ISSN 2029–2236 (print)
ISSN 2029–2244 (online)
SOCIALINIŲ MOKSLŲ STUDIJOS
SOCIETAL STUDIES
2011, 3(1), p. 153–171.

TAPATYBĖS VAGYSTĖS ELEKTRONINĖJE ERDVĖJE KRIMINALIZAVIMAS: LYGINAMIEJI ASPEKTAI*

Darius Štitilis, Paulius Pakutinskas, Inga Dauparaitė

Mykolo Romerio universiteto Socialinės informatikos fakulteto
Elektroninio verslo katedra
Ateities g. 20, LT-08303 Vilnius, Lietuva
Telefonas (+370 5) 2714 572
Elektroninis paštas stitilis@mruni.eu

Marius Laurinaitis

Mykolo Romerio universiteto Ekonomikos ir finansų valdymo fakulteto
Bankininkystės ir investicijų katedra
Ateities g. 20, LT-08303 Vilnius, Lietuva
Telefonas (+370 5) 2714 550
Elektroninis paštas laurinaitis@mruni.eu

Pateikta 2010 m. gruodžio 21 d., parengta spausdinti 2011 m. vasario 28 d.

Anotacija. *Straipsnyje nagrinėjama tapatybės vagystės elektroninėje erdvėje kriminalizavimo būklė pasirinktose užsienio valstybėse, nustatant atitinkamų baudžiamųjų normų dispozicijas, įskaitant sankcijas. Analizuojamos pasirinktų aštuonių užsienio valstybių (Jungtinių Amerikos Valstijų, Jungtinės Karalystės, Nigerijos, Prancūzijos, Suomijos, Estijos, Rusijos, Kinijos) ir Lietuvos baudžiamųjų įstatymų teisės normos, nagrinėjant tapatybės vagystės kriminalizavimo būklę lyginamuoju aspektu.*

Tapatybės vagystės elektroninėje erdvėje kriminalizavimo būklė pasirinktose užsienio valstybėse analizuojama remiantis trijų stadijų tapatybės vagystės elektroninėje erdvėje kriminalizavimo modeliu. Analizuojama, kaip pasirinktose valstybėse kriminalizuotos atitinkamos modelio stadijos, apibendrinamos už pavojingas veikas nustatytų sankcijų rūšys ir dydžiai.

Reikšminiai žodžiai: *tapatybės vagystė elektroninėje erdvėje, kriminalizavimas.*

* Straipsnis paskelbtas pagal projektą, kurį finansavo Lietuvos mokslo taryba (angl. Research Council of Lithuania). Projekto finansavimo sutarties Nr. MIP-17/2010.

Įvadas

Temos aktualumas: asmens tapatybės vagystė – elektroninėje erdvėje santykinai nauja pavojinga ir žalinga asmeniui bei visuomenei veika. Dėl šios priežasties pastaruoju metu mokslinėse diskusijos keliamas tapatybės vagystės elektroninėje erdvėje tinkamo teisinio įvertinimo ir kriminalizavimo klausimas. Nacionalinės baudžiamosios teisės skirtingai vertina šią veiką, todėl labai svarbu išanalizuoti tapatybės vagystės elektroninėje erdvėje kriminalizavimą ir įvertinti esamą užsienio valstybių patirtį.

Mokslinio straipsnio tikslas – išnagrinėti tapatybės vagystės kriminalizavimo būklę užsienio valstybėse (nustatant atitinkamų baudžiamųjų normų dispozicijas, įskaitant sankcijas), kad vėlesniuose tyrimuose būtų galima įvertinti atitinkamų baudžiamųjų normų efektyvumą.

Tyrimo objektas: tapatybės vagystė elektroninėje erdvėje, jos kriminalizavimas.

Tyrimo metodai: pagrindinis tyrimas atliekamas taikant lyginamąjį metodą (siekiama nustatyti tiriamo objekto, t. y. pasirinktų užsienio valstybių įstatymų baudžiamųjų normų, nustatančių baudžiamąją atsakomybę už tapatybės vagystę elektroninėje erdvėje, panašumus ir skirtumus), taip pat taikyti loginis, sisteminis, analizės, statistinis ir kiti metodai. Tyrimo pagrindas – įvairių užsienio valstybių teisės norminiai aktai (įskaitant baudžiamuosius įstatymus), mokslo literatūra, tarptautinių organizacijų ataskaitų medžiaga, tarptautiniai ir Lietuvos Respublikos norminiai aktai, statistinė informacija ir kiti šaltiniai.

Rezultatai: laukiami rezultatai – tapatybės vagystės elektroninėje erdvėje kriminalizavimo užsienio valstybėse būklės analizė lyginamuoju aspektu. Autoriai siekia nustatyti, kokios tapatybės vagystės elektroninėje erdvėje stadijos (ir atitinkami šių stadijų elementai) kriminalizuotos pasirinktų užsienio valstybių baudžiamuosiuose įstatymuose, kokios atitinkamų baudžiamųjų normų dispozicijos ir sankcijos.

Tyrimo rezultatai naudingi įstatymo leidėjui, o realizavus tyrimo siūlymus teisės norminiuose aktuose, ir teisėsaugos institucijoms, kovojančioms su nusikaltimais elektroninėje erdvėje, bei visuomenei apsisaugant nuo žalingų ir pavojingų veikų. Vadovaujantis išanalizuotais kitų valstybių norminiais aktais ir geriausią praktiką perkėlus į nacionalinius norminius aktus, tyrimo rezultatai gali būti pritaikomi praktikoje, teisėsaugos institucijoms tiriant elektroninius nusikaltimus ir sprendžiant padarytų pavojingų veikų elektroninėje erdvėje baudžiamojo-teisinio vertinimo problemas.

Originalumas / vertingumas, taip pat ištirtumas, naujumas: tiriama tema Lietuvos teisės moksle nenagrinėta, pasauliniame teisės moksle dėl tapatybės vagystės elektroninėje erdvėje vyksta tik pradinės diskusijos (Rees, M.; Cuganesan, S.; Lacey, D. ir kt.), o šios pavojingos veikos kriminalizavimo klausimas keliamas tik vienu aspektu: ar ši veika kriminalizuotina, ar ne (Gercke, M.). Vis dėlto paminėtina, kad kol kas tapatybės vagystė elektroninėje erdvėje kaip socialinis-teisinis reiškinys daugiausia analizuojama teisinėse-ekonominėse studijose, bet labai menkai – atskirų mokslininkų darbuose.

Tyrimo naujumas pasireiškia tuo, jog pirmą kartą lyginamuoju aspektu analizuojamas tapatybės vagystės elektroninėje erdvėje kriminalizavimas, aptariant kriminalizavimo situaciją ir Lietuvoje. Vadovaudamiesi atliktu tyrimu autoriai kviečia į mokslinę

diskusiją dėl tapatybės vagystės elektroninėje erdvėje kaip savarankiškos pavojingos veikos kriminalizavimo, įskaitant kriminalizavimą Lietuvos Respublikos baudžiamajame kodekse.

1. Tapatybės vagystės elektroninėje erdvėje kriminalizavimo prielaidos

Asmens tapatybės vagystė elektroninėje erdvėje yra santykinai naujas socialinis-teisinis reiškinys, susijęs su vartotojų teisių, informacijos saugumo, privatumo, taisyklių, reglamentuojančių nepageidaujamos informacijos gavimą, ir kitais pažeidimais.

Globalus elektroninės erdvės pobūdis ir specifinės jos savybės leidžia teisės pažeidėjams veikti gana saugioje aplinkoje, nukreipti savo veiksmus bet kuria linkme ir veikti bet kurioje vietoje, veikas atlikti labai plačiu mastu, visiškai nepaisant valstybių sienų ir jurisdikcijos. Todėl ir tapatybės vagystė elektroninėje erdvėje yra globali problema. Mokslinėje literatūroje nurodoma, jog tapatybės vagystės elektroninėje erdvėje pasekmės gali apimti daugelį visuomenės aspektų, nuo ekonomikos iki nacionalinio saugumo[1].

Pastaruoju metu pasauliniu lygiu vyksta diskusijos, ar ši pavojinga veika turėtų būti kriminalizuota ir ar tokios veikos sudėties įtraukimas į valstybių baudžiamuosius įstatymus padėtų efektyviau kovoti su šiuo reiškiniu. Išsiskiria dvi konfrontuojančios pozicijos: vieni teigia, jog tapatybės vagystė turėtų būti kvalifikuojama kaip atskira, savo sudėtį turinti nusikalstama veika[2], t. y. siūlo šią veiką kriminalizuoti, argumentuodami, jog tais atvejais, kai užsienio valstybė neturi įstatymų, kriminalizuojančių tapatybės vagystę elektroninėje erdvėje kaip atskirą veiką, varžomos informaciją renkančios valstybės galimybės rinkti tapatybės vagystės elektroninėje erdvėje įrodymus atitinkamoje užsienio valstybėje. Teisėsaugos institucijoms tokiu atveju nėra suteikiama pakankamai įgaliojimų veiksmingai kovoti su tokio pobūdžio veikomis, apsunkinamas tokių veikų susekimas, tyrimas ir baudžiamasis persekiojimas nacionaliniu bei tarptautiniu lygiu. Tinkamai neįvertinus tapatybės vagystės pasyviai laukiama kitų dažnai sudėtingai ištiriamų tarptautinių nusikaltimų pasekmių ir tik tuomet pradedamos tirti kriminalizuotos veikos. Šios pozicijos oponentai tapatybės vagystę traktuoja kaip priemonę teisės pažeidimams ir (ar) nusikalstamoms veikoms atlikti ir teigia, jog ši veika patenka į jau kriminalizuotas veikas reglamentuojančių straipsnių veikimo sritį, todėl tapatybės vagystę elektroninėje erdvėje kriminalizuoti kaip savarankišką veiką nebūtina.

Todėl autoriai mano, jog būtinas tapatybės vagystės elektroninėje erdvėje kriminalizavimo būklės pasirinktose užsienio valstybėse tyrimas. Šis tyrimas galėtų būti dviejų etapų: pirmame etape galėtų būti nustatoma kriminalizavimo būklė, o antrame – tiriamas atitinkamų baudžiamųjų normų efektyvumas.

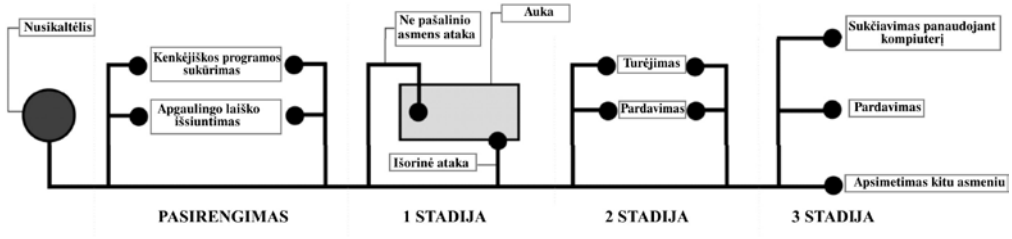
---

1 Hoffman, S. K. *Identity Theft: A Reference Handbook*. Santa Barbara, California, 2010, p. 1

2 Štitilis, D.; Laurinaitis, M. Tapatybės vagystė elektroninėje erdvėje. *Informacijos mokslai.* 2009, 50: 244–245.

Šiame straipsnyje tyrimas sutelktas į pirmąjį etapą (dėl antrojo etapo autoriai ketina atlikti papildomus tyrimus ir rezultatus paskelbti kituose savo moksliniuose darbuose) ir analizuojamos pasirinktų aštuonių užsienio valstybių (Jungtinių Amerikos Valstijų, Jungtinės Karalystės, Nigerijos, Prancūzijos, Suomijos, Estijos, Rusijos, Kinijos ir Lietuvos) baudžiamųjų įstatymų teisės normos, nagrinėjant tapatybės vagystės kriminalizavimo būklę lyginamuoju aspektu.

Mokslinėje literatūroje dažniausiai skiriamos trys tapatybės vagystės stadijos: pirma stadija – su tapatybe susijusios informacijos gavimas, antra stadija – sąveika su tapatybe susijusia informacija, trečia stadija – su tapatybe susijusios informacijos panaudojimas siekiant padaryti nusikaltimą[3].



1 pav. Tapatybės vagystės trijų stadijų modelis

Šaltinis: Gercke Marco. Internet-related identity thef. Project on Cybercrime, 2007[4].

Kai kurie autoriai laikosi pozicijos, jog yra tik dvi tapatybės vagystės stadijos: pirma stadija – su tapatybe susijusios informacijos gavimas, antra stadija – neteisėtas su tapatybe susijusios informacijos panaudojimas[5], tačiau šiame straipsnyje bus laikomasi naujausioje mokslinėje literatūroje siūlomo tapatybės vagystės skirstymo į tris stadijas, o nagrinėjant užsienio valstybių baudžiamuosius įstatymus bus siekiama nustatyti, ar šiuose įstatymuose yra įtvirtinta tapatybės vagystės, kaip savarankiškos nusikalstamos veikos, sudėtis, taip pat ar yra kriminalizuotos atskiros tapatybės vagystės stadijos ir jų elementai bei kokios sankcijos numatomos už tapatybės vagystę ar atskirus jos elementus.

2. Tapatybės vagystės elektroninėje erdvėje kriminalizavimas užsienio valstybėse

Toliau išsamiai bus pristatomos dvi pasirinktos valstybės: JAV ir Nigerija. JAV pasirinkta dėl to, jog šioje valstybėje, kaip parodė tyrimas, kriminalizuotos visos tapatybės vagystės stadijos, be to, JAV kovai su elektroniniais nusikaltimais skiria labai didelį

3 Gercke, M. Internet-related identity thef. *Project on Cybercrime* [Interaktyvus]. 2007, p. 17−20 [žiūrėta 2010-11-07]. <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>.

4 *Ibid*.

5 Rannenberg, K.; Royer, D.; Deuker, A. *The Future of Identity in the Information Society: Challenges and Opportunities*. Berlin: Springer, 2009, p. 321.

dėmesį, todėl išsamus šios valstybės gerosios praktikos pristatymas labai naudingas. Nigerija pasirinkta dėl to, jog šios šalies baudžiamajame kodekse yra atskiras skirsnis, numatantis atsakomybę už apsimetimą kitu asmeniu. Pateikiama apibendrinta bei pagrindinius kriminalizavimo aspektus atskleidžianti ir kitų analizuotų valstybių informacija – ji irgi turėtų būti naudinga. Detalesnes kitų valstybių analizes autoriai pateiks kituose savo darbuose.

2.1. Tapatybės vagystės elektroninėje erdvėje kriminalizavimas Jungtinėse Amerikos Valstijose

Jungtinės Amerikos Valstijos baudžiamosios teisės normų, nustatančių atsakomybę už tapatybės nusikaltimus, analizei buvo pasirinktos dėl to, jog JAV pagal nusikaltėlių, veikiančių elektroninėje erdvėje, skaičių užima antrą vietą pasaulyje[6], turi didžiulę patirtį kovojant su elektroniniais nusikaltimais, yra viena iš Konvencijos dėl elektroninių nusikaltimų[7] iniciatorių (Konvenciją dėl elektroninių nusikaltimų ratifikavo 2006 m. rugsėjo 29 d., šalyje ji 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, EBPO[8] 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 pirmą kartą buvo kodifikuoti visi federaliniai įstatymai. Įstatymai, reglamentuojantys baudžiamosios teisės santykius, buvo įtraukti į JAV įstatymų sąvado 18 **s**kirsnį „Nusikaltimai ir baudžiamasis procesas“.

JAV įstatymų sąvado 18 skirsnio 1 dalies 47 skyrius įtvirtina nusikaltimų, susijusių su sukčiavimu ir melagingais pareiškimais, sudėtis. Iš šio skyriaus detaliau reikėtų paanalizuoti keletą veikų, kurios susijusios su tapatybės vagystės atskirų stadijų kriminalizavimu. Pavyzdžiui, 1002 straipsnyje kriminalizuotas suklastotų dokumentų[9] 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[10], baudžiamas laisvės atėmimu iki 5 metų.

---

6 Review 2005 of the Data Protection Ombudsman [interaktyvus]. [žiūrėta 2010-11-07]. <www.tietosuoja.fi/uploads/q0vw1ft5.rtf>.

7 Convention on Cybercrime [interaktyvus]. Budapest, 2001 [žiūrėta 2010-11-07]. <http://conventions.coe.int>.

8 Ekonominio bendradarbiavimo ir plėtros organizacija [interaktyvus]. [žiūrėta 2010-11-07]. <http://www.oecd.org>.

9 Daugelyje JAV įstatymų (Elektroninio parašo ir elektroninio autentifikavimo įstatymas, Elektroninių sandorių įstatymas, Elektroninių parašų ir elektroninės komercijos įstatymas ir kt.) elektroninei informacija suteikiama teisinė vertė, todėl „dokumento“ kategorija taip pat apima ir elektroninius dokumentus.

10 United States Code („U. S. C“) [Interaktyvus], Title 18, Part I, Chapter 47, Section 1002. [žiūrėta 2010-11-07]. <http://www.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00001028----000-.html>.

1028 straipsnis 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 pavogta arba neteisėtai pagaminta; 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[11] (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 padaryti 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[12]. Bausmė, numatoma už tokį nusikaltimą, yra laisvės atėmimas iki penkerių metų, o jei nusikaltimas padarytas sunkinančiomis aplinkybėmis[13] – laisvės atėmimas iki penkiolikos metų.

1030 straipsnis numato atsakomybę už sukčiavimą, naudojant kompiuterį. Pavyzdžiui, minėto straipsnio 2 dalyje numatyta baudžiamoji atsakomybė tam, kas naudojasi kompiuteriu, neturėdamas prisijungimo teisių arba viršydamas suteiktas prisijungimo teises, ir taip 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[14]. Jei nusikalstama veika buvo

---

11 Identity Theft and Assumption Deterrence Act [interaktyvus]. 1998 [žiūrėta 2010-11-07]. <http://www.ftc.gov/os/statutes/itada/itadact.htm>

12 United States Code („U. S. C“), *op. cit.,* Title 18, Part I, Chapter 47, Section 1028 (a) (7).

13 Sunkinančios aplinkybės numatytos 2004 m. Bausmės už tapatybės vagystę padidinimo akte (angl. *Identity Theft Enhancement Penalty Act*) [interaktyvus]. [žiūrėta 2010-11-07]. <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ275.108.pdf>.

14 United States Code („U. S. C“), *supra* note 10, Title 18, Part I, Chapter 47, Section 1030 (2).

atlikta siekiant komercinės naudos ar turint asmeninio finansinio pasipelnymo tikslą arba tokia nusikalstama veika buvo padaryta siekiant palengvinti padaryti nusikaltimą ar deliktinį pažeidimą, kuris laikomas Konstitucijos, Federacijos įstatymo ar bet kurios valstijos įstatymo pažeidimu, arba kai gautos informacijos vertė viršija 5 000 dolerių, baudžiama laisvės atėmimu iki 5 metų. 4 dalis 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 kompiuterio naudojimo vertė sudaro ne daugiau kaip 5 000 dolerių per 1 metus. Už šį nusikaltimą baudžiama laisvės atėmimu iki 5 metų.

1037 straipsnyje kriminalizuotas sukčiavimas naudojant elektroninį paštą. Pavyzdžiui, pagal šio straipsnio 4 dalį baudžiamojon atsakomybėn bus patrauktas tas, kas, naudodamas informaciją, 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[15]. Už tokį nusikaltimą baudžiama laisvės atėmimu iki 1 metų, o jei buvo suklastota 20 ir daugiau pašto dėžučių ar vartotojų registracijų arba buvo suklastota 10 ir daugiau domenų vardų registracijų – laisvės atėmimas iki 3 metų, o jeigu buvo siekiama padaryti 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 padaryti nusikaltimą – yra kriminalizuotos. 1 stadija patenka į JAV įstatymų sąvado 18 skirsnio 1 dalies 47 skyriaus 1030 straipsnio, reglamentuojančio sukčiavimą, naudojant kompiuterį, veikimo sritį, 2 stadija patenka į 1002 straipsnio (suklastotų dokumentų turėjimas) bei 1028 straipsnio, numatančio baudžiamąją atsakomybę už sukčiavimą, susijusį su tapatybės nustatymo dokumentais, autentifikavimo priemonėmis ir informacija (perdavimas, turėjimas, prekyba) veikimo sritį, o 3 tapatybės vagystės stadija kriminalizuota minėtame 1028 straipsnyje (neteisėtas dokumentų, autentifikavimo priemonių ir informacijos gaminimas, klastojimas) bei 1037 straipsnyje, kuriame numatoma baudžiamoji atsakomybė už sukčiavimą naudojant elektroninį paštą. Pažymėtina, jog 2 ir 3 tapatybės vagystės stadijos kriminalizuotos 1028 straipsnio (a) dalies (7) punkte, įtvirtinančiame tapatybės vagystės, kaip savarankiškos nusikalstamos veikos, sudėtį.

2.1. Tapatybės vagystės elektroninėje erdvėje kriminalizavimas Nigerijoje

Nigerijos baudžiamojo įstatymo normų, kriminalizuojančių tapatybės vagystės elementus, analizė pasirinkta dėl to, kad Nigerija laikoma falsifikuotų internetinių tinklala-

15 United States Code („U. S. C“), *supra* note 10, Title 18, Part I, Chapter 47, Section 1037 (4).

pių pradininke (tapatybės vagystės grėsmė, kurios šaltinis – Nigerija, identifikuota jau 1984 m.[16]), 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 padarymo būdai vis sudėtingėja, ir Nigerijos rūpesčiu tapo nusikaltėliai, kurie pagrobia kreditinių ir debetinių banko kortelių PIN kodus, pasinaudodami tokiais metodais kaip falsifikuoti internetiniai tinklalapiai, 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 tikroji svetainė, o asmuo gauna elektroninį paštą, kur teigiama, jog 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[17], todėl šalis šiuo metu bendradarbiauja su JAV vyriausybe, mėgindama gelbėti savo reputaciją ir atsikratyti įvaizdžio, kad ji yra elektroninių nusikaltimų ir liūdnai pagarsėjusių falsifikuotų internetinių tinklalapių ašis bei kovoti su elektroniniais nusikaltimais. Šalies įvaizdžiui didžiulę neigiamą įtaką padarė elektroniniai laiškai su nuorodomis į falsifikuotus internetinius tinklalapius; šie laiškai, kaip juose melagingai buvo teigiama, buvo platinami Nigerijos institucijų.

Iš elektroninių nusikaltimų padarymo būdų Nigerijoje labiausiai paplitę būtent apgaulingi elektroniniai laiškai, kurie Nigerijoje ir visame pasaulyje žinomi kaip „apgaulė 419“. Skaičius 419 yra nuoroda į Nigerijos baudžiamojo kodekso straipsnį, 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[18] 38 skyrius numato baudžiamąją atsakomybę už nuosavybės įgijimą apgaulės būdu, sukčiavimą. 419 straipsnis numato, jog 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 nairų[19] – laisvės atėmimu iki septynerių metų.

---

16 Biegelman, M. T. *Identity Theft Handbook: Detection, Prevention and Security*. John Wiley & Sons, Inc., 2010, p. 58.

17 Internet Crime Report [interaktyvus]. Internet Crime Complaint Center, 2009 [žiūrėta 2010-11-07]. <http://www.ic3.gov/media/annualreport/2009_ic3report.pdf>.

18 Nigerijos baudžiamasis kodeksas [interaktyvus]. [žiūrėta 2010-11-06]. <http://www.nigeria-law.org/Criminal%20Code%20Act-Tables.htm>.

19 Naira (NGN) – Nigerijos nacionalinis piniginis vienetas. 1 LTL ~ 61 NGN.

421 straipsnis numato, jog 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 straipsnis įtvirtina, kad asmuo, kuris sulaiko paštą, turėdamas tikslą apieškoti ar pagrobti pašto korespondencijos siuntą, laikomas padaręs sunkų nusikaltimą ir baudžiamas laisvės atėmimu iki gyvos galvos[20]. 162 straipsnyje 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 straipsnis 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 straipsnyje 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 padaro nusikalstamą veiką, kad įgytų tokią nuosavybę ar pareigas, baudžiamas laisvės atėmimu iki 14 metų.

486 straipsnis numato baudžiamąją atsakomybę asmeniui, kuris išleidžia į apyvartą bet kokį dokumentą[21], kurį kitam asmeniui išdavė teisėta institucija, kai toks dokumentas patvirtina asmens įgytą kvalifikaciją, einamas pareigas, teisę užsiimti tam tikra profesija, prekyba, verslu ar turimas teises arba privilegijas, arba laipsnį ar padėtį, ir apgaulės būdu save pristato tuo asmeniu, kurio vardu išduotas dokumentas, laikomas padaręs tokį patį nusikaltimą[22] 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,

20 Nigerijos baudžiamasis kodeksas, *supra* note 18, 161 str.

21 Pagal Nigerijos baudžiamojo kodekso 463 str. įtvirtintas „dokumento“ bei „rašto“ sąvokas, „dokumento“ kategorija apima ir elektroninius dokumentus. Nors minėtose sąvokose elektroniniai dokumentai aiškiai nėra išskirti, aiškinant sąvokas galima prieiti prie išvados, jog elektroniniai dokumentai patenka į „dokumento“ kategoriją

22 Nigerijos baudžiamasis kodeksas, *supra* note 18, 486 str.

perdavimą ar paskolinimą kitam asmeniui, kad šis galėtų apsimesti tuo asmeniu, kuriam toks dokumentas buvo išduotas (487 str.).

488 straipsnyje įtvirtinta baudžiamojo nusižengimo sudėtis: asmuo, kuris turėdamas tikslą gauti darbą, išleidžia į apyvartą tokį dokumentą, kaip kito asmens rekomendacija ar charakteristika[23], laikomas padaręs baudžiamąjį nusižengimą ir baudžiamas laisvės atėmimu iki 1 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, jog 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 1 tapatybės vagystės stadiją – su tapatybe susijusios informacijos gavimą – baudžiamoji atsakomybė kyla pagal 161 ir 162 straipsnius, reglamentuojančius nusikalstamas veikas, susijusias su pašto ir telekomunikacijų paslaugomis, ar pagal 419 ir 421 straipsnius, numatančius baudžiamąją atsakomybę už nuosavybės įgijimą apgaulės būdu, sukčiavimą. Atsakomybė už antrą stadiją – sąveiką su tapatybe susijusia informacija (pardavimą, perdavimą, paskolinimą) – numatyta 487 straipsnyje, tačiau antros stadijos elementas – su tapatybe susijusios informacijos turėjimas – pagal Nigerijos baudžiamąjį kodeksą baudžiamosios atsakomybės neužtraukia. Trečia tapatybės vagystės stadija patenka į Nigerijos baudžiamojo kodekso 44 skyriaus normų (pvz., 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 ir 421 straipsnių, kriminalizuojančių nuosavybės įgijimą apgaulės būdu, sukčiavimą, veikimo sritį.

2.3. Tapatybės vagystės elektroninėje erdvėje kriminalizavimas tirtose užsienio valstybėse – pagrindiniai apibendrinantys aspektai

Tapatybės vagystės elektroninėje erdvėje kriminalizavimo tyrimo rezultatai pateikiami 1 lentelėje. Tapatybės vagystės elektroninėje erdvėje kriminalizavimo būklė aprašoma remiantis pateiktu trijų stadijų modeliu.

23 Nigerijos baudžiamasis kodeksas, *supra* note 18, 488 str.

1 lentelė. Tapatybės vagystės elektroninėje erdvėje kriminalizavimas pasirinktose užsienio valstybėse

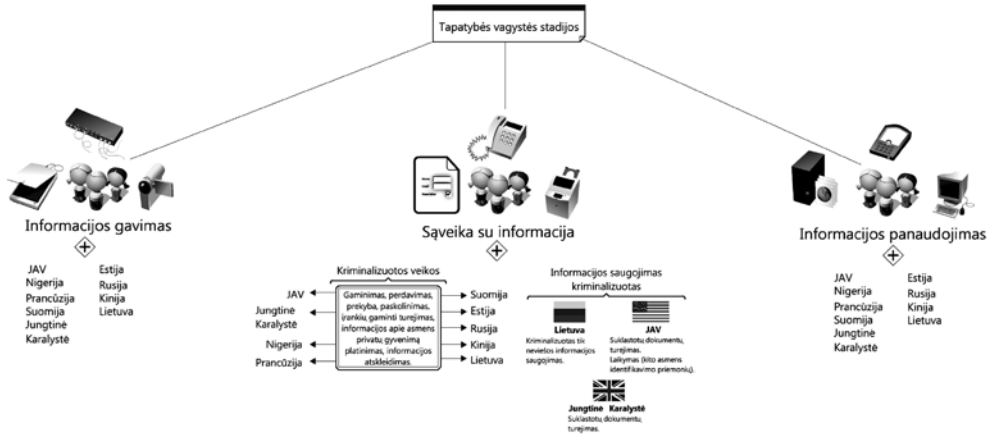
Šalis / Ar yra įtvirtinta tapatybės vagystės kaip savarankiškos nusikalstamos eikos sudėtis?	**Informacijos gavimas**	**Sąveika su informacija**	**Informacijos panaudojimas**
JAV/ Taip	Sukčiavimas naudojant kompiuterį (naudotis kompiuteriu neturint teisių, viršyti suteiktas teises, gauti informaciją)	• Suklastotų dokumentų turėjimas, siekiant suklaidinti • Sukčiavimas, susijęs su tapatybės nustatymo dokumentais, autentifikavimo priemonėmis ir informacija (gaminimas, turėjimas, perdavimas, įrankių gaminti turėjimas, prekyba) • **Tyčia perdavimas, laikymas, naudojimas, neturint tam teisės, kito asmens identifikavimo priemones, turint tikslą padaryti bet kokią neteisėtą veiką** • Neteisėtas dokumentų, autentifikavimo priemonių ir informacijos gaminimas, klastojimas • 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, kompiuterių sistemų, tinklų naudojimas pašalinant kodus, slaptažodžius ar kitas apsaugos priemones	Jautrių 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 kitokią naudą 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 instrumentų 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 matome iš lentelės, tik vienoje valstybėje (t. y. JAV) yra įtvirtinta savarankiška tapatybės vagystės elektroninėje erdvėje sudėtis. Tik trijose valstybėse kriminalizuotas

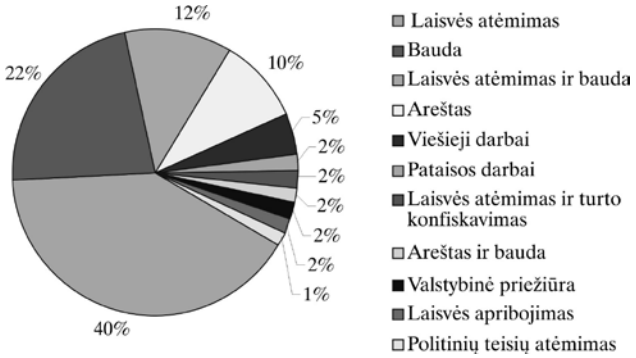
(skirtinga apimtimi) vienas iš antros stadijos elementų – neteisėtas tapatybės informacijos turėjimas, turint tikslą padaryti nusikaltimą. Apibendrinant tapatybės vagystės elektroninėje erdvėje stadijų kriminalizavimą tirtose valstybėse galima pavaizduoti taip:



2 pav. Tapatybės vagystės elektroninėje erdvėje stadijų kriminalizavimas

Autorių nuomone, vieno iš antros 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 neigiamai veikia kovą su šia pavojinga veika. Nesant tinkamai nustatytos atsakomybės, gali susidaryti sąlygos tolesniam sparčiam šios pavojingos veikos plitimui.

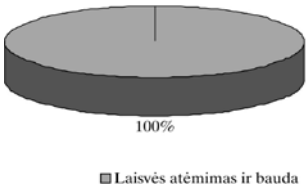
Tačiau ne vien veikos kriminalizavimo faktas svarbus tiriant tapatybės vagystę elektroninėje erdvėje ir teisinės prevencijos priemones. Atitinkamas autorių pristatomas tyrimas neapsiribojo vien tik kriminalizavimo būklės įvertinimu tirtose valstybėse. Taip pat buvo tiriamos ir sankcijos už įvairius tapatybės nusikaltimus. Toliau pateikiami sankcijų už tapatybės vagystės elektroninėje erdvėje neteisėtas veikas tyrimo rezultatai.



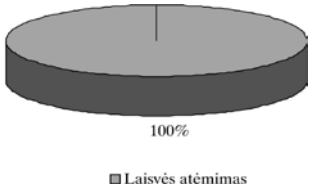
3 pav. Sankcijos už tapatybės vagystės elektroninėje erdvėje nusikaltimus

Taigi, kaip matyti iš 3 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 sankcijų įvairovės visiškai nėra. Tai Prancūzija ir JAV bei 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 kitos sankcijos svyruoja nuo 3 iki 6 metų (pvz., Prancūzijoje). Nigerijoje už tapatybės vagystės elektroninėje erdvėje elementus gali būti baudžiama laisvės atėmimu iki 14 metų.

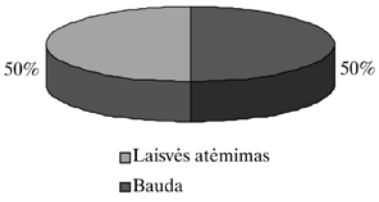


4 pav. Sankcijos už tapatybės vagystės elementus Prancūzijoje

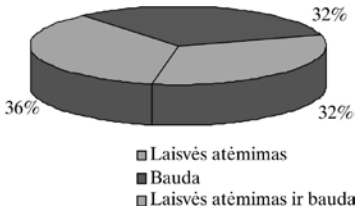


5 pav. Sankcijos už tapatybės vagystės elementus JAV ir Nigerijoje

Panaši padėtis ir Suomijoje, Estijoje bei Jungtinėje Karalystėje – čia sankcijos už tapatybės vagystės elektroninėje erdvėje nusikaltimus apsiriboja laisvės atėmimu ir bauda.

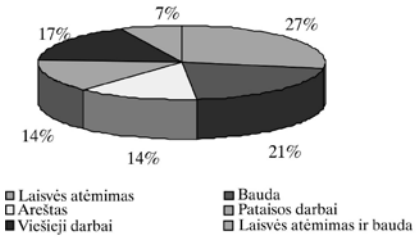


6 pav. Sankcijos už tapatybės vagystės elementus Suomijoje ir Estijoje

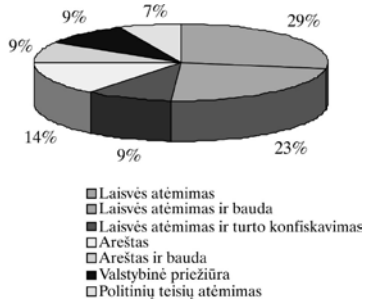


7 pav. Sankcijos už tapatybės vagystės elementus Jungtinėje Karalystėje

Tuo tarpu sankcijos už tapatybės vagystės nusikaltimus Rusijoje ir Kinijoje labai įvairios.

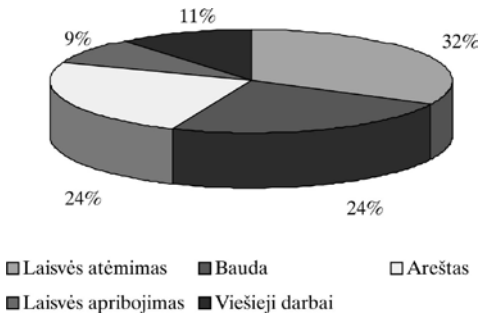


8 pav. Sankcijos už tapatybės vagystės elementus Rusijoje



9 pav. Sankcijos už tapatybės vagystės elementus Kinijoje

Bauda už atitinkamas pavojingas veikas, susijusias su tapatybės vagyste, Lietuvoje gali siekti iki 26 000 Lt, o gresiantis laisvės atėmimas už atitinkamas povojingas veikas – nuo 3 iki 6 metų.



10 pav. Sankcijos už tapatybės vagystės elementus Lietuvoje

Apibendrinant pasirinktų užsienio valstybių baudžiamuosiuose įstatymuose numatytas sankcijas už tapatybės vagystės nusikaltimus, galima pažymėti, jog sankcijos yra labai įvairios, vienos valstybės tapatybės vagystę elektroninėje erdvėje vertina kaip lengvesnę pavojingą veiką, kitos – atvirkščiai. Tai, kad valstybės numato skirtingas sankcijas ir skirtingą jų dydį, yra paskata nusikaltimus daryti tose valstybėse, kur sankcijos už tapatybės vagystę elektroninėje erdvėje yra mažesnės. Todėl įstatymų leidėjams taip pat svarbu suvienodinti sankcijas už šią pavojingą veiką elektroninėje erdvėje.

Išvados

Atlikus Jungtinių Amerikos Valstijų, Jungtinės Karalystės, Nigerijos, Prancūzijos, Suomijos, Estijos, Rusijos, Kinijos ir Lietuvos baudžiamųjų įstatymų teisės normų analizę, nustatyta, jog 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 gavimas, sąveika su tokio pobūdžio informacija bei su tapatybe susijusios informacijos panaudojimas siekiant padaryti nusikaltimą. Kitose valstybėse tapatybės vagystė laikoma kitų nusikalstamų veikų sudedamąja dalimi.

Tik trijose valstybėse kriminalizuotas (skirtinga apimtimi) vienas iš antros stadijos elementų – neteisėtas tapatybės informacijos turėjimas, turint tikslą padaryti nusikaltimą. Tokia padėtis, autorių nuomone, susidarė dėl istorinio aspekto, t. y. dėl to, jog istoriškai tapatybės vagystė elektroninėje erdvėje yra naujo tipo socialinis-teisinis reiškinys ir įstatymų leidėjai kol kas neskiria deramo dėmesio šios veikos uždraudimui.

Tapatybės vagystės elektroninėje erdvėje kaip pavojingos veikos vertinimas baudžiamosios teisės požiūriu skirtingose valstybėse skiriasi, ir tai, kad tapatybės vagystė nėra kriminalizuota kaip savarankiška nusikalstama veika, apsunkina tokių veikų susekimą, tyrimą ir baudžiamąjį persekiojimą nacionaliniu bei tarptautiniu lygiu, todėl, nepradėjus laiku tirti tapatybės vagystės ir neužkardžius šios veikos, sudaromos prielaidos

atsirasti kitiems sunkiai išaiškinamiems ir sunkiems nusikaltimas, kuriems tapatybės vagystė yra būtina arba pagalbinė sąlyga, o dalis žalingų veikų lieka net netiriamos.

Už tapatybės vagystę elektroninėje erdvėje (ar atskiras jo stadijas) 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. Sankcijų rušių bei dydžių už tapatybės vagystę elektroninėje erdvėje įvairovė taip pat turėtų neigiamai veikti šios pavojingos veikos plitimą. Įstatymų leidėjų požiūris į šią pavojingą veiką turėtų būti vienodinamas.

Literatūra

APWG Phishing Activity Trends Report for the Month of December, 2007 [interaktyvus]. [žiūrėta 2010-11-07]. <http://www.antiphishing.org/reports/apwg_report_dec_2007.pdf>.

APWG Phishing Activity Trends Report. 1st Quarter 2010 [interaktyvus]. [žiūrėta 2010-11-07]. <http://www.antiphishing.org/reports/apwg_report_Q1_2010.pdf>.

Biegelman, M. T. *Identity Theft Handbook: Detection, Prevention and Security*. John Wiley & Sons, Inc., 2010.

Computer Misuse Act 1990 [interaktyvus]. [žiūrėta 2010-11-14]. <http://www.legislation.gov.uk/ukpga/1990/18/contents>.

Convention on Cybercrime [interaktyvus]. Budapest, 2001 [žiūrėta 2010-11-07]. <http://conventions.coe.int>.

Estijos baudžiamasis kodeksas [interaktyvus]. [žiūrėta 2010-11-07]. <http://www.legislationline.org/download/action/download/id/1280/file/4d16963509db70c09d23e52cb8df.htm/preview>.

Fraud Act 2006 [interaktyvus]. [žiūrėta 2010-11-14]. <http://www.opsi.gov.uk/acts/acts2006/pdf/ukpga_20060035_en.pdf>.

Gercke M. Internet-related identity thef. *Project on Cybercrime* [interaktyvus]. 2007 [žiūrėta 2010-11-07]. <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>.

Hoffman, S. K. *Identity Theft: A Reference Handbook*. Santa Barbara, California, 2010.

Identity Cards Act 2006 [interaktyvus]. [žiūrėta 2010-11-07]. <http://www.legislation.gov.uk/ukpga/2006/15/introduction>.

Identity Theft and Assumption Deterrence Act [interaktyvus]. 1998 [žiūrėta 2010-11-07]. <http://www.ftc.gov/os/statutes/itada/itadact.htm>.

Identity Theft Enhancement Penalty Act, 2004. [žiūrėta 2010-11-07]. <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ275.108.pdf>.

Internet Crime Report [interaktyvus]. Internet Crime Complaint Center, 2009 [žiūrėta 2010-11-07]. <http://www.ic3.gov/media/annualreport/2009_ic3report.pdf>.

Kinijos baudžiamasis kodeksas [interaktyvus]. [žiūrėta 2010-11-07]. <http://www.cecc.gov/pages/newLaws/criminalLawENG.php>.

Nigerijos baudžiamasis kodeksas [interaktyvus]. [žiūrėta 2010-11-06]. <http://www.nigeria-law.org/Criminal%20Code%20 Act-Tables.htm>.

Personal Data Is Pirated From Russian Phone Files [interaktyvus]. *The New York Times*. January 23, 2003 [žiūrėta 2010-11-07]. <http://www.nytimes.com/2003/01/23/busi-

ness/personal-data-is-pirated-from-russian-phone-files.html>.

Police and Justice Act 2006 [interaktyvus]. [žiūrėta 2010-11-14]. <http://www.legislation.gov.uk/ukpga/2006/48/contents>.

Prancūzijos baudžiamasis kodeksas [interaktyvus]. [žiūrėta 2010-11-07]. <http://www.legislationline.org/documents/section/criminal-codes>.

Rannenberg, K.; Royer, D.; Deuker, A. *The Future of Identity in the Information Society: Challenges and Opportunities*. Berlin, Springer, 2009.

Review 2005 of the Data Protection Ombudsman [interaktyvus]. [žiūrėta 2010-11-07]. <www.tietosuoja.fi/uploads/q0vw1ft5.rtf>.

Rusijos Federacijos baudžiamasis kodeksas [interaktyvus]. [žiūrėta 2010-11-07]. <http://www.legislationline.org/documents/section/criminal-codes>.

Suomijos baudžiamasis kodeksas [interaktyvus]. [žiūrėta 2010-11-07]. <http://www.legislationline.org/documents/section/criminal-codes>.

Štitilis, D.; Laurinaitis, M. Tapatybės vagystė elektroninėje erdvėje. *Informacijos mokslai*. 2009, 50.

United States Code („U. S. C“) [Interaktyvus]. [žiūrėta 2010-11-07]. <http://www.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00001028----000-.html>.

CRIMINALIZATION OF ONLINE IDENTITY THEFT: COMPARATIVE ASPECTS

Darius Štitilis, Paulius Pakutinskas, Inga Dauparaitė, Marius Laurinaitis

Mykolas Romeris University, Lithuania

Summary. *The authors of the present article analyze the criminal legislation of eight foreign countries (the United States, the United Kingdom, Nigeria, France, Finland, Estonia, Russia, China) as well as Lithuania in order to discuss and compare the criminalization aspects of online identity theft. Online identity theft is a rather new phenomenon and dangerous not only to separate individuals but to the whole society. It is concerned with the violation of consumer protection rules, security and privacy and anti-spam rules, etc. Online identity theft is a global problem, and this leads to the discussions whether it should be criminalized or not.*

The analysis is focused on the Three-Phase Model of online identity theft: obtaining identity-related information (phase 1), interaction with identity-related information (phase 2) and the use of the identity-related information in relation to a criminal offence (phase 3). The authors analyze whether in the countries under investigation online identity theft is treated as a criminal act or separate phases of it are considered as constituent elements of common crimes such as unlawful access to data, fraud, forgery, etc. only.

The authors present a more comprehensive analysis of two countries—the United States and Nigeria. The choice is based on the fact that the United States has a great experience of fighting cyber crimes and, as research has shown, is the only country where online identity theft is criminalized. While the situation in Nigeria is taken for an in-depth consideration because

of its Criminal Code Act having a separate chapter in which personation is criminalized.

Also, in this article, summarized information about other analyzed countries is presented, the differences of the existing criminal legislation are described and the variety of sanctions for online identity theft phases is discussed. However, the research has shown that the penalties imposed for online identity thefts (or its separate phases) are mostly fines or imprisonment.

In this article, it is emphasized that online identity theft is not criminalized (except the United States), and this impedes the detection, investigation and prosecution of such conduct at both domestic and international levels. Therefore, the authors are going to bring online identity criminalization up for discussion on the basis of the research presented in this article.

Keywords: *online identity theft, criminalization.*

Darius Štitilis, Mykolo Romerio universiteto Socialinės informatikos fakulteto Elektroninio verslo katedros docentas. Mokslinių tyrimų kryptys: elektroninė komercija, elektroniniai nusikaltimai, asmens duomenų teisinės apsauga.

Darius Štitilis, Mykolas Romeris University, Faculty of Social Informatics, Department of Electronic Business, associate professor. Research interests: electronic commerce, cybercrime, personal data protection.

Paulius Pakutinskas, Mykolo Romerio universiteto Mokslo centro mokslo darbuotojas, socialinių mokslų daktaras (teisė). Mokslinių tyrimų kryptys: elektroninių ryšių teisė, interneto teisė, IT teisė.

Paulius Pakutinskas, Mykolas Romeris University Research Center, young researcher. Research interests: electronic communications law, internet law, IT law.

Inga Dauparaitė, Mykolo Romerio universiteto Mokslo centro jaunesnioji mokslo darbuotoja. Mokslinių tyrimų kryptis: IT teisė.

Inga Dauparaitė, Mykolas Romeris University, Faculty of Social Informatics, Information Technology Law graduate student. Research interests: IT law.

Marius Laurinaitis, Mykolo Romerio universiteto Ekonomikos ir finansų valdymo fakulteto Bankininkystės ir investicijų katedros lektorius. Mokslinių tyrimų kryptys: elektroninės mokėjimų sistemos, elektronianai pinigai, mobilūs atsiskaitymai, pinigų plovimo prevencija.

Marius Laurinaitis, Mykolas Romeris University, Faculty of Economics and Finance Management, Department of Banking and Investments, lecturer. Research interests: electronic payment system, e-money, mobile payment, money laundering prevention.