ISSN 1392-1592. TEISĖS PROBLEMOS. 2012. Nr. 3 (77)

Vaidas KALPOKAS
Teisės instituto kriminologinių tyrimų
skyriaus jaunesnysis mokslo darbuotojas

Renata MARCINAUSKAITĖ
Teisės institutas

TAPATYBĖS VAGYSTĖ ELEKTRONINĖJE ERDVĖJE: TECHNOLOGINIAI ASPEKTAI IR BAUDŽIAMASIS TEISINIS VERTINIMAS

Straipsnyje analizuojamas vienas iš sukčiavimo elektroninėje erdvėje etapų – neteisėtas disponavimas konfidencialiais asmens tapatybę elektroninėje erdvėje patvirtinančiais duomenimis. Straipsnyje apžvelgti ne tik technologiniai asmens identifikavimui elektroninėje erdvėje naudojamų duomenų neteisėto gavimo būdai, bet ir pagrindinės tokio pobūdžio nusikalstamų veikų kvalifikavimo problemos. Taip pat, atsižvelgiant į teismų praktiką, pasiūlyti kylančių tapatybės vagystės kvalifikavimo problemų sprendimo variantai.

1. ĮVADAS

Tobulėjant informacinėms technologijoms, sparčiai plečiasi jų pritaikymo ir suteikiamų galimybių įvairovė, didėja jomis besinaudojančių gyventojų skaičius. Į internetą pamažu persikelia vis daugiau kasdienio žmonių gyvenimo ir visuomenės veiklos sričių. Atitinkamai atsiranda ir įmantresnių neteisėtos veiklos skaitmeninėje erdvėje būdų, nusikalstamų veikų schemos tampa sudėtingesnės. Neteisėta veikla skaitmeninėje erdvėje, iš pradžių labiau panėšėjusi į nekaltus papokštavimus, chuliganiškus veiksmus ar vandalizmą (pvz., kompiuteriniai virusai, skirti kompiuterių operacinės sistemos veiklai sutrikdyti, arba internetinių puslapių išvaizdos pakeitimas (angl. *defacement*), laikui bėgant tapo vis labiau finansiškai motyvuota, orientuota į tiesioginės piniginės naudos siekimą. Informacinės technologijos ir internetas pradėti naudoti kaip naujos ir patogios priemonės vykdyti tradicines nusikalstamas veikas (pvz., sukčiavimą, pinigų plovimą, seksualinį priekabiavimą, šantažą ir kt.). Taip pat atsirado ir naujų nusikalstamų veikų, būdingų ir įmanomų atlikti tik skaitmeninėje erdvėje (pvz., neteisėtas

prisijungimas, kompiuteriniai virusai, kompiuterinių sistemų atakos ir pan.). Dažnai minėtas veikas vykdo ir koordinuoja jau nebe pavieniai asmenys, o gerai organizuotos grupės, kurios, bendradarbiaudamos tarpusavyje, specializuojasi konkrečiose srityse: kurdamos ir platindamos kenkimo programinę įrangą, išgaudamos konfidencialią vartotojų informaciją (prisijungimo slaptažodžius, mokėjimo kortelių numerius, PIN kodus ir kt.), realizuodamos šią informaciją, išgrynindamos gautas pajamas ir pan.[1]

Toks veiklos sričių pasidalijimas neretai būdingas ir veikoms, kurias apibendrintai galima pavadinti sukčiavimu elektroninėje erdvėje (angl. *internet fraud, computer fraud*). Bendriausia prasme tai tokios veikos, kuriose informacinės technologijos panaudojamos sukčiavimui atlikti. Kiek supaprastinant, galima teigti, kad daugumos sukčiavimo būdų pagrindiniai principai yra labai panašūs – tai tam tikros informacijos gavimas ir jos panaudojimas, siekiant gauti turtinės naudos. Informacija čia gali būti laikomi įvairūs elektroninėje erdvėje naudojami vartotoją identifikuojantys duomenys, prisijungimo kodai bei slaptažodžiai, mokėjimo kortelių duomenys, banko sąskaitų rekvizitai ir t. t. Todėl apie įvairias neteisėto asmens tapatybę elektroninėje erdvėje patvirtinančių duomenų gavimo, jų turėjimo savo žinioje ir panaudojimo baudžiamojo teisinio vertinimo problemas leidžia kalbėti būtent sukčiavimo elektroninėje erdvėje specifika, tapatybės nustatymo elektroninėje erdvėje ir įvairių elektroninių paslaugų (elektroninės bankininkystės, elektroninių parduotuvės ir kita) ypatumai.

Atsirandant vis naujiems identifikavimui elektroninėje erdvėje naudojamų duomenų neteisėto gavimo būdams, aktualu apžvelgti ne tik juos, bet ir pagrindines padarytų nusikalstamų veikų kvalifikavimo problemas. Todėl šiame straipsnyje apibendrinti pagrindiniai tapatybės vagystės padarymo būdai, taip pat, atsižvelgiant į besiformuojančią teismų praktiką, aptarti ir tokios veikos įvairūs baudžiamojo teisinio vertinimo probleminiai aspektai. Kadangi neteisėtas disponavimas konfidencialiais asmens tapatybę elektroninėje erdvėje patvirtinančiais duomenimis yra vienas iš elektroninio sukčiavimo etapų, todėl tinkamas tokio pobūdžio nusikalstamų veikų kvalifikavimas užtikrintų ir tinkamą baudžiamosios atsakomybės taikymą už sukčiavimo padarymą. Atsižvelgiant į tai, straipsnyje pasiūlyti įvairių baudžiamojo įstatymo taikymo metu kylančių tapatybės vagystės kvalifikavimo problemų sprendimo variantai.

2. SUKČIAVIMO ELEKTRONINĖJE ERDVĖJE IR TAPATYBĖS VAGYSTĖS SĄSAJA

Sukčiavimui elektroninėje erdvėje apibūdinti, be apgaulės ir turtinės naudos gavimo

[1] *Graham J., Howard R.* Cyber fraud: tactics, techniques, and procedures. New York (N.Y.): CRC Press, 2009, p. 21.

pasitelkus ir būtiną poveikio informacinei sistemai ar elektroniniams duomenims elementą,[2] šios veikos padarymas neišvengiamai susiejamas ir su įvairiais elektroninių duomenų ir informacinių sistemų konfidencialumo pažeidimais. Kadangi asmuo skaitmeninėje erdvėje dažniausiai atpažįstamas per tarpininkus – informacijos ir komunikacijos technologijas, todėl apgaule yra siekiama suklaidinti būtent šias technologijas. Joms suklaidinti (apgaulei įgyvendinti) dažniausiai yra būtini asmens tapatybę elektroninėje erdvėje patvirtinantys ir įvairius veiksmus joje leidžiantys atlikti duomenys.

Kalbant apie įvairius apgaulės elektroninėje erdvėje aspektus reikėtų pabrėžti, kad šie atvejai išeina už tradicinės apgaulės ribų, nes pateiktomis melagingomis žiniomis yra suklaidinamas ne fizinis asmuo, o elektroninė sistema.[3] Tai leidžia kalbėti apie specifinę apgaulės formą elektroninių duomenų perdavimo sistemose.[4] Šio požiūrio ištakos yra siejamos su kasacinio teismo praktika. Lietuvos Aukščiausiojo Teismo 2001 m. spalio 9 d. nutartyje kasacinėje byloje Nr. 2K-682/2001 išaiškinta, kad „*jei kodą surenka ir komandą duoda asmuo, neturintis teisės atlikti operacijų su sąskaitoje esančiomis piniginėmis lėšomis, jis pateikia operacinei sistemai ir bankui save kaip kitą asmenį, turintį tokią teisę, ir taip suklaidina elektroninę sistemą ir kartu banką*“. Nutartyje minimas elektroninės sistemos suklaidinimo aspektas kartu leidžia pažymėti ir tai, kad asmens identifikavimui elektroninėje erdvėje pakankamų duomenų neteisėtas įgijimas dažnai yra tarpinis etapas siekiant padaryti kitas nusikalstamas veikas. Šie duomenys gali būti neteisėtai realizuojami (pavyzdžiui, prekybos neteisėtai pasisavintais duomenimis atveju), panaudojami darant sukčiavimą ir kt.

Tolesnėje analizėje pagrindinis dėmesys bus skiriamas vienam iš sukčiavimo elektroninėje erdvėje etapų – tapatybės vagystei (angl. *identity theft*), pradedant nuo paprasčiausių apgaulingų elektroninio pašto laiškų ir pereinant prie sudėtingesnių konfidencialios vartotojų informacijos išgavimo būdų. Taip pat bus aptartos

---

[2] Europos Tarybos konvencijos dėl elektroninių nusikaltimų (Lietuva ratifikavo 2004 m. sausio 22 d.) 8 straipsnis ir Tarybos pamatinio sprendimo, skirto kovai su sukčiavimu negrynosiomis mokėjimo priemonėmis ir jų klastojimu, 3 straipsnis, be apgaulės ir turtinės naudos gavimo požymių, leidžia išskirti trečiąjį – kompiuterinės sistemos panaudojimo – požymį. Jis minėtuose tarptautiniuose instrumentuose apibūdinamas per elektroninių duomenų *(„įvedant, pakeičiant, sunaikinant kompiuterinius duomenis arba panaikinant galimybę naudotis tokiais duomenimis“)* ir informacinių sistemų saugumo *(„paveikiant kompiuterinės sistemos darbą“)* pažeidimus. Šio trečiojo sukčiavimo elektroninėje erdvėje atpažinimui svarbaus elemento atsiradimą iš esmės lėmė kompiuterinių technologijų ir išskirstytų technologijų, pagrįstų kelių kompiuterių sąveika per tinklą, viena pagrindinių savybių – galimybė keistis duomenimis tarp sujungtų, tačiau savarankiškai veikiančių kompiuterių.

[3] *Pranka D.* Apgaulės samprata ir reikšmė atribojant sukčiavimą ir civilinės teisės pažeidimą. Socialinių mokslų studijos. 2012, 4(2), p. 666.

[4] *Sinkevičius E.* Neteisėtas banko kredito gavimas arba panaudojimas ir jų kvalifikavimas. Vilnius: Lietuvos teisės universiteto Leidybos centras, 2002, p. 51.

ir pagrindinės tokio pobūdžio pavojingos veikos baudžiamojo teisinio vertinimo problemos.

3. PAGRINDINIAI TAPATYBĖS VAGYSTĖS PADARYMO BŪDAI

3.1. *Fišingas*[5]

Kasdien interneto vartotojų elektroninio pašto dėžutes pasiekia daugybė nepageidaujamų elektroninių laiškų. Jų paskirtis gali būti įvairi. Mažiausiai kenksminguose tiesiog įkyriai reklamuojamos įvairios prekės ar paslaugos, tam tikra dalis gali būti skirta kompiuteriniams virusams ar kitoms kenksmingoms programoms platinti (apie tai kalbėsime vėliau), bet dažnai pasitaiko tokių, kuriuose apgaulingomis manipuliacijomis bandoma išvilioti gavėjų pinigus ar kitą informaciją. Egzistuoja daugybė tokių laiškų ir juose pasakojamų istorijų modifikacijų, tačiau daugumoje jų bandoma išnaudoti patiklių žmonių norą lengvai ir greitai praturtėti, pigiau įsigyti kokių nors prekių arba išvengti tam tikrų nemalonumų. Vis dėlto tikimybė, kad potenciali sukčiavimo auka patikės apgaule, yra labai nedidelė. Šie sukčiavimo būdai jau gana gerai žinomi interneto vartotojams ir platesnei visuomenei. Iš pirmo žvilgsnio tikroviškai atrodantys elektroniniai laiškai vėliau nesunkiai atpažįstami, nes pagrindiniai jų principai išlieka nepakitę, modifikuojamas tik laiškų turinys, pritaikant prie aktualių pasaulio ar konkrečios šalies įvykių. Visa tai verčia sukčiautojus ieškoti išradingesnių apgaulės ir reikiamos informacijos ar pinigų išviliojimo būdų.

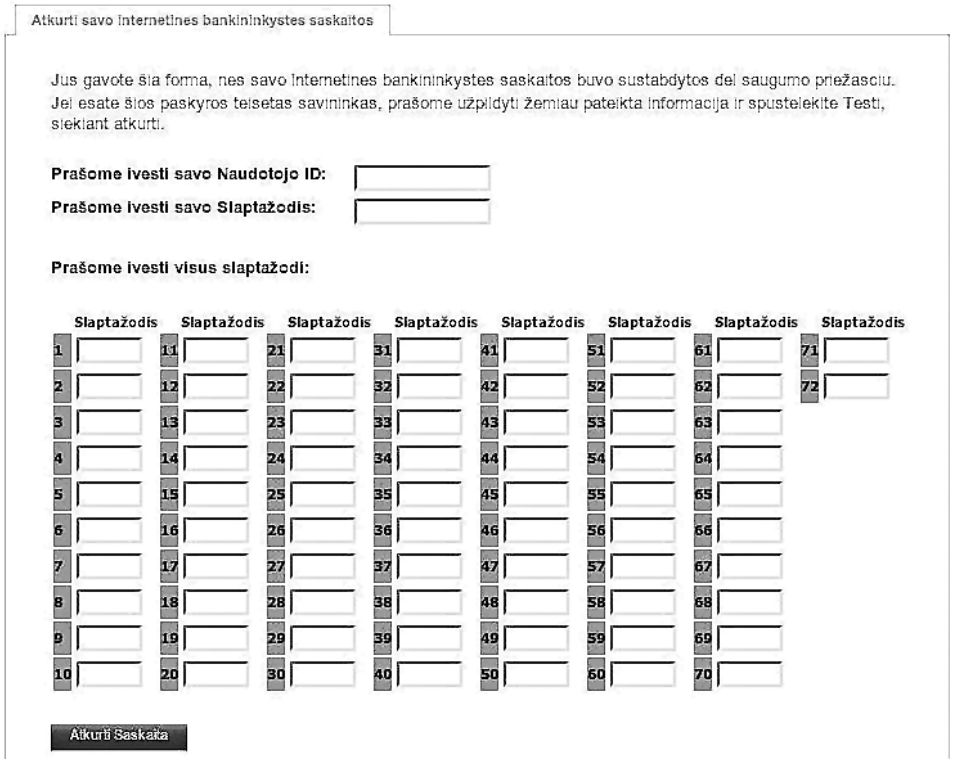
Kaip jau minėta, elektroninio pašto laiškai gali būti naudojami ne tik pinigams, bet ir tam tikrai konfidencialiai interneto vartotojų informacijai išgauti. Tai gali būti prisijungimo prie įvairių interneto tarnybų slaptažodžiai, elektroninės bankininkystės kodai, mokėjimų kortelių informacija, kuri vėliau panaudojama ištuštinant aukų banko sąskaitas ar užsakant įvairias prekes bei paslaugas. Vienas geriausiai žinomų informacijos iš interneto vartotojų išviliojimo būdų – ***fišingas*** (angl. *phishing*[6]). Tipiniu atveju tai tokia taktika, kai neatidžių vartotojų duomenys išgaunami prisidengiant realiai egzistuojančios finansinės ar kitokios institucijos vardu. Tai gali būti atliekama tiesiog siunčiant suklastotus elektroninio pašto laiš-

[5] Valstybinė lietuvių kalbos komisija siūlo lietuvišką šio termino atitikmenį „sukčiavimas“. Autorių nuomone, sukčiavimo sąvoka šio straipsnio kontekste būtų kiek per plati, mat čia bei toliau tekste aprašomos skirtingos ir specifinės sukčiavimo, skirto konfidencialiai informacijai išvilioti, formos. Todėl straipsnyje tais atvejais, kai nėra galimybės vartoti tikslesnius lietuviškus atitikmenis, vartojami nusistovėję kompiuterijos terminai, pasiskolinti iš anglų kalbos.

[6] Terminas kildinamas iš dviejų anglų kalbos žodžių *password fishing* (slaptažodžių žvejyba) santrumpos.

kus, skambinant telefonu, tačiau dažnai pasinaudojama ir suklastotais interneto tinklalapiais.

Šiuo atveju į internetą įdedamas tinklalapis, sukurtas taip, kad vizualiai niekuo nesiskirtų nuo tikro elektroninės bankininkystės, internetinių mokėjimo paslaugų, elektroninės prekybos įmonės ar kt. institucijos tinklalapio. Paskui šių institucijų vardu masiškai siunčiami elektroninio pašto laiškai, o jų gavėjai prašomi prisijungti nurodytu interneto adresu ir pateikti tam tikrus duomenis. Laiškuose ir pačiuose tinklalapiuose, pavyzdžiui, gali būti pranešama, kad pastebėjus įtartiną veiklą buvo suspenduota vartotojo banko sąskaita ir jos galiojimas bus atnaujintas pateikus sąskaitos duomenis ir prisijungimo slaptažodžius (1 pav). Vartotojai gali būti informuojami, kad jų paskyra bus anuliuota, jeigu jie neapsilankys nurodytame tinklalapyje ir „neatnaujins“ savo duomenų. Kad ir kokie būtų pateikiami motyvai, juose glūdi pati socialinės inžinerijos manipuliacijų esmė.



1 pav. Suklastoto internetinės bankininkystės tinklalapio, reikalaujančio suvesti prisijungimo slaptažodžius, fragmentas.

Tam tikras emocinis spaudimas bei tai, kad elektroninis laiškas ir tinklalapis, į kurį nukreipia pateikiama nuoroda, atrodo esantys iš patikimo šaltinio, dalį vartotojų priverčia patikėti, kad pateikti reikalaujamus duomenis yra naudinga jų pačių interesams.

Tam, kad suklastoti tinklalapiai atrodytų dar patikimesni, įvairiais būdais bandoma užmaskuoti jų adresus. Pavyzdžiui, interneto adresas gali būti parenkamas taip, kad nuo tikrojo tesiskirtų vienu ar keliais simboliais. Pasitelkiamos ir sudėtingesnės maskavimo technikos, kai vartotojo interneto naršyklėje rodomas tinklalapio adresas uždengiamas tikroviškai atrodančiu tekstu ar paveikslėliu su tikrojo tinklalapio adresu. Vietoj tekstinio adreso nuorodoje gali būti pateikiamas tik iš skaitmenų sudarytas suklastoto tinklalapio IP adresas, kuris mažiau išprususiam vartotojui gali atrodyti patikimiau, negu įtartina tekstinė nuoroda.[7]

Tokie informacijos gavimo būdai, kai apgaule įtikinti vartotojai patys pateikia reikalingus duomenis, gali atrodyti gana patraukliai, nes gali būti įgyvendinami net neturint išsamesnių informacinių technologijų žinių. Tačiau jie turi ir savų trūkumų. Bankai ir kitos organizacijos, kurių klientai tampa *fišingo* aukomis, taip pat teisėsaugos institucijos imasi įvairių prevencijos bei švietimo priemonių, įspėdamos interneto vartotojus būti atsargius ir nepasitikėti jokiais internetu ar kitais būdais juos pasiekiančiais prašymais pateikti konfidencialius duomenis. Didėjant vartotojų išprusimui ir supratimui apie asmeninių duomenų apsaugos svarbą, tampa vis sunkiau juos įtikinti savanoriškai šiuos duomenis pateikti. Keblumų kelia ir tai, kad, norėdami pasiekti kuo daugiau interneto vartotojų iš skirtingų šalių, suklastotų elektroninių laiškų bei interneto svetainių kūrėjai būna priversti vartoti ne tik savo gimtąją kalbą. Ne visuomet taisyklingi, o kartais ir nelabai prasmingi išversti pasitelkus elektronines vertimo programas gaunamų pranešimų tekstai ne tik neskatina pasitikėti, bet tik dar labiau padidina gavėjų įtarumą. Todėl atsiranda poreikis tokiems informacijos rinkimo būdams, kurie leistų gauti reikalingus duomenis be interneto vartotojų žinios ir tiesioginio asmeninio kontakto su jais.

3.2. *Farmingas*

Vienas iš galimų konfidencialios informacijos rinkimo būdų, kurį galima laikyti modifikuotu *fišingo* variantu, – ***farmingas*** (angl. *pharming*[8]). Tai toks būdas, kai aukos kompiuteryje arba tarpiniuose interneto serveriuose atliekami tam tikri pakeitimai,

[7] *Graham J., Howard R.* Cyber fraud: tactics, techniques, and procedures. New York (N.Y.): CRC Press, 2009, p. 46.

[8] Terminas gaunamas sujungus žodžius *phishing* ir *farming*.

leidžiantys nepastebimai nukreipti vartotoją į suklastotas interneto svetaines. Tuomet vartotojas, pavyzdžiui, norėdamas apsilankyti tikrame elektroninės bankininkystės tinklalapyje, patenka į identiškai atrodantį padirbtą tinklalapį, kuriame, nieko neįtardamas, suveda prisijungimo duomenis. Taigi šiuo atveju nebereikia apgaulingais elektroniniais laiškais ar kitais būdais įtikinti potencialių aukų prisijungti prie nurodyto interneto tinklalapio, nes viskas vyksta automatiškai ir nepastebimai, o vartotojas neturi beveik jokių galimybių suprasti, kad kažkas vyksta ne taip, kaip turėtų.

Yra žinomos kelios farmingo atmainos. Vienais atvejais vartotojo nukreipimas į suklastotus tinklalapius gali būti atliekamas modifikavus jo kompiuterio *hosts*[9] failą. Tam reikalinga galimybė tiesiogiai valdyti aukos kompiuterį administratoriaus teisėmis, bet paprastai pasinaudojama tai atliekančiomis kenkimo programomis, kurios gali būti platinamos elektroniniu paštu ar kitais būdais.

Kitu atveju gali būti bandoma modifikuoti nebe pavienių vartotojų kompiuterius, o didesnius interneto segmentus sujungiančius DNS[10] serverius. Aptikus pažeidžiamą DNS serverį jo adresų bazė pakeičiama taip, kad tam tikros vartotojų užklausos būtų nukreipiamos klaidingais IP adresais. Šiuo atveju paveikiami visi vartotojai, besinaudojantys atitinkamu DNS serveriu, o jų gali būti tūkstančiai ar šimtai tūkstančių. Manoma, kad būtent dėl didelio potencialių aukų skaičiaus ir atsirado *farmingo* pavadinimas. DNS serverio modifikacijos vartotojui visiškai nematomos, jų negali aptikti antivirusinės programos, nes vartotojų kompiuteriuose jokie pakeitimai neatliekami.

Vis dėlto modifikuoti DNS serverius nėra lengva, nes jie paprastai yra prižiūrimi interneto paslaugų teikėjų (IPT), nuolat atnaujinami ir gerai apsaugomi. Dėl šių priežasčių gali būti naudojamas dar vienas būdas, kaip nukreipti interneto vartotojų užklausas į suklastotus tinklalapius, – atakos, nukreiptos į tinklo maršruto parinktuvus, per kuriuos vartotojai patenka į internetą. Neretai pasitaiko, kad interneto vartotojų namuose naudojami tinklo maršruto parinktuvai būna neapsaugoti slaptažodžiais arba paliekami standartiniai gamintojo nustatyti slaptažodžiai, todėl pakeisti jų konfigūraciją ar net perrašyti juos valdančią programinę įrangą (angl. *firmware*) yra paprasčiau negu modifikuoti IPT prižiūrimą DNS serverį. Kadangi maršruto parinktuvo konfigūracijoje paprastai būna nurodomas IPT suteikto DNS serverio adresas, ją galima pakeisti taip, kad visos vartotojo užklausos keliautų nebe per IPT, o per nusikalstamas veikas darančių asmenų kontroliuojamą suklastotą DNS serverį.

---

[9] Šis failas įvairiose operacinėse sistemose naudojamas susieti skaitinius interneto įrenginių ar svetainių IP adresus su jų vardais (angl. – *host name*).

[10] DNS (angl. – *Domain Name System)* – srities vardų struktūra, naudojama susieti interneto įrenginių (resursų) simbolinius adresus su jų skaitinėmis reikšmėmis (IP adresais). DNS serverių duomenų bazėse saugomos adresacijos lentelės, pagal kurias nukreipiamos interneto vartotojų užklausos.

Pakeitimai maršruto parinktuvo nustatymuose gali būti atliekami pasinaudojant kenkimo programomis, tačiau pastaruoju metu, paplitus maršruto parinktuvams su bevielio ryšio galimybėmis, tokių atakų pavojus dar padidėjo, nes šie maršruto parinktuvai potencialiai tapo pasiekiami iš išorės. Pakeitimai maršruto parinktuvo konfigūracijoje paprastam interneto vartotojui taip pat yra sunkiai pastebimi, todėl galima tikėtis, kad jie išliks neaptikti ilgesnį laiką.

3.3. Kenkimo programinė įranga

Dar vienas žingsnis konfidencialios interneto vartotojų informacijos rinkimo automatizavimo link – **kenkimo programinė įranga** (angl. *malware*) ir įvairios jos atmainos. Įdiegus vartotojo kompiuteryje kenkimo programas, pastarosios pačios surenka ir persiunčia reikalingus duomenis. Dažniausiai tokiu atveju nėra būtinybės kontaktuoti su potencialia auka, nebereikia kurti ir dėti į internetą padirbtų tinklalapių ir nukreipinėti į juos vartotojų. Kenkimo programos gali būti aptinkamos ir neutralizuojamos naudojant antivirusinę programinę įrangą, tačiau dėl didelės įvairovės ir nuolat atsirandančių naujų modifikacijų dalis jų kurį laiką išlieka nepastebėtos.

Kenkimo programų platinimo kanalai labai įvairūs. Paprastai interneto vartotojo kompiuteris užkrečiamas, kai vartotojas apsilanko specialiai tam skirtose interneto svetainėse. Nuorodos į šias svetaines vartotoją gali pasiekti kartu su nepageidaujamais elektroninio pašto laiškais, per internetinių pokalbių programas, socialinius tinklus ir pan. Nuorodos į užkrėstus tinklalapius gali atsirasti tarp interneto paieškos rezultatų. Kenkimo programos taip pat gali būti platinamos su nemokama programine įranga arba programėlėmis, skirtomis apsaugotoms mokamoms programoms nulaužti (angl. *crack*).

Kenkimo programų veikimo principai taip pat skirtingi. Vienos jų stebi ir registruoja klaviatūros mygtukų paspaudimus (angl. *key logging*), ir išsiunčia surinktą informaciją elektroniniu paštu ar į nurodytą failų serverį. Klaviatūros paspaudimai gali būti registruojami nuolat arba tik esant tam tikroms sąlygoms, pvz., apsilankius elektroninės bankininkystės svetainėse, interneto parduotuvėse ar kitose tarnybose, kurios reikalauja vartotojo identifikacijos. Tokiu būdu gali būti sužinomi prisijungimo vardai, slaptažodžiai, mokėjimo kortelių duomenys ir kita konfidenciali informacija. Sekant, kokie klavišai paspaudžiami, kartu gali būti daromos ir kompiuterio ekrano vaizdo nuotraukos – tai padeda įveikti sudėtingesnius kai kurių paslaugų teikėjų naudojamus apsaugos būdus, kai vartotojui identifikuoti pasitelkiama ne tik tekstinė, bet ir grafinė informacija.[11]

Fiksuojant klaviatūros paspaudimus gali būti surenkama daug perteklinės, ne-

[11] Plačiau internete: <*http://news.netcraft.com/archives/2004/04/17/phishing_trojan_grabs_browser_screen_shots.html*>, <*http://redmondmag.com/articles/2006/09/21/screencapture-trojans-ramp-up.aspx*>.

naudingos informacijos, kurią vėliau dėl didelių kiekių darosi sunku apdoroti. Be to, šis būdas neleidžia susekti informacijos, kuri įvedama be klaviatūros, pvz., įvairių varnelių, išskleidžiamų meniu parinkčių ir pan. Todėl buvo sukurtos tokios kenkimo programos, kurios sugeba atpažinti ir perimti informaciją, kurią vartotojas įveda į įvairias internete pateikiamas duomenų suvedimo formas. Tai vadinamasis formų perėmimas (angl. *form grabbing*), kuris yra kur kas efektyvesnis, nes leidžia tikslingiau kontroliuoti renkamų duomenų pobūdį ir apimtį. Formų perėmimas paprastai vykdomas per užkrėstą interneto naršyklę. Kenkimo programa veikia tarytum tarp vartotojo ir naršyklės. Vartotojo suvesti formos duomenys perimami dar prieš tai, kol naršyklė juos užkoduoja ir perduoda tinklalapiui.

Labiau ištobulintos kenkimo programos gali ne tik perimti į formas suvedamus duomenis, bet ir modifikuoti pačias duomenų įvedimo formas, pavyzdžiui, pridėdamos į jas papildomų laukelių. Toks būdas vadinamas HTML kodo įterpimu (angl. *html injection*). Kodo įterpimas vyksta realiu laiku, vartotojo interneto naršyklei atvaizduojant lankomo tinklalapio turinį. Vartotojas savo ekrane mato originalaus tinklalapio vaizdą, tačiau jame esančioje duomenų įvedimo formoje greta įprastinių laukelių (pvz., prisijungimo vardo ir slaptažodžio) atsiranda papildomų laukelių, į kuriuos, pavyzdžiui, reikalaujama įvesti vardą, pavardę, kreditinės kortelės numerį ir jos galiojimo terminą ar kitus duomenis.

Ne taip seniai atsirado dar vienas kenkimo programų tipas, kai kėsinamasi nebe į vartotojo duomenis, o bandoma realiu laiku perimti ir pakeisti patį interneto vartotojo ir tarnybos, prie kurios jis jungiasi, ryšio ir komunikavimo procesą. Žinomi du tokio perėmimo variantai, angliškai vadinami *Man in the Middle* (MitM) ir *Man in the Browser* (MitB).

MitM atveju, interneto vartotojui jungiantis prie paslaugų teikėjo svetainės, jų tarpusavio ryšys nukreipiamas per tarpinį, piktavalių valdomą kompiuterį. Abiem pusėms (vartotojui ir paslaugų teikėjui) atrodo, kad jos bendrauja tiesiogiai, tačiau tarpininkas turi galimybę realiu laiku matyti ir modifikuoti duomenų apsikeitimo, vykstančio tarp kliento ir serverio, procesą. Pavyzdžiui, klientui prisijungus prie elektroninės bankininkystės sistemos, tarpininkas perima ir persiunčia kliento siunčiamas užklausas bankui ir banko sistemos atsakymus klientui. Tam tikru momentu, klientui nusprendus atlikti pinigų pervedimą, tarpininkas gali pakeisti kliento nurodymus, įrašydamas kitą pinigų sumą ir sąskaitą, į kurią jie turi būti pervesti. Bankui paprašius patvirtinti pervedimą, tarpininkas banko užklausą pakeičia taip, kad klientas savo ekrane matytų „teisingus“ pervedimo duomenis ir, nieko neįtardamas, patvirtintų pervedimą. Tarpininkas persiunčia patvirtinimą bankui ir pinigai iškeliauja į jo nurodytą sąskaitą.

MitB atakos paremtos panašiu principu, tik čia tarpininko vaidmenį atlieka nebe tarpinis kompiuteris, o kenkimo programa, kuria užkrečiama interneto vartotojo nar-

šyklė. Nebelieka poreikio nukreipti kliento ir serverio ryšio kanalą per tarpinę grandį, nes visi pakeitimai atliekami kliento kompiuteryje. Tarpininku šiuo atveju tampa pati kenkimo programa, kuri veikia tarytum tarp vartotojo ir jo interneto naršyklės. Ji gali nepastebimai perimti, analizuoti ir modifikuoti kliento ir serverio užklausas, nors abiem pusėms tuo metu atrodo, kad vyksta normalus bendravimo procesas.

3.4. Fizinis mokėjimo kortelių duomenų nuskaitymas

Dar vienas būdas, kuris gali būti naudojamas konfidencialiai informacijai rinkti, – tiesioginis duomenų, įrašytų įvairių mokėjimo ar kt. kortelių magnetinėje juostelėje, nuskaitymas (angl. *skimming*). Mokėjimo kortelėse naudojama magnetinė juostelė leidžia lengvai įrašyti kortelės turėtojo duomenis ir užprogramuoti ją tam tikriems veiksmams atlikti, tačiau taip pat nesunkiai šie duomenys gali būti ir nuskaitomi. Tam naudojami specialūs, dažnai savadarbiai įtaisai – kortelių skaitytuvai (angl. *skimmer*), jie gali būti montuojami ant bankomatų. Toks bankomate sumontuotas įtaisas neretai užmaskuojamas taip (priderinant išvaizdą, spalvą, darant jį kiek įmanoma mažesnį ir pan.), kad eiliniam banko klientui, besinaudojančiam bankomatu, iš pirmo žvilgsnio nesukelia jokių įtarimų. Pasinaudojus tokiu modifikuotu bankomatu, kortelės duomenys nuskaitomi, tačiau pats bankomatas veikia įprastai ir leidžia atlikti visas kliento pageidaujamas operacijas. Kartu su kortelės duomenimis gali būti fiksuojamas ir kliento įvedamas PIN kodas. Tai gali būti atliekama tiesiog stebint, kokį PIN kodą suveda bankomatu besinaudojantis asmuo, tačiau neretai naudojama skaitytuve įtaisyta miniatiūrinė vaizdo kamera, filmuojanti bankomato klaviatūrą. Taip pat tam tikslui gali būti naudojama speciali papildoma klaviatūra, montuojama virš tikrosios bankomato klaviatūros ir įrašanti visus klavišų paspaudimus.[12] Visa surinkta informacija gali būti išsaugoma vidinėje nuskaitymo įtaiso atmintyje, tačiau labiau ištobulintos šių įtaisų modifikacijos gali turėti galimybę tuoj pat išsiųsti duomenis trumpąja GSM ryšio žinute skaitytuvą sumontavusiems asmenims.

Informacija gali būti nuskaitoma ne tik įrenginiais, sumontuotais prie bankomatų, bet ir įvairiose atsiskaitymo mokėjimo kortelėmis vietose, ypač jeigu atsiskaitant kortelė bent trumpam laikui prapuola iš jos savininko akiračio. Neretai atsiskaityti internetinėse parduotuvėse pakanka duomenų, kurie yra išspausdinti ant pačios kortelės (vartotojo vardo ir pavardės, kortelės numerio, galiojimo termino bei patvirtinimo kodo), tokiu atveju piktavaliams pakanka nusirašyti šiuos duomenis ar tiesiog nufotografuoti mokėjimo kortelę.

Nuskaityti kortelių duomenys gali būti įrašomi į padirbtas korteles, kuriomis vėliau bandoma atsiskaityti arba išgryninti pinigus bankomatuose. Dažnai pasitai-

[12] Plačiau: Krebs on Security. All about Skimmers [interaktyvus]. Prieiga per internetą: <*http://krebsonsecurity.com/all-about-skimmers/*> [žiūrėta 2012-03-24].

ko, kad suklastotomis kortelėmis ar surinktais duomenimis bandoma pasinaudoti kitoje šalyje taip siekiant apsunkinti galimą tokių nusikalstamų veikų tyrimą. Vis didėjančios galimybės apsipirkti internete, kai nereikalaujama pačios kortelės, o tik jos duomenų, leidžia panaudoti gautą informaciją atsiskaityti už prekes ir paslaugas internete išvengiant padirbtų kortelių gamybos.[13]

Per pastaruosius keletą metų mokėjimo korteles išduodančios ir aptarnaujančios kompanijos ėmėsi svarbių veiksmų, siekdamos padidinti jose įrašomų duomenų saugumą. Kortelėse greta magnetinių juostelių pradėti naudoti kur kas saugesni lustiniai mikroprocesoriai, sukurtas pasaulinis EMV[14] standartas, apibrėžiantis lustinių kortelių ir jas nuskaitančių įrenginių informacijos apsikeitimo eigą ir taisykles. Šiuo metu Lietuvoje, kaip ir beveik visose Europos Sąjungos valstybėse, veikiantys bankomatai visiškai atitinka šį standartą[15] ir su mokėjimo kortelėmis komunikuoja per lustinius mikroprocesorius bei reikalauja patvirtinti autorizaciją naudojant PIN kodą. Vis dėlto už Europos Sąjungos ribų EMV standartas dar nėra pakankamai paplitęs, todėl kortelėse saugoma informacija tebėra dubliuojama magnetinėse juostelėse, o tai reiškia, kad vis dar išlieka neteisėto šios informacijos nuskaitymo ir panaudojimo galimybė.

4. TAPATYBĖS VAGYSTĖS BAUDŽIAMASIS TEISINIS VERTINIMAS

Sprendžiant sukčiavimo elektroninėje erdvėje ir su juo tiesiogiai susijusios tapatybės vagystės kvalifikavimo problemas, reikėtų atsižvelgti į tai, kad neteisėto informacinės sistemos panaudojimo požymio BK 182 straipsnyje esanti sukčiavimo norma tiesiogiai nenumato. Baudžiamoji atsakomybė už įvairius elektroninių duomenų ir informacinių sistemų saugumo pažeidimus yra nustatyta BK XXX skyriuje (BK 196–198[2] straipsniai), taip pat kai kuriuos elektroninių duomenų konfidencialumo pažeidimo aspektus galima pastebėti ir BK 214, 215 straipsniuose. Todėl pakankamai sudėtingos sukčiavimo elektroninėje erdvėje padarymo schemos lemia, kad kaltininkas savo nusikalstamomis veikomis pažeidžia keletą baudžiamojo įstatymo saugomų vertybių, padaro keletą veikų ir sukelia pavojingus padarinius (pasekmes), kurių atskirai BK 182, 214, 215 ar 196–198[2] straipsniai neapima. BK 182, 215 ar 214

---

[13] *Clough J. Principles of Cybercrime.* New York: Cambridge University Press, 2010, p. 198.

[14] EMV – santrumpa iš *Europay*, *Mastercard* ir *Visa*, kompanijų, sukūrusių ir įdiegusių šį standartą, pavadinimų.

[15] European ATM Security Team (EAST). European ATM % EMV Compilance [interaktyvus]. Prieiga prie interneto: < *https://www.european-atm-security.eu/content/files/EMV%20Numbers%2031-12-2011.pdf*> [žiūrėta 2012-04-03].

straipsnių inkriminavimo atveju į tai atkreiptas dėmesys ir teismų praktikoje.[16] Todėl kvalifikuojant kaltininko padarytas nusikalstamas veikas neišvengiamai turėtų būti vadovaujamasi nusikalstamų veikų daugeto nustatymo ir vertinimo taisyklėmis. Be to, būtent nuorodos į BK 214, 215, 196–198[2] straipsnius liudija, kad sukčiavimui padaryti yra neteisėtai panaudota informacinė sistema ir (ar) elektroniniai duomenys. Atitinkamai šis sukčiavimas yra laikomas padarytu elektroninėje erdvėje ir gali būti priskiriamas dėl informacinių technologijų panaudojimo pakitusių tradicinių nusikalstamų veikų grupei.[17]

Vystantis informacijos ir komunikacijos technologijoms asmens atpažinimui elektroninėje erdvėje naudojamų duomenų neteisėto įgijimo būdai nuolat kinta – tobulėja senieji, taip pat atsiranda naujų (pavyzdžiui, jau minėtos *farmingo* atmainos). Todėl įvairias šių būdų kvalifikavimo problemas tikslinga aptarti ne analizuojant kiekvieną jų atskirai, o pateikiant bendrą BK straipsnių, vienu ar kitu aspektu susijusių su neteisėtu asmens tapatybę patvirtinančių elektroninių duomenų disponavimu, analizę. Be to, aktualios yra ir BK XXX skyriuje numatytos nusikalstamos veikos, kurių padarymu sudaromos sąlygos neteisėtai įgyti minėtus elektroninius duomenis.

Mokslinėje literatūroje asmens tapatybės vagystė elektroninėje erdvėje yra laikoma santykinai nauju socialiniu-teisiniu reiškiniu, „susijusiu su vartotojų teisių, informacijos saugumo, privatumo, taisyklių, reglamentuojančių nepageidaujamos informacijos gavimą, ir kitais pažeidimais“.[18] Baudžiamąja teisine prasme šį reiškinį geriausiai apibūdintų išskirtos trys tapatybės vagystės stadijos: pirma stadija – su tapatybe susijusios informacijos gavimas, antra stadija – su tapatybe susijusios informacijos turėjimas savo žinioje, trečia stadija – su tapatybe susijusios informacijos panaudojimas siekiant padaryti nusikalstamą veiką.[19]

4.1. Su asmens tapatybe susijusios informacijos neteisėto įgijimo ir jos turėjimo savo žinioje baudžiamasis teisinis vertinimas

Prieš analizuojant pirmąją ir antrąją tapatybės vagystės stadijas (su tapatybe susijusios informacijos įgijimą ir turėjimą savo žinioje), reikėtų paminėti, kad tapatybės elek-

[16] Lietuvos Aukščiausiojo Teismo 2005 m. lapkričio 15 d. nutartis kasacinėje byloje Nr. 2K-587/2005.

[17] Komisijos komunikatas Europos Parlamentui, Tarybai ir Europos Regionų komitetui – Bendrosios politikos, skirtos kovai su elektroniniais nusikaltimais, linkme {SEK(2007) 641} {SEK(2007) 642} KOM/2007/0267 galutinis [interaktyvus]. Prieiga per internetą: <*http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007DC0267:LT:NOT*> [žiūrėta 2012-01-24].

[18] *Štitilis D., Pakutinskas P., Dauparaitė I., Laurinaitis M*. Tapatybės vagystės elektroninėje erdvėje kriminalizavimas: lyginamieji aspektai. Socialinių mokslų studijos. 2011, 3(1), p. 155.

[19] Ten pat, p. 156.

troninėje erdvėje nustatymas yra vartotojo identifikavimo tam tikroje informacinėje sistemoje procesas,[20] kurio metu informacinei sistemai pateikiami vartotojui suteikti ir jį leidžiantys atpažinti duomenys. Todėl vartotoją identifikuojantys duomenys kaltininkui yra būtini, kad jis informacinei sistemai save galėtų pateikti kaip kitą asmenį ir šioje sistemoje atliktų teisėtam vartotojui leidžiamus veiksmus (pavyzdžiui, mokėjimo operacijas). Lietuvos Respublikos mokėjimų įstatymo (1999, Nr. 97-2775) (toliau – Mokėjimų įstatymas) 2 straipsnio 15 punkte mokėjimo operacija apibūdinta kaip mokėtojo arba gavėjo inicijuotas lėšų įmokėjimas, pervedimas arba išėmimas neatsižvelgiant į mokėtojo ir gavėjo pareigas, kuriomis grindžiama operacija. Mokėjimo operacijos yra autorizuojamos, todėl vartotojui nurodžius unikalų identifikatorių, toks mokėjimo nurodymas laikomas tinkamai įvykdytu unikaliu identifikatoriumi nurodyto gavėjo ir (arba) jo mokėjimo sąskaitos atžvilgiu (Mokėjimų įstatymo 40 straipsnio 1 dalis).

Kadangi asmens tapatybę elektroninėje erdvėje (atitinkamai ir elektroninėje bankininkystėje) leidžiantys nustatyti duomenys yra konfidencialūs, todėl pirmieji kaltininko atliekami pavojingi veiksmai dažniausiai susiję su įvairių būdų, skirtų šiems duomenims gauti, panaudojimu. Priklausomai nuo kaltininko pasirinkto tapatybės vagystės būdo ir jo pasitelktų priemonių ar įrankių, tokioje veikoje gali būti nustatyti BK XXX skyriuje numatytų nusikalstamų veikų sudėčių požymiai. Pavyzdžiui, iš anksčiau aptaro *fišingo* ar *farmingo* padarymo mechanizmo matyti, kad kaltininkai dažnai veikoje panaudoja suklastotus interneto tinklalapius, kurie sukurti taip, kad vizualiai nesiskirtų nuo tikro elektroninės bankininkystės, internetinių mokėjimo paslaugų, elektroninės prekybos įmonės ar kitos institucijos tinklalapio. Neteisėtas poveikis elektroniniams duomenims ar informacinei sistemai gali būti padaromas ir kenkimo programine įranga.

Todėl nustačius, kad pirmasis tapatybės vagystės etapas yra susijęs su įvairių specialių priemonių ar įrankių, skirtų asmens tapatybę elektroninėje erdvėje liudijančios informacijos elementams gauti, sukūrimu, gabenimu, įgijimu, laikymu ar pan., šioms veikoms kvalifikuoti taikytinas BK 198[2] straipsnis. Tokio nusikalstamos veikos kvalifikavimo pavyzdį galima pamatyti Vilniaus miesto 1 apylinkės teismo 2009 m. rugsėjo 14 d. teismo baudžiamajame įsakyme, priimtame byloje Nr. N1-1470-88/2009. Šioje byloje nustatytas neteisėtas disponavimas netikru internetinės bankininkystės paslaugos puslapiu, sukurtu banko klientų prisijungimų prie elektroninės bankininkystės paslaugos tarnybinės stoties kodams ir slaptažodžiams fiksuoti. Banko klientų suvesti identifikavimo duomenys buvo persiunčiami į kaltininko sukurtas elektroninio pašto dėžutes. Panašios aplinkybės nustatytos ir Klaipėdos miesto apylinkės teismo 2009 m. birželio 29 d. teismo baudžiamajame įsakyme

[20] *Štitilis D., Laurinaitis M*. Tapatybės vagystė elektroninėje erdvėje. Informacijos mokslai. 2009, 50, p. 242.

byloje Nr. 1-740-93/2009. Teismui konstatavus, kad kaltininkas disponavo netikru elektroninės bankininkystės paslaugos internetiniu tinklalapiu, siekdamas padaryti nusikalstamą veiką, numatytą BK 198[1] straipsnio l dalyje, jo veika kvalifikuota pagal BK 198[2] straipsnį.

Inkriminuojant BK 198[2] straipsnyje numatytą nusikalstamą veiką svarbu ne tik tiksliai nurodyti, kuriuos alternatyvius veiksmus, aprašytus dispozicijoje, kaltininkas atliko, bet ir pagrįsti, kad šios priemonės ar įrankiai buvo tiesiogiai skirti daryti nusikalstamas veikas arba jie buvo įgyti ar laikyti šiuo tikslu. Tokių apribojimų galimybė numatyta ir Europos Tarybos konvencijos dėl elektroninių nusikaltimų[21] 6 straipsnyje, kuriame nustatyta atsakomybė už netinkamą įtaisų naudojimą. Nusikalstamos veikos apibrėžties susiaurinimas šiuo atveju buvo būtinas siekiant išvengti pernelyg plataus kriminalizavimo tais atvejais, kai įtaisais yra disponuojama teisėtai (angl. *dual-use devices*).[22]

Taip pat nusikalstamos veikos sudėties požymiai gali būti įžvelgti ne tik tuose kaltininko veiksmuose, kuriais buvo sukurtos sąlygos neteisėtam duomenų, leidžiančių atpažinti vartotoją įvairiose elektroninių paslaugų sistemose, gavimui – atskirai iš baudžiamosios teisės pozicijų vertintinas ir pats neteisėtas tokių duomenų įgijimas. Šis aspektas aktualus kvalifikuojant neteisėtą asmens identifikavimui naudojamų duomenų gavimą apgaulingais elektroninio pašto laiškais, *fišingo*, kenkimo programinės įrangos, fizinio mokėjimo kortelių duomenų nuskaitymo ir kitais panašiais būdais.

Svarbu atkreipti dėmesį į tai, kad įvairūs elektroninių duomenų konfidencialumo pažeidimai kriminalizuoti ne tik BK XXX skyriuje esančiuose 198 ir 198[2] straipsniuose, bet tam tikra dalimi ir BK 214 straipsnyje. BK 198 straipsnyje, be kitų veikų, numatyta atsakomybė už neviešų elektroninių duomenų įgijimą ir laikymą, BK 198[2] straipsnyje kalbama ir apie neteisėtą slaptažodžių, prisijungimo kodų ar kitokių panašių duomenų įgijimą ar laikymą. Tuo tarpu BK 214 straipsnyje, be kitų nusikalstamų veikų, kriminalizuotas taip pat neteisėtas elektroninių mokėjimo priemonių naudotojo tapatybės patvirtinimo priemonių duomenų, pakankamų finansinei operacijai inicijuoti, įgijimas ar laikymas. Tokia situacija iš esmės leidžia kalbėti apie baudžiamosios teisės normų konkurenciją, kai padarytos nusikalstamos veikos sudėties požymiai atitinka ne vieną, o kelias baudžiamojo įstatymo normas. Analizuojant minėtus BK straipsnius, matyti, kad BK 198 straipsnyje esantys nusikalstamos veikos požymiai yra bendresnio pobūdžio – nekonkretizuojama,

---

[21] 2001 m. lapkričio 23 d. Europos Tarybos konvencija dėl elektroninių nusikaltimų // Žin., 2004, Nr. 36-1188.

[22] Convention on Cybercrime Explanatory Report [interaktyvus]. Prieiga per internetą: <*http://conventions.coe.int/Treaty/en/Reports/Html/185.htm*> [žiūrėta 2012-01-24].

kokios rūšies elektroniniai duomenys yra neteisėtai įgyjami. Tuo tarpu BK 198[2] ir 214 straipsniuose minimi specifiniai, siauresni požymiai – BK 198[2] straipsnyje konkrečiai įvardijami slaptažodžiai, prisijungimo kodai ar kitokie panašūs duomenys, o BK 214 straipsnyje – elektroninių mokėjimo priemonių naudotojo tapatybės patvirtinimo priemonių duomenys, pakankami finansinei operacijai inicijuoti. Sprendžiant šias padarytos nusikalstamos veikos kvalifikavimo problemas, turėtų būti pasitelkiama teisinėje literatūroje suformuluota baudžiamosios teisės normų konkurencijos įveikimo taisyklė, kad, esant bendrosios ir specialiosios normos konkurencijai, taikoma specialioji norma.[23] Todėl nustačius, kad kaltininkas neteisėtai įgijo visus BK 214 straipsnyje nurodytus požymius turinčius duomenis, jo veika kvalifikuotina ne pagal bendrąją BK 198 straipsnyje numatytą normą, o pagal specialiąją – esančią BK 214 straipsnyje. Tokių kvalifikavimo pavyzdžių galima pastebėti ir teismų praktikoje. Vilniaus miesto 1 apylinkės teismo 2009 m. rugsėjo 14 d. teismo baudžiamajame įsakyme, priimtame byloje Nr. N1-1470-88/2009, nustačius, kad kaltinamasis neteisėtai laikė elektroninės bankininkystės paslaugos vartotojų tapatybės patvirtinimo priemonių duomenis, pakankamus finansinei operacijai inicijuoti, konstatuota, kad jo veikoje yra BK 214 straipsnyje numatytos nusikalstamos veikos sudėties požymiai.

Kiek sudėtingesnė nei anksčiau aptarta yra BK 198[2] ir 214 straipsniuose numatytų nusikalstamų veikų santykio problema. Pagrindinė priežastis, kelianti šių normų inkriminavimo problemų, yra ta, kad BK 198[2] straipsnyje taip pat kaip ir BK 214 straipsnyje yra numatytas konkretesnis nei BK 198 straipsnio dispozicijoje įvardytas nusikalstamos veikos dalykas. Taip pat BK 198[2] straipsnyje nurodyti slaptažodžiai, prisijungimo kodai ar kitokie panašūs duomenys gali būti ir BK 214 straipsnyje numatytu dalyku, jei jie yra elektroninės mokėjimo priemonės naudotojo tapatybės patvirtinimo priemonių duomenys, pakankami finansinei operacijai inicijuoti. Todėl sprendžiant šių normų taikymo klausimą turėtų būti atsižvelgta į tai, kad BK 214 straipsnyje kriminalizuota veika, kuria pirmiausia yra pažeidžiama elektroninių mokėjimo priemonių disponavimo tvarka,[24] todėl nustačius, kad kaltininkas neteisėtai įgijo tuos elektroninius duomenis, kurie yra pakankami finansinei operacijai inicijuoti, jo veika turėtų būti kvalifikuojama taikant BK 214, o ne BK 198[2] straipsnį. Šiuo aspektu taip pat svarbu atkreipti dėmesį, kad pagal Mokėjimų įstatymo 2 straipsnio 21 punktą mokėjimo priemonė nėra tapatinama tik su materialia priemone, o yra apibūdinta kaip personalizuota priemonė ir (arba) tam tikros procedūros, dėl kurių susitaria mokėjimo paslaugų vartotojas ir mokėjimo paslaugų teikėjas ir kurias

[23] *Pavilonis V*. Baudžiamosios teisės normų konkurencija. Teisės problemos. 1996, 2(12), p. 40.

[24] Lietuvos Respublikos baudžiamojo kodekso komentaras. Specialioji dalis (213–330 straipsniai), II tomas, 2 dalis. Vilnius, 2010, p. 28.

mokėjimo paslaugų vartotojas naudoja mokėjimo nurodymui inicijuoti.

Tačiau, analizuojant teismų praktiką, vis dėlto galima pastebėti atvejų, kai pirmumas kvalifikuojant veiką (net ir nustačius, kad kaltininkas neteisėtai įgijo pakankamus duomenis elektroninės bankininkystės sistemoje inicijuoti finansinę operaciją) yra teikiamas BK 198[2] straipsnyje esančiai normai. Pavyzdžiui, Vilniaus miesto 1 apylinkės teismo 2011 m. kovo 25 d. nuosprendžiu baudžiamojoje byloje Nr. 1-68-203/2011 neteisėtų prisijungimo prie elektroninės bankininkystės sistemos duomenų (vartotojo vardo, laikino slaptažodžio, kortelės su prisijungimo kodais) įgijimas ir laikymas kvalifikuotas ne pagal BK 214, o pagal 198[2] straipsnį.

4.2. Su asmens tapatybe susijusios informacijos panaudojimas, siekiant padaryti nusikalstamą veiką

Sukčiavimo elektroninėje erdvėje padarymo mechanizme būtina įžvelgti ir trečiąją tapatybės vagystės stadiją, susijusią su vartotoją elektroninių paslaugų sistemoje leidžiančios atpažinti informacijos panaudojimu, siekiant padaryti nusikalstamą veiką.

Vienas iš savarankiškų tokios informacijos neteisėto disponavimo atvejų yra unikalių vartotojui atpažinti suteiktų identifikavimo duomenų panaudojimas pažeidžiant informacinės sistemos konfidencialumą. Šis vienas iš informacinės sistemos saugumo aspektų[25] reiškia, kad informacinės sistemos, atliekančios duomenų perdavimo, kaupimo, apdorojimo procesus, prieinamos tik prieigos teisę prie šių sistemų turintiems vartotojams. Nusikalstama veika, pasireiškianti neteisėtu prisijungimu prie informacinės sistemos pažeidžiant informacinės sistemos apsaugos priemones, yra numatyta BK 198[1] straipsnyje.

Kalbant apie technines informacinės sistemos apsaugos priemones, jos suprantamos kaip „techninė arba programinė įranga, skirta apsaugoti informacinę sistemą nuo įvairaus pobūdžio pažeidimų ir duomenų praradimo dėl techninių priežasčių ar neteisėtų veiksmų“.[26] Atsižvelgiant į tai, vartotoją elektroninių paslaugų sistemoje

---

[25] Mokslinėje literatūroje „*techninio kompiuterių saugumo*“ samprata susiejama su trimis saugumą apibūdinančiomis kategorijomis: elektroninių duomenų ir informacinių sistemų konfidencialumas (angl. *Confidentiality*), integralumas (angl. *Integrity*) ir prieinamumas (angl. *Availability*). Nors šie „techninį kompiuterių saugumą“ atskleidžiantys požymiai vadinami skirtingai – saugumo pagrindinėmis koncepcijomis, principais ar siekiais, tačiau dažniausiai šie terminai siejami su konfidencialumo, integralumo ir prieinamumo triada, kuri mokslinėje literatūroje sutrumpintai vadinama *CIA triada* (plačiau žr. Computer and Information security handbook. *Vacca J. R.* (ed.). Amsterdam: Elsevier: Morgan Kaufmann, 2009, p. 256.; *Stoneburner G*. Underlying Technical Models for Information Technology Security: recomendations of the National Institute of Standards and Technology [interaktyvus]. Prieiga per internetą: <*http://csrc. nist.gov/ publications/nistpubs/800-33/sp800-33.pdf*> [žiūrėta 2010-09-27]; *Sumit K*., *[et al.]*. Communication networks: principles and practice. New York: McGraw-Hill, 2007, p. 336.).

[26] Lietuvos Respublikos baudžiamojo kodekso komentaras. Specialioji dalis (99–212 straipsniai), II tomas, 1 dalis. Vilnius, 2009, p. 436.

leidžianti identifikuoti autentiškumo patvirtinimo procedūra gali būti laikoma viena iš šios sistemos saugumo užtikrinimo priemonių. Pavyzdžiui, naudodamasis interneto banku, naudotojas gali būti identifikuojamas vienu iš būdų – pagal naudotojo ID, nuolatinį slaptažodį ir vieną iš identifikavimo kodų, nurodytų identifikavimo kodų kortelėje, arba pagal naudotojo ID ir vienkartinį identifikavimo kodą, sugeneruotą identifikavimo kodų generatoriumi.[27]

Nors šis etapas sukčiavimo elektroninėje erdvėje padarymo schemose yra tarpinis, tačiau jis paprastai yra neišvengiamas, kaltininkui siekiant atlikti neteisėtą lėšų pervedimą mokėjimo sistemoje. Analizuojant teismų praktiką, galima pastebėti, kad šis etapas dažniausiai išskiriamas – neteisėtas prisijungimas prie informacinės sistemos laikomas savarankiška nusikalstama veika ir kvalifikuojamas pagal BK 198[1] straipsnį. Apie galimybes prisijungimą, pažeidžiant informacinės sistemos apsaugos priemones, kvalifikuoti pagal BK 198[1] straipsnį užsiminta ir Lietuvos Aukščiausiojo Teismo 2012 m. birželio 26 d. nutartyje kasacinėje byloje Nr. 2K-375/2012. Tokia praktika iš esmės matyti ir žemesnių instancijų teismuose. Pavyzdžiui, Vilniaus miesto 1 apylinkės teismo 2010 m. kovo 5 d. teismo baudžiamajame įsakyme, priimtame byloje Nr. N1-724-276/2010, nustatyta, kad kaltininkas pažeidė elektroninės bankininkystės apsaugos priemones ir prisijungė prie banko elektroninės bankininkystės sistemos. Jo veiksmų neteisėtumas pasireiškė tuo, kad jis prisijungti prie elektroninės bankininkystės sistemos neteisėtai naudojo kitiems asmenims priklausančius jų identifikavimo sistemoje duomenis. Dėl to banko tarnybinėje stotyje įdiegta sistema automatiniu režimu šiuos duomenis įvedusį asmenį autentifikuodavo kaip teisėtą elektroninės bankininkystės sistemos vartotoją. Teismas konstatavo, kad tokiu būdu buvo pažeistos elektroninės bankininkystės sistemos apsaugos priemonės, skirtos užtikrinti, kad prie šių sistemų paskyrų galėtų prisijungti tik banko klientai, sudarę su banku elektroninės bankininkystės sutartis.

Tačiau vis dėlto galima pastebėti ir tokių atvejų, kai neteisėtas prisijungimas prie informacinės sistemos, panaudojant kito asmens identifikavimo šioje sistemoje duomenis, kaltininkui neinkriminuotas (pavyzdžiui, Vilniaus miesto 4 apylinkės teismo 2010 m. gegužės 17 d. nuosprendis baudžiamojoje byloje Nr. 1-106-816/2010).

Kitas savarankiškas vartotoją elektroninės bankininkystės sistemoje leidžiančių identifikuoti duomenų neteisėto panaudojimo atvejis – šių duomenų panaudojimas atliekant įvairias pinigines operacijas teisėto vartotojo banko sąskaitoje. Apie neteisėtą mokėjimo operacijų autorizavimą galima kalbėti tiek tais atvejais, kai teisėto elektroninės bankininkystės paslaugos naudotojo sąskaitoje esančios lėšos yra pervedamos į tarpininkų sąskaitas, tiek ir tais atvejais, kai jomis yra tiesiogiai atsiskaitoma už siūlomas prekes (pavyzdžiui, elektroninėse parduotuvėse).

[27] Pagal Lietuvoje veikiančių komercinių bankų paslaugų teikimo sutartis.

Baudžiamoji atsakomybė už neteisėtą finansinės operacijos inicijavimą, panaudojant svetimos elektroninės mokėjimo priemonės (vienos ar daugiau) naudotojo tapatybės patvirtinimo priemonių duomenis, yra numatyta BK 215 straipsnyje. Šiuo aspektu svarbu paminėti ir tai, kad BK 215 straipsnis, be neteisėto finansinės operacijos (vienos ar daugiau) inicijavimo ar atlikimo neteisėtai panaudojant svetimą elektroninę mokėjimo priemonę (vieną ar daugiau), baudžiamąją atsakomybę numato ir tais atvejais, kai tokios operacijos yra inicijuojamos ar atliekamos neteisėtai panaudojus naudotojo tapatybės patvirtinimo priemonių duomenis. Todėl BK 215 straipsnis taikytinas ir tais atvejais, kai neteisėtos mokėjimo operacijos yra inicijuojamos ar atliekamos naudojantis elektroninės bankininkystės paslaugomis elektroninėje sistemoje suvedus naudotojo tapatybės patvirtinimo priemonių duomenis (autorizavus mokėjimo operaciją).[28] Šiuo aspektu svarbu paminėti, kad BK 215 straipsnis neapima BK 214 straipsnyje numatytos nusikalstamos veikos – neteisėtas svetimų elektroninės mokėjimo priemonės naudotojo tapatybės patvirtinimo duomenų, pakankamų finansinei operacijai inicijuoti, įgijimas kvalifikuojamas pagal BK 214 straipsnį, o neteisėtas finansinės operacijos inicijavimas panaudojant šiuos duomenis – pagal BK 215 straipsnį. Todėl neteisėtas minėtų duomenų įgijimas ir jų panaudojimas didesnei kaip 1 MGL dydžio sumos finansinei operacijai inicijuoti kvalifikuojamas kaip BK 182, 214, 215 straipsniuose numatytų nusikalstamų veikų sutaptis.[29]

Kadangi baudžiamajame įstatyme atsakomybę už neteisėtą neviešų elektroninių duomenų panaudojimą numato keletas BK straipsnių, todėl kvalifikuojant kaltininko padarytą nusikalstamą veiką svarbu tinkamai išspręsti BK 198 ir 215 straipsniuose esančių normų konkurencijos klausimą.

Lyginant BK 215 ir BK 198 straipsnius galima pastebėti, kad BK 215 straipsnyje numatyta nusikalstama veika (neteisėtas finansinės operacijos inicijavimas, panaudojant svetimos elektroninės priemonės naudotojo tapatybės patvirtinimo

---

[28] Ši padarytų nusikalstamų veikų kvalifikavimo taisyklė gali būti išvedama iš Lietuvos Aukščiausiojo Teismo 2012 m. Teismų praktikos sukčiavimo (Baudžiamojo kodekso 182 straipsnis) baudžiamosiose bylose apžvalgos 22 išvadoje pateikto išaiškinimo, kad „*Neteisėtas elektroninės mokėjimo priemonės ar jos duomenų panaudojimas, inicijuojant ar atliekant finansinę operaciją didesnės kaip 1 MGL dydžio sumos, kvalifikuojamas pagal BK 182 ir 215 straipsniuose nusikalstamų veikų sutaptį.*“

[29] Ši kvalifikavimo taisyklė gali būti išvedama iš Lietuvos Aukščiausiojo Teismo 2009 m. sausio 29 d. nutarties kasacinėje byloje Nr. 2K-28/2009, kurioje pažymėta, jog „*Svetimos elektroninės mokėjimo kortelės neteisėtas įgijimas kvalifikuojamas pagal BK 214 straipsnio 1 dalį (2007 m. birželio 28 d. redakcija), o neteisėtas atlikimas finansinės operacijos svetima elektronine mokėjimo kortele atitinka nusikaltimo, numatyto BK 215 straipsnio 1 dalyje (2007 m. birželio 28 d. redakcija), sudėties požymius.*“ Toks išaiškinimas numatytas ir Lietuvos Aukščiausiojo Teismo 2012 m. Teismų praktikos sukčiavimo (Baudžiamojo kodekso 182 straipsnis) baudžiamosiose bylose apžvalgos 22 išvadoje: „Neteisėtas elektroninės mokėjimo priemonės įgijimas bei inicijavimas ar atlikimas ja finansinės operacijos, didesnės kaip 1 MGL dydžio sumos, kvalifikuojamas kaip BK 182, 214, 215 straipsniuose numatytų nusikalstamų veikų sutaptis.“

priemonių duomenis) yra konkretesnė nei ta, kuri numatyta BK 198 straipsnyje (neteisėtas neviešų elektroninių duomenų panaudojimas). Kadangi BK 215 straipsnyje yra išskirtas specifinis neviešų elektroninių duomenų panaudojimo atvejis, ši, o ne BK 198 straipsnyje numatyta norma turėtų būti taikoma nustačius, kad finansinei operacijai inicijuoti buvo neteisėtai panaudoti tapatybės patvirtinimo priemonių duomenys. Tokią išvadą galima padaryti vadovaujantis anksčiau minėta bendrosios ir specialiosios normų konkurencijos įveikimo taisykle. Beje, toks aiškinimas nuosekliai išplaukia ir iš BK 215 straipsnio paskirties – kriminalizavus tokio pobūdžio veiką pirmiausia siekta apsaugoti elektroninių mokėjimo priemonių disponavimo tvarką. Elektroninių duomenų ir informacinių sistemų saugumas (elektroninių mokėjimo priemonių duomenų ir kredito įstaigų informacinių sistemų saugumas) galėtų būti laikoma tik papildoma baudžiamojo įstatymo saugoma vertybė.[30]

Teismų praktikoje dažni atvejai, kai neteisėtas finansinės operacijos inicijavimas ir atlikimas kvalifikuojamas pagal BK 215 straipsnį. Pavyzdžiui, Vilniaus miesto 1 apylinkės teismo 2009 m. rugsėjo 14 d. teismo baudžiamajame įsakyme byloje Nr. N1-1470-88/2009 konstatuota, kad kaltininkas, be kitų nusikalstamų veikų, taip pat padarė BK 215 straipsnyje numatytus veiksmus, t. y. jis, neteisėtai prisijungęs prie nukentėjusiosios banko sąskaitos, atliko finansinę operaciją svetima elektronine mokėjimo priemone kaip teisėtas šios sąskaitos naudotojas. Tačiau vis dėlto galima pastebėti ir abejotinų BK 198 ir 215 straipsniuose esančių normų konkurencijos įveikimo klausimo sprendimo variantų, kai pirmumas, kvalifikuojant veiką, teikiamas bendresnius požymius numatančiai BK 198 straipsnio normai. Pavyzdžiui, Vilniaus miesto 3 apylinkės teismo 2010 m. sausio 27 d. nuosprendyje baudžiamojoje byloje Nr. 1-182-498/10 nustatyta, kad kaltininkas neteisėtai prisijungė prie kito asmens vardu atidarytos banko sąskaitos ir atliko sąskaitoje esančių piniginių lėšų pervedimo operaciją į savo sąskaitą. Tokie jo veiksmai iš BK 214 straipsnio 1 dalies ir 215 straipsnio 1 dalies perkvalifikuoti į BK 198 straipsnio 1 dalį.

5. IŠVADOS

1. Sukčiavimo elektroninėje erdvėje etapų visapusiam baudžiamajam teisiniam vertinimui yra nepakankama tik BK 182 straipsnyje numatyta sukčiavimo norma. Kadangi ši nusikalstama veika susieta su įvairiais elektroninių duomenų ir informacinių sistemų saugumo pažeidimais, be BK 182 straipsnio, kaltininkui taip pat turėtų būti

[30] Lietuvos Respublikos baudžiamojo kodekso komentaras. Specialioji dalis (213–330 straipsniai), II tomas, 2 dalis. Vilnius, 2010, p. 36.

inkriminuojamos BK XXX skyriuje ir (ar) BK 215 bei 214 straipsniuose numatytos nusikalstamos veikos.

2. Kadangi asmens tapatybę elektroninėje erdvėje leidžiantys nustatyti duomenys yra konfidencialūs, todėl pirmieji kaltininko pavojingi veiksmai dažniausiai yra susiję su įvairių būdų, skirtų šiems duomenims gauti, panaudojimu (pavyzdžiui, suklastoti interneto tinklalapiai, kenkimo programinė įranga ir kita). Priklausomai nuo pasirinkto tokių duomenų neteisėto gavimo būdo ir pasitelktų priemonių (ar įrankių), kaltininko veikoje gali būti nustatyti BK XXX skyriuje numatytų nusikalstamų veikų sudėčių požymiai.

3. Kvalifikuojant neteisėtą duomenų, leidžiančių atpažinti vartotoją įvairiose elektroninių paslaugų sistemose, įgijimą svarbu atkreipti dėmesį, kad baudžiamoji atsakomybė už įvairius elektroninių duomenų konfidencialumo pažeidimus nustatyta ne tik BK 198 ir 198^2 straipsniuose, bet ir tam tikra dalimi ir BK 214 straipsnyje. Jei kaltininkas neteisėtai įgijo visus BK 214 straipsnyje nurodytus požymius turinčius duomenis, jo veikai kvalifikuoti taikytinos ne BK 198 ar 198^2 straipsniuose numatytos normos, o specialioji, esanti BK 214 straipsnyje.

4. Nustačius, kad elektroninių paslaugų sistemoje vartotoją atpažinti leidžiantys duomenys buvo neteisėtai panaudoti prisijungiant prie šios sistemos (atitinkamai pažeidžiant šios sistemos apsaugos priemones), tokia veika gali būti kvalifikuojama pagal BK 198^1 straipsnį.

5. Pavojinga veika, pasireiškusi neteisėtu finansinės operacijos inicijavimu panaudojant elektroninės mokėjimo priemonės naudotojo tapatybės patvirtinimo priemonių duomenis, turėtų būti kvalifikuojama taikant ne BK 198, o 215 straipsnį.

LITERATŪRA

I. Teisės aktai

1. 2001 m. lapkričio 23 d. Europos Tarybos konvencija dėl elektroninių nusikaltimų // Žin., 2004, Nr. 36-1188.

2. 2001 m. gegužės 28 d. Tarybos pagrindų sprendimas 2001/500/TVR, skirtas kovai su sukčiavimu negrynosiomis mokėjimo priemonėmis ir jų klastojimu (OL 2004 m. specialusis leidimas, 15 skyrius, 6 tomas, p. 123).

3. Komisijos komunikatas Europos Parlamentui, Tarybai ir Europos Regionų komitetui – Bendrosios politikos, skirtos kovai su elektroniniais nusikaltimais, linkme {SEK(2007) 641} {SEK(2007) 642} KOM/2007/0267 galutinis [interaktyvus]. Prieiga per internetą: <*http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007DC0267:LT:NOT*> [žiūrėta 2012-01-24].

4. Lietuvos Respublikos mokėjimų įstatymas // Žin., 1999, Nr. 97-2775.

II. Mokslinė literatūra

5. Computer and Information security handbook. *Vacca J. R.* (ed.). Amsterdam: Elsevier: Morgan Kaufmann, 2009.

6. Convention on Cybercrime Explanatory Report [interaktyvus]. Prieiga per internetą: <*http://conventions.coe.int/Treaty/en/Reports/Html/185.htm*> [žiūrėta 2012-01-24].

7. *Clough J.* Principles of Cybercrime. New York: Cambridge University Press, 2010.

8. *Graham J., Howard R.* Cyber fraud: tactics, techniques, and procedures. New York (N.Y.): CRC Press, 2009.

9. Lietuvos Respublikos baudžiamojo kodekso komentaras. Specialioji dalis (213–330 straipsniai), II tomas, 2 dalis. Vilnius, 2010.

10. Lietuvos Respublikos baudžiamojo kodekso komentaras. Specialioji dalis (99–212 straipsniai), II tomas, 1 dalis. Vilnius, 2009.

11. *Pavilonis V.* Baudžiamosios teisės normų konkurencija // Teisės problemos. 1996, 2(12).

12. *Pranka D.* Apgaulės samprata ir reikšmė atribojant sukčiavimą ir civilinės teisės pažeidimą. Socialinių mokslų studijos. 2012, 4(2).

13. *Sinkevičius E.* Neteisėtas banko kredito gavimas arba panaudojimas ir jų kvalifikavimas. Vilnius: Lietuvos teisės universiteto Leidybos centras, 2002.

14. *Stoneburner G.* Underlying Technical Models for Information Technology Security: recomendations of the National Institute of Standards and Technology [interaktyvus]. Prieiga per internetą: <*http://csrc.nist.gov/ publications/nistpubs/800-33/sp800-33.pdf*> [žiūrėta 2010-09-27].

15. *Sumit K.*, *[et al.].* Communication networks: principles and practice. New York: McGraw-Hill, 2007.

16. *Štitilis D.*, *[et. al.]* Tapatybės vagystė elektroninėje erdvėje: socialiniai, elektroninio verslo ir teisinio reguliavimo aspektai. Vilnius: Mykolo Romerio universitetas, 2011.

17. *Štitilis D., [et. al.].* Tapatybės vagystės elektroninėje erdvėje kriminalizavimas: lyginamieji aspektai. Socialinių mokslų studijos. 2011, 3(1).

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

III. Teismų praktika:

19. Lietuvos Aukščiausiojo Teismo 2012 m. Teismų praktikos sukčiavimo (Baudžiamojo kodekso 182 straipsnis) baudžiamosiose bylose apžvalga. Teismų praktika Nr. 36.

20. Lietuvos Aukščiausiojo Teismo 2001 m. spalio 9 d. nutartis kasacinėje byloje Nr. 2K-682/2001.

21. Lietuvos Aukščiausiojo Teismo 2005 m. lapkričio 15 d. nutartis kasacinėje byloje Nr. 2K-587/2005.

22. Lietuvos Aukščiausiojo Teismo 2009 m. sausio 29 d. nutartis kasacinėje byloje Nr. 2K-28/2009.

23. Lietuvos Aukščiausiojo Teismo 2012 m. birželio 26 d. nutartis kasacinėje byloje Nr. 2K-375/2012.

24. Vilniaus miesto 1 apylinkės teismo 2011 m. kovo 25 d. nuosprendis baudžiamojoje byloje Nr. 1-68-203/2011.

25. Vilniaus miesto 3 apylinkės teismo 2010 m. sausio 27 d. nuosprendis baudžiamojoje byloje Nr. 1-182-498/10.

26. Vilniaus miesto 1 apylinkės teismo 2010 m. kovo 5 d. teismo baudžiamasis įsakymas byloje Nr. N1-724-276/2010.

27. Vilniaus miesto 4 apylinkės teismo 2010 m. gegužės 17 d. nuosprendis baudžiamojoje byloje Nr. 1-106-816/2010.

28. Klaipėdos miesto apylinkės teismo 2009 m. birželio 29 d. teismo baudžiamasis įsakymas byloje Nr. 1-740-93/2009.

29. Vilniaus miesto 1 apylinkės teismo 2009 m. rugsėjo 14 d. teismo baudžiamajame įsakyme, priimtame byloje Nr. N1-1470-88/2009.

Vaidas KALPOKAS
Renata MARCINAUSKAITĖ
Law Institute

IDENTITY THEFT IN CYBERSPACE: TECHNOLOGICAL ASPECTS AND CRIMINAL LEGAL ASSESSMENT

Summary

The article analyses one of the stages of fraud in cyberspace, i.e. illegal disposal of confidential data proving personal identity in cyberspace. The specifics of fraud in cyberspace, particularities of identity verification in cyberspace and various e-services (e-banking, e-shops, etc.) allow us considering different issues concerning criminal legal assessment of illegal receipt of data, proving personal identity in the cyberspace, their possession at one's disposal and use.

The article discusses currently the most frequent illegal methods to receive data used for identification in cyberspace, such as phishing, pharming, malware, skimming. In addition, considering the evolving jurisprudence, various problematic aspects of qualification of such act are also discussed. According to the authors, only fraud norm, specified in the Article 182 of the Criminal Code of the Republic of Lithuania (hereinafter – CC), is insufficient for a comprehensive criminal legal assessment of fraud in cyberspace. Whereas such criminal act is related to various breaches of security of electronic data and information systems, in addition to the CC Article 182, the perpetrator should also be incriminated offences, specified in the CC Chapter XXX and (or) the CC Articles 215 and 214.

Considering quite different qualification practice, identity theft problem solving options are suggested in the article. First of all, it is suggested to qualify the perpetrator's actions, using various methods to receive data for verification of personal identity in cyberspace, as an independent criminal act. Depending on the chosen method, the features of criminal acts, specified in the CC Chapter XXX, may be determined in the act. Secondly, the article emphasises that if the perpetrator unlawfully receives data with all features, specified in the CC Article 214, the special norm, indicated in the CC Article 214 is applicable instead of the norms, indicated in the CC Articles 198 or 198^2, in order to qualify his act. Thirdly, if it is determined that data, enabling identification of a consumer in electronic service system, have been illegally used for the connection to this system (thus breaching the security measures of this system), it is suggested to qualify such act pursuant to the CC Article 198^1. And fourthly, it is concluded that dangerous act, featuring the initiation of illegal transaction, using data for verification of consumer's identity for online payment measures, should be qualified by applying the CC Article 215, not 198.

Straipsnis redakcijai įteiktas 2012 m. birželio 28 d.