinė mokslo monografija

Redagavo *Nijolė Žuvininkaitė*
Viršelio dailininkė *Dovilė Petrauskienė*
Maketavo *Birutė Bilotienė*

SL 585. 2011 12 01. 27,48 leidyb. apsk. l.
Tiražas 100 egz. Užsakymas 14 523
Išleido Mykolo Romerio universitetas
Ateities g. 20, Vilnius
Puslapis internete www.mruni.eu
El. paštas leidyba@mruni.eu
Parengė spaudai ir atspausdino UAB „Baltijos kopija“
Kareivių g. 13B, Vilnius
Puslapis internete www.kopija.lt
El. paštas info@kopija.lt