

## Tapatybės vagystė elektroninėje erdvėje

### Darius Štītis

Mykolo Romerio universiteto Socialinės informatikos fakulteto Elektroninio verslo katedros docentas, daktaras  
Mykolas Romeris University, Faculty of Social Informatics, Department of Electronic Business, Assoc. Prof., Doctor  
Ateities g. 20, LT-08303 Vilnius  
Tel. 236 75 76; faks. 278 34 82  
El. paštas: stitilis@mruni.lt  
Asmeninio tinklapio adresas: <http://stitilis.home.mruni.lt/>

### Marius Laurinaitis

Mykolo Romerio universiteto Ekonomikos ir finansų valdymo fakulteto Bankininkystės ir investicijų katedros lektorius  
Mykolas Romeris University, Faculty of Economics and Finance Management, Department of Banking and Investments, Lector  
Ateities g. 20, LT-08303 Vilnius  
Tel. (8 5) 2714571, faks. 278 34 82  
El. paštas: marius.laurinaitis@gmail.com  
Asmeninio tinklapio adresas: <http://laurinaitis.home.mruni.lt/>

*Straipsnyje analizuojama tapatybės vagystė elektroninėje erdvėje ir pagrindiniai šios pavojingos veikos požymiai. Straipsnį sudaro keturios dalys. Pirmoje dalyje analizuojamos tapatybės ir identifikavimo elektroninėje erdvėje kategorijos. Antroji dalis skirta aptarti ir susisteminti tapatybės elektroninėje erdvėje vagystės būdams ir formoms. Trečioje straipsnio dalyje pateikiama tapatybės vagystės elektroninėje erdvėje samprata. Ketvirtoji straipsnio dalis skirta tapatybės vagystės elektroninėje erdvėje, kaip atskiros veikos, kriminalizavimo aptarčiai. Straipsnyje atlikta analizė leidžia teigti, kad tapatybės vagystės elektroninėje erdvėje būdai ir formos yra labai įvairūs ir nuolat kinta, atsiranda vis naujų. Įvairiuose šaltiniuose iki šiol diskutuojama dėl tapatybės vagystės sampratos. Atlikę analizę autoriai siūlo naudoti tapatybės vagystės elektroninėje erdvėje sampratos variantą. Straipsnyje taip pat pateikiamos naujausios tapatybės vagystės elektroninėje erdvėje kriminalizavimo tendencijos.*

### Įvadas

Sparčiai auganti interneto ekonomika turi ir neigiamų padarinių. Vienas iš jų – tapatybės vagystė elektroninėje erdvėje. Dėl tapatybės vagystės elektroninėje erdvėje daroma žala paprastiems vartotojams, finansų institucijoms ir galiausiai visai ekonomikai. JAV Federalinės prekybos komisijos duomenimis, pastaraisiais metais tapatybės vagystė buvo labiausiai paplitusi iš visų sukčiavimo atvejų, o pavojingos veikos aukos tapatybės vagystę įvardijo kaip vieną iš trijų didžiausių grėsmių (Federal Trade..., 2007).

2006 metų ataskaitoje apie tapatybės vagystę taip pat nurodoma, jog 2005 metais apie 8,3 mln. JAV piliečių nukentėjo dėl tapatybės vagystės. Kitose užsienio valstybėse atlikti ty-

rimai taip pat patvirtina didelius tapatybės vagystės mastus ir jos daromą didžiulę finansinę žalą. Tapatybės vagystė dažnai netgi vadinama greičiausiai plintančia XXI amžiaus nusikalstama veika (Online Identity ..., 2008).

Tapatybės vagystės elektroninėje erdvėje grėsmė mažina pasitikėjimą elektronine komercija, sandorių internete skaičių ir sykiu lėtina interneto ekonomiką. Elektroninės erdvės saugumo aljanso ataskaitoje pažymima, kad 2005 metais apie 48 procentų vartotojų vengė internete įsigyti prekių ar paslaugų vien dėl rizikos prarasti savo finansinę informaciją (Federal Trade..., 2007).

Tapatybės vagystė elektroninėje erdvėje įgaivo naujų bruožų, palyginti su tapatybės vagyste nenaudojant šios erdvės. Dėl to reikia išsamiai išnagrinėti šią naujo tipo veiklą, jos požymius ir ke-

liamą grėsmę visuomeniniams santykiams (t. y. įvertinti veiką iš baudžiamosios teisės pozicijų).

Deja, Lietuvos moksle tapatybės vagystės elektroninėje erdvėje tema iš viso nenagrinėta, užsienyje pastebimos tik tapatybės vagystės elektroninėje erdvėje analizės apraiškos – dažniausiai įvairių ataskaitų ir studijų publikavimas. Mokslinėje literatūroje ši tema kol kas labai mažai diskutuota. Iki šiol literatūroje tapatybės vagystė elektroninėje erdvėje suvokiama labai įvairiai, pateikiamos šios veikos sampratos labai skiriasi, požymiai ir būdai nesusisteminti, o kriminalizavimo klausimu pastebimos tik pradinų diskusijų apraiškos.

Šio straipsnio tikslas – išnagrinėti tapatybės vagystę elektroninėje erdvėje, susisteminant esminius tapatybės vagystės kaip pavojingos veikos požymius. Straipsnio objektas – tapatybės vagystė elektroninėje erdvėje kaip pavojinga veika. Straipsnyje naudojamas loginis, lyginamasis, sisteminis, analizės, statistinis ir kiti metodai. Tyrimo pagrindas – įvairių užsienio valstybių mokslo literatūra, tarptautinių organizacijų ataskaitų medžiaga, tarptautiniai ir Lietuvos Respublikos norminiai aktai, statistinė informacija ir kiti šaltiniai. Straipsnyje aptariami tapatybės vagystės elektroninėje erdvėje būdai ir formos, šios pavojingos veikos samprata ir kriminalizavimas.

Tiriama tema Lietuvos teisės moksle nenagrinėta. Tyrimo naujumas pasireiškia tuo, jog pirmą kartą sistemškai analizuojama tapatybės vagystė kaip pavojinga veika, pateikiama apibendrinto pobūdžio ir susisteminta tapatybės vagystės samprata, susisteminti tapatybės vagystės elektroninėje erdvėje būdai, analizuojami šios pavojingos veikos kriminalizavimo klausimai ir keliama atskiros veikos (t. y. tapatybės vagystės elektroninėje erdvėje) įvardijimo savarankišku nusikaltimu Lietuvos Respublikos baudžiamajame kodekse problema. Remdamiesi atliktu tyrimu, autoriai siūlo tapatybės vagystę elektroninėje erdvėje kaip savarankišką pavojingą veiką kriminalizuoti Lietuvos Respublikos baudžiamajame kodekse.

## Tapatybė ir identifikavimas

Šiuolaikinė visuomenė vis labiau tampa priklausoma nuo asmeninės informacijos, skirtos

įvairiose situacijose identifikuoti asmenis. Tokia informacija gali būti naudojama prisijungti prie elektroninių banko sistemų, gauti e. valdžios paslaugas ir pan. Kaip tapatybės siejasi su identifikavimu?

Visų pirma reikia paminėti, jog tapatybė neatskirama nuo individualumo (Cuganesan, Lacey, 2003). Tapatybė gali būti nustatoma naudojant identifikatorius: biometrinius identifikatorius (pvz., pirštų atspaudai, balsas), rašytinius identifikatorius (pvz., vairuotojo pažymėjimas), finansinius identifikatorius (pvz., banko sąskaita) (Identity Crime..., 2007).

Tapatybė sietina ir su asmens duomenimis. 1981 m. Europos Tarybos konvencijoje „Dėl asmenų apsaugos, susijusios su automatizuotu asmens duomenų apdorojimu“ asmens duomenys apibrėžiami kaip bet kokia informacija, susijusi su identifikuotu ar identifikuotinu asmeniu (Convention..., 1981). Taigi bet kuri konkretų fizinį asmenį identifikuojanti informacija sudaro tapatybės elektroninėje erdvėje turinį.

Tarptautinių žodžių žodyne (Bendorienė ir kt., 2003) tapatybė sutapatinama su identitetu. Identitetas (*identitas*, kilm. *identitatis*) – tapatybė, ko nors apibrėžtumas, individualumas. Lietuvių kalbos žodynas tapatybę apibrėžia kaip objekto lygybę pačiam sau arba kitam objektui, tolygumą, vienodumą. Identifikavimas suprantamas kaip tapatybės pripažinimas, nustatymas; sutapatinimas (Naktinienė ir kt., 2005).

Taip pat būtina pabrėžti, kad tapatybė fizinėje erdvėje yra visiškai kitokia 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. Jis sistemoje turi būti unikalus. Slaptažodis – ženklų seka, žinoma tik paslaugos teikėjui ir jos vartotojui, pagal kurią paslaugos teikėjas patikrina į jį besikreipiančiojo tapatybę (Dagienė ir kt., 2008). 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.

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 (EDS sistema Lietuvoje, pasitikėjimo šalis – bankas, identifikuojantis vartotoją elektroninėje erdvėje).

Pažymėtina, kad tapatybės nusikaltimai dažnai susiję su asmens suklastotos tapatybės naudojimu. Manoma, kad suklastota tapatybė gali būti susijusi su fiziniu arba juridiniu asmeniu. Gali būti naudojama ir fiktyvi, nerealaus asmens tapatybė (Identity Crime..., 2007).

EBPO elektroninio identifikavimo rekomendacijoje identifikavimas suprantamas kaip vartotojo tapatybės nustatymas informacinėje sistemoje (OECD Recommendation..., 2007). Taigi tapatybės elektroninėje erdvėje nustatymo procesas gali būti laikomas asmens identifikavimu.

## Tapatybės vagystės būdai ir formos

Tapatybės vagystė elektroninėje erdvėje yra sudėtingas reiškinys. Dažniausiai ji įvykdoma naudojant skirtingus veiksmus (Online Identity..., 2009).

Tapatybės vagystė dažniausiai yra tokių nusikaltimų kaip nelegali imigracija, terorizmas ir šnipinėjimas, šantažas, finansinių nusikaltimų palengvinimo priemonė. Ne visais atvejais motyvas yra finansinės priežastys, tai gali būti asmens persekiojimas, troškimas būti kitu. Tačiau suklastotos tapatybės kūrimas pats savaime yra nusikalstama veika. Nusikaltimas gali prasidėti suklastojus tapatybę, kuri tampa būsimų nusikaltimų pradžia. Tapatybės vagystė neapsiriboja tik apsimetimu kitu asmeniu. Ji taip pat apima melagingos dokumentacijos naudojimą, teigiantį neegzistuojantį ryšį su teisėtomis kompanijomis, neegzistuojančiomis korporacijomis ar sukčiavimui naudojamomis organizacijomis. Suklastotos, netikros tapatybės naudojamos įkuriant teisiškai tvarkingas

kompanijas. Sukurtos netikros tapatybės – klastotės, vėliau padeda išvengti atsakomybės, kilusios dėl neteisėtus tokių kompanijų veiklos.

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

- tradicinius sukčiavimus, atliekamus fiziniame erdvėje;
- modernių technologijų sukčiavimus, atliekamus elektroninėje erdvėje.

Nagrinęjant tapatybės vagystę elektroninėje erdvėje pastebima, kad dažniausiai pasitaiko šie nusikaltimai pasitelkiant modernias technologijas (Identity Theft..., 2007):

- **Įsibrovimas** (angl. *hacking*). Dažniausiai sukčius apeidamas sistemos slaptažodžius, saugumo priemones, patenka į sistemą. Ypač stengiamasi pasinaudoti saugumo spragomis, neapsaugotais bevieliais, intraneto tinklais, taip pat ieškoma sistemų, kuriose dauguma apsaugos funkcijų yra išjungtos.
- **Šnipinėjimo programa** (angl. *spyware*). Tai programinė įranga, kuri be asmens žinios renka ir siunčia jo asmeninius duomenis nurodytu adresu. Dažniausiai pažeidinėjami privatumo lygiai. Renkami ir fiksuojami asmens naršymo įpročiai, dažnai lankomų svetainių adresai. Rinkodaros kompanijos kasmet išleidžia milijonus dolerių bandydamos nustatyti vartotojų išlaidų įpročius. Naršymo įpročiai paprastai nusiunčiami reklamos kompanijai, kuri ateityje pateikia tuos įpročius atitinkančią reklamą.
- **Slaptažodžio žvejyba** (angl. *phishing*, *Password phishing*). Pasinaudojant nepageidaujamomis elektroninio pašto žinutėmis ar netikrais internetiniais tinklalapiais bandoma išgauti prisijungimo prie informacinių sistemų slaptažodžius, kitus asmeninius duomenis. Dažniausiai tokių sukčiavimų aukos yra banko klientai, siekiama sužinoti jų prisijungimo prie elektroninės bankininkystės sistemų slaptažodžius ar kreditinių kortelių duomenis. Gauta informacija gali būti panaudota pasipelnymo tikslais vykdant nusikalstamas veikas, neteisėtus prisijungimus prie in-

formacinių sistemų, vagystės 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*), apgaulingas laiškas (angl. *scam*). Tai nėra baigtinis sukčiavimų sąrašas, kiti būdai ir metodai labai panašūs į ką tik aptautosius.

- **Trojos arklys** (angl. *trojans*). Programa, sprendžianti kokį nors naudingą uždavinį, tačiau iš tikrųjų atliekanti kitą darbą. Naikina, sugadina kompiuteryje esančius duomenis, programas. Dažniausiai trojos arkliai skirstomi į kirminams artimas programas, jos platina savo kopijas kompiuterių tinkluose. Kita rūšis – nuotolinio valdymo programos. Tai įprastos programos, naudojamos nuotoliniam sistemų administravimui. Pavojingiausias programos pasisavina informaciją, ją persiunčia tretiesiems asmenims, dažnai net naudoja paprastą el. pašta ar svetaines.
- **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) eksploatavimo pažeidimais. Pažeisti sričių vardų serveriai vadinami užnuodytais (angl. *dns cache poisoning*).
- **Pakartojimo ataka** (angl. *replay attack*) – mėginama prisijungti prie kompiuterio tinklo, siekiant pakartotinai išsiųsti vartotojo informaciją. Jeigu informacija koduojama, galima pakartoti tą patį duomenų siuntimą tikintis, kad serveris patikės, jog tai tas pats vartotojas.

Pasaulyje egzistuoja daugelis kitų metodų, bet visi jie veikia panašiai, išnaudodami tinklų, sistemų saugumo ar technologines spragas.

Atsirandantys nauji metodai verčia informacinių technologijų gamintojus keisti saugumo, duomenų perdavimo ar apsaugos standartus. Vienintelis galimas būdas užtikrinti tapatybę elektroninėje erdvėje – galinga kriptografija. Būtent kriptografijos metodas labai sumažina tapatybės vagystės riziką.

Literatūroje dažniausiai įvardijami šie tapatybės vagystės elektroninėje erdvėje motyvai: kitų nusikaltimų įvykdymas (pvz., sukčiavimo naudojant kompiuterį), informacijos pardavimas, realios tapatybės nuslėpimas, ir tokios stadijos: pasirengimas, 1 stadija (su tapatybe susijusios informacijos gavimas), 2 stadija (sąveika su tapatybe susijusia informacija (turėjimas, pardavimas) ir 3 stadija (su tapatybe susijusios informacijos panaudojimas siekiant įvykdyti nusikaltimą) (Gercke, 2007).

## Tapatybės vagystės elektroninėje erdvėje samprata

Šiuo metu visuotinai priimtina tapatybės vagystės elektroninėje erdvėje samprata nėra galutinai susiformavusi, netgi pačios veikos pavadinimas skiriasi. Tai sunkina kovą su šiuo pavojingu reiškiniu.

JAV, Kanadoje, Korėjoje vartojama tapatybės vagystės (angl. *id theft*) sąvoka, o ES šalyse tapatybės sukčiavimo (angl. *identity fraud*) arba tapatybės nusikaltimo (angl. *identity crime*) sąvokos kaip sinonimai. Prancūziškai kalbančiose valstybėse vartojamos tapatybės vagystės (pranc. *vol d'identile*) arba apsimetimo (pranc. *usurpation d'identile*) sąvokos (Scoping paper..., 2008).

Pasak Europolo 2006 metų ES organizuoto nusikalstamumo grėsmių įvertinimo dokumento (angl. *EU Organized Crime Threat Assessment („OCTA“)*), tapatybės vagystė ir tapatybės sukčiavimas yra sudedamosios tapatybės nusikaltimo dalys. Tapatybės vagystė laikoma tapatybės sukčiavimo subkategorija, nes tapatybės vagystė apsiriboja kito asmens tapatybės vagyste, o tapatybės sukčiavimas yra susijęs su kito asmens tapatybės naudojimu sukčiavimo tikslais.

Jungtinių Tautų tarpvyriausybės ekspertų grupės parengtoje sukčiavimo ir tapatybės klastojimo studijoje tapatybės vagystė ir sukčiavimas taip pat laikomi tapatybės nusikaltimo (t. y. visų neteisėtų veikų, susijusių su tapatybe) sudedamosiomis dalimis. Studijoje išskiriamos tapatybės vagystės ir tapatybės sukčiavimo veikos apibrėžiamos taip:

- *tapatybės vagystė* (angl. *identity theft*) – tokia veika, kai su tapatybe susijusi informacija (kuri gali būti esminė identifikuojanči

informacija arba tam tikrais atvejais – kita asmeninė informacija, pvz., asmens duomenys yra pavagiama / pasisavinama, įskaitant ir nematerialios informacijos vagystę / pasisavinimą;

- *tapatybės sukčiavimas* (angl. *identity fraud*) – identifikuojančios informacijos naudojimas padaryti kitiems nusikaltimams arba siekiant išvengti nustatymo ar baudžiamojo persekiojimo (The United Nations..., 2007).

Taigi, sukčiavimo terminas studijoje siejamas su vėlesniu pavogtos / pasisavintos tapatybės informacijos panaudojimu, siekiant apgauti kitus asmenis, t. y. įvykdyti nusikaltimą/(-us).

Jungtinėje Karalystėje tapatybės vagystė apibrėžiama kaip „veika, kurios metu gaunama pakankamai informacijos apie tapatybę, siekiant įvykdyti tapatybės sukčiavimą“ (Scoping paper..., 2008). Vadinasi, tapatybės vagystė suprantama kaip parengiamieji veiksmai įvykdyti sukčiavimą.

EBPO tapatybės vagystės elektroninėje erdvėje 2008 metų ataskaitoje siūloma tokia tapatybės vagystės samprata: „Tapatybės vagystė įvykdoma, kai asmuo neteisėtai įgyja, siunčia, valdo ar naudoja kito asmens asmeninę informaciją, ketinant įvykdyti ar vykdant sukčiavimą ar kitus nusikaltimus“ (Scoping Paper..., 2008). Identiška samprata pateikiama EBPO 2009 metų dokumente dėl tapatybės vagystės elektroninėje erdvėje, čia taip pat pažymima, kad kol kas nėra visuotinai priimtinos tapatybės vagystės elektroninėje erdvėje sampratos (Identity Theft..., 2009). Panašios nuomonės laikosi ir Europos Komisija, komunikate dėl elektroninių nusikaltimų pateikdama tokią tapatybės vagystės sampratą: „asmenį identifikuojančios informacijos naudojimas kaip priemonės įvykdyti kitus nusikaltimus“ (Communication..., 2007).

Mokslinėje literatūroje tapatybės vagystės / sukčiavimo sampratos kol kas neaptiriamos.

Apibendrinant galima daryti išvadą, kad egzistuoja dvi veikos – piktnaudžiavimas tapatybe elektroninėje erdvėje (šiuo atveju nėra tikslo įvykdyti nusikaltimą/(-us) ir tapatybės vagystė (sukčiavimas) elektroninėje erdvėje (kai yra konkretus tikslas įvykdyti nusikaltimą, dažniausiai susijęs su materialinės naudos gavimu). Pastarajai, pavojingesnei, veikai apibrėžti autoriai

siūlo vartoti šią tapatybės vagystės elektroninėje erdvėje sampratą: pagrindinių asmens tapatybę liudijančios informacijos elementų (elektroninėje erdvėje) gavimas siekiant apsimesti tuo asmeniu, turint tikslą atlikti nusikaltimus. Kai nėra tikslo atlikti nusikaltimus, veika gali būti apibrėžiama kaip piktnaudžiavimas tapatybe. Kai naudojama si neegzistuojančio asmens tapatybe, veika turėtų būti vadinama tapatybės klastote.

Reikėtų pažymėti, kad vienoda samprata galėtų užtikrinti efektyvesnę kovą su tokio tipo veikomis, ypač atsižvelgiant į galimą tarptautinį tapatybės vagystės veikos pobūdį.

### **Baudžiamoji atsakomybė už tapatybės vagystę elektroninėje erdvėje**

Tapatybės vagystės elektroninėje erdvėje sudėtingumas lemia nevienodą praktiką vertinant šią pavojingą veiką. Vis dažniau kyla diskusijos dėl baudžiamosios atsakomybės už tapatybės vagystę elektroninėje erdvėje. Atsižvelgdamos į tapatybės vagystės keliamas grėsmes, tiek Europos Komisija, tiek Ekonominio bendradarbiavimo ir plėtros organizacija kelia tapatybės vagystės elektroninėje erdvėje veikos kriminalizavimo klausimą. EBPO laikosi nuomonės, kad valstybės narės turi kriminalizuoti tapatybės vagystę kaip atskirą nusikaltimą (Online ID..., 2009). Europos Komisijos komunikate dėl elektroninių nusikaltimų nurodoma, kad lengviau įrodyti tapatybės vagystės nusikaltimą nei sukčiavimą, dėl to tapatybės vagystės kriminalizavimas visose valstybėse narėse pageidautinas ir tai padėtų užtikrinti geresnį teisėsaugos institucijų bendradarbiavimą (Communication..., 2007).

Beje, tapatybės vagystė elektroninėje erdvėje kaip savarankiška pavojinga veika jau kriminalizuota JAV, Honkonge, Indijoje ir kai kuriose kitose valstybėse. Pavyzdžiui, JAV pagal federalinius ir valstijų įstatymus, tapatybės vagystė yra specifinis kriminalinis nusikaltimas, kuris įvyksta, kai „kas nors žinomai siunčia, laiko, naudoja, neturėdamas teisės, kitą asmenį identifikuojančią informaciją, siekdamas įvykdyti įstatymų uždraustą veiką (Online Identity..., 2009). Taigi, kai kuriose valstybėse tapatybės vagystė laikoma nusikaltimu *per se*. Kitose vals-



tybėse tapatybės vagystė elektroninėje erdvėje neišskiriama kaip savarankiškas nusikaltimas ir laikoma sudedamąja kitų pavojingų veikų dalimi (pvz., sukčiavimo, klastojimo ir kt.).

Tam tikrose valstybėse vyksta tapatybės vagystės elektroninėje erdvėje kaip savarankiškos veikos kriminalizavimas. Pavyzdžiui, Kanados vyriausybė pateikė projektą, pagal kurį tapatybės vagystė elektroninėje erdvėje laikoma savarankišku nusikaltimu (Online Identity..., 2009). Nors kai kurios su tapatybės vagyste elektroninėje erdvėje susijusios veikos Kanados baudžiamajame kodekse jau kriminalizuotos (pvz., klastojimas), šiuo projektu siekiama kriminalizuoti parengiamuosius veiksmus (pvz., tapatybės informacijos laikymą sukčiavimo tikslais), kurie iki šiol nėra kriminalizuoti.

Tačiau, pavyzdžiui, Prancūzijoje pateiktas įstatymo projektas, kuriuo ketinta kriminalizuoti tapatybės vagystę kaip atskirą veiką, Prancūzijos teisingumo ministro buvo sukritikuotas ir atmetas kaip perteklinis, nes Prancūzijos įstatymų tam tikromis normomis jau numatyta atsakomybė už tapatybės vagystę (Rees, 2006).

Jungtinėje Karalystėje tapatybės vagystė elektroninėje erdvėje nelaikoma savarankišku nusikaltimu. Vis dėlto pagal Jungtinės Karalystės 2006 metų Sukčiavimo įstatymą, kuris įsigaliojo nuo 2007 metų, sukčiavimas kaip savarankiška pavojinga veika apima ir sukčiavimą elektroninėje erdvėje. Šioje šalyje buvo kriminalizuotos ir kitos naujos veikos: „nesąžiningas paslaugų gavimas“, „sukčiavimas internete naudojant kreditines korteles“, „kenkiančių kompiuterių programų naudojimas“ ir kt. Australijoje tapatybės vagystė elektroninėje erdvėje taip pat nelaikoma savarankišku nusikaltimu (Online Identity..., 2009).

Taigi, priešinga nuomonė – tapatybės vagystė kaip tokia nėra atskiras pažeidimas, o kai kurie tapatybės vagystės epizodai traktuojami kaip privatumo, saugumo ar finansiniai pažeidimai arba kaip pasikėsinimas padaryti tokius pažeidimus.

Pagal galiojančią Lietuvos Respublikos baudžiamąjį kodeksą tam tikri tapatybės vagystės elektroninėje erdvėje elementai galėtų būti vertinami kaip pavojingos veikos. Pavyzdžiui, jei siekiant neteisėtai gauti asmens duomenis ir vėliau šiuos duomenis panaudoti kitam nusikaltimui įvykdy-

ti, išsilaužiama į kito vartotojo kompiuterį, veika galėtų būti vertinama kaip neteisėtas prisijungimas prie informacinės sistemos pagal Lietuvos Respublikos baudžiamojo kodekso 198-1 straipsnį: „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“ (Lietuvos Respublikos baudžiamasis kodeksas, 2000). Taip pat galima atsakomybė pagal Lietuvos Respublikos baudžiamojo kodekso 198 straipsnio (Neteisėtas elektroninių duomenų perėmimas ir naudojimas) dispoziciją. Vis dėlto Lietuvos Respublikos baudžiamajame kodekse tapatybės vagystės elektroninėje erdvėje atvejais reikėtų kalbėti apie nusikalstamų veikų daugetą. Kitaip tariant, galima nusikalstamų veikų sutaptis pagal Lietuvos Respublikos baudžiamojo kodekso 198-1 str. ar 198 str. ir kitus Lietuvos Respublikos baudžiamojo kodekso straipsnius: neteisėtas informacijos apie asmens privatą gyvenimą rinkimas pagal 167 str., neteisėtas informacijos apie asmens privatą gyvenimą atskleidimas ir panaudojimas pagal 168 str., sukčiavimas pagal 182 str., kreditinis sukčiavimas pagal 207 str., neteisėtas elektroninės mokėjimo priemonės ar jos duomenų panaudojimas pagal 215 str., dokumento suklastojimas ar disponavimas suklastotu dokumentu pagal 300 str. ir t. t. Tokiais atvejais taikomos Lietuvos Respublikos baudžiamajame kodekse numatytos bausmių subendrinimo taisyklės. Beje, pagal Lietuvos Respublikos baudžiamojo kodekso 21 str. bei 22 str. baudžiamoji atsakomybė kyla ir už rengimąsi bei kėsimąsi padaryti nusikaltimą.

Deja, reikia pasakyti, kad ne visas tapatybės vagystės elektroninėje erdvėje veikas ar jų epizodus galima įvertinti pagal atitinkamus Lietuvos Respublikos baudžiamojo kodekso straipsnius: pirmos ir trečios stadijos veiksmai gali būti vertinami pagal atitinkamus kodekso straipsnius, o tapatybės vagystės elektroninėje erdvėje antros stadijos veika negali būti laikoma nusikalstama. Pavyzdžiui, vien su tapatybe susijusios informacijos turėjimas arba pardavimas neužtraukia baudžiamosios atsakomybės, nebent tokią veiką vertintume kaip rengimąsi įvykdyti kitą nusikaltimą. Kita galimybė išvengti baudžiamosios

atsakomybės tokia: 198 straipsnio 1 dalies dispozicija apima tik neviešą informaciją, o juk tapatybės vagystės elektroninėje erdvėje atvejais gali būti naudojama ir vieša informacija apie fizinį asmenį, t. y. viešai skelbiami asmens duomenys.

Pirmiau pateikta informacija rodo, kad tapatybės vagystės elektroninėje erdvėje vertinimas iš baudžiamosios teisės pozicijų yra per daug sudėtingas. Dėl to, autorių nuomone, savarankišką nusikalstamą veiką – tapatybės vagystę elektroninėje erdvėje – reikia įvardyti Lietuvos Respublikos baudžiamajame kodekse, siekiant panaikinti teisinio reguliavimo spragas, nes tokią veiką lengviau įrodyti ir kvalifikuoti nei kad vėliau kylančias tradicines nusikalstamas veikas. Tuomet vietoje nusikalstamų veikų daugeto tektų įrodinėti tik vieną nusikalstamą veiką.

Tapatybės vagystė elektroninėje erdvėje yra visuotinė problema, todėl ypač svarbi užsienio teisės saugos institucijų pagalba. Tačiau tai, kai užsienio valstybės neturi vienodų įstatymų, kriminalizuojančių tapatybės vagystę elektroninėje erdvėje, labai varžo informaciją renkančios valstybės galimybes rinkti tapatybės vagystės elektroninėje erdvėje įrodymus atitinkamoje užsienio valstybėje. Tad, autorių nuomone, tikslinga suvienodinti tapatybės vagystės elektroninėje erdvėje kriminalizavimo praktiką visose valstybėse, šią pavojingą veiką įvardijant savarankišką nusikaltimu.

Tapatybės vagystės elektroninėje erdvėje dispozicijoje turėtų būti įvardijamas ir veikos tikslas – įvykdyti kitą nusikaltimą. Tokios nusikalstamos veikos sudėtis turėtų būti formalioji, t. y. kai veika nesukelia žalingų padarinių. Vis dėlto pažymėtina, kad tapatybės vagystės elektroninėje erdvėje kaip savarankiško nusikaltimo požymio detalesnis apibūdinimas ir analizė – tolesnių mokslinių tyrimų objektas.

## LITERATŪRA

Tarptautinių žodžių žodynas. Vilnius: Alma littera, 2003.

*Communication from the Commission to the European Parliament, the Council and the Committee of the Regions “Towards general policy on the fight against cyber crime”* (2007). COM(2007)267 final. Brussels, 2007 [interaktyvus], p. 8 [žiūrėta

## Išvados

Tapatybė laikytina asmens identitetu, o tapatybės elektroninėje erdvėje nustatymas – varotojo identifikavimo tam tikroje informacinėje sistemoje procesu. Kitaip tariant, tapatybės nustatymas elektroninėje erdvėje – veiksmas kieno nors tapatybei nustatyti kompiuterių tinkle vartojant slaptažodį ar kitą informaciją.

Tapatybės vagystės elektroninėje erdvėje būdai yra labai įvairūs ir lemia sąvokų įvairovę. Tapatybės vagystė kaip neatlygintinis pasisavinimas gali būti atlikta naudojant specifinius metodus ir būdus. Tapatybės vagystės atmaina yra klastotė, kurios tikslas – apgauti, suklaidinti, tapatybę padaryti netikrą. Taikomi metodai ir būdai skiriasi pagal tai, ko siekiama – pavogti, ar suklastoti.

Šiuo metu nėra vienodos tapatybės vagystės elektroninėje erdvėje sampratos. Tai lemia skirtingą veikos vertinimą. Autoriai siūlo skirti dvi veikas – pavojingesnę ir mažiau pavojingą, ir pavojingesnės veikos aspektu vartoti šią tapatybės vagystės (sukčiavimo) elektroninėje erdvėje sampratą: tai pagrindinių asmens tapatybę liudijančios informacijos elementų (elektroninėje erdvėje) gavimas, siekiant apsimesti tuo asmeniu, kad galėtum atlikti nusikaltimus. Mažiau pavojinga veika gali būti laikoma piktnaudžiavimu tapatybe ir apibrėžiama be nusikalstamo požymio. Su realiu asmeniu nesusijusios tapatybės panaudojimas turėtų būti siejamas su tapatybės klastote.

Tapatybės vagystės elektroninėje erdvėje kaip pavojingos veikos vertinimas baudžiamosios teisės požiūriu įvairiose valstybėse skiriasi. Tačiau pastebima ir tendencija – tapatybės vagystė turėtų būti kriminalizuota kaip atskira pavojinga veika, t. y. pati tapatybės vagystė valstybių baudžiamuosiuose įstatymuose turėtų būti įvardyta kaip nusikaltimas. Tapatybės vagystę elektroninėje erdvėje autoriai siūlo įvardyti kaip savarankišką nusikalstamą veiką.

2009 m. gegužės 3 d.]. Prieiga per internetą: <[http://eurlex.europa.eu/LexUriServ/site/en/com/2007/com2007\\_0267en01.pdf](http://eurlex.europa.eu/LexUriServ/site/en/com/2007/com2007_0267en01.pdf)>.

*Convention for the Protection of Individuals with Regard to Automatic Protection of Personal Data* (1981). Strasbourg, January 28, 1981 [interaktyvus], 2 str. [žiūrėta 2009 m. gegužės 3 d.]. Prieiga per inter-

netą: <<http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>>.

CUGANESAN, S.; LACEY, D. (2003). *Identity fraud in Australia: An evaluation of its nature, cost and extent*. Securities Industry Research Centre of Asia-Pacific, Sydney, p. 1.

DAGIENĖ, A.; GRIGAS, G.; JEVSIKOVA, T. (2008) *Enciklopedinis kompiuterijos žodynas*. Vilnius: TEV.

*Federal Trade Commission – 2006 Identity Theft Survey Report* (2007) [interaktyvus] p. 4–11 [žiūrėta 2009 m. gegužės 3 d.]. Prieiga per internetą: <<http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf>>.

GERCKE, Marc (2007). *Internet-related identity theft*. [interaktyvus] p. 17–20 [žiūrėta 2009 m. gegužės 3 d.]. Prieiga per internetą: <[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](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)>.

*Identity Crime* (2007). Model Criminal Law Officer's Committee of the Standing Committee of Attorney General: Discussion Paper. April, 2007 [interaktyvus], p. 3–4 [žiūrėta 2009 m. gegužės 3 d.]. Prieiga per internetą: <[http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/\(4341200FE1255EFC59DB7A1770C1D0A5\)~MCLOC-draft-identity-crime-discussion-paper-march+2007.pdf/\\$file/MCLOC-draft-identity-crime-discussion-paper-march+2007.pdf](http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(4341200FE1255EFC59DB7A1770C1D0A5)~MCLOC-draft-identity-crime-discussion-paper-march+2007.pdf/$file/MCLOC-draft-identity-crime-discussion-paper-march+2007.pdf)>.

*Identity Theft Protection* (2007) [interaktyvus] [žiūrėta 2009 m. gegužės 11 d.]. Prieiga per internetą: <http://www.identitytheftsecurity.com/protect.shtml#phone>.

*Lietuvos Respublikos baudžiamasis kodeksas* (2000) [interaktyvus] [žiūrėta 2009 m. gegužės 15 d.]. Prieiga per internetą: <<http://www.lrs.lt>>.

NAKTINIENĖ, G. (vyr. redaktorė); PAULAUŠKAS, J.; PETRONIENĖ, R.; VITKAUAKAS, V.;

ZABARSKAITĖ, J. (2005). *Lietuvių kalbos žodynas*. Vilnius: Lietuvių kalbos institutas, 2005 [interaktyvus] [žiūrėta 2009 m. gegužės 10 d.]. Prieiga per internetą: <[www.lkz.lt](http://www.lkz.lt)>.

OECD Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication (2007) [interaktyvus], p.16 [žiūrėta 2009 m. gegužės 3 d.]. Prieiga per internetą: <[http://www.oecd.org/document/7/0,3343,en\\_2649\\_34255\\_38909\\_639\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/7/0,3343,en_2649_34255_38909_639_1_1_1_1,00.html)>.

*Online ID Theft: More Efforts Needed to Fight Online Identity Theft* (2009) [interaktyvus] [žiūrėta 2009 m. gegužės 3 d.]. Prieiga per internetą: <[http://www.oecd.org/document/59/0,3343,en\\_2649\\_34223\\_40830139\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/59/0,3343,en_2649_34223_40830139_1_1_1_1,00.html)>.

*Online Identity Theft*. OECD (2009) [interaktyvus] p. 16, 48 [žiūrėta 2009 m. gegužės 3 d.]. Prieiga per internetą: <<http://browse.oecdbookshop.org/oecd/pdfs/browseit/9309021E.PDF>>.

*Online Identity Theft*. OECD Observer No. 268 (2008) [interaktyvus] [žiūrėta 2009 m. gegužės 3 d.]. Prieiga per internetą: <[http://www.oecdobserver.org/news/fullstory.php/aid/2662/Online\\_identity\\_theft.html](http://www.oecdobserver.org/news/fullstory.php/aid/2662/Online_identity_theft.html)>.

REES, Marc (2006). *L'usurpation d'identité sur Internet n'aura pas sa loi* [interaktyvus] [žiūrėta 2009 m. gegužės 3 d.]. Prieiga per internetą: <<http://fr.news.yahoo.com/23102006/308/l-usurpation-d-identite-sur-Internet-n-aura-pas-sa.html>>.

*Scoping Paper on Online ID Theft*. OECD, Ministerial Background Report (2008) [interaktyvus], p. 12–60 [žiūrėta 2009 m. gegužės 3 d.]. Prieiga per internetą: <<http://www.oecd.org/dataoecd/35/24/40644196.pdf>>.

*The United Nations Study on fraud and the criminal misuse and falsification of identity* (2007) [interaktyvus], p. 17 [žiūrėta 2009 m. gegužės 3 d.]. Prieiga per internetą: <<http://www.itu.int/osg/csd/cybersecurity/pgc/2007/events/presentations/session5-chryssikos-C5-meeting-14-may-2007.pdf>>.

## ONLINE IDENTITY THEFT

Darius Štītīlis, Marius Laurinaitis

### Summary

The article analyzes the identity theft in electronic space, and the main aspects of this dangerous crime. The article consists of four parts. The first part analyzes the identity and identification in electronic space category. The second part is dedicated to discussing and systematizes techniques and forms of identity theft in electronic space. The third paragraph proposes the conception of the identity theft in electronic space. The fourth paragraph analyzes identity theft in electronic space as the

individual crime, and proposes criminalize aspects. The analysis in this article suggests that the methods of identity theft in electronic space are very different and constantly changing, as well as new ways and forms. In different sources there are a lot of discussions about the concept of identity theft. The authors carried out suggest using of identity theft in electronic space version as the concept. The article also includes the latest identity theft in electronic space criminalize aspects.