MYKOLO ROMERIO UNIVERSITETAS
EKONOMIKOS IR FINANSŲ VALDYMO FAKULTETAS
INFORMATIKOS IR STATISTIKOS KATEDRA

REMIGIJUS MULIUOLIS

ASMENS TAPATYBĖS NUSTATYMAS INTERNETE, TEISINIAI ASPEKTAI

Magistro baigiamasis darbas

Vadovas
Lekt. K.Spalveters

VILNIUS, 2008

MYKOLO ROMERIO UNIVERSITETAS
EKONOMIKOS IR FINANSŲ VALDYMO FAKULTETAS
INFORMATIKOS IR STATISTIKOS KATEDRA

REMIGIJUS MULIUOLIS

ASMENS TAPATYBĖS NUSTATYMAS INTERNETE, TEISINIAI ASPEKTAI

Magistro baigiamasis darbas

Vadovas
Lekt. K.Spalveters

VILNIUS, 2008

TURINYS

ĮVADAS

Internetas yra pasaulinis kompiuterių tinklas, jungiantis daugybę kitų tinklų ir veikiantis Transporto valdymo ir Interneto (TCP/IP) protokolų pagrindu. Jo dėka milijonai žmonių visame pasaulyje gali bendrauti vieni su kitais „virtualioje erdvėje“ ir naudotis tinkle esančia gausia informacija. Internetas – tai milžiniška informacijos saugykla; milijonai prie jo prijungtų kompiuterių kimšte prikimšti programų, dokumentų, knygų, piešinių ir kitokios informacijos, kuri specialių technologijų dėka yra lengvai pasiekiama bet kuriam vartotojui.

Interneto paplitimas suteikė daug galimybių žmonijai, tačiau atnešė ne tiktai teigiamos naudos, tačiau ir neigiamų pasekmių. Pastaruoju metu pastebimas neteisėto ir žalingo turinio medžiagos plitimas elektroninėje erdvėje. Literatūroje nurodoma, kad tai yra sparčiai plintančių nusikaltimų elektroninėje erdvėje sritis. Pornografinio turinio medžiagos internete platinimas, rasistinių nuostatų skleidimas kelia klausimus dėl baudžiamosios teisės vaidmens vertinant šias veikas. Naudodamiesi Interneto galimybėmis galime ne tik naudotis teikiama informacija, bet taip pat ją laisvai duoti kitiems vartotojams. Interneto turinio autoriai, turinio tiekėjai, interneto paslaugų tiekėjai bei vartotojai teikdami informaciją bei bendraudami tiek viešai, tiek tarpusavyje, turi laikytis tos šalies galiojančių teisės normų.

Kadangi internete gaunama ne tiktai naudinga, bet ir nepageidaujama informacija, kuri daro žalingą poveikį pažeidžiamoms socialinėms grupėms bei visai visuomenei, taip pat informacija, kurios viešą skelbimą įstatymai riboja ar draudžia, atsiranda priežastys, lemiančios interneto turinio reguliavimą.

Temos aktualumas ir naujumas. Asmens tapatybės nustatymas Internete – šią temą autorius pasirinko todėl, kad ji yra aktuali jo tiesioginiame darbe. Nusikalstamumas nenumaldomai auga, ypatingai elektroninėje erdvėje, nusikaltimų padarymo priemonių ir būdų arsenalą nuolat papildo naujausi mokslo ir technikos pasiekimai. Kasmet vis daugiau yra tiriama baudžiamųjų bylų, kuomet reikalinga nustatyti asmens tapatybę, kuri vienaip ar kitaip yra susijusi su padaryta nusikalstama veika elektroninėje erdvėje, o kaip taisyklė – žinių ir informacijos kiekis kaip aiškinti tokio pobūdžio nusikalstamas veikas yra labai ribotas. Rašydamas šį darbą autorius susidūrė su plačia temos apimtimi bei literatūros stoka.

Darbo hipotezė – asmens tapatybės nustatymo internete samprata bei praktinis realizavimas yra neaiški ir nepakankamai teisiškai reglamentuota, taip pat reiktų kriminalizuoti asmens tapatybės klastotę elektroninėje erdvėje, atribojant ją nuo paprasto sukčiavimo.

Tyrimo tikslas - išanalizuoti teisinius ir praktinius asmens tapatybės Internete buvimo, slėpimo ir klastojimo aspektus, nurodyti pagrindines teisines problemas, su kuriomis susiduriama siekiant išlikti anonimiškam. Tema yra nauja, praktiškai detaliai neišnagrinėta nei Lietuvoje, nei kitose šalyse. Savo darbe autorius stengėsi remtis įvairiais straipsniais ir publikacijomis Internete, taip pat publikacijomis moksliniuose leidiniuose bei tarnybinio pobūdžio informacija iš Policijos departamento prie LR VRM.

Tyrimo uždaviniai magistro baigiamajame darbe yra šie:

1) visapusiškai ir išsamiai pateikti teisines žinias apie asmens tapatybės paslėpimą ir nustatymą Internete;
2) išanalizuoti bei įvertinti svarbiausius Lietuvos Respublikos, Europos Sąjungos ir kitus Tarptautinės teisės aktus, reglamentuojančius asmens tapatybės nustatymą internete;
3) išdėstyti ir pateikti išsamų problemų, susijusių su asmens tapatybės paslėpimu bei anonimiškumu, klastojimu ir atskleidimu ratą bei įtakoti tolimesnes studijas šioje srityje;
4) išnagrinėti šiandien dar retus, tačiau tiek Lietuvos, tiek kitų valstybių praktikoje rastus praktinius asmens tapatybės nustatymo Internete kriminalizuotus atvejus ir situacijas;
5) pateikti teisinius ir praktinius pasiūlymus.

Šio darbo autorius bandys suformuluoti asmens tapatybės nustatymo Internete apibrėžimą, analizuos asmens tapatybės klastojimo ir paslėpimo bei anonimiškumo būdus, taip pat teisinius aspektus. Atskirose darbo dalyse bus nagrinėjami Lietuvoje ir užsienio šalių praktikoje rasti asmens tapatybės klastotės ir paslėpimo bei anonimiškumo elektroninėje erdvėje atvejai, analizuojama praktika kokiais atvejais galima nustatyti, klastoti asmens tapatybę, bei kada ir kiek leidžiama išlikti anonimišku. Taip pat bus nagrinėjama kada anonimiškumas ar psiaudoanonimiškumas gali būti ribojamas ir iš to kylančios teisinės problemos. Šiame darbe taip pat bus analizuojama teisinė bazė, reguliuojanti asmens duomenų apsaugą elektroninėje erdvėje, tam tikrų nusikaltimų, susijusių su asmens tapatybės klastojimu ir paslėpimu Internete, reglamentavimas Lietuvoje ir užsienio šalyse bei kiti iškilę klausimai, susiję su šia autoriaus

pasirinkta tema. Autoriaus pasirinkta tema šiandien yra dar aktuali ir tuo, kad įdiegiant naujausias technologijas, kurios paskutiniu dešimtmečiu vystosi nenuspėjamu greičiu, įstatymų leidėjai Lietuvoje nespėja įsigilinti į technines galimybes ir kriminalizuoti į Lietuvą atėjusių naujų nusikaltimų rūšių, kas paskatina ne visiškai teisingai kvalifikuoti nusikalstamas veikas bei tirti tokius nusikaltimus. Turbūt pagrindinė šiuo metu kylanti problema yra Asmens tapatybės nustatymas ir pačios tapatybės klastotės kriminalizavimas.

Tyrimo šaltiniai ir metodai. Magistro baigiamojo darbo tyrimo pagrindas: Lietuvos teisės aktai, teisinės patirties ir minties šaltiniai, publikacijos Internete ir mokslinės publikacijos, baudžiamosios teisės, baudžiamojo proceso ir kitų mokslo šakų literatūra. Taip pat remtasi autoriaus profesinės patirties apibendrinimu. Magistro darbo teiginiai paremti ir autoriaus atliktu kokybiniu tyrimu. Kokybinio tyrimo metu buvo tiesiogiai bendrauta su 4 Policijos departamento prie Vidaus reikalų ministerijos Lietuvos kriminalinės policijos biuro Nusikaltimų elektroninėje erdvėje tyrimo skyriaus tyrėjais bei 2 Kauno apskrities Vyriausiojo policijos komisariato tyrėjais iš **kurių buvo paimti interviu**. Visi kokybinio tyrimo rezultatai išanalizuoti, apibendrinti ir pateikti magistro darbo dėstomojoje dalyje.

Magistro baigiamajame darbe remtasi bendraisiais teoriniais tyrimo metodais: analize, lyginamuoju teisiniu, loginiu, istoriniu, sisteminės analizės, interviu ir profesinės patirties apibendrinimo metodais.

1. ASMENS TAPATYBĖS SĄVOKA IR SAMPRATA

Aiškinant sąvokas, reiktų pažymėti, kad Lietuvių kalboje nėra aiškiai apibrėžtos sąvokos kaip asmens tapatybė. Aiškinant gramatiškai, iš Lietuvių kalbos žodyno, matyti, kad sąvoka „Asmuo“ - reiškia žmogų kaip atskirą individą. Sąvoka „Tapatybė“ – aiškinama kaip objekto lygybė pačiam sau arba kitam objektui. Sąvoką „Nustatyti asmens tapatybę“, pasitelkę tarptautinių žodžių žodynus galime paaiškinti kaip asmens identifikavimą (angl. *Personal identity*), arba tiesiog pripažinti tuo pačiu, nustatyti esant tą patį. Dar pridėjus sąvokos Internetas paaiškinimą – (lot. *inter* –tarp, angl. *Net* - tinklas) pasaulinis kompiuterinis tinklas, galime teigti, jog „Asmens tapatybės nustatymas Internete“, reiškia atskiro individo pripažinimą juo pačiu pasauliniame kompiuteriniame tinkle.

Asmens tapatybė yra neįmanoma be asmens duomenų. Tiek pagal 1981 m. Europos Tarybos konvenciją “Dėl asmenų apsaugos, susijusios su automatizuotu asmens duomenų apdorojimu”, tiek pagal EBPO Rekomendaciją “Dėl asmens privatumo apsaugos ir asmens duomenų judėjimo tarp valstybių narių gairių” asmens duomenys apibrėžiami kaip bet kokia informacija, susijusi su identifikuotu ar identifikuotinu asmeniu. [1]

Pagal Duomenų apsaugos direktyvos 95/46/EB 2 str. asmens duomenys reiškia bet kurią informaciją, susijusią 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 ir netiesiogiai, ypač pasinaudojus nurodytu asmens identifikavimo kodu arba vienu ar keliais to asmens fizinei, fiziologinei, protinei, ekonominei, kultūrinei ar socialinei tapatybei būdingais veiksniais.[2]

Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo[3] (toliau - ADTAĮ) 2 straipsnis pateikia tokią asmens duomenų sąvoką – 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

---

[1] www.itc.tf.vu.lt/mokslas/asmens%20duomenu%20teisines%20apsaugos%20klausimai%20interneto%20kontekste.doc ASMENS DUOMENŲ TEISINĖ APSAUGA INTERNETO KONTEKSTE PAGAL EUROPOS SĄJUNGOS IR TARPTAUTINĘ TEISĘ, Teisės fakulteto V kurso Tarptautinės ir Europos Sąjungos teisės specializacijos studentė Kristina Spalveters, Vilnius 2003. (žr. 2008-05-25)

[2] Toks pats asmens duomenų apibrėžimas pateikiamas Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo 2 str. // V.Ž., 1996, Nr. 63-1479

[3] Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas// Valstybės žinios. 1996, Nr. 63-1479.

būdingi fizinio, fiziologinio, psichologinio, ekonominio, kultūrinio ar socialinio pobūdžio požymiai.

2. ANONIMIŠKUMAS INTERNETE

Anonimiškumas Internete yra toks metodas, kurio pagalba asmenys siunčia informaciją ir tvarko verslo reikalus Internetu, neatskleisdami tikro savo tapatumo. Informacija, kurią nori atskleisti tokie asmenys, kontroliuoja jie patys savarankiškai. Tokią informaciją sudaro visi asmeniniai duomenys, o taip pat kompiuterio bei vietos, iš kurios vyksta informacijos perdavimas ar siuntimas duomenys. Išlaikyti anonimiškumą internete reiškia naudotis Internetu, nesuteikiant niekam galimybės nei surasti tikro prisijungimo pėdsako, nei atsekti kitų sąsajų prie asmeninės informacijos.

R. Gavison teigė, kad asmens teisę į privatumą sudaro trys elementai: "anonimiškumas" (tai asmens teisė išlikti neatpažintam), "vienatvė" (tai asmens teisė nebūti stebimam) ir "intymumas" (tai asmens teisė bendrauti su paties pasirinktais asmenimis, nepatiriant išorinio kišimosi).[4]

Tie, kas domisi anonimiškumo internete klausimais dažnai šneka apie slapukus. Slapukai (angl. *cookies*) sukelia daugiausiai diskusijų pokalbiuose apie pavojų asmens privatumui. Slapukai yra užslėptas tekstas, parsiųstas į tinklo naršyklę apie svetainę ar puslapį, kuriuose buvo lankstąsi. Šitas tekstas sukauptas kompiuterio atmintyje ir yra siunčiamas atgal kiekvieną kartą, kai tam tikras tinklalapis būna aplankomas iš naujo. Tai yra daroma tam, kad greičiau atverstų puslapį, kadangi kompiuteriui, gaunančiam prieigą prie puslapio, slapukas nustato autentiškumą. Slapukai taip pat kaupia savyje tokią specifinę informaciją apie vartotoją kaip: slaptažodžiai, prisijungimo vardai su slaptažodžiais ir netgi informaciją apie krepšelių turinį, kas buvo pirkta elektroninėse parduotuvėse. Todėl slapukas interneto vartotojų yra laikomas vienu iš pavojaus privatumui šaltinių, o tie, kas rengiasi naršyti Internete, pirmiausiai slapukus išjungia.

[4] *Ruth Gavison.* Privacy and the Limits of the Law // Yale Law Journal. – Jan. 1980, vol 89, no 3, P. 428.

Anonimiškumo Internete gynėjai teigia, kad anonimiškumas yra pats svarbiausias žodžio laisvės internete aspektas. Anonimiškumas suteikia galimybę Interneto vartotojams laisvai, be baimės reikšti savo mintis, nesibaiminant būti surastiems, susektiems ar išjuoktiems. Tai ypač svarbu vykstant tiesioginėms (angl. *online*) diskusijoms ir forumams internetu, ypač kuomet yra gvildenami asmeniniai klausimai ar temos, ir kuriose dalyviai nenori, kad būtų nustatyta nei jų tapatybė, nei buvimo vieta. Labai vykęs tokio svarbaus anonimiškumo pavyzdys yra pokalbiai medicinos forumuose, kur pacientai laisvai, nesivaržydami gali užduoti su gydymu susijusius klausimus patiems gydytojams ar kitiems ligoniams su panašiais ligų simptomais. Anonimiškumo Internete gynėjai taip pat teigia, kad interneto anonimiškumas yra būtinas perdavimui tokios informacijos, kuri turi ir likti anoniminė. Pranešimai Internetu apie neteisėtas veikas ir padarytus nusikaltimus taip pat yra geras pavyzdys to, koks anonimiškumas gali būti svarbus: tai suteikia liudytojui ar pranešusiam asmeniui patogumo ir saugumo jausmą, reikalingą parodymų davimui. [5]

Priešininkai teigia, kad anonimiškumas Internete suteikia dideles galimybes piktnaudžiavimui ir neteisėtiems veiksmams. Brukalų siuntinėjimas (angl. *Spam*) arba neprašyto elektroninio pašto siuntinėjimas, yra labiausiai paplitęs teisės pažeidimas, naudojantis interneto anonimiškumu. Daugiausia brukalų yra ne grėsmė, o tiktai šiukšlės elektroninio pašto dėžutėse, tačiau, buvo fiksuota atvejų, kai brukalai buvo panaudoti tam, kad išreikšti neapykantą, grasinimus ir šmeižimą, ir tokių brukalų anonimiškumas labai apsunkino, ar padarė neįmanomu brukalų kūrėjų nustatymą. Anonimiškumo oponentai taip pat teigia, jog anonimiškumas Internete saugo nusikaltėlius ir seksualinius priekabiautojus. Šitie pažeidėjai ypač noriai dalyvauja diskusijose ir forumuose, kuriuose saugomas visų vartotojų tapatumas, tam, kad surasti sau auką per Internetą.

Jeigu kalbėti apie internetinę komerciją, galima pažymėti, jog vienas iš tokios komercijos privalumų yra tas, kad internetas sukuria galimybę internetinių sandorių šalims išlikti anonimiškoms[6]. Pvz., 2000 m. lapkritį Niudžersio teismas nusprendė, kad programinės įrangos kompanija neturi teisės sužinoti tikrosios atsakovų, pasivadinusių "John Doe", tapatybės, kurie Yahoo pranešimų lentoje patalpinio kritines pastabas.

---

[5] http://whatismyipaddress.com/staticpages/index.php/internet-anonymity , prisijungimo laikas 2008-05-25 16:53;

[6] http://www.itc.tf.vu.lt/ Šalių anonimiškumo problema interneto kontekste, Autorius: M.Civilka, prisijungimo laikas 2008-11-26 12:53;

Vienas esminių klausimų, susijusių su šalių anonimiškumu, yra tas, ar galioja ir ar teisiniu požiūriu pripažintinas anonimišku būdu sudarytas elektroninis kontraktas? Kitaip tariant, ar toks elektroninis kontraktas sukelia teisines pasekmes ir yra įgyvendinamas priverstine tvarka?

Anonimiškumas nėra fiksuota asmens charakteristika. Pvz., aš nesu anonimiškas sau pačiam ar mane žinantiems asmenims. Taigi, anonimiškumas yra požymis, taikytinas trečiųjų asmenų atžvilgiu, atliekančių savotišką stebėtojų, žiūrovų funkciją. Anonimiškas sandoris yra toks sandoris, kai neįmanoma (nepasitelkiant neproporcingai didelių pastangų) nustatyti šalių tapatybės. Nors retai kada daromas skirtumas tarp anonimiškumo laipsnių, jų išskyrimas turi reikšmės įvertinant teisines anonimiško sandorio pasekmes. Šia prasme išskirtinos tokios esminės anonimiškų sandorių rūšys:

a) absoliučiai anonimiški sandoriai (nėra jokių ženklų, remiantis kuriais būtų įmanoma nustatyti tikrąją šalies tapatybę);

b) pusiau anonimiški sandoriai (yra palikta ženklų, remiantis kuriais būtų įmanoma nustatyti tikrąją šalies tapatybę);

c) personalizuoti sandoriai (sudaryti pasinaudojant asmeniniais duomenimis, kurie buvo patikrinti trečiosios šalies).

Šio skirstymo esminis kriterijus – tai, ar šalis pasinaudojo pseudonimu, kurio pagrindu galima atsekti tikrąjį asmens identitetą. Šiuo atveju pseudonimas suprastinas plačiąja prasme – kaip bet koks ženklas, kodas, asmens numeris, elektroninis parašas, PIN kodas ar netgi biometrinis numeris, tiek pasirinktas spontaniškai slapyvardis (*angl. nick*), tiek ir organizuotas. Organizuotas pseudonimas reiškia trečiosios šalies (pvz., valstybinės institucijos, banko) išduotą patvirtintą pseudonimą (pvz., PIN kodą, registracijos numerį, e-parašo sertifikatą ir pan.)[7].

Pseudonimų naudojimas svarbus tuo, kad jų pagrindu asmuo gali tapti atpažįstamu visiškai neatskleidus jo tapatybės. Pseudonimas suteikia galimybę likti anonimišku vienai šaliai ir būti visiškai žinomu kitai. Pvz., jeigu bankas išduoda PIN kodą, jis, išleisdamas PIN kortelę, gali nustatyti tikrąjį kortelės turėtoją. Jeigu vėliau asmuo panaudoja kortelę atlikti mokėjimams, PIN

[7] http://www.itc.tf.vu.lt/ ir http://www.google.lt/search?q=anonimi%C5%A1kumas+internete&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-US:official&client=firefox-a , Šalių anonimiškumo problema interneto kontekste (46 kb) Autorius: M.Civilka, prisijungimo laikas 2008-11-26 12:53;

kodo pagalba apmokėjimo gavėjas (pvz., parduotuvė) sužino tik tiek, kad mokėtojas yra teisėtas kortelės turėtojas.

Kraštutinis santykių užmezgimo ir palaikymo atvejis – absoliučiai anonimiškas bendravimas. Tokio anonimiškumo realizavimo pavyzdžiu galėtų būti viešai apmokamų telefonų aparatai (taksofonai) arba iš anksto apmokamos SIM kortelės. Jeigu bent vienas iš santykių dalyvių žino ar gali sužinoti asmens tikrąją tapatybę, galima kalbėti tik apie pusiau anonimiškumą. Tai santykiai, kuriuose dalyvauja trečiosios šalys (*ang. intermediaries*), galinčios bet kada nustatyti asmens tapatybę. Tokio pusiau anonimiškumo pavyzdžiu galėtų būti transporto priemonės registracijos numeris, anonimiškas dalyvavimas aukcione ir pan.. Jeigu asmens tikroji tapatybė yra žinoma arba gali būti lengvai nustatyta, mes kalbame apie personalizuotus sandorius.

Kiekvieną dieną yra sudaroma daugybė sandorių, kurių viena iš šalių lieka anonimiška, kadangi ji už įsigyjamą produktą sumoka grynaisiais piningais produkto įsigijimo momentu. Pavyzdžiui, jeigu asmuo į gaivinančiųjų gėrimų automatą įmetą monetą, teisine prasme yra sudaromas sandoris, nors pirkėjas apie tai retai susimąsto. Akivaizdu, kad šiuo požiūriu būtina skirti realines sutartis, kurios įvykdomos sutarties sudarymo metu, nuo konsensualinių, kuriose prievolių įvykdymo pareiga gali atsirasti ir vėliau.

Anonimiški elektroniniai kontraktai sudaromi per atstumą be jokio tiesioginio ar netiesioginio (pvz., su kavos automato savininku) fizinio kontakto tarp sandorio šalių, todėl pardavėjui yra kur kas sunkiau nustatyti teisinį perkančiosios šalies statusą. Taigi, privatinės teisės požiūriu kyla vienas svarbesnių klausimų – ar sutarčių teisė pripažįsta anonimiškus sandorius? [8]

Vienas esminių principų, įtvirtintų Lietuvos Respublikos Civiliniame kodekse[9] yra pagrįstas nuostata, kad bendrąja taisykle sandoriai gali būti sudaryti nesilaikant jokios privalomosios formos. Kita vertus, itin svarbu tai, kad jeigu tai neprieštarauja imperatyviosioms teisės normoms, šalys gali susitarti, kad sutartyje privaloma nurodyti tikrąją šalių tapatybę.

---

[8] http://www.itc.tf.vu.lt/ ir http://www.google.lt/search?q=anonimi%C5%A1kumas+internete&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-US:official&client=firefox-a , Šalių anonimiškumo problema interneto kontekste (46 kb) Autorius: M.Civilka, prisijungimo laikas 2008-11-26 12:53;

[9] http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=322201&p_query=&p_tr2= , Lietuvos Respublikos Civilinis kodeksas, patvirtintas 2000-07-18 įstatymu Nr. VIII-1864;

Svarbu tai, kad Lietuvos Respublikos Civilinio kodekso[10] 6.188 straipsnis, reglamentuojantis vartojimo sutarčių ypatumus, nustato sąrašą preziumuojamai nesąžiningų vartojimo sandorio sąlygų, kurios suteikia pagrindą tokius sandorius ar sąlygas teismine tvarka pripažinti negaliojančiais. Vienas iš vartojimo sandorio pagrindu atsirandančių teisinių santykių ypatumų yra tas, kad viena tokių santykių šalių yra profesionali šalis ar verslininkas, o kita – vartotojas, tai yra asmuo, kuris tam tikrą produktą įsigyja ne savo profesinės, komercinės ir pan. veiklos tikslais. Taigi, tokia santykių prigimtis neišvengiamai suponuoja būtinybę šalims žinoti viena kitos teisinį statusą, padėtį vartotojo/profesionalios šalies dichotomijos aspektu nes, pvz., pardavėjas, neturintis protingų priemonių įsitikinti tuo, kad kita šalis – vartotojas, negali patirti neigiamų pasekmių, susijusių su vartotojų teisių apsauga.

Lietuvos Respublikos Civilinio kodekso 6.163[11] straipsnis, nustatantis šalių pareigas ikisutartinių santykių atžvilgiu, šalis įpareigoja atskleisti viena kitai joms žinomą informaciją, turinčią esminę reikšmę sutarties sudarymui. Vis dėlto, daugeliu atveju šalių asmens tapatybės negalima vertinti kaip sąlygos, esminės sutarties sudarymui.

Sandorių galiojimo prasme Lietuvos Respublikos Civilinis kodeksas[12] įtvirtina visą eilę teisinių reikalavimų, kuriuos galima sugrupuoti į tris grupes:

a) reikalavimai sandorio šalims (veiksnumas, teisnumas);

b) reikalavimai sandorio šalių valios išreiškimo formai;

c) reikalavimai sandorio turiniui.

Tam, kad viena šalis galėtų įsitikinti kitos šalies teisiniu subjektiškumu, visiškai nebūtinas kitos šalies tapatybės atskleidimas – teisinio subjektiškumo įvertinimas gali sekti iš kitų aplinkybių – sudarant sandorį internete, pardavėjas gali reikalauti, kad perkančioji šalis patvirtintų, jog ji atitinka kriterijus, keliamus veiksniam subjektui, pvz.: jog jam (jai) ne mažiau kaip 18 metų ir pan. Kitų dviejų reikalavimų atžvilgiu anonimiškumas taipogi nesukuria kažkokių išskirtinių problemų.

[10] http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=322201&p_query=&p_tr2= , Lietuvos Respublikos Civilinis kodeksas, patvirtintas 2000-07-18 įstatymu Nr. VIII-1864;
[11] Ten pat;
[12] Ten pat;

Taigi, apibendrintai galima teigti, kad vien tik tas faktas, kad sandoris sudaromas tarp asmenų, kurie net nežino vienas kito tapatybės, iš tokio sandorio neatima teisinės galios. Vis dėlto, esminės teisinės problemos yra susiję su absoliučiai anonimiškų sandorių įgyvendinimu[13]:

a) visiškai anonimiško sandorio atveju tampa labai apsunkintas pažeistų ar ginčijamų teisių gynimo, įgyvendinimo ar realizavimo mechanizmas;

b) Lietuvos Respublikos Civilinio kodekso[14] 1.76 straipsnio 2 dalis numato, kad jeigu sandoris buvo sudarytas panaudojant telekomunikacijų galinius įrenginius, tai visais atvejais privalo būti pakankamai duomenų sandorio šalims nustatyti. Jeigu tokių duomenų nėra, šalys, kilus ginčui, sandorio sudarymo faktui įrodyti negali remtis liudytojų parodymais; kaip matyti, ši Civilinio kodekso nuostata skiriama būtent elektroniniams sandoriams, tačiau ji pilna apimtimi taikytina tik visiškai anonimiškų sandorių atžvilgiu;

c) kaip jau minėta aukščiau, formalūs reikalavimai gali tapti kliūtimi įgyvendinant galiojančius anonimiškus sandorius. Kita vertus, tokį sandorį pripažinus negaliojančiu ab inintio, restitucija tampa praktiškai neįmanoma;

d) remiantis Lietuvos Respublikos Civilinio kodekso 1.92 straipsniu, gali būti pripažįstamas negaliojančiu įgaliojimus viršijusio atstovo sudarytas sandoris, jeigu atstovaujamasis nepatvirtino sandorio. Visiškai anonimiško sandorio atveju tampa problematiškas tokio sandorio pripažinimas negaliojančiu, kadangi atstovaujamasis nežino atstovo tapatybės;

e) tampa neįmanomas *actio Pauliana*, *actio negatoria* ir kitų specifinių reikalavimų patenkinimas;

f) kyla problemos tais atvejais, kai įstatymas įsakmiai reikalauja, jog prieš priverstine tvarka įgyvendinant savo teisę, šalis privalo apie tai įspėti sutartinių prievolių nevykdančiąją šalį;

---

[13] http://www.itc.tf.vu.lt/ ir http://www.google.lt/search?q=anonimi%C5%A1kumas+internete&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-US:official&client=firefox-a , Šalių anonimiškumo problema interneto kontekste (46 kb) Autorius: M.Civilka, prisijungimo laikas 2008-11-26 12:53;

[14] http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=322201&p_query=&p_tr2= , Lietuvos Respublikos Civilinis kodeksas, patvirtintas 2000-07-18 įstatymu Nr. VIII-1864;

g) Šalių patirties ir profesionalumo lygis yra itin reikšminga aplinkybė įvertinant šalių atsakomybę, vykdant savo sutartinius įsipareigojimus; absoliutais anonimiškumo atveju šios aplinkybės tinkamas įvertinimas tampa labai apsunkintu;

h) Visiškai anonimiško sandorio atveju tampa suvaržytas civilinės atsakomybės ir kitų teisinių gynybos priemonių praktinis pritaikymas.

Reziumuojant aukščiau pateiktą svarbesnių anonimiškumo teisinių padarinių sąrašą, tampa aišku, kad šalių tapatybė nėra esminė galiojančio sandorio sąlyga, tačiau jos nebuvimas labai apriboja praktinį absoliučiai anonimiško sandorio įgyvendinamumą ir tokiu būdu sumenkina jo teisinę vertę.

Analizuojant pusiau anonimiškus sandorius, galima pasiremti aukščiau pateiktais argumentais. Vis dėlto, galima išskirti šiuos specifinius pusiau anonimiškų sandorių įgyvendinimo ypatumus[15]:

a) vartojimo sandorio atžvilgiu itin svarbu tai, kad jeigu vartotojas, nurodydamas savo pseudonimą, nenurodo savo tikrojo statuso (tai yra, kad jis yra vartotojas), jis vėliau negali reikalauti pripažinti negaliojančiomis vartojimo sutarties sąlygas, prieštaraujančias sąžiningumo kriterijams;

b) pseudonimiškumas reikalauja trečiosios šalies, išduodančios pseudonimą ir jį susiejančios su konkrečiu asmeniu, įsikišimo. Vartotojas, kuris naudojasi tokio tarpininko paslaugomis tam, kad galėtų sudarinėti ir vykdyti pusiau anonimiškus sandorius internete, su tokiu tarpininku sudaro sutartį, aptariančią tokios trečiosios šalies atsakomybės pagrindai. Kyla klausimas, ar tokia trečioji šalis gali būti laikoma atsakinga už kokius nors pseudoniminio sandorio trūkumus? Išanalizavus tipines anonimizavimo sutarčių sąlygas, darytina išvada, kad tokių tarpininkavimo paslaugų teikėjai paprastai apriboja savo atsakomybę.

[15] http://www.itc.tf.vu.lt/ ir http://www.google.lt/search?q=anonimi%C5%A1kumas+internete&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-US:official&client=firefox-a , Šalių anonimiškumo problema interneto kontekste (46 kb) Autorius: M.Civilka, prisijungimo laikas 2008-11-26 12:53;

Atlikus šiuo metu galiojančių teisės normų analizę, galima daryti išvadą, kad dabartinis Lietuvoje veikiantis teisinis reguliavimas nėra pritaikytas anonimiškumui elektroninėje erdvėje, todėl galima siūlyti įstatymų leidėjui įvertinti dvi pagrindines išeitis:

1. Derinti šiuo metu galiojančias prekybos ir paslaugų taisykles prie elektroninės komercijos keliamų poreikių. Didžiausią dėmesį skirti anonimiškų vartotojų, ypatingai tų, kurie naudojasi elektroninėmis priemonėmis, teisių apsaugai.

2. Sukurti visiškai naują reguliacinę bazę, kuri reguliuotų visiškai anonimiškų sandorių keliamus poreikius, o taip pat konkretizuotų teises ir pareigas abiems sandorių pusėms.

3. ASMENS TAPATYBĖS VAGYSTĖ, KLASTOTĖ, ANONIMIŠKUMAS IR KYLANČIOS TEISINĖS PASEKMĖS

Vienas iš dažniausiai pasitaikančių nusikaltimų elektroninėje erdvėje yra tapatybės vagystė. Ji pasižymi bankų sąskaitų atidarymu svetima pavarde, asmens duomenų vagyste ir netgi pasų padirbinėjimu. Vien tik Didžiojoje Britanijoje tapatybės vagystės ekonomikai kasmet atneša nuostolius, siekiančius 1.7 mlrd. svarų, o grynųjų pinigų vogimas iš netinkamai saugomų banko sąskaitų – 14 mlrd. svarų. Apie 29.7 mlrd. svarų nuostolių atsiranda dėl lengvabūdiško elgesio asmenų, kurių korteles nusikaltėliai nukopijavo pasinaudodami išmestose ataskaitose surastais duomenimis. Tapatybės duomenų vagystės yra viena greičiausiai plintančių nusikalstamų veikų pasaulyje. Spartus šio pobūdžio nusikaltimų skaičiaus augimas susijęs su tuo, kad asmens duomenų vagims rizika būti pagautiems minimali, tuo tarpu pasipelnyti galima ypač sėkmingai. Prieš keletą metų tokios vagystės būdavo retenybė, tačiau dabar kiekvieną savaitę Europos sąjungos šalyse fiksuojami keli tokie atvejai. Sužinodami žmonių asmens kodus, kreditinių kortelių ar kitų asmeninių dokumentų duomenis, nusikaltėliai nesunkiai jais pasinaudoja. Pasisavinę asmens tapatybės duomenis, jie gali išsiimti pinigus iš svetimų banko sąskaitų, įsigyti naujas kreditines korteles, daryti užsakymus, apsipirkti ir pan. Kadangi tokiu būdu užvaldomas kito asmens gyvenimas, labai dažnai duomenų vagystės pasireiškia ir psichologiniu smurtu.

Amerikos tyrimų kompanijos *Gartner* duomenimis, asmens duomenų vagysčių skaičius nuo 2003 metų padidėjo 50 procentų. Apie 15 mln. amerikiečių per 2006 metus tapo šio nusikaltimo aukomis. Vidutinis nuostolis tenkantis vienai aukai padvigubėjo, kai tuo tarpu šių nuostolių susigrąžinimas sumažėjo 26 procentais lyginant su 2005 metų duomenimis. Tyrimo metu taip pat paaiškėjo, kad vidutinės išlaidos, tenkančios kiekvienam tokiam nusikaltimui išaiškinti, yra apie 8200 USD ir 600 darbo valandų.

2007 m. lapkritį Didžiosios Britanijos Biudžeto ir muitinės departamente buvo prarasti duomenys apie 25 mln. pretendentų į vaiko pašalpą, dar po savaitės dingo informacija apie 3 milijonus besimokančiųjų vairuoti, o 2008 m. sausio 9 d. Birmingame buvo pavogta maždaug 600 tūkst. žmonių duomenų. Pavogtajame nešiojamame kompiuteryje buvo asmeninė informacija apie maždaug 600 tūkst. žmonių, kurie arba išreiškė norą įstoti, arba jau yra įstoję į Karališkojo jūrų laivyno, Karališkųjų jūrų pėstininkų ar Karališkųjų oro pajėgų gretas. Kaip pranešė Didžiosios Britanijos Gynybos ministerijos atstovai, išsamesni asmens tapatybės duomenys buvo jau pateikusių prašymą stoti į Pajėgas asmenų duomenys: paso informacija, draudimo numeris, vairuotojo pažymėjimo detalės, šeimos duomenys, gydytojų adresai ir sveikatos pažymėjimo numeris[16].

Beveik kiekvieną dieną mums reikia tapatybę įrodyti ir kitiems asmenims ar kompiuterių sistemoms, kai tvarkome savo finansus banke ar pasiimame pinigus iš bankomato, kertant valstybių sienas arba tiesiog pasitikrinant savo elektroninio pašto dėžutę. Nurodžius galiojančius kito asmens vartotojo vardą ir slaptažodį, kompiuterių sistemos traktuos tokį vartotoją kaip teisėtą ir suteiks prieigą prie visų tikrajam vartotojui pasiekiamų duomenų. Jei kitas asmuo pasinaudotų mūsų tapatybės įrodymo identifikatoriais, jis galėtų apsimesti mumis ir pasinaudoti tik mums skirtais ištekliais. Taigi tapatybės vagystė yra pasinaudojimas kito asmens tapatybės identifikatoriais ir veikimas jo vardu ir teisėmis.

Tapatybės vagystės ar klastotės pasekmės yra neigiamos ir dažniausiai susijusios su didesniais ar mažesniais nuostoliais. 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 vartotojo identifikatorių ir slaptažodžius. Jei tokie vartotojų identifikatoriai ir slaptažodžiai patektų

[16] http://www.bernardinai.lt/index.php?url=articles/72769 , prisijungimo laikas 2008-10-25 16:53;

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 asmeninė 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 pažymėjimas gali būti parduotas asmeniui, kuriam yra atimta teisė vairuoti.

Bet kuriuo tapatybės vagystės atveju bus sugaišta daug brangaus laiko įrodymų rinkimui, kad įrodyti, jog 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.

3.1. ASMENS TAPATYBĖS VAGYSTĖ

Beveik kiekvieną dieną mums reikia tapatybę įrodyti tiek kitiems asmenims, tiek kompiuterių sistemoms, kai tvarkome savo finansus banke ar pasiimame pinigus iš bankomato, kertant valstybių sienas arba tiesiog pasitikrinant savo elektroninio pašto dėžutę. Nurodžius galiojančius kito asmens vartotojo vardą ir slaptažodį, kompiuterių sistemos traktuos tokį vartotoją kaip teisėtą ir suteiks prieigą prie visų tikrajam vartotojui pasiekiamų duomenų. Jei kitas asmuo pasinaudotų mūsų tapatybės įrodymo identifikatoriais, jis galėtų apsimesti mumis ir pasinaudoti tik mums skirtais ištekliais. Taigi tapatybės vagystė yra pasinaudojimas kito asmens tapatybės identifikatoriais ir veikimas jo vardu ir teisėmis.

Neteisėtas pasinaudojimas asmens tapatybės duomenimis (pavarde, vardu, gimimo data) reiškia, kad pažeidėjas naudojasi kito asmens tapatybės duomenimis, pvz., kai asmuo naudojasi svetimu tapatybės dokumentu padarydamas žalą tikrajam jo savininkui.

Sužinojęs apie neteisėtą naudojimąsi asmens tapatybės duomenimis, suinteresuotas asmuo turėtų kreiptis į artimiausią policijos įstaigą, pateikti savo duomenis, tapatybės dokumente nurodytą informaciją ir, jeigu leidžiama pagal nacionalinę teisę, pirštų atspaudus bei nuotraukas.

Tokiu atveju specialus SIS mechanizmas užtikrina, kad atlikus paiešką duomenų bazėje, sistema nurodo, jog turi būti kreipiamasi į nacionalinį SIRENE biurą siekiant patikrinti, ar tikrinamo asmens duomenys yra tikri, ir ar jis yra nukentėjęs nuo tapatybės duomenų vagystės.

Tvarkant nukentėjusio nuo neteisėto pasinaudojimo tapatybės duomenimis, asmens duomenis būtinas aiškus šio asmens sutikimas, o tokie duomenys gali būti naudojami tik siekiant nustatyti tikrąją tikrinamo asmens tapatybę, jokiais kitais tikslais. Asmens tapatybės vagystė apskritai nustatoma kaip neteisėtas tapatybės duomenų pasisavinimas (tokių kaip vardas, pavardė, gimimo data, gyvenamoji vieta ar buvusios gyvenamosios vietos) iš kito asmens, kuris apie tai nežino ir net neįtaria apie tai. Šitie tapatybės duomenys yra naudojami tada, kai norima apsimetus kitu asmeniu, jo vardu pirkti įvairias prekes[17]. Tapatybės klastotė kaip sukčiavimas (apsimetant kitu asmeniu) kartais yra naudojama kaip sinonimas, nors pati sukčiavimo apsimetant kita tapatybe sąvoka taip pat apima melagingą (išgalvotą, nebūtinai realiai egzistuojančią) tapatybę. Asmens tapatybės vagystė (taip pat ir Asmens tapatybės klastotė), kaip šiuolaikinis reiškinys prasidėjo ir išpopuliarėjo JAV ir Kanadoje. Tačiau, šiuo metu, tai vis didėjanti problema Europoje, įtraukianti į tai vis didesnį skaičių asmenų.

Apmokėjimo srityje tokio pobūdžio sukčiavimai daro didelę neigiamą įtaką proceso dalyviams, o dažniausiai nukentėjusiesiems asmenims (finansinės įstaigos ir apmokėjimų naudotojai: tiek fiziniai, tiek juridiniai asmenys), t.y. tiems asmenims, kurie patiria ne tiktai įprastą finansinę žalą. Iš tikrųjų, emociniai nuostoliai ir padaryta žala dėl asmens vardo panaudojimo, jo reputacijos gali būti didžiuliai.

Padidėjęs nusikalstamų veikų, susijusių su Asmens tapatybės vagystėmis, lygis aiškinamas tuo, jog tokią veiklą sąlyginai yra sunku aptikti ir nustatyti, o dar didesnėje dalyje atvejų tirti ir pritaikyti baudžiamojo poveikio priemones.

Ypatingai JAV pastaruoju metu asmens tapatybės vagystės, kai nusikaltėliai, turėdami tikslą identifikuotis kitais asmenimis, naudoja pagrobtus asmens duomenis "*personally*

[17] CIFAS, the UK Fraud Prevention Service 2008-09-28 http://ec.europa.eu/internal_market/fpeg/identity-theft_en.htm , prisijungimo laikas 2008-10-25 16:53;

identifiable information (PII)“, kaip pvz.: kreditinės kortelės ar socialinio draudimo pažymėjimas, kelia didelį susirūpinimą. Didžiulis asmens tapatybių vagysčių skaičius JAV buvo fiksuotas 2005 metais, kai preliminariais duomenimis, buvo įvykdyta apie 1 mln. tokių vagysčių[18]. Daugelis sieja tokias vagystes su Internetu, tačiau tyrimai ir apklausos parodė priešingai. Daugumas nukentėjusių žmonių nurodė Internetą kaip priemonę vogti tapatybės duomenis. Tai būtų galima paaiškinti taip, kad daugumas nukentėjusiųjų net nežino apie naudojimosi Internetiniu ryšiu galimybes, ypatingai apie praktiką, kuri vadinama „*PHISHING*“.

Nežiūrint į paplitusią nuomonę, kad Internetas yra pagrindinis padaugėjusių asmens tapatybės vagysčių kaltininkas, tyrimai rodo, jog sąlyginai mažai žmonių žino kaip vagys pagrobė jo asmens tapatybės duomenis (*personally identifiable information (PII)*). Ta mažuma vieningai nurodo, jog asmens tapatybės duomenys (PII) buvo pagrobti per Internetą.

Specialistai nurodo kelis asmens tapatybės duomenų grobimo metodus: nesinaudojant programine įranga - kai nusikaltėliai užvaldo asmens duomenis nesinaudodami technologijomis (vagysčių metu (pavogus piniginę ar apvogus butą) ir radybų metu) bei panaudojus programinę įrangą (pasitelkus „Phishing“ technologijas (netikras svetaines, elektroninius laiškus su nuorodomis) bei virusines programas).

Kompiuteriniai nusikaltimai nebūtinai turi būti padaromi per Internetą, jie gali būti įvykdyti per prastą duomenų apsaugą ar kompiuterinių tinklų apsaugos taisyklių pažeidimus (pavyzdžiui kai nusikaltimą padaro įmonės darbuotojas). Pavyzdžiui: 2004 m. spalį Kalifornijos (JAV) universiteto tinkle buvo paviešinti 1.4 mln. žmonių, dalyvavusių Kalifornijos valstijos namų saugumo programoje („*home care program*“) asmens tapatybės duomenys: vardai, pavardės, adresai, gimimo datos, telefonų numeriai, socialinio draudimo pažymėjimų numeriai) [19].

Tapatybės vagystėmis yra siekiama gauti prieiga. 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

[18] http://italy.usembassy.gov/pdf/other/RS22082.pdf , prisijungimo laikas 2008-11-02 15:15;

[19] http://www.usatoday.com/tech/news/computersecurity/hacking/2005-02-16-choicepoint-hacked_x.htm , prisijungimo laikas 2008-11-02 16:25;

ar patalpas, darbuotojų pažymėjimai, įeigos kontrolės kortelės ir apsauginės signalizacijos atjungimo kodai taip pat gali tapti nusikaltėlių taikiniu. Tai ypač aktualu kritinės infrastruktūros objektų apsaugai: elektros ir vandentiekio tiekimo sistemoms, traukinių ir lėktuvų valdymo įrangai.

Tapatybės vagystę dažniausiai yra sunku nustatyti prieš prasidedant neigiamoms pasekmėms. Jei sąskaita jūsų banke pradeda mažėti, o stambesnių įsigijimų nebuvo daryta, galima įtarti, kad kažkas neteisėtai naudojasi Jūsų sąskaita. Tai taip pat gali būti banko apskaitos klaida, tačiau patikimuose ir dideliuose bankuose tai įvyksta retai. Prašymai apmokėti už prekes ar paslaugas, kurių neužsisakėte, taip pat nurodo, kad galėjo būti įvykdyta tapatybės vagystė. Jei prekes užsisakėte interneto parduotuvėje, o prekės nėra pristatytos laiku, pats laikas pasitikrinti savo banko sąskaitą, ar ji nėra ištuštinta. Padidėjusios sąskaitos už internetu teikiamas apmokestinamas paslaugas arba jų teikimo nutraukimas gali reikšti, kad tomis paslaugomis naudojasi dar kažkas. Taip pat galima sulaukti telefono skambučių arba elektroninio pašto laiškų, su prašymais suteikti prekių ar paslaugų, už kurias jau buvo sumokėta. Teisėsaugos institucijų reikalavimai pasiaiškinti už nusikalstamą Jūsų vardu atliktą veiklą vienareikšmiškai reiškia, kad jūsų tapatybe pasinaudojo kiti.

Nusikaltėliai gali perskaityti elektroninio pašto žinutes arba pasiklausyti telefonu perduodamos informacijos, Tapatybės nustatymo duomenys taip pat gali būti nugirsti per pašnekesį viešose vietose. Jei prie kompiuterio ir jame saugomų duomenų gali prieiti pašaliniai asmenys arba kompiuteris nėra tinkamai apsaugotas nuo nesankcionuoto prisijungimo per internets kompiuteryje saugomi tapatybės duomenys (identifikatoriai, slaptažodžiai) gali patekti į svetimas rankas. Jei tapatybės duomenys yra saugomi centralizuotoje duomenų bazėje, neteisėtai prie jos prisijungus galima daugelio asmenų tapatybės vagystė.

Be to, visada yra tikimybė, kad tapatybės duomenų prieigą turintys nesąžiningi darbuotojai (registrų prižiūrėtojai ar kompiuterių tinklų administratoriai), neteisėtai pasinaudos duomenimis, kuriuos jie turi saugoti.

Kai kurie tapatybės nustatymo duomenų surinkimo būdai yra labai paprasti. Su jumis tiesiogiai, telefonu ar elektroniniu paštu bendraujantis asmuo gali tiesiog paprašyti pasakyti jam PIN kodą, slaptažodį ar kitokios svarbios informacijos. Nors tai ir atrodo neįtikėtina, tačiau kai kurie žmonės net nesusimąstę suteikia tokią informaciją visiškai nepažįstamiems asmenims, kurie prisistato kito asmens vardu ir teigia atstovaujantys realiai arba išgalvotai įstaigai. Tai yra

vadinamoji socialinė inžinerija. Taip nesąžiningi asmenys gali išgauti svarbią finansinę, asmeninę arba konfidencialią informaciją ir ja pasinaudoti savais tikslais. Kad prieš asmenį naudojama socialinės inžinerijos ataka, galima nuspėti, jei pateikiami per daug patrauklūs pasiūlymai, užduodami neįprasti prašymai, prašoma pateikti asmeninę informaciją, prašomą informaciją reikia pateikti kiek galima skubiau, nurodomos jūsų bendradarbių arba pažįstamų pavardės, atsisakymo pateikti informaciją grasinama pasiskųsti jūsų vadovybei.

Kitas populiarus socialinės inžinerijos būdas yra vadinamoji „žvejyba“ (*angl. phishing*). Internetinės bankininkystės vartotojams elektroniniais laiškais yra išsiuntinėjama informacija, kad vyksta sistemos pertvarkymas ir visi vartotojai turi atnaujinti savo duomenis. Elektroniniame laiške yra pateikiama nuoroda į banko tinklapį. Spustelėjus tokią nuorodą yra patenkama į tinklapį, kuris visiškai neskiria nuo internetinės bankininkystės tinklapio ir jame prašoma įvesti vartotojo vardą ir slaptažodį. Tačiau iš tikrųjų toks tinklapis yra tik banko tinklapio kopija ir per jį yra siekiama neleistinai sužinoti banko klientų identifikatorius ir slaptažodžius.

3.2. ASMENS TAPATYBĖS KLASTOTĖ IR ANONIMIŠKUMAS

Tapatybės klastotė yra neteisėtai įgytos asmens tapatybės (pavogtos ar surastos) neteisėtas panaudojimas, siekiant apsimesti kitu asmeniu ir gauti iš to naudos sau ar kitiems. Tai paprastai yra susiję su asmens tapatybę patvirtinančių dokumentų, tokių kaip asmens tapatybės kortelė, asmens pasas, vairuotojo ar Sodros pažymėjimas, praradimu, pametimu ar vagyste.

Specialistai išskiria du asmens tapatybės klastojimo būdus:

a) techninė klastotė;

b) psiaudoklastotė.

Techninę klastotę Policijos departamento specialistai nusako kaip būdą nuslėpti tikrąją tapatybę, pasinaudojus tam tikrom, būtent tam sukurtom, techninėm priemonėm (pvz. naudoti ne savo IP adresus, svetimus proxy serverius, įvairius anonimizatorius), kad būtų neįmanoma visiškai nustatyti tikrosios tapatybės. Paprastai tokiomis priemonėmis naudojasi asmenys, gerai

išmanantys programavimo subtilybes ir siekiantys neteisėtų tikslų, iš anksto gerai pasiruošę ir gerai apgalvoję savo veiksmus bei linkę išlikti anonimiški ir nenustatyti teisėssaugos įstaigų pareigūnų. Nustatyti tokių asmenų tapatybę yra arba be galo sunku, arba net visiškai neįmanoma.

Psiaudoklastotę arba netikrą klastotę Policijos departamento specialistai nurodė, kai asmuo pasivadinės susigalvotu psiaudonimu (*angl. Nick*) ar išgalvotu vardu arba svetimu vardu, mano ar bent tikisi, jog niekas jo tikrosios asmenybės nenustatys, ir net nesuvokia, jog techninėmis priemonėmis tai galima sėkmingai nustatyti. Tokiu budu savo tapatybę paprastai slepia vaikai ar mažai išsilavinę ir neturintys didelio supratimo apie galimybę nustatyti asmens tapatybę techninėmis priemonėmis asmenys. Psiaudoklastotė dažniausiai naudojama iš pykčio, siekiant kažką apšmeižti, paskleisti paskalas ar atkeršyti.

Tačiau psiaudoklastotę kai kuriais atvejais galima prilyginti ir anonimiškumui. Juk pasivadinęs kitu vardu ar psiaudonimu asmuo stengiasi išlikti anonimiškas. Nėra tokio teisės akto, kuris įpareigotų asmenį, dalyvaujantį forumuose, jog jis pateiktų savo tikrus anketinius duomenis, o tie duomenys dar papildomomis priemonėmis būtų sulyginami su duomenų bazėmis. Gana dažnas internautas diskusijų forumuose ar straipsnių įvairiuose žinių portaluose komentarų skelbėjas nenori nurodyti savo tikro vardo ar kitų savo asmens duomenų. Kiekvienas turime teisę į anonimiškumą. Tačiau teisė į anonimiškumą nėra absoliuti ir negali būti absoliučiai anonimiška elektroninėje erdvėje[20]. Lietuvos Respublikos konstitucijos 22 straipsnyje ir Žmogaus teisių apsaugos ir pagrindinių laisvių konvencijos 2 dalies 8-tame straipsnyje yra numatyta, kad atsiradus tam tikroms aplinkybėms žmogaus teisės gali būti ribojamos. Konstitucija nustato, kad informacija apie asmeninį gyvenimą gali būti renkama tiktai argumentuota Teismo nutartimi ir tiktai įstatymų numatytais atvejais. Žmogaus teisių apsaugos ir pagrindinių laisvių konvencija nustato, kad valstybinės institucijos neturi teisės riboti žmogaus teisių, išskyrus atvejus, kai, įstatymų numatytais pagrindais, tai yra būtina valstybės ir visuomenės saugumui bei ekonominiam gerbūviui, užkardyti teisėtvarkos pažeidimus ir nusikaltimus, o taip pat kai tai yra būtina sveikatos apsaugai, etikai bei kitoms žmogaus teisėms ir laisvėms užtikrinti.

Akivaizdu, kad išankstinė sąlyga apribojant asmens teisę į anonimiškumą atsižvelgiant į viešąjį interesą yra ta, kad bet kokio tipo apribojimai būtų proporcingi siekiamam juridiniam tikslui. Ne paslaptis, kad nusikaltėliai visaip bando pateisinti savo elektroninį bendravimą,

[20] Legal privacy, De la presente edicion, Prensas Universitarias de Zaragoza, 2008. Limitation of the right to anonymity as a partof the right to privacy in cyberspace for the suppression of terrorism in the Republic of Lithuania. Rimantas Petrauskas and Kristina Spalveters, p. 293-303.

prisidengdami žmogaus teisėmis, tačiau valstybės ir visuomenės saugumas visados lieka prioritetinė sritis. Būtent todėl visiškas anonimiškumas elektroninėje erdvėje darosi neįmanomas. 1995 metų deklaracija La Gomera teigia, kad teroras yra vienas iš pagrindinių demokratijos ir teisės viršenybės pažeidimų. 2003 m. gruodžio 12 d. Europos saugumo strategija įvardina terorizmą viena didžiausių šio amžiaus grėsmių.

Kalbant apie teisių apribojimą anonimiškai būti elektroninėje erdvėje, kad užkardyti terorizmą, galima pažymėti, kad Lietuvos Respublikos baudžiamajame kodekse nėra nei tikslaus terorizmo apibrėžimo nei terorozmo apibūdinimo kaip nusikalstamos veikos (išskyrus patį teroro aktą), todėl Lietuvoje netinkamai įgyvendinamas proporcingas ir sąžiningas teisės į anonimiškumą kibernetinėje erdvėje apribojimas.

Europos Sąjungos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje, teigia, kad: "Valstybės narės užtikrina pranešimų ir su jais susijusių srauto duomenų, perduodamų per viešųjų ryšių tinklą ir teikiant viešai prieinamas elektroninių ryšių paslaugas, konfidencialumą, taikydamos nacionalinės teisės aktus. Klausymas, filmavimas, duomenų rinkimas ar perėmimo ir duomenų srauto kontrolė be šių duomenų tiesioginio naudotojo sutikimo yra draudžiami. Valstybėms narėms pavesta savo teisės normų pagalba uždrausti klausytis, įrašyti, kaupti ar kitu būdu perimti arba sekti pranešimus ir duomenų srautus, o taip pat perduoti juos kitiems nei naudotojai asmenims, be pačių naudotojų sutikimo.

Srauto duomenys, susiję su abonentais ir naudotojais, po apdorojimo ir saugojimo viešai prieinamų elektroninių ryšių paslaugų teikėjo turi būti sunaikinami arba padaromi anoniminiais. Tačiau, teisė į anonimiškumą gali būti apribota, jei toks ribojimas yra būtina, tinkama ir proporcinga priemonė demokratinėje visuomenėje siekiant užtikrinti nacionalinį saugumą (t.y. valstybės saugumą), gynybą, visuomenės saugumą ir nusikaltimų prevenciją bei tyrimą.

Europos konvencijos dėl elektroninių nusikaltimų, priimtos 2001 metais, taryba be įprastų procedūrų elektroninėje erdvėje tokių kaip krata ir turto areštas, ėmėsi naujų priemonių, kad užtikrinti eksploatuojamų duomenų sulaikymą, kas turėtų garantuoti, kad įprastos priemonės rinkti įrodymams būtų taip pat veiksmingos ir elektroninėje erdvėje. Įprastos įrodymų rinkimo priemonės, tokios kaip duomenų srauto kaupimas realiuoju laiku ir perimami duomenų srautai yra naudojami siekiant surinkti duomenis informacijos perdavimo proceso metu.

Lietuvos Respublikos Baudžiamojo proceso kodekso 154 straipsnyje yra numatyta galimybė kontroliuoti informaciją, perduodamą elektroninėje erdvėje, ir daryti tokios informacijos įrašus, tikslu – rinkti įrodymus ikiteisminio tyrimo metu.

Pagal Lietuvos Respublikos Operatyvinės veiklos įstatymą, Elektroninių ryšių operatoriai ir paslaugų tiekėjai privalo pateikti duomenis, gaunamus bendraujant elektroninėje erdvėje, reikalingus operatyviniam tyrimui, tiktai motyvuotu teismo sprendimu, priimtu remiantis operatyvinio subjekto, atliekančio operatyvinį tyrimą, motyvuotu teikimu.

Lietuvos Respublikos Operatyvinės veiklos įstatymas Elektroninių ryšių operatorius ir paslaugų tiekėjus įpareigoja užtikrinti technines galimybes kontroliuoti informacijos, perduodamos per elektroninių ryšių tinklus, turinį. Lietuvos Respublikos Elektroninių ryšių įstatymas numato, kad esant motyvuotam teismo sprendimui, įmonės, teikiančios elektroninių ryšių tinklų prieigas ar paslaugas privalo teikti operatyvinėms tarnyboms duomenis apie ryšius, tokius kaip duomenų srauto rinkimas realiu laiku ir duomenų turinio perėmimas, kad užtikrinti duomenų rinkimą informacijos perdavimo metu.

Lietuvos Respublikos Elektroninių ryšių įstatymo 77 straipsnyje yra nustatytos Elektroninių ryšių srautų priežiūros ir stebėjimo teisės bei pareigos ūkio subjektams. Ūkio subjektai, teikiantys elektroninių ryšių tinklus ir (ar) paslaugas, turi teisę fiksuoti ir saugoti elektroninių ryšių įvykius ir jų dalyvius tik tiek, kiek yra būtina šių ūkio subjektų ūkinei veiklai užtikrinti. Ūkio subjektai, teikiantys elektroninių ryšių tinklus ir (ar) paslaugas, privalo įstatymų nustatyta tvarka turimą ir nusikalstamoms veikoms užkardyti, tirti, nustatyti reikalingą informaciją pateikti operatyvinės veiklos subjektų pagrindinėms institucijoms, Vyriausybės nurodytoms ikiteisminio tyrimo įstaigoms, prokurorui, teismui ar teisėjui. Šią informaciją ūkio subjektai, teikiantys elektroninių ryšių tinklus ir (ar) paslaugas, neatlygintinai teikia operatyvinės veiklos subjektų pagrindinėms institucijoms, Vyriausybės nurodytoms ikiteisminio tyrimo įstaigoms pagal jų paklausimus elektroniniu būdu ir nedelsdami. Vyriausybės nurodytos ikiteisminio tyrimo įstaigos Vyriausybės nustatyta tvarka organizuoja ir sudaro galimybę gauti šią informaciją savo padaliniams ir (ar) kitoms ikiteisminio tyrimo įstaigoms. Visi asmenys, dalyvaujantys keičiantis duomenimis, Vyriausybės nustatyta tvarka ir sąlygomis imasi būtinų priemonių duomenų saugumui užtikrinti, o tam reikalinga papildoma įranga įsigyjama ir išlaikoma valstybės lėšomis. Jeigu ikiteisminiame tyrime reikia patvirtinti ūkio subjekto, teikiančio elektroninių ryšių tinklus ir (ar) paslaugas informacijos tikslumą, ikiteisminio tyrimo

pareigūnas tiesiogiai raštu kreipiasi į ūkio subjektą ir gauna atsakymą raštu. Ūkio subjektai, teikiantys elektroninių ryšių tinklus ir (ar) paslaugas, elektroninių ryšių metu naudojamą techninę informaciją saugo tiek, kiek reikia jų ūkinei veiklai užtikrinti, bet ne ilgiau kaip 6 mėnesius, išskyrus nustatytus atvejus[21], taip pat, jeigu ši informacija reikalinga operatyvinės veiklos subjektams, ikiteisminio tyrimo įstaigoms, prokurorui, teismui ar teisėjui nusikalstamoms veikoms užkardyti, tirti, nustatyti, Vyriausybės įgaliotos institucijos – operatyvinės veiklos subjekto – nurodymu ūkio subjektai, teikiantys elektroninių ryšių tinklus ir (ar) paslaugas, turi tokią informaciją saugoti ilgiau, bet ne ilgiau kaip 6 mėnesius papildomai. Už tokios informacijos saugojimą apmokama valstybės lėšomis Vyriausybės nustatyta tvarka.

Kai yra motyvuota teismo nutartis, ūkio subjektai, teikiantys elektroninių ryšių tinklus ir (ar) paslaugas, privalo sudaryti techninę galimybę operatyvinės veiklos subjektams įstatymų nustatyta tvarka, o ikiteisminio tyrimo įstaigoms – Baudžiamojo proceso kodekso nustatyta tvarka, kontroliuoti elektroninių ryšių tinklais perduodamos informacijos turinį. Tam reikalinga įranga įsigyjama ir išlaikoma valstybės lėšomis.

Vyriausybės įgaliota institucija – operatyvinės veiklos subjektas – organizuoja ir Vyriausybės nustatyta tvarka kiekvienam operatyvinės veiklos subjektui, o baudžiamajame procese – ir ikiteisminio tyrimo įstaigai, sudaro technines galimybes savarankiškai kontroliuoti elektroninių ryšių tinklais perduodamos informacijos turinį.

Ūkio subjektai, teikiantys elektroninių ryšių tinklus ir (ar) paslaugas, apie savo tinkle ar savo ir kitų elektroninių ryšių operatorių sujungimo taškuose numatomus daryti pakeitimus, galinčius turėti įtakos įrangos, veikimui ir pateikiamos informacijos kiekiui, privalo Vyriausybės įgaliotai institucijai – operatyvinės veiklos subjektui – ir Ryšių reguliavimo tarnybai pranešti, kai tik apie tai sužino.

Elektroninių ryšių tinklu siunčiamos techninės komandos pradėti ar nutraukti pasiklausymą ar kitą elektroninių ryšių tinklais perduodamos informacijos kontrolę saugomos Vyriausybės įgaliotos institucijos – operatyvinės veiklos subjekto – patalpose taip, kad komandų duomenų negalėtų pakeisti jas siuntusi Vyriausybės įgaliota institucija ar komandą gavęs ūkio subjektas. Šios dalies nuostatų įgyvendinimą kontroliuoja Lietuvos Respublikos generalinis prokuroras ar jo įgaliotas prokuroras.

---

[21] http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=331096&p_query=&p_tr2 LIETUVOS RESPUBLIKOS, ELEKTRONINIŲ RYŠIŲ, ĮSTATYMAS, 2004 m. balandžio 15 d. Nr. IX-2135, Vilnius

Nustatytos ribos riboja žmogaus teisę likti anonimu elektroninėje erdvėje, leidžiama rinkti asmens tapatybės duomenis, siekiant išaiškinti padarytą nusikalstamą veiką.

4. ASMENS TAPATYBĖS NUSTATYMAS

Beveik kiekvieną dieną mums reikia tapatybę įrodyti tiek kitiems asmenims, tiek kompiuterių sistemoms, kai tvarkome savo finansus banke ar pasiimame pinigus iš bankomato, kertant valstybių sienas arba tiesiog pasitikrinant savo elektroninio pašto dėžutę. Nurodžius galiojančius kito asmens vartotojo vardą ir slaptažodį, kompiuterių sistemos traktuos tokį vartotoją kaip teisėtą ir suteiks prieigą prie visų tikrajam vartotojui pasiekiamų duomenų. Jei kitas asmuo pasinaudotų mūsų tapatybės įrodymo identifikatoriais, jis galėtų apsimesti mumis ir pasinaudoti tik mums skirtais ištekliais.

Valstybės, savivaldos institucijos, įmonės bei pavieniai asmenys, teikdami informacines paslaugas, įgyvendindami elektroninius atsiskaitymus, siųsdami ir gaudami elektroninius laiškus, vykdydami įvairias marketingo akcijas, siūlo užpildyti įvairias anketas, renka, kaupia, apdoroja ir platina informaciją, taip pat ir fizinių bei juridinių asmenų duomenis. Informacija ir duomenys yra renkami pačiais įvairiausiais būdais: anketavimo, apklausų, socialinių tyrimų procedūrų realizavimo metu ir t.t.. Kita asmens duomenų teikimo bei rinkimo procedūra – kai veiksmas vyksta betarpiškai tarp asmens duomenų subjekto ir duomenų rinkėjo – tai pirkimo elektroninėse parduotuvėse procedūros, bilietų ir viešbučių rezervavimas, elektroniniai atsiskaitymai, bankinės paslaugos internetu. Daugumoje atvejų, kuomet duomenų subjektas įvykdo pirkimą arba naudojasi paslauga (pvz., prenumerata), yra privaloma pateikti asmens duomenis pardavėjui arba paslaugos teikėjui, siekiant patvirtinti pirkėjo autentiškumą, suteikti apmokėjimo garantijas, bei fizinį arba elektroninį adresą prekių bei paslaugų pristatymui.

4.1. ASMENS TAPATYBĖS NUSTATYMO BŪDAI (IDENTIFIKAVIMAS)

Asmens tapatybės identifikavimą (angl. *Personal identity*), pasitelkę tarptautinių žodžių žodynus kitaip galime apibrėžti kaip „Asmens tapatybės nustatymą“. Kitaip sakant, asmens identifikavimas yra tiesiog pripažinimas juo pačiu arba nustatymas esant jį būtent tuo pačiu. Bendrąja prasme identifikacija (nuo lotyniško žodžio indentificare) – tai kokio nors objekto (daikto, žmogaus ir pan.) tapatybės nustatymas, sutapatinimas. Taigi, identifikacija kriminalistikoje – objektų tapatybės nustatymas pagal jų paliktus pėdsakus arba kitokius atspindžius, siekiant išaiškinti asmenis bei daiktus, susijusius su tiriamuoju įvykiu[22]. Kyla klausimas: kam reikalingas tas asmens tapatybės identifikavimas Internete? Elektroninės parduotuvės, kai kurios paieškos sistemos, elektroniniai atsiskaitymai, žaidimai Internete ar tinkle – tai tik keletas Interneto paslaugų pavyzdžių. Visos jos pasižymi reikalavimu identifikuotis (atskleisti savo tapatybę) bei potencialia galimybe itin greitai ir efektyviai rinkti bei platinti vartotojų duomenis.

Kiekvienas asmuo, naudodamasis Internetu, aplankytoje interneto erdvėje palieka savo skaitmeninį pėdsaką. Kadangi vis didesnė socialinio elgesio dalis yra įgyvendinama būtent internete, vis daugiau vartotojų veiklos ir elgesio yra įrašoma. Bet pavojai asmeniniam privatumui slypi ne tik milžiniškame informacijos, esančios internete, kiekyje, tačiau programinėje įrangoje, kuri įgalina atlikti paiešką internete ir surinkti į vieną vietą visus duomenis apie vieną konkretų individą. JAV praktikoje buvo susiklosčiusi situacija, kada programinės įrangos pagalba buvo sukompiliuota detali biografija apie atsitiktinai pasirinktą asmenį ir panaudojant informaciją, surinktą iš visų diskusijų forumų ir grupių, kuriose tik dalyvavo tas asmuo, sužinotas asmens adresas, telefono numeris, gimimo vieta, studijų vieta, profesija, dabartinė darbovietė, domėjimasis teatru, mėgstamiausia alaus rūšis ir restoranas, atostogų praleidimo būdai[23]. JAV teismuose nagrinėta byla *McVeigh v Cohen*[24] puikiai iliustruoja pavojus, kuriuos internetas sukelia individų privatumui. Ieškovas, JAV povandeninio laivo jūreivis, nusiuntė elektroninį pranešimą civilinio jūrų laivyno darbuotojai, jos prašydamas nurodyti vaikų, esančių laive, amžių tam, kad jis galėtų suorganizuoti žaislų atidavimą. Tačiau ji neatpažino jo elektroninio pašto adreso, todėl sukontaktavo su IAP-AQL, kuris jai atsiuntė

[22] Kurapka E., Malevski H., Palskys E., Kuklianskis S. Kriminalistikos technikos pagrindai,-Vilnius, 1998.P.16.

[23] Asmens duomenų apsauga Tarptautinėje teisėje http://www.itc.tf.vu.lt/paskaitos/paskait/ada_1.12.pdf ; prisijungimo laikas 2008-10-08 20:20;

[24] http://lw.bna.com/lw/19980210/98116.htm ; prisijungimo laikas 2008-10-15 16:53;

naudotojo dosjė. Be kitų dalykų, dosjė buvo nurodytas vedybinis jūreivio statusas – gėjus. Ši informacija buvo perduota McVeigh vadui, ko pasekoje pastarasis buvo atleistas iš pareigų.

Taigi, asmens tapatybę Internete galima identifikuoti keliais būdais: pasitelkus programavimą (specialiąsias programas, kurios gali rinkti asmens duomenis) ir pasitelkiant trečiuosius asmenis.

Identifikavimo kriterijus užtikrinamas pasitelkiant trečiąjį asmenį – sertifikavimo paslaugų teikėją, kuris per išduodamą sertifikatą (liudijimą) susieja pasirašančio asmens tapatybę (ja sertifikavimo paslaugų teikėjas įsitikina (Elektroninio parašo įstatymo 4 str. 2 d.)) su parašo formavimo ir tikrinimo duomenimis bei suteikia galimybę bet kam susipažinti su sertifikatu ir šiame įrašytų tikrinimo duomenų pagalba įsitikinti, jog pasirašęs asmuo yra tas pats, kuris save tokiu nurodo. Siekiant geriau ginti parašo naudotojų teises yra reglamentuojamas kvalifikuotas sertifikatas, kuriame nurodomai informacijai ir kurio išdavėjui (sertifikavimo paslaugų teikėjui) keliami papildomi reikalavimai, tačiau tai, kad parašas neparemtas kvalifikuotu sertifikatu dar automatiškai neatima iš šio parašo juridinės galios.

Fizinis asmuo paprastai identifikuojamas pagal tokią informaciją kaip vardas, pavardė, amžius, gimimo data, akių spalva ir t. t. arba pagal jam suteiktą tam tikrą numerį (kodą), pavyzdžiui, asmens kodą, vairuotojo pažymėjimo, socialinio draudimo, kreditinės kortelės numerį. Asmens duomenys tarsi sugrupuojami į dvi kategorijas: identifikatorius ir kitus duomenis. Identifikatoriai tiesiogiai ir vienareikšmiškai nurodo konkretų asmenį. Tipiškiausias identifikatoriaus pavyzdys – asmens kodas, registracijos numeris, leidimo numeris ir pan. Visi duomenys, identifikatoriaus susieti su asmens duomenų subjektu, tampa asmens duomenimis. Jeigu identifikatoriaus nėra, duomenys nebetenka asmens duomenų statuso, nors ir susiję su realiu asmeniu. Vis dėlto, asmeninė informacija gali tapti asmens duomeniu, tai yra tapti pakankama identifikuoti tam tikrą asmenį ne vien tik identifikatoriaus pagalba. Taip gali atsitikti tais atvejais, kai asmeninės informacijos sankaupa, sistema, kurios atskiri elementai yra susiję su konkrečiu asmeniu, tačiau vienareikšmiškai negali patvirtinti jo tapatybės, įgauna naują savybę, kuria negali pasižymėti jos sudedamosios dalys – identifikuoti konkretų asmenį. Šioje vietoje kyla asmeninės informacijos ir asmens duomens santykio problema. Asmeninė informacija savaime nėra ir negali būti asmens duomeniu iki tol, kol ją susiejus su kita asmenine informacija arba identifikatoriumi tampa įmanomas konkretaus asmens identifikavimas. Asmeninės informacijos ir asmens duomens santykio klausimas itin svarbus tuo, kad asmens duomenų apsaugos reikalavimai taikomi ne bet kokiai asmeninei informacijai, o tik tokiai, kurios pagalba galima konkretaus asmens identifikacija.

Asmens duomenys apie rasinę kilmę, politinius, religinius ar kitus įsitikinimus, taip pat duomenys apie teistumą, sveikatą ar intymų gyvenimą pagal 1981 m. Europos Tarybos konvenciją "Dėl asmenų apsaugos, susijusios su automatizuotu asmens duomenų apdorojimu" priskiriami specialioms asmens duomenų apsaugos kategorijoms ir negali būti apdorojami automatizuotai, nebent nacionalinėje teisėje būtų numatyta tinkama jų apsauga. Duomenų apsaugos direktyva 95/46/EB tokio pobūdžio duomenis įvardija kaip ypatingus asmens duomenis ir leidžia jų tvarkymą tik ypatingais atvejais.

Internetas pakeitė nusistovėjusią pusiausvyrą tarp teisės į informaciją ir teisės į privatumą. Pasikeitė visuomenės požiūris į informaciją – informacijos rinkimas, jos apdorojimas tapo svarbus ir ekonomine, ir moksline prasme.

Valstybės, savivaldos institucijos, įmonės bei pavieniai asmenys, teikdami informacines paslaugas, įgyvendindami elektroninius atsiskaitymus, siųsdami ir gaudami elektroninius laiškus, vykdydami įvairias marketingo akcijas, siūlo užpildyti įvairias anketas, renka, kaupia, apdoroja ir platina informaciją, taip pat ir fizinių bei juridinių asmenų duomenis. Informacija ir duomenys[25] yra renkami pačiais įvairiausiais būdais: anketavimo, apklausų, socialinių tyrimų procedūrų realizavimo metu ir t.t.. Kita asmens duomenų teikimo bei rinkimo procedūra – kai veiksmas vyksta betarpiškai tarp asmens duomenų subjekto ir duomenų rinkėjo – tai pirkimo elektroninėse parduotuvėse procedūros, bilietų ir viešbučių rezervavimas, elektroniniai atsiskaitymai, bankinės paslaugos internetu. Daugumoje atvejų, kuomet duomenų subjektas įvykdo pirkimą arba naudojasi paslauga (pvz., prenumerata), yra privaloma pateikti asmens duomenis pardavėjui arba paslaugos teikėjui, siekiant patvirtinti pirkėjo autentiškumą, suteikti apmokėjimo garantijas, bei fizinį arba elektroninį adresą prekių bei paslaugų pristatymui. Klientas pats elektroniniu būdu pateikia paslaugos teikėjui savo asmens duomenis – kreditinės kortelės numerį, adresą, nurodo darbovietę, pareigas, amžių ir kt.. Tuo pat metu šie asmenys susiduria su kita rizika. Kadangi internetas yra atviras viešas tinklas su gerai žinomais protokolais[26], orientuotais daugiau į

[25] Informacijos ir duomenų sąvokos skiriasi. Duomenys lietuvių kalboje kildinami iš žodžio "duoti", jie apibūdina tai, kas duota, kuo remiantis daroma išvada. Tuo tarpu informacija yra žinios arba reikšmė, kurią supranta žmonės, sužinoję duomenis. (*Sabaliauskas G.* Informacijos saugumas internete: teisininkų ir informatikų problema // Justitia 2001 Nr. 1, psl. 28 – 30.) Teisėje "informacija" dažniausia yra nagrinėjama, kaip teisinių santykių objektas, t.y. vertybė, kurią įgyja ir kuria pasinaudoti siekia teisinio santykio dalyviai, įgyvendindami savo teises. (*A. Vaišvila.* Teisės teorija: vadovėlis.- Vilnius:Justitia, 2000, P. 324.)

[26] Interneto komunikacijos procese naudojami įvairūs aukštesnio ir žemesnio lygmens protokolai, padedantys kompiuteriams tarpusavyje komunikuoti: *HTTP* (*HyperText Transport Protocol*) - naudojamas naršymui; *FTP* (*File Transfer Protocol*) - naudojamas bylų persiuntimui; *NNTP* (*News Network Transport Protocol*) - naudojamas norint prieiti prie naujienų grupių; SMTP (Simple Mail Transport Protocol) ir POP3 protokolai - elektroninio pašto žinutėms siųsti ir gauti.

pasidalinimą informacija, o ne į jos konfidencialumo ar saugumo užtikrinimą, yra gana nesudėtinga bet kam, kas turi bent kiek techninių žinių, surasti tam tikrus programinės įrangos instrumentus, leidžiančius perimti ir atskleisti internetu persiunčiamus duomenis. Taip pat yra įmanoma apsimesti kita kompanija, pasitelkti įvairius apgaulės būdus siekiant gauti informacijos, kuri vėliau galėtų būti panaudota kokiems nors nusikalstamais tikslais[27].

Strasbūro konvencijoje dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu asmens duomenimis pripažįstama informacija, kuria remiantis galima nustatyti asmens tapatybę . Analogiškai galime daryti išvadą: jei naršymo duomenis susiejus su kitais duomenimis apie asmenį, galima nustatyti jo tapatybę[28], vadinasi tokius duomenis galime laikyti asmens duomenimis. Įvertinus visą anksčiau pateiktą informaciją galima daryti vieningą išvadą, kad interneto aplinkoje surinkti duomenys apie asmenis, jei juos susiejus su kitais duomenimis galima identifikuoti asmenį, turi būti laikomi asmens duomenimis.

Lietuviškasis elektroninio parašo įstatymas numato dvejopus elektroninio parašo naudojimo subjektus – tai pasirašantis asmuo ir parašo naudotojas. Pasirašantis asmuo apibūdinamas tik kaip fizinis asmuo, kuris turi parašo formavimo įrangą ir, veikdamas savo valia ir savo arba kito asmens, kuriam jis atstovauja vardu, sukuria elektroninį parašą (Elektroninio parašo įstatymo 2 str. 7 d.), o parašo naudotojas yra asmuo (pagal Elektroninio parašo įstatymo 2 str. 1 d. tai įmonė, neturinti juridinio asmens teisių, fizinis, arba juridinis asmuo), savo veikloje naudojantis elektroninį parašą arba iš kitų asmenų (vėlgi ne tik fizinių asmenų) gaunantis pasirašytus duomenis. Taigi pagrindinis skirtumas – pasirašyti gali tik fizinis asmuo, o parašą naudoti - jau bet kokio teisinio statuso asmenys. Painiavą tarp šių sąvokų įveda įstatymo 3 str. 1 d., nurodanti, kad sertifikavimo paslaugų teikėjas sukuria parašo formavimo ir tikrinimo duomenis asmens, nutarusio savo veikloje naudoti elektroninį parašą (t.y., parašo naudotojo) prašymu ir sukuria šį parašą šiam asmeniui. Čia tai pat nurodoma, kad duomenis gali susikurti ir pats asmuo. Tačiau analizuojant 2 str. 15 d. (sertifikato, patvirtinančio parašą ir nurodančio duomenis apie pasirašantį asmenį turinys), 3 str. 3 d., 4 str. 2 d., 4 str. 4 d. 1 p.ir 6 str. nuostatas aiškėja, kad parašo formavimo ir tikrinimo duomenys kuriami tik fiziniam asmeniui, kuris

---

[27] Panašiai pasielgė ir korporacija V2X, sukūrusi AudioGalaxy muzikos mainų sistemos vartotojų kompiuteriuose įdiegtoms programoms tam tikrus nepastebimus priedus, kurie sekė šios paslaugos vartotojus. Šių priedų pagalba buvo registruojami naršymo internete įpročiai, duomenys, kuriuos žmogus įveda į įvairiausias interneto anketas (spėjama, kad galbūt ir banko sąskaitų bei kreditinių kortelių numeriai). *Civilka M.* Asmens duomenų apsaugos teisinis reguliavimas interneto kontekste. <http://www.itc.tf.vu.lt/mokslas/mokslas.html>. Taip pat <www.ebiz.lt>, <www.delfi.lt>.

[28] 1981 m. Strasbūro konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu, 2 str. // Pagrindinės Europos Tarybos sutartys. - Vilnius: Europos Tarybos informacijos ir dokumentacijos centras, 2000.

vienintelis jais disponuoja. Įstatymo projekto aiškinamajame rašte taip pat nurodoma, kad elektroninis parašas susiejamas būtent su fiziniu asmeniu[29].

Asmens tapatybės nustatymo būdai, pasak ekspertų gali būti dvejopi: teisėti ir neteisėti. Teisėtas asmens tapatybės nustatymo būdas yra naudojamas tų asmenų ar organizacijų, kurios tam turi atitinkamus, valstybės suteiktus, įgaliojimus: visos ikiteisminio tyrimo įstaigos ir operatyviniai subjektai.

Lietuvos ikiteisminio tyrimo įstaigos – Vidaus reikalų ministerijos įstaigos (Policija, Valstybės sienos apsaugos tarnyba, Finansinių nusikaltimų tyrimo tarnyba), Muitinės sistemų (Muitinės kriminalinė tarnyba), Krašto apsaugos (Karo policija), Valstybės saugumo departamento, Specialiųjų tyrimų tarnybos padaliniai bei visų lygių prokuratūros (apylinkių ir apygardų bei Generalinė prokuratūra).

Lietuvos operatyviniai subjektai - specialius valstybės įgaliojimus turintys krašto apsaugos, vidaus reikalų, muitinės sistemų, Valstybės saugumo departamento, Specialiųjų tyrimų tarnybos padaliniai, kuriems pavedama operatyvinė veikla ir kurių pareigūnai įgaliojami ją vykdyti. Šių padalinių sąrašą sudaro ir jų operatyvinės veiklos mastą nustato Vyriausybė. Operatyvinės veiklos subjektų pagrindinės institucijos – Antrasis operatyvinių tarnybų departamentas prie Krašto apsaugos ministerijos, Finansinių nusikaltimų tyrimo tarnyba prie Vidaus reikalų ministerijos, Muitinės departamentas prie Finansų ministerijos, Policijos departamentas prie Vidaus reikalų ministerijos, Specialiųjų tyrimų tarnyba, Vadovybės apsaugos departamentas prie Vidaus reikalų ministerijos, Valstybės saugumo departamentas, Valstybės sienos apsaugos tarnyba prie Vidaus reikalų ministerijos[30].

Neteisėtą asmens tapatybės nustatymo būdą paprastai naudoja nusikaltėliai, tačiau neretai šį būdą panaudoja ir teisėsaugos įstaigų darbuotojai (neteisėti veiksmai – nusikaltimai tarnybai). Dažniausiai sutinkamas vienas iš neteisėtų asmens tapatybės nustatymo būdų yra neteisėtas asmens duomenų rinkimas, pasitelkiant „Phishing“ programas.

---

[29] Lietuvos Respublikos Valdymo reformų ir savivaldybių reikalų ministerija. Lietuvos Respublikos elektroninio parašo įstatymo projekto aiškinamasis raštas, 2000 05 26, Nr. P-2567, http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=101575 ,prisijungimo laikas 2008-10-25 16:53;

[30] Lietuvos Respublikos Operatyvinės veiklos įstatymas, 2002 m. birželio 20 d. Nr. IX-965, http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=169652&p_query=&p_tr2= ,prisijungimo laikas 2008-11-03 13:55;

Kas yra „Phishing“? Tai naujoviškas sukčiavimo būdas, pasitelkiant programinę įrangą. „Phishing“-o metu, nusikaltėliai iškreipia savo duomenis ar tinklapio duomenis ir panaudodami programinę įrangą išgauna iš kito asmens tapatybę patvirtinančius bei kitus asmens duomenis. Kai kuriais sukčiavimo, pasitelkiant „phishing“-o programas, atvejais nusikaltėliai naudojasi elektroniniu paštu, apsimesdami finansinių institucijų atstovais, Interneto paslaugų tiekėjo atstovu, ar kitos įstaigos, kuria „auka“ labai pasitiki, taip stengdamiesi gauti kuo daugiau ir tikslesnių asmens duomenų. Faktiškai „Phishing“-o atveju „auka“ nukreipiamas į netikrą (falsifikuotą, kuris yra labai panašus į tikrą) arba klaidingą tinklapį (angl. „*website*“), kur yra prašome suvesti savo tikrus duomenis, tokius kaip vardas, pavardė, kreditinės kortelės numeris, Socialinio draudimo pažymėjimo numeris ar kt., ir visokeriopai stengiamasi surinkti kuo daugiau asmens tapatybę patvirtinančių duomenų, kuriuos nusikaltėliai vėliau gali panaudoti vykdant nusikalstamas veikas, įskaitant ir asmens tapatybės klastotę.

4.2. ASMENS TAPATYBĖS NUSTATYMO TEISINIS REGULIAVIMAS

Lietuvos Respublikos Konstitucijos 22 straipsnyje teigiama: „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. Įstatymas ir teismas saugo, kad niekas nepatirtų savavališko ir neteisėto kišimosi į jo asmeninį ir šeimyninį gyvenimą, kėsinimosi į jo garbę ir orumą". Lietuvos Respublikos Konstitucinio Teismo jurisprudencijoje teigiama, 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.".

Žmogaus teisių ribojimo klausimu pasisakė ir Lietuvos Respublikos Konstitucinis Teismas. 2002 m. rugsėjo 19 d. Lietuvos Respublikos Konstitucinio Teismo nutarime teigiama, kad pagal Konstituciją riboti konstitucines žmogaus teises ir laisves galima, jeigu laikomasi šių sąlygų:

- tai daroma pagal įstatymą;

- ribojimai yra būtini demokratinėje visuomenėje siekiant apsaugoti kitų asmenų teises bei laisves ir Konstitucijoje įtvirtintas vertybes, taip pat konstituciškai svarbius tikslus;
- ribojimais nėra paneigiama teisių ir laisvių prigimtis bei jų esmė;
- yra laikomasi konstitucinio proporcingumo principo.

„Pagal Lietuvos Respublikos Civilinio kodekso 2.23 straipsnyje įtvirtintą teisės į privatų gyvenimą sampratą privatus yra toks žmogaus gyvenimas, kuris vyksta ne viešumoje, vieša darbo vieta nėra privati asmens sfera. Pardavėjas negali reikalauti, kad jam būtų užtikrintas privatumas jo darbo vietoje prekybos salėje, todėl pardavimo salės, kartu ir pardavėjo darbo, stebėjimas nėra slaptas asmens privataus gyvenimo stebėjimas".

Tačiau teisė į privatų gyvenimą nėra absoliuti - ji nepriskirta toms žmogaus teisėms, kurių ribojimas nėra galimas. Įgyvendindamas savo teises ir naudodamasis savo laisvėmis žmogus privalo laikytis Lietuvos Respublikos Konstitucijos ir įstatymų, nevaržyti kitų žmonių teisių ir laisvių. Todėl toks žmogus, kuris negerbia kitų žmonių teisių ir laisvių, negali tikėtis savo teisių ir laisvių, įskaitant privataus gyvenimo neliečiamumą, užtikrinimo. Lietuvos Respublikos Konstitucinis Teismas pažymėjo, kad „asmuo, darydamas nusikalstamas ar kitas priešingas teisei veikas, neturi ir negali tikėtis privatumo. Žmogaus privataus gyvenimo apsaugos ribos baigiasi tada, kai jis savo veiksmais nusikalstamai ar kitaip neteisėtai pažeidžia teisės saugomus interesus, daro žalą atskiriems asmenims, visuomenei ir valstybei".

Elektroniniai ryšiai - signalų perdavimas laidinėmis, radijo, optinėmis ar kitomis elektromagnetinėmis priemonėmis - sudaro galimybę žmonėms bendrauti nepaisant jų fizinio buvimo vietos. Tačiau elektroniniai ryšiai suteikia ne tik neabejotinų pranašumų, bet ir kelia vis didesnę grėsmę žmogaus privačiam gyvenimui. Elektroninių ryšių paslaugų ir tinklų teikėjai, vykdydami savo veiklą, tvarko daugybę duomenų, kurių dauguma priskirtina prie asmens duomenų. Elektroniniais ryšiais taip pat perduodama elektroninių ryšių paslaugų gavėjų siunčiama informacija (turinys). Todėl toks duomenų tvarkymas ir perdavimas neabejotinai turi didelį poveikį elektroninių ryšių paslaugų gavėjų privatumui.

Europos Sąjungos privatumo ir asmens duomenų apsaugos elektroniniuose ryšiuose reguliavimas pritaikytas išimtinai elektroninių ryšių sektoriui. Tam skirta 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva Nr. 2002/5 8/EB[31] dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje („Direktyva dėl privatumo ir elektroninių

[31] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0058:20060503:LT:PDF ; prisijungimo laikas 2008-11-14 17:29;

ryšių“). Viešųjų elektroninių ryšių paslaugų abonentai gali būti fiziniai ar juridiniai asmenys, tad 2002/58/EB direktyva siekiama apsaugoti fizinių asmenų teises ir ypač jų teisę į privatumą, taip pat teisėtus juridinių asmenų interesus.

Lietuvos Respublikos Informacinės visuomenės paslaugų įstatymas (2006 m. gegužės 25 d. Nr. X-614) reglamentuoja informacinės visuomenės paslaugų teikimą ir kitą informacinės visuomenės paslaugų teikėjų veiklą. Lietuvos Respublikos Visuomenės informavimo įstatymas (2006 m. liepos 11 d. Nr. X-752) nustato viešosios informacijos rinkimo, rengimo, skelbimo ir platinimo tvarką, viešosios informacijos rengėjų, skleidėjų, jų dalyvių, žurnalistų ir jų veiklą reglamentuojančių institucijų teises, pareigas ir atsakomybę.

Lietuvos Respublikos Konstitucija nustato, kad informacija apie asmeninį gyvenimą gali būti renkama tiktai argumentuota Teismo nutartimi ir tiktai įstatymų numatytais atvejais. Ne paslaptis, kad nusikaltėliai visaip bando pateisinti savo elektroninį bendravimą, prisidengdami žmogaus teisėmis, tačiau valstybės ir visuomenės saugumas visados lieka prioritetinė sritis. Būtent todėl visiškas anonimiškumas elektroninėje erdvėje darosi neįmanomas.

Kalbant apie teisių apribojimą anonimiškai būti elektroninėje erdvėje, kad užkardyti terorizmą, galima pažymėti, kad Lietuvos Respublikos baudžiamąjame kodekse nėra nei tikslaus terorizmo apibrėžimo nei terorozmo apibūdinimo kaip nusikalstamos veikos (išskyrus patį teroro aktą), todėl Lietuvoje netinkamai įgyvendinamas proporcingas ir sąžiningas teisės į anonimiškumą kibernetinėje erdvėje apribojimas.

Europos konvencijos dėl elektroninių nusikaltimų, priimtos 2001 metais, taryba be įprastų procedūrų elektroninėje erdvėje tokių kaip krata ir turto areštas, ėmėsi naujų priemonių, kad užtikrinti eksploatuojamų duomenų sulaikymą, kas turėtų garantuoti, kad įprastos priemonės rinkti įrodymams būtų taip pat veiksmingos ir elektroninėje erdvėje. Įprastos įrodymų rinkimo priemonės, tokios kaip duomenų srauto kaupimas realiuoju laiku ir perimami duomenų srautai yra naudojami siekiant surinkti duomenis informacijos perdavimo proceso metu.

Lietuvos Respublikos Operatyvinės veiklos įstatymas Elektroninių ryšių operatorius ir paslaugų tiekėjus įpareigoja užtikrinti technines galimybes kontroliuoti informacijos, perduodamos per elektroninių ryšių tinklus, turinį. Lietuvos Respublikos Elektroninių ryšių įstatymas numato, kad esant motyvuotam teismo sprendimui, įmonės, teikiančios elektroninių ryšių tinklų prieigas ar paslaugas privalo teikti operatyvinėms tarnyboms duomenis apie ryšius,

tokius kaip duomenų srauto rinkimas realiu laiku ir duomenų turinio perėmimas, kad užtikrinti duomenų rinkimą informacijos perdavimo metu.

Lietuvos Respublikos Elektroninių ryšių įstatymo 77 straipsnyje yra nustatytos Elektroninių ryšių srautų priežiūros ir stebėjimo teisės bei pareigos ūkio subjektams. Ūkio subjektai, teikiantys elektroninių ryšių tinklus ir (ar) paslaugas, turi teisę fiksuoti ir saugoti elektroninių ryšių įvykius ir jų dalyvius tik tiek, kiek yra būtina šių ūkio subjektų ūkinei veiklai užtikrinti. Ūkio subjektai, teikiantys elektroninių ryšių tinklus ir (ar) paslaugas, privalo įstatymų nustatyta tvarka turimą ir nusikalstamoms veikoms užkardyti, tirti, nustatyti reikalingą informaciją pateikti operatyvinės veiklos subjektų pagrindinėms institucijoms, Vyriausybės nurodytoms ikiteisminio tyrimo įstaigoms, prokurorui, teismui ar teisėjui. Šią informaciją ūkio subjektai, teikiantys elektroninių ryšių tinklus ir (ar) paslaugas, neatlygintinai teikia operatyvinės veiklos subjektų pagrindinėms institucijoms, Vyriausybės nurodytoms ikiteisminio tyrimo įstaigoms pagal jų paklausimus elektroniniu būdu ir nedelsdami. Vyriausybės nurodytos ikiteisminio tyrimo įstaigos Vyriausybės nustatyta tvarka organizuoja ir sudaro galimybę gauti šią informaciją savo padaliniams ir (ar) kitoms ikiteisminio tyrimo įstaigoms.

5. LIETUVOS IR UŽSIENIO ŠALIŲ PRAKTIKOJE PAPLITĘ NUSIKALTIMAI INTERNETE

XXI a. sparčiai tobulėjant kompiuterių bei interneto technologijoms, šiuolaikinės informacinės visuomenės gyvenime ne viskas taip spindi, kaip daugeliui atrodo. Interneto bei pažangių technologijų ir programinės įrangos teikiamos galimybės atveria vis platesnius kelius moderniems sukčiams.

Pasaulyje ir Lietuvoje dažnėjantys nusikaltimai elektroninėje erdvėje – virusų kūrimas, kompiuterinių įsilaužėlių atakos, įvairiausių sukčių, turto prievartautojų, vaikų pornografijos gamintojų ir platintojų veikla – akylai stebimi. Lietuvoje, kaip ir pasaulyje, elektroninėje erdvėje populiariausi sukčiavimo būdai – naudojantis banko mokėjimo kortelių duomenimis ar svetimomis sąskaitomis.

Be kita ko, pastaruoju metu Lietuvoje būdingi ir kitokie sukčiavimai išviliojant pinigus, neteisėtas informacijos rinkimas apie privatų asmens gyvenimą, įsilaužimas į duomenų bazes, vaikų pornografija, turto prievartavimas, virusų kūrimas, nelegalūs lošimai „DDos“ atakos, (pavyzdys: Estijoje, kai buvo išvestos iš rikiuotės valstybės institucijų darbo stotys, o atakos buvo susijusios su sovietinės Bronzinio kario skulptūros perkėlimu į kitą vietą, Lietuvoje, kai į visą eilę tinklalapių buvo įdėta Sovietinė simbolika) „botnetai“ ir kita.. Nepaisant to, kad ES valstybės nuolat griežtina internetiniams nusikaltėliams skiriamas bausmes (pavyzdžiui, Vokietijoje programišius gali netekti laisvės 10-čiai metų), tokio tipo nusikaltimų nemažėja. „Symantec“ [32] kompanija kompiuterių-zombių tinklų naudojimą DDoS atakoms, vadina viena didžiausių grėsmių internetiniam verslui praėjusiais metais.

Taip pat atsiranda ir naujų grėsmių, tokių kaip elektroninis terorizmas. Nebūtina žvanginti ginklais, užtenka įvykdyti elektroninę ataką, per kurią iš rikiuotės išvedamos svarbios darbo stotys, prarandamas ryšys su pasauliu, ką jau kalbėti apie finansinį nuostolį.

JAV nusikaltimams internete Federalinis tyrimų biuras (toliau FTB) skiria labai daug dėmesio. Pagal FTB numatytus prioritetus – elektroniniai nusikaltimai yra trečioje vietoje. FTB pareigūnas, kaip dažniausius nusikaltimus, nurodė įsilaužimus, vaikų pornografiją, neteisėtą kreditinių kortelių duomenų pardavimą, įvairų sukčiavimą internetu bei autorinių teisių pažeidimus.

Ypatingai JAV pastaruoju metu asmens tapatybės vagystės, kai nusikaltėliai, turėdami tikslą identifikuotis kitais asmenimis, naudoja pagrobtus asmens duomenis “*personally identifiable information* (PII)“, kaip pvz.: kreditinės kortelės ar socialinio draudimo pažymėjimas, kelia didelį susirūpinimą. Didžiulis asmens tapatybių vagysčių skaičius JAV buvo fiksuotas 2005 metais, kai preliminariais duomenimis, buvo įvykdyta apie 1 mln. tokių vagysčių[33]. Daugelis sieja tokias vagystes su Internetu, tačiau tyrimai ir apklausos parodė priešingai. Daugumas nukentėjusių žmonių nurodė Internetą kaip priemonę vogti tapatybės duomenis. Tai būtų galima paaiškinti taip, kad daugumas nukentėjusiųjų net nežino apie naudojimosi Internetiniu ryšiu galimybes, ypatingai apie praktiką, kuri vadinama „*PHISHING*“.

[32] http://cybercrimes.eu/index.php?topic=4.0 ; prisijungimo laikas 2008-11-28 17:29;
[33] http://italy.usembassy.gov/pdf/other/RS22082.pdf , prisijungimo laikas 2008-11-02 15:15;

Lietuvoje kredito kortelėmis sukčiaujama naudojant kitų žmonių duomenis, įsilaužimas į internetines banko sąskaitas tikrai nėra dažnas reiškinys. Tik vieną kartą buvo gautas pranešimas apie galimą įsilaužimą, į banko serverių sistemą, bet ir ši informacija nepasitvirtino. Šiais laikais bankai investuoja tikrai dideles sumas į apsaugos modernizavimą.

Lietuvoje pasitaikė keletas atvejų, kai asmenys, neteisėtai įgiję svetimus prisijungimo prie sąskaitų internete identifikavimo duomenis, ištuštindavo tas sąskaitas. Ne paslaptis, kad prisijungti internetu prie banko sąskaitos reikalinga kodų kortelė, kurioje yra nuo 24 iki 36 kodų (atsižvelgiant į kortelę išdavusį banką), vartotojo ID ir nuolatinis slaptažodis, kurį, deja, retai kas keičia. Šnipinėjimo programos ar virusai per mėnesį gali juos visus nesunkiai „sugaudyti“, todėl apsisaugoti nuo tokių įsilaužimų savo sistemas įdiegę bankai ir siūlo klientams naudoti elektroninius kodų generatorius. Tačiau JAV prekyba banko kortelėse esančių duomenų informacija – gan dažnas reiškinys[34].

Vadinamasis “nugriebimas “ (angl. skiming) buvo plačiai įsišaknijęs JAV, tačiau pradėjus su juo vis stipriau kovoti, tokių sukčiavimo atvejų sumažėjo. Pats principas veikia labai paprastai – slaptu skaitytuvu perbraukus kortelę nukopijuojama visa informacija. Tereikia kortelės PIN kodo.

Lietuvoje „nugriebimas“ (angl. skiming) anksčiau buvo populiarus, tačiau šiuo metu tokių nusikaltimų užfiksuojama vis mažiau. Lietuviai tiesiog perka vogtą kortelių informaciją internetu iš užsienio sukčių.

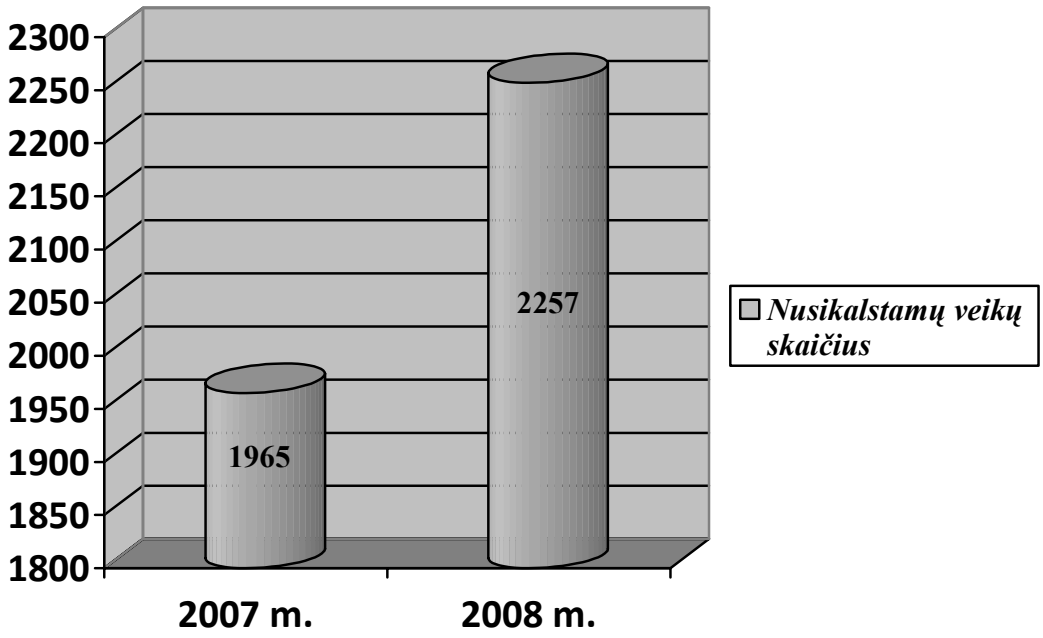
Įsilaužimas į duomenų bazes tapo itin dažnu reiškiniu. Vienur laužiamasi dėl smalsumo, kitur pakeičiama ar ištrinama informacija. Tačiau didžiosios kompanijos investuoja vis daugiau lėšų savo duomenų saugumui užtikrinti. Didžiausia problema yra ta, kad kompanijos, į kurių duomenų bazes buvo įsilaužta, dažnai linkusios nuslėpti tokius atvejus. Baiminamasi, jog taip nukentės jų prestižas ar bijoma prarasti dalį klientų.

Šiandien sudaryti nusikaltimų elektroninėje erdvėje statistiką gana sunku. Lietuviai gali atakuoti Kinijos, Australijos ar JAV duomenų bazes, todėl apie tai galime ir nesužinoti. Ekspertai teigia, kad pelnas iš elektroninių nusikaltimų viršija pelną, gaunamą iš prekybos narkotikais.

[34] http://italy.usembassy.gov/pdf/other/RS22082.pdf , prisijungimo laikas 2008-11-02 15:15;

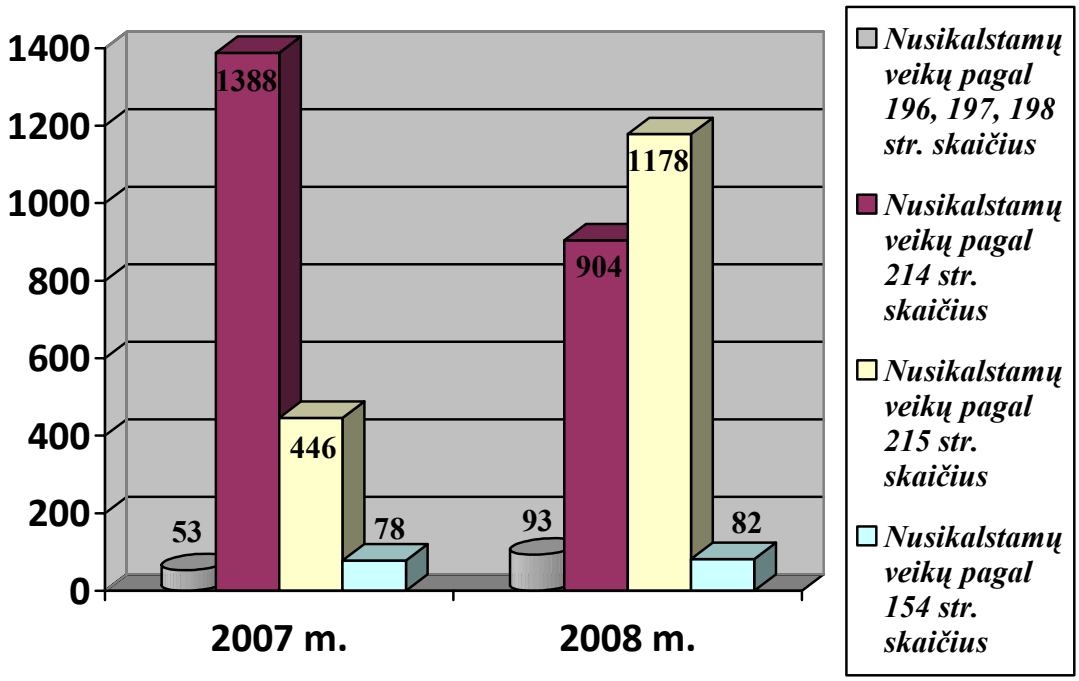
Be to, pertvarkius pagrindines duomenų bazes Lietuvos Respublikos Vidaus reikalų ministerijoje (Policijos departamente ir Informatikos ir ryšių departamente), neįdiegus papildomų programų, praktiškai neįmanoma surinkti statistinių duomenų pagal atskiras nusikaltimų rūšis. Šio darbo autoriui taip ir nepavyko gauti tikslių statistinių duomenų apie nusikaltimų elektroninėje erdvėje statistiką ir dimamiką Lietuvoje.

Atlikus analizę apie visas registruotas nusikalstamas veikas, kurios galėjo būti padarytos ir elektroninėje erdvėje, numatytas Lietuvos Respublikos Baudžiamojo kodekso[35] (toliau LR BK) 196 (Neteisėtas poveikis elektroniniams duomenims), 197 (Neteisėtas poveikis informacinei sistemai), 198 (Neteisėtas elektroninių duomenų perėmimas ir panaudojimas), 1981 (Neteisėtas prisijungimas prie informacinės sistemos),1982 (Neteisėtas disponavimas įrenginiais, programine įranga, slaptažodžiais, prisijungimo kodais ir kitokiais duomenimis), 214 (Netikros elektroninės mokėjimo priemonės gaminimas, tikros elektroninės mokėjimo priemonės klastojimas ar neteisėtas disponavimas elektronine mokėjimo priemone arba jos duomenimis), 215 (Neteisėtas elektroninės mokėjimo priemonės ar jos duomenų panaudojimas), 154 (Šmeižimas) straipsniuose, nustatyta, kad viso tokių veikų Lietuvoje buvo registruota:



1 pav. Nusikaltimų skaičius pagal LR BK 196 197 198 214 215 154 str.

[35] http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=111555 Lietuvos Respublikos Baudžiamasis kodeksas, patvirtintas įstatymu Nr. VIII-1968 ; prisijungimo laikas 2008-11-28 17:29;



2 pav. Analizė registruotų nusikalstamų veikų pagal atskirus nusikaltimų (padarytų ir internetu) straipsnius

Lietuvos kriminalinės policijos biuro nusikaltimų elektroninėje erdvėje tyrimo skyriaus padalinys turi savo viziją, kaip kovoti su nusikaltimais elektroninėje erdvėje. Artimiausiu metu bus struktūrinių vidinių pertvarkymų, kurie leis veiksmingiau kovoti su tokio pobūdžio nusikaltimais. Lietuvos kriminalinės policijos biuro nusikaltimų elektroninėje erdvėje tyrimo skyrių (toliau NEETS) ruošiamasi reorganizuoti į valdybą ir išplėsti skyriaus veiklą, kadangi šis kriminalinės policijos padalinysiki šiol tiria tik sunkius ir labai sunkius ar rezonansą sukėlusius nusikaltimus. Dažnai pasitaiko atvejų, kai Lietuvos piliečius, besikreipiančius į NEETS dėl mažareikšmių nusikaltimų šioje srityje, tenka nukreipti į teritorinius policijos komisariatus. Deja, jie nėra pakankamai aprūpinti įranga ir priemonėmis. Taip pat trūksta kvalifikacijos, todėl tokių tyrimų rezultatai dažnai nepateisina nukentėjusiųjų lūkesčių.

6. NUSIKALTIMŲ IR PAŽEIDIMŲ, SUSIJUSIŲ SU ASMENS TAPATYBĖS PASLĖPIMU AR KLASTOJIMU INTERNETE TYRIMAS LIETUVOJE

Dažniausiai Lietuvoje pasitaikantys teisės pažeidimai: skiriamos kelios komentarais internete objektyviai pasireiškiančios teisės pažeidimų rūšys: visuomenės grupių nesantaika, asmenų šmeižtas, įžeidimas bei kiti.. Atlikus kokybinį tyrimą, nustatyta, jog absoliuti dauguma pastaruosius 2 metus vyraujančių nusikalstamų veikų, kuomet reikėjo nustatyti asmens tapatybę, yra asmenų šmeižimas.

Atsakomybė už šmeižimą ir įžeidimą reglamentuojama Baudžiamojo kodekso XXII skyriuje „Nusikaltimai ir baudžiamieji nusižengimai asmens garbei ir orumui“. 154 straipsnyje „šmeižimas“ apibrėžiamas kaip „paskleidimas apie kitą žmogų tikrovės neatitinkančios informacijos, galinčią paniekinti ar pažeminti tą asmenį arba pakirsti pasitikėjimą juo“. Kvalifikuojančios aplinkybės – šmeižimas, neva asmuo padarė sunkų ar labai sunkų nusikaltimą; šmeižimas per visuomenės informavimo priemonę ar spaudinyje.

Pažymėtina, kad pagrindinė „šmeižimo“ savybė – tikrovės neatitinkanti informacija. Daugelyje šmeižimo bylų diskutuojama, ar atitinkama informacija iš tiesų neatitiko tikrovės (t.y. buvo melas). Svarbu, kad Europos žmogaus teisių teismas žiniasklaidos atstovams šią teisę aiškina pabrėždamas saviraiškos laisvės principų bei visuomenės informavimo principų svarbą. Todėl tas pats eilinio piliečio ir žurnalisto teiginys iš tiesų gali būti įvertintas tik dėl subjekto veiklos pobūdžio – ar jis veikia kaip žiniasklaidos atstovas, siekdamas informuoti (įspėti) visuomenę.

Administracinių teisės pažeidimų kodekso[36] 214^{12}-214^{13} straipsniai gina nacionalinę, rasinę ar religinę santaiką. Pirmasis straipsnis draudžia gaminti ar laikyti turint tikslą platinti, taip pat platinti arba viešai demonstruoti spaudinius, vaizdo, garso ar kitokią produkciją, propaguojančios nacionalinę, rasinę ar religinę nesantaiką. Antrasis draudžia kurti ar dalyvauti organizacijos, propaguojančios nacionalinę, rasinę ar religinę nesantaiką, veikloje.

Neapykanta pagal Baudžiamojo kodekso XXV skyriaus „Nusikaltimai ir baudžiamieji nusižengimai asmens lygiateisiškumui ir sąžinės laisvei“ nuostatas gali pasireikšti tautybės, rasės, lyties, seksualinės orientacijos, kalbos, kilmės, socialinės padėties, religijos, įsitikinimų ar

[36] http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=331762 Lietuvos Respublikos Administracinių teisės pažeidimų kodeksas, patvirtintas įstatymu Nr. X-1766 ; prisijungimo laikas 2008-02-03 15:29;

pažiūrų, kitos grupinės priklausomybės atžvilgiu. Kodekso 169 straipsnis draudžia diskriminaciją dėl subjektų priklausymo tokioms grupėms, 170 straipsnis nustato atsakomybę už tyčiojimąsi, niekinimą, neapykantos skatinimą ar kurstymą diskriminuoti, smurtauti, fiziškai susidoroti, o 171 straipsnis skirtas religinių įsitikinimų apsaugai ir draudžia trikdyti pamaldas, kitas apeigas arba iškilmes.

155 kodekso straipsnyje nustatoma atsakomybė už „įžeidimą“ – t.y. užgaulų žmogaus pažeminimą veiksmu, žodžiu ar raštu. Atsakomybė mažinama, jeigu įžeidimas buvo neviešas. Pagrindinis „įžeidimo“ ir „šmeižimo“ skirtumas, jog įžeisti gali ir tikrovę atitinkanti informacija (t.y. teisybė). Pavyzdžiui, pagal Baudžiamąjį kodeksą turėtų atsakyti asmuo viešai tyčiojęsis (t.y. žeminęs) iš fiziškai neįgalių asmenų.

Lietuvoje iki šiol nė karto nebuvo pritaikytas Administracinių teisės pažeidimų kodekso 214^6 straipsnis „Respublikos Prezidento įžeidimas arba šmeižimas masinės informacijos priemonėse“, tačiau akivaizdu, kad išrinkus Rolandą Paksą Lietuvos Respublikos Prezidentu bei iki jį nušalinant apkaltos proceso metu žiniasklaidoje buvo dešimtys, jei ne šimtai, atvejų, kai tuometinis Prezidentas buvo laikomas Rusijos specialiųjų pajėgų statytiniu (tai atitiktų „šmeižimą“, nes toks kaltinimas vėliau buvo visiškai atmestas), žeminamas kaip žmogus (pavyzdžiui, tyčiojantis dėl fizinės būklės).

Atskirai paminėti verta komercinių (gamybinių) ir profesinių paslapčių atskleidimą. Kaip nustato Civilinio kodekso I knygos 116 straipsnis, informacija laikoma komercine (gamybine) paslaptimi, jeigu turi tikrą ar potencialią komercinę (gamybinę) vertę dėl to, kad jos nežino tretieji asmenys ir ji negali būti laisvai prieinama. Už tokios informacijos atskleidimą atsako asmenys, neteisėtais būdais įgiję informaciją, darbuotojai, pažeidę darbo sutartį, kitokios sutarties šalis, atskleidusi gautą komercinę paslaptį.

Tuo tarpu profesinė paslaptis – tai informacija, kurią pagal įstatymus ar sutartį privalo saugoti tam tikros profesijos asmenys (advokatai, gydytojai, auditoriai ir kt.). Dėl neteisėto profesinės paslapties atskleidimo padaryta žala atlyginama bendrais pagrindais.

Valstybės ir tarnybos paslapčių įstatymas detalizuoja, kokia informacija sudaro valstybės ar tarnybos paslaptį. Pirmąją gali sudaryti net 28, o antrąją – 25 kategorijų informacija.

Atskira teisės pažeidimų grupė – tai viešosios informacijos, darančios neigiamą poveikį nepilnamečių vystymuisi, skleidimas. Tokios informacijos požymius nustato Nepilnamečių

apsaugos nuo neigiamo viešosios informacijos poveikio įstatymo 4 straipsnis, o atsakomybę įtvirtina Administracinių teisės pažeidimų kodekso 214[19] straipsnis[37].

Bendru atveju už bet kurį paminėtą teisės pažeidimą atsako viešosios informacijos rengėjas (komentaro internete atveju - komentaro autorius) ir skleidėjas (tiesiogiai taikant analogiją su tradicine žiniasklaida tokiu reikėtų laikyti interneto portalo valdytoją ir (arba) interneto paslaugų tiekėją.

Kaip jau minėta, viena iš esminių komentarų internete savybių – automatizuotas turinio generavimas. Tai reiškia, kad redakcinis interneto portalų valdytojų įsikišimas iš esmės neegzistuoja. Tokiu atveju visa atsakomybė turėtų tekti komentaro autoriui. Tradicinėje žiniasklaidoje taikoma atsakomybė visuomenės informavimo priemonės rengėjui (skleidėjui) galėtų būti keičiama į atsakomybę interneto portalo valdytojui ar interneto paslaugų tiekėjui, užtikrinančiam prieigą prie tarnybinės stoties ir jos veikimą, tačiau ES elektroninės komercijos direktyvos 14-15 straipsniai imperatyviai draudžia atsakomybę skirti tarpinių informacinės visuomenės paslaugų tiekėjams, kuriais šiuo atveju ir reikėtų laikyti tiek interneto portalo valdytojus, tiek interneto paslaugų tiekėjus.

Tad esminiai klausimai, nagrinėjant komentarų internete autorių atsakomybę, yra du:

- Autorių identifikavimas (asmens tapatybės nustatymas);
- Turinio autorizavimas (valios pateikti atitinkamą turinį buvimas).

Pagrindinis asmens tapatybės identifikavimo įrankis – komentarą pateikusio įrenginio IP (*angl. internet protocol*) adresas. Daugeliu atveju tai yra pakankama informacija, leidžianti nustatyti komentaro kilmės šaltinį. Interneto paslaugų tiekėjo vidinių duomenų bazių įrašai leidžia vienareikšmiškai nustatyti fizinį ar juridinį asmenį, kuriam atitinkamu momentu buvo suteiktas atitinkamas IP adresas. Nors technologiškai gali atsirasti kliūčių dėl tarpinių (pavyzdžiui, proxy) tarnybinių stočių veikimo ar jurisdikcijos klausimų, tačiau viskas yra įmanoma.

Turinio autorizavimo klausimas yra faktinio pobūdžio, todėl kiekvienu atveju turi būti sprendžiamas individualiai. Pavyzdžiui, tėvui ginčijant, kad atžalos nepaskelbė ginčą sukėlusios

[37] http://liutauras.blogas.lt/150807/komentarai-internete-kas-turetu-atsakyti.html ; prisijungimo laikas 2008-11-03 15:29;

komentaro, įrodinėjimo pareigos paskirstymas leidžia rasti teisinio ginčo balansą. Interneto kavinių, viešų terminalų ar kitų neregistruojamos prieigos situacijų atvejais būtent paslaugų tiekėjai turėtų įvertinti savo teikiamų paslaugų naudojimo pavojus ir sukurti priemones, kurios leistų identifikuoti atitinkamą turinį skelbiančius asmenis.

Kai kuriuos atsakomybės subjekto klausimus galima būtų spręsti ir savireguliacijos metodais. Pavyzdžiui, komentarų internete skelbimui dažniausiai taikomi trys baziniai modeliai:

- Pilna asmens tapatybės identifikacija – šiuo atveju asmens tapatybė yra nustatoma vienareikšmiškai (pavyzdžiui, bankų paslaugos internete, deklaracijų teikimas Valstybinei mokesčių inspekcijai);

- Dalinė asmens tapatybės identifikacija – komentaras interneto portale skelbiamas tik praėjus tam tikrą registracijos procedūrą (tai gali būti veikiančio el. pašto tikrinimas, kreditinių kortelių autorizacija, minimalių duomenų pateikimas). El. pašto registracijos reikalavimas buvo laikinai naudojamas interneto portale www.bernardinai.lt, tačiau vėliau jo atsisakyta;

- Savanoriška asmens tapatybės identifikacija – lankytojai gali pateikti savo duomenis, tačiau tai nėra privaloma (pavyzdžiui, interneto portalai www.delfi.lt, www.omni.lt pateikia galimybę įvesti savo vardą, el. pašto duomenis ir pateikti savo komentarą, tačiau šių duomenų nepateikus komentaras vis tiek skelbiamas).

Akivaizdu, kad griežtesni reikalavimai tiesiogiai mažina lankytojų skaičių, todėl interneto portalo valdytojai visada sieks mažinti privalomus reikalavimus. Tokią tendenciją visuomenė turi vertinti rezervuotai, nes kartu tai simbolizuoja ir komentarų autorių baimę ginti savo nuomonę, tam tikrą atsiribojimą nuo jos.

Nors galiojančios Viešo naudojimo kompiuterių tinkluose neskelbtinos informacijos kontrolės ir ribojamos viešosios informacijos platinimo tvarkos 11 punktas[38] įtvirtina nuostatą, kad už interneto tinklalapio turinį atsako to interneto tinklalapio įkūrėjas (valdytojas), tačiau

[38] http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=206198 Dėl viešo naudojimo kompiuterių tinkluose neskelbtinos informacijos kontrolės ir ribojamos viešosios informacijos platinimo tvarkos patvirtinimo 2003 m. kovo 5 d. Nr. 290 ; prisijungimo laikas 2008-10-03 11:42;

reglamentavimą iš esmės pakeitė Visuomenės informavimo įstatymas[39], kuris pateikė dvi naujoves. Nustatė, jog už informacinės visuomenės informavimo priemonėse (ši sąvoka apima ir interneto portalus) pateikiamą informaciją atsako interneto svetainės (t.y. portalo) valdytojas, o taip pat, įtvirtino, kad atsakomybės reguliavimo principai įtvirtinami pagal ES elektroninės komercijos direktyvą parengtame informacinės visuomenės paslaugų įstatyme.

Informacinės visuomenės paslaugų įstatymo 14-15 straipsniai[40], atkartodami ES elektroninės komercijos direktyvos nuostatas numato, kad paslaugos teikėjas, paslaugos gavėjo prašymu saugantis jo pateiktą informaciją, už ją neatsako, jeigu:

- neturi faktinių duomenų apie neteisėtą paslaugos gavėjo veiklą arba apie tai, kad paslaugos gavėjo pateikta informacija įgyta, sukurta, pakeista ar naudojama neteisėtu būdu ir, kai reikalaujama atlyginti žalą, nežino apie faktus ir aplinkybes, rodančius neteisėtą paslaugos gavėjo veiklą arba tai, kad paslaugos gavėjas teikia neteisėtu būdu įgytą, sukurtą, pakeistą ar naudojamą informaciją;

- sužinojęs arba gavęs žinių apie neteisėtą paslaugos gavėjo veiklą arba apie tai, kad paslaugos gavėjo pateikta informacija įgyta, sukurta, pakeista ar naudojama neteisėtu būdu, skubiai imasi veiksmų, kad panaikintų galimybę tokią informaciją pasiekti[41].

Kadangi internete gaunama ne tiktai naudinga, bet ir nepageidaujama informacija, kuri daro žalingą poveikį pažeidžiamoms socialinėms grupėms bei visai visuomenei, taip pat informacija, kurios viešą skelbimą įstatymai riboja ar draudžia, atsiranda priežastys, lemiančios interneto turinio reguliavimą.

Bendrosios interneto turinio teisinio reguliavimo tendencijos:

- iki interneto atsiradimo galiojusių teisės aktų, reglamentuojančių informacijos naudojimą, pritaikymas publikuojant ir tvarkant informaciją internete;
- interneto paslaugų teikėjų atsakomybės reglamentavimas;
- savireguliavimo priemonių skatinimas;

---

[39] http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=107744&p_query=&p_tr2= Lietuvos Respublikos Visuomenės informavimo įstatymas 2000 m. rugpjūčio 29 d. Nr. VIII-1905,; prisijungimo laikas 2008-11-03 15:42;

[40] http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=277491&p_query=&p_tr2= Lietuvos Respublikos Informacinės visuomenės paslaugų įstatymas 2006 m. gegužės 25 d. Nr. X-614,; prisijungimo laikas 2008-11-03 10:42;

[41] http://liutauras.blogas.lt/150807/komentarai-internete-kas-turetu-atsakyti.html ; prisijungimo laikas 2008-11-03 15:42;

- specifinių teisių ir pareigų interneto paslaugų teikėjams nustatymas specialiaisiais teisės norminiais aktais siekiant užtikrinti veiksmingą nusikaltimų tyrimą kovą su tarptautiniu terorizmu, nacionalinio bei visuomenės saugumo bei kitų interesų apsaugą.

Pagal šiandien galiojančius norminius aktus žalingo turinio ir neskelbtinos informacijos viešą skelbimą Lietuvoje reglamentuoja:

1. 2000 m. rugpjūčio 29 d. Lietuvos Respublikos visuomenės informavimo įstatymas Nr. VIII-1905;
2. 1996 m. kovo 14 d. Lietuvos Respublikos vaiko teisių apsaugos įstatymas Nr. 1-1234;
3. 2002 m. rugsėjo 10 d. Lietuvos Respublikos nepilnamečių apsaugos nuo neigiamo viešosios informacijos poveikio įstatymas Nr. IX-1067;
4. 2004 m. balandžio 15 d. Lietuvos Respublikos elektroninių ryšių įstatymas Nr. IX-2135;
5. 1999 m. lapkričio 25 d. Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymas Nr. VIII-1443;
6. 2003 m. kovo 5 d. Lietuvos Respublikos Vyriausybės nutarimas Nr. 250 „Dėl viešo naudojimo kompiuterių tinkluose neskelbtinos informacijos kontrolės ir ribojamos viešosios informacijos platinimo tvarkos patvirtinimo";
7. 2006 m. gegužes 25 d. Lietuvos Respublikos informacinės visuomenės paslaugų įstatymas Nr. X-614.

Autorius, siekdamas atskleisti ar asmens tapatybės nustatymo internete samprata bei praktinis realizavimas yra aiški ir pakankamai teisiškai reglamentuota, taip pat ar reiktų kriminalizuoti atskirai asmens tapatybės klastotę elektroninėje erdvėje, atribojant ją nuo paprasto sukčiavimo atliko kokybinį tyrimą su 4 Policijos departamento prie Vidaus reikalų ministerijos Lietuvos kriminalinės policijos biuro Nusikaltimų elektroninėje erdvėje tyrimo skyriaus tyrėjais bei 2 Kauno apskrities Vyriausiojo policijos komisariato tyrėjais, kurie nepageidavo būti įvardintais. Šie tyrėjai buvo pasirinkti todėl, kad jų darbo profilis, specifika ir žinios nukreiptos į nusikaltimų, padarytų elektroninėje erdvėje tyrimą. Juos drąsiai galima įvardinti kaip tyrimo ekspertus. Kai kurie netgi veda mokymus Lietuvos policijos mokymo centre ir yra išleidę metodines rekomendacijas Kriminalinės policijos darbuotojams nusikaltimų elektroninėje erdvėje užkardymo, atskleidimo ir tyrimo klausimais Policijos departamento prie Lietuvos Respublikos Vidaus reikalų ministerijos leidžiamuose Kriminalinės informacijos biuleteniuose. Tyrimas buvo

atliktas tokia tvarka: buvo susitikta su kiekvienu tyrėju atskirai ir kiekvienam buvo užduoti iš anksto paruošti tie patys 6 klausimai. Klausimai buvo užduodami paeiliui, atsakius į pirmesnį buvo užduodamas sekantis klausimas.

Ekspertams užduoti klausimai:

1. Kokie vyraujantys nusikaltimai Lietuvoje, kai tenka nustatinėti asmens tapatybę Internete?

2. Kokios kyla teisinės problemos kvalifikuojant nusikaltimus ir įrodinėjant padarytą nusikalstamą veiką, kai tenka nustatinėti asmens tapatybę Internete? Ar reikia kriminalizuoti asmens tapatybės klastotę?

3. Ar Lietuvoje yra sukurta tinkama teisinė bazė tirti nusikaltimus elektroninėje erdvėje? Kokie yra pasiūlymai ir sprendimo būdai?

4. Kaip prognozuotų naujų, Lietuvai dar nebūdingų nusikaltimų atsiradimą ir protrūkį Lietuvoje (kokių nusikaltimų galima tikėtis ateinant iš užsienio)?

Apibendrinęs ekspertų interviu duotus atsakymus ir paaiškinimus, autorius nustatė, jog tiriant bet kokį nusikaltimą, padarytą elektroninėje erdvėje reikalinga nustatyti asmens tapatybę. Vienais atvejais tapatybė nustatoma lengviau, kitais sunkiau (tai dažniausiai priklauso nuo pačios nusikalstamos veikos ir tyrimo situacijos), tačiau praktiškai visais atvejais, tiriant nusikaltimus, padarytus Lietuvoje Lietuvos Respublikos piliečių, asmens tapatybės buvo nustatytos. Visi ekspertai nurodė, jog dažniausiai padaromos nusikalstamos veikos yra kvalifikuojamos pagal LR BK 214(Netikros elektroninės mokėjimo priemonės gaminimas, tikros elektroninės mokėjimo priemonės klastojimas ar neteisėtas disponavimas elektronine mokėjimo priemone arba jos duomenimis) ir 215 straipsnį (Neteisėtas elektroninės mokėjimo priemonės ar jos duomenų panaudojimas). Bylų apie kreditinį sukčiavimą Internetu Lietuvoje dar nebuvo registruota, nes veikos kvalifikuojamos arba pagal LR BK 214 str. arba 215 str..

Kvalifikuojant padarytas neteisėtas veikas Internete, vyrauja idealioji nusikaltimų sutaptis: sukčiavimas ir neteisėtas disponavimas elektronine mokėjimo priemone arba jos duomenimis. Tačiau dažniausiai kvalifikuojama kaip neteisėtas disponavimas elektronine mokėjimo priemone arba jos duomenimis ir tik po to – kaip sukčiavimas. Pasak ekspertų, pati

tapatybės klastotė yra kriminalizuota LR BK 214 ir 215 straipsniuose, todėl papildomai kriminalizuoti tokios sąvokos kaip aasmens tapatybės klastotė ekspertų nuomone visiškai nereikia. Su visais sprendėme kokia apskritai gali būti atsakomybė už tapatybės klastojimą Internete? Visų be išimties specialistų nuomone atsakomybės už tapatybės klastotę internete negali būti visai. Juk niekas negali drausti dalyvaujant diskusijose, forumuose ar kuriant elektroninį paštą pasivadinti kitokiu vardu, pavarde ar psiaudonimu. Kitaip bus varžomos žmogaus teisės. Juk neprivalu tokiais atvejais nurodyti savo tikrus asmens duomenis.

Visai kitas atvejis, jeigu asmuo nori Internetu gauti finansinę paramą ar paskolą, tuomet jis turi prisistatyti savo anketiniais duomenimis. Jeigu toks asmuo nurodo savo tikrus anketinius duomenis ir turi tikslą pinigų negrąžinti, jo veika bus kvalifikuojama kaip eilinis sukčiavimas (LR BK 182 str. 1 d.).

Jeigu toks asmuo nurodo savo netikrus anketinius duomenis, o suklastotus (išgalvotus), būtų galima veiką kvalifikuoti taip pat kaip paprastą sukčiavimą, nes bet kokiu atveju tokią veiką darančio asmens tikslas yra negrąžinti gautų pinigų. Tačiau Internetine bankininkyste užsiimančios kredito įmonės turi išsprendę galimybę nepasinaudoti tokia veika. Yra sukurtas visas mechanizmas kaip išvengti tokios asmens tapatybės klastotės, kadangi visi anketiniai duomenys yra tikrinami su esama LR VRM gyventojų registro duomenų baze ir esant išgalvotiems asmens tapatybės duomenims, elektroninė sistema paprasčiausiai neduoda galimybės gauti paskolos internetu. Taigi vėl priėjome tos pačios išvados, jog nėra reikalo kriminalizuoti pačią tapatybės klastotę, jeigu tą suponuoja sukčiavimas.

Jeigu pilietis bando paimti kreditą ir pateikia svetimus, tačiau tikrus asmens tapatybės duomenis, veiką tyrėjai kvalifikuoja kaip idealiąją sutaptį sukčiavimo (LR BK 182 str.) ir kaip neteisėtu disponavimu elektronine mokėjimo priemone arba jos duomenimis (LR BK 214 str.). Realiai galima traktuoti kaip savo asmens tapatybės klastojimą, pasinaudojant svetimais tapatybės duomenimis, tačiau visa tai ir apima pati sukčiavimo forma: „Tas, kas apgaule ar kitų naudai įgijo svetimą turtą ar turtinę teisę, išvengė turtinės prievolės arba ją panaikino“.

Vieninga visų ekspertų nuomonė: kad kriminalizuoti asmens tapatybės klastotę, reiktų išspręsti retorinį klausimą: kada galima sukčiauti, o kada negalima? Kuriant elektroninį paštą ar dalyvaujant forumuose ir diskusijose įstatymų leidėjas negali tokių dalykų atriboti, kad kriminalizuoti atsmens tapatybę per sukčiavimo prizmę. Kadangi skirtingose situacijose gali kilti

skirtingi teisiniai niuansai: vienais atvejais gali būti leista asmens tapatybę klastoti, kitais gi – griežtai draudžiama.

Anksčiau, kai nebuvo atsakomybės už neteisėtą disponavimą elektronine mokėjimo priemone arba jos duomenimis, tada neteisėtos veikos buvo kvalifikuojamos kaip paprastas sukčiavimas ar pasikėsinimas sukčiauti. Tačiau po 2007 m. liepos 21 d. įsigaliojusių pakeitimų LR BK 214 ir 215 str. (V.Ž. 2007-07-21 Nr.81-3309) ir šių straipsnių išplėtimo visos problemos buvo išspręstos.

Nėra nei vieno ruošiamo, priimto ar galiojančio teisės akto ir tvarkos, kurie reglamentuotų asmens tapatybę ir jos nustatymą Internete. Visų ekspertų nuomone teisinė bazė Lietuvoje dėl asmens tapatybės klastojimo, siekiant įvykdyti nusikalstamą veiką yra pilnai reglamentuota. Papildomų įstatymų priimti nereikia.

LR BK 214 ir 215 straipsnių Lietuvoje pilnai pakanka, kad kvalifikuoti teisingai ir patraukti atsakomybėn visus tuos asmenis, kurie bando prisistatyti kitu vardu ar pateikia netikrus duomenis apie save, arba svetimus mokėjimo duomenis (suklastoja savo tapatybę elektroninių atsiskaitymų metu) kad įgyti finansinę naudą ar teisę į ją.

Visai kitaip yra šmeižimo bylose: čia tapatybė yra slepiama ar klastojama tam, kad toks asmuo nenori, jog jis būtų surastas ir išvengti atsakomybės (subjektyvioji pusė). Čia negali būti net kalbos apie asmens tapatybės klastojimo kriminalizavimą.

Internetinė tapatybė yra labai lengvai nuslepiama ir niekas jos negali kriminalizuoti.

Techninę klastotę ekspertai nusakė kaip būdą nuslėpti tikrąją tapatybę, pasinaudojus tam tikrom, būtent tam sukurtom, techninėm priemonėm (pvz. naudoti ne savo IP adresus, svetimus proxy serverius, įvairius anonimizatorius), kad būtų neįmanoma visiškai nustatyti tikrosios tapatybės. Paprastai tokiomis priemonėmis naudojasi asmenys, gerai išmanantys programavimo subtilybes ir siekiantys neteisėtų tikslų, iš anksto gerai pasiruošę ir gerai apgalvoję savo veiksmus bei linkę išlikti anonimiški ir nenustatyti teisėssaugos įstaigų pareigūnų. Nustatyti tokių asmenų tapatybę yra arba be galo sunku, arba net visiškai neįmanoma.

Psiaudoklastotę arba netikrą klastotę ekspertai nurodė, kai asmuo pasivadinės susigalvotu psiaudonimu (*angl. Nick*) ar išgalvotu vardu arba svetimu vardu, mano ar bent tikisi, jog niekas jo tikrosios asmenybės nenustatys, ir net nesuvokia, jog techninėmis priemonėmis tai

galima sėkmingai nustatyti. Tokiu budu savo tapatybę paprastai slepia vaikai ar mažai išsilavinę ir neturintys didelio supratimo apie galimybę nustatyti asmens tapatybę techninėmis priemonėmis asmenys. Psiaudoklastotė dažniausiai naudojama iš pykčio, siekiant kažką apšmeižti, paskleisti paskalas ar atkeršyti, kai techninėm priemonėm maskuoja tapatybę ir kai nenaudoja jokių papildomų techninių priemonių, tiktai pasirašo išgalvotu vardu.

Viskas kas yra sugalvojama neteisėto pasaulyje, sėkmingai ateina ir į Lietuvą.

Pastaruoju metu visos neteisėtos veikos per Internetą yra nukreiptos į finansinę naudą, t.y. gauti kuo daugiau finansinės naudos. Virusų (Trojos arklių, worm-ų) kūrimas, DOS atakos yra daromi pirmiausiai siekiant finansinės naudos. Įvairūs virusai ir jų atmainos yra kuriami asmens duomenų vagystėms, siekiant užkrėsti vartotojų kompiuterius ir pasisavinti šių vartotojų konfidencialią informaciją apie bankininkystę. Žlugdant konkurentus įvairiose verslo struktūrose specialiais užsakymais yra labai plačiai vartojami būdai, kad nulaužti tinklalapių kodus ir patalpinti kompromituojančią įmonę ar akcininkus informaciją į tinklalapį, arba tiesiog sustabdyti įprastą veiklą Internetu.

Phishingui labai aktyviai naudojami netikrų (suklastotų) finansinių institucijų tinklalapių kūrimas, pastaruoju metu labai dažnai pasitaiko Lietuvoje. Praktiškai kiekvienais metais tokių nusikaltimų skaičius didėja proporcingai kas 100%. Daugiausiai yra kuriami identiški bankų tinklalapiai, „eBay“ ar „PayPal“ sistemų tinklalapiai, kur bandoma gauti mokėjimų duomenis ir vėliau jais pasinaudoti. Kiekvienais metais tokių nusikaltimų daugėja.

Vieni nusikaltimai yra padaromi siekiant finansinės naudos, tokių būna apie 85-90%, kiti – apie 10% - nusikaltimai tokie kaip pornografinio turinio, kuriuose atvaizduotas vaikas, produkcijos įgijimas platinimas ar laikymas (pvz. vaikų pornografija, pedofilija) daromi savo liguistų seksualinių aistrų tenkinumui. Tokių nusikaltimų tyrimui aktyviai yra bendraujama su Europolo pareigūnais, betarpiškai keičiamasi informacija. Pastebima tendencija, jog dažniausiai tokio pobūdžio pornografinio turinio su vaikais produkcija yra platinama per P2P programas, tačiau techninėmis priemonėmis labai lengvai yra nustatoma asmenų tapatybė, atliekamos kratos ir asmenys patraukiami baudžiamojon atsakomybėn.

Ir tiktai maždau apie 2 % visų nusikaltimų apima įsilaužimas Internetu dėl chuliganiškų paskatų kai laužomi finansinių ar valstybinių institucijų tinklalapiai, įsilaužiama į teisėsaugos ar kariuomenės duomenų bazes, serverius, tikslu pasirodyti prieš kitus programišius, kad įrodyti

savo profesionalumą ir apsaugos sistemų silpnasias puses, arba kitų šalių žvalgybos įstaigų užsakymu, tikslu pažeisti šalies internetinę infrastuktūrą ir nustatyti jos silpnąsias puses. Lietuvoje tokių nusikaltimų yra praktiškai labai mažai, jų tyrimas paprastai yra labai sudėtingas, nes visi keliai veda į užsienio šalis, o ne visos šalys, ypatingai Rytų pusėje noriai bendradarbiauja tyrimo klausimais.

Dėl nusikaltimų latentiškumo:

Rečiausiai kreipiasi įpolicijos įstaigas mažos įmonės. Lietuvos bankai kreipiasi į Policijos departamentą visais atvejais, kai fiksuojamas neteisėtas įsibrovimas į banko duomenų bazes, Phishingo atveju ar kitais atvejais, kai neteisėtai buvo pasinaudota banko klijento duomenimis Internetu. Praktiškai prie nusikaltimų, padaromų elektroninėje erdvėje latentiškumo Lietuvos bankai neprisideda. Visos baudžiamosios bylos, kuriose ikiteisminis tyrimas buvo pradėtas pagal bankų pranešimus apie 90 % buvo ištirtos, o nusikaltimus padarę asmenys – patraukti baudžiamojon atsakomybėn.

Apibendrinus ir išanalizavus visų 6 ekspertų interviu apklausas galima daryti išvadas, jog Lietuvoje yra pakankama teisinė bazė, todėl papildomai kriminalizuoti tokios neteisėtos veikos kaip asmens tapatybės klastotė – nereikia. Nėra nei vieno ruošiamo, priimto ar galiojančio teisės akto ir tvarkos, kurie reglamentuotų asmens tapatybę ir jos nustatymą Internete.

IŠVADOS IR PASIŪLYMAI

Lietuvoje dėl milžiniškų informacinių technologijų vystymosi tempų teisės mokslas nebesuspėja tinkamai išnagrinėti ir įvertinti naujai atsirandančių santykių dėl ko teisės normos tik iš dalies sprendžia praktines problemas. Tuo pat metu daugelis autorių pateikia skirtingas nuomones, kaip spręsti iškilusias problemas, o teismų sprendimų asmens tapatybės nustatymo internete klausimais iš viso nėra. Darbe buvo atskleistos asmens tapatybės galimos būsenos internete, kylančios iš to teisinės problemos, nurodomi galimi sprendimo būdai, priderinti prie dabar galiojančių teisės aktų. Atsižvelgiant į tai būtina išskirti ir sistemiškai pristatyti pagrindines šio darbo išvadas:

1. Darbe iškelta hipotezė nepasitvirtino šiais aspektais:

- Lietuvoje nėra atskirai išskirta ir kriminalizuota asmens tapatybės klastotė Internete, tačiau to ir nereikia, kadangi visiškai užtenka šiuo metu galiojančių teisės aktų.

- Lietuvoje teisinė bazė pilnai reglamentuota ir pakankama, kad tinkamai kvalifikuoti nusikalstamas veikas, padaromas elektroninėje erdvėje.

2. Nėra nei vieno ruošiamo, priimto ar galiojančio teisės akto ir tvarkos, kurie reglamentuotų asmens tapatybę ir jos nustatymą Internete.

3. Šalių tapatybė nėra esminė galiojančio sandorio sąlyga, tačiau jos nebuvimas labai apriboja praktinį absoliučiai anonimiško sandorio įgyvendinamumą ir tokiu būdu sumenkina jo teisinę vertę.

4. Dabartinis Lietuvoje veikiantis teisinis reguliavimas nėra pritaikytas anonimiškumui elektroninėje erdvėje. Siūlytina derinti šiuo metu galiojančias prekybos ir paslaugų taisykles prie elektroninės komercijos keliamų poreikių. Didžiausią dėmesį skirti anonimiškų vartotojų, ypatingai tų, kurie naudojasi elektroninėmis priemonėmis, teisių apsaugai. Taip pat siūlytina sukurti visiškai naują reguliacinę bazę, kuri reguliuotų visiškai anonimiškų sandorių keliamus poreikius, o taip pat konkretizuotų teises ir pareigas abiems sandorių pusėms.

5. Kalbant apie teisių apribojimą anonimiškai būti elektroninėje erdvėje, kad užkardyti terorizmą, galima pažymėti, kad Lietuvos Respublikos baudžiamąjame kodekse nėra nei tikslaus terorizmo apibrėžimo nei terorizmo apibūdinimo kaip nusikalstamos veikos (išskyrus patį teroro aktą), todėl Lietuvoje netinkamai įgyvendinamas proporcingas ir sąžiningas teisės į anonimiškumą elektroninėje erdvėje apribojimas. Siūlytinas terorizmo kaip nusikalstamos veikos apibūdinimas Lietuvos Respublikos Baudžiamąjame kodekse.

6. Asmens tapatybę Internete galima identifikuoti keliais būdais: pasitelkus programavimą (specialiąsias programas, kurios gali rinkti asmens duomenis) ir pasitelkiant trečiuosius asmenis.
7. Internetas pakeitė nusistovėjusią pusiausvyrą tarp teisės į informaciją ir teisės į privatumą. Pasikeitė visuomenės požiūris į informaciją – informacijos rinkimas, jos apdorojimas tapo svarbus ir ekonomine, ir moksline prasme.

NAUDOTOS LITERATŪROS SĄRAŠAS

ĮSTATYMAI

1. Lietuvos Respublikos Konstitucija// Valstybės Žinios, 1992, Nr. 33-1014 (1992-11-30)

2. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas// Valstybės žinios. 1996, Nr. 63-1479.

3. Lietuvos Respublikos Civilinis kodeksas, patvirtintas// Valstybės žinios. 2000-07-18 Nr. VIII-1864;

4. LIETUVOS RESPUBLIKOS, ELEKTRONINIŲ RYŠIŲ, ĮSTATYMAS// Valstybės žinios. 2004 m. balandžio 15 d. Nr. IX-2135;

5. Lietuvos Respublikos Operatyvinės veiklos įstatymas// Valstybės žinios, 2002 m. birželio 20 d. Nr. IX-965,

6. Lietuvos Respublikos Baudžiamasis kodeksas// Valstybės žinios, Nr. VIII-1968;

7. Lietuvos Respublikos Administracinių teisės pažeidimų kodeksas// Valstybės žinios, Nr. X-1766;

8. Dėl viešo naudojimo kompiuterių tinkluose neskelbtinos informacijos kontrolės ir ribojamos viešosios informacijos platinimo tvarkos patvirtinimo// Valstybės žinios, 2003 m. kovo 5 d. Nr. 290

9. Lietuvos Respublikos visuomenės informavimo įstatymas// Valstybės žinios, 2000 m. rugpjūčio 29 d. Nr. VIII-1905;

10. Lietuvos Respublikos vaiko teisių apsaugos įstatymas// Valstybės žinios, 1996 m. kovo 14 d. Nr. 1-1234;

11. Lietuvos Respublikos nepilnamečių apsaugos nuo neigiamo viešosios informacijos poveikio įstatymas// Valstybės žinios, 2002 m. rugsėjo 10 d. Nr. IX-1067;

12. Lietuvos Respublikos elektroninių ryšių įstatymas// Valstybės žinios, 2004 m. balandžio 15 d. Nr. IX-2135;

13. Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymas// Valstybės žinios, 1999 m. lapkričio 25 d. Nr. VIII-1443;

14. „Dėl viešo naudojimo kompiuterių tinkluose neskelbtinos informacijos kontrolės ir ribojamos viešosios informacijos platinimo tvarkos patvirtinimo"// Valstybės žinios, 2003 m. kovo 5 d. Lietuvos Respublikos Vyriausybės nutarimas Nr. 250;

15. Lietuvos Respublikos informacinės visuomenės paslaugų įstatymas// Valstybės žinios, 2006 m. gegužes 25 d. Nr. X-614.

KITA LITERATŪRA

16. Legal privacy, De la presente edicion, Prensas Universitarias de Zaragoza, 2008. Limitation of the right to anonymity as a partof the right to privacy in cyberspace for the suppression of terrorism in the Republic of Lithuania. Rimantas Petrauskas and Kristina Spalveters, p. 293-303.

17. Milana Homsi, I Know What You Did Last Night (and this morning too): Protecting Your Anonymity in a World of Identifying Technologies, University of Ottawa, Faculty of Common Law, Faculty Supervisor: Professor Ian Kerr, October 31,2003.

18. Jonathan Turley, Registering publius: The supreme court and the right to anonymity, 2002, CATO supreme court review.

19. Sabaliauskas G. Informacijos saugumas internete: teisininkų ir informatikų problema // Justitia 2001 Nr. 1, psl. 28 – 30.

20. Brian Kim, Chris Laas, Sbelly O'Gilvie, Alexander Yip Anonymity Tools for the Internet, May 17, 2001

21. A.Vaišvila. Teisės teorija: vadovėlis.- Vilnius:Justitia, 2000, P. 324.

22. 1981 m. Strasbūro konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu, 2 str. // Pagrindinės Europos Tarybos sutartys. - Vilnius: Europos Tarybos informacijos ir dokumentacijos centras, 2000.

23. R. Dingledine, "The Free Haven project: Design and deployment of an anonymous secure data haven," Master's thesis, Massachusetts Institute of Technology, 2000

24. D. M. Roger Dingledine, Michael Freedman, "The Free Haven project: Distributed anonymous storage service," in Proceeding* of the Workshop on Design Issues in Anonymity and VnobservabUity, July 2000.

25. S.Fisher-Hubner, G.Quirchmayr, L.Yngstrom, User Identification&Privacy Protection, 1999, Kista, Sweden

26. Jonathan D. Wallace, Nameless in Cyberspace Anonymity on die Internet, December 8,1999, No.54

27. Kurapka E., Malevski H., Palskys E., Kuklianskis S. Kriminalistikos technikos pagrindai,-Vilnius, 1998.P.16.

28. Ruth Gavison. Privacy and the Limits of the Law // Yale Law Journal. – Jan. 1980, vol 89, no 3, P. 428.

INTERNETINĖS NUORODOS

29. www.itc.tf.vu.lt/mokslas/asmens%20duomenu%20teisines%20apsaugos%20klausimai%20interneto%20kontekste.doc ASMENS DUOMENŲ TEISINĖ APSAUGA INTERNETO KONTEKSTE PAGAL EUROPOS SĄJUNGOS IR TARPTAUTINĘ TEISĘ, Teisės fakulteto V kurso Tarptautinės ir Europos Sąjungos teisės specializacijos studentė Kristina Spalveters, Vilnius 2003. (žr. 2008-05-25)

30. http://www.itc.tf.vu.lt/ Šalių anonimiškumo problema interneto kontekste, Autorius: M.Civilka, prisijungimo laikas 2008-11-26 12:53;

31. http://www.bernardinai.lt/index.php?url=articles/72769 , prisijungimo laikas 2008-10-25 16:53;

32. http://whatismyipaddress.com/staticpages/index.php/internet-anonymity , prisijungimo laikas 2008-05-25 16:53;

33. CIFAS, the UK Fraud Prevention Service 2008-09-28 http://ec.europa.eu/internal_market/fpeg/identity-theft_en.htm , prisijungimo laikas 2008-10-25 16:53;

34. http://italy.usembassy.gov/pdf/other/RS22082.pdf , prisijungimo laikas 2008-11-02 15:15;

35. http://www.usatoday.com/tech/news/computersecurity/hacking/2005-02-16-choicepoint-hacked_x.htm , prisijungimo laikas 2008-11-02 16:25;

36. Asmens duomenų apsauga Tarptautinėje teisėje http://www.itc.tf.vu.lt/paskaitos/paskait/ada_1.12.pdf ; prisijungimo laikas 2008-10-08 20:20;

37. http://lw.bna.com/lw/19980210/98116.htm ; prisijungimo laikas 2008-10-15 16:53;

38. *Civilka M.* Asmens duomenų apsaugos teisinis reguliavimas interneto kontekste. <http://www.itc.tf.vu.lt/mokslas/mokslas.html

39. Lietuvos Respublikos Valdymo reformų ir savivaldybių reikalų ministerija. Lietuvos Respublikos elektroninio parašo įstatymo projekto aiškinamasis raštas, 2000 05 26, Nr. P-2567, http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=101575 ,prisijungimo laikas 2008-10-25 16:53;

40. http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0058:20060503:LT:PDF ; prisijungimo laikas 2008-11-14 17:29;

41. http://cybercrimes.eu/index.php?topic=4.0 ; prisijungimo laikas 2008-11-28 17:29;

42. http://liutauras.blogas.lt/150807/komentarai-internete-kas-turetu-atsakyti.html; prisijungimo laikas 2008-11-03 15:29;

SANTRAUKA LIETUVIŲ KALBA

Magistro baigiamąjame darbe nagrinėjama asmens tapatybės nustatymo internete samprata bei praktinis realizavimas, analizuojama ar pakankamai teisiškai reglamentuota, taip pat ar yra būtinumas kriminalizuoti asmens tapatybės klastotę elektroninėje erdvėje, atribojant ją nuo paprasto sukčiavimo.

Pagrindinis tyrimo tikslas - išanalizuoti teisinius ir praktinius asmens tapatybės Internete buvimo, slėpimo ir klastojimo aspektus, nurodyti pagrindines teisines problemas, su kuriomis susiduriama siekiant išlikti anonimiškam, o taip pat pateikti išvadas ir siūlymus kaip tobulinti teisinį reguliavimą.

Darbe iškelta hipotezė, kad asmens tapatybės nustatymo internete samprata bei praktinis realizavimas yra neaiški ir nepakankamai teisiškai reglamentuota, taip pat reiktų kriminalizuoti asmens tapatybės klastotę elektroninėje erdvėje, atribojant ją nuo paprasto sukčiavimo, nepasitvirtino šiais aspektais:

- Lietuvoje nėra atskirai išskirta ir kriminalizuota asmens tapatybės klastotė Internete, tačiau to ir nereikia, kadangi visiškai užtenka šiuo metu galiojančių teisės aktų.

- Lietuvoje teisinė bazė pilnai reglamentuota ir pakankama, kad tinkamai kvalifikuoti nusikalstamas veikas, padaromas elektroninėje erdvėje.

Dabartinis Lietuvoje veikiantis teisinis reguliavimas nėra pritaikytas anonimiškumui elektroninėje erdvėje, todėl siūlytina derinti šiuo metu galiojančias prekybos ir paslaugų taisykles prie elektroninės komercijos keliamų poreikių. Didžiausią dėmesį skirti anonimiškų vartotojų, ypatingai tų, kurie naudojasi elektroninėmis priemonėmis, teisių apsaugai. Taip pat siūlytina sukurti visiškai naują reguliacinę bazę, kuri reguliuotų visiškai anonimiškų sandorių keliamus poreikius, o taip pat konkretizuotų teises ir pareigas abiems sandorių pusėms.

Kalbant apie teisių apribojimą anonimiškai būti elektroninėje erdvėje, kad užkardyti terorizmą, nustatyta, kad Lietuvos Respublikos baudžiamąjame kodekse nėra nei tikslaus terorizmo apibrėžimo nei terorizmo apibūdinimo kaip nusikalstamos veikos, siekiant Lietuvoje tinkamai įgyvendinant proporcingą ir sąžiningą teisės į anonimiškumą elektroninėje erdvėje

apribojimą, siūlytinas terorizmo kaip nusikalstamos veikos apibūdinimas Lietuvos Respublikos Baudžiamąjame kodekse.

Pagrindinės sąvokos: asmens tapatybė, asmens tapatybės vagystė, anonimiškumas, asmens tapatybės klastotė, terorizmas, slėpimo ir klastojimo aspektai, teisinis reguliavimas, teisiniai aspektai.

SANTRAUKA ANGLŲ KALBA

Keywords: personal identity, theft of personal's identity, anonymity, fraud of personal's identity, terrorism, evasion and fraud aspects, legal regulation, legal aspects.