VYTAUTO DIDŽIOJO UNIVERSITETAS
MCMXXII

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (14), 2016, p. 250-266

NETEISĖTO PRISIJUNGIMO PRIE INFORMACINĖS SISTEMOS KRIMINALIZAVIMO YPATUMAI IR KVALIFIKAVIMO PROBLEMOS[1]

Renata Marcinauskaitė[2]
DOI: http://dx.doi.org/10.7220/2029-4239.14.15

SANTRAUKA

Straipsnyje, atsižvelgiant į tarptautinius ir Europos Sąjungos teisės aktus bei teismų praktikos aktualijas, aptariami įvairūs neteisėto prisijungimo prie informacinės sistemos aiškinimo ir kvalifikavimo aspektai. Nors, kaip pabrėžiama, ši informacinės sistemos konfidencialumą pažeidžianti veika Lietuvoje yra kriminalizuota daugiau nei prieš dešimtmetį, tikrosios jos inkriminavimo problemos išryškėjo palyginti neseniai. Straipsnyje bandoma išsiaiškinti, ar iš tiesų tinkamai nustatomas šios veikos santykis su kitomis elektroninėje erdvėje padaromomis nusikalstamomis veikomis, taip pat ar nekelia problemų besiformuojantis šios veikos sudėties požymių aiškinimas..

REIKŠMINIAI ŽODŽIAI

Baudžiamoji teisė, neteisėtas prisijungimas prie informacinės sistemos, nusikalstamų veikų kvalifikavimas, kriminalizavimas.

Ironiška, bet dėl to, kad pagrindinės <...> infrastruktūros sistemos modernizuojamos, jos susiduria su didėjančia planuojamo ar nerūpestingo prisijungimo prie tinklo rizika.
GENE HODGES[3]

1 Straipsnis buvo publikuotas recenzuojamame mokslinių straipsnių rinkinyje „Baudžiamoji justicija ir verslas“.

2 Renata Marcinauskaitė yra Mykolo Romerio universiteto Teisės fakulteto Baudžiamosios teisės ir proceso instituto lektorė, Socialinių (teisės) mokslų daktarė.

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (14), 2016, p. 250-266

ĮVADAS

Nuolatinė kompiuterinių informacinių technologijų ir elektroninių ryšių raida sudaro prielaidas duomenų sklaidai, taip pat naujiems prieigos prie informacinių sistemų (toliau – IS) ir jose esančių duomenų būdams atsirasti. Elektroninė erdvė, kuri paprastai apibūdinama kaip nuolat kintanti terpė[4] arba metaforiškai vadinama „erdve už ekrano“[5], yra sukurta funkcionuoti kaip vieta, kurioje gali būti tvarkomi elektroniniai duomenys, gaunama prieiga prie IS, komunikuojama, dalyvaujama virtualiose veiklose ir pan. Tačiau elektroninės erdvės plėtra yra neatsiejama ir nuo joje kylančių grėsmių, ypač jei kalbama apie šioje erdvėje padaromas nusikalstamas veikas. Atsižvelgiant į 2015 m. Lietuvos Respublikos baudžiamojo kodekso (toliau – BK) XXX skyriaus pakeitimus ir Lietuvos teismų praktikos aktualijas, straipsnyje pasirinkta analizuoti neteisėto prisijungimo prie IS veika, numatyta BK 198[1] straipsnyje.

Ši IS saugumą, tiksliau − jos konfidencialumą pažeidžianti veika Lietuvos BK buvo kriminalizuota 2004 m., tačiau reikėtų pripažinti, kad sukūrus teisinius pagrindus baudžiamajai atsakomybei už ją kilti gilesnių diskusijų dėl šios veikos sudėties požymių aiškinimo ir galimų jos kvalifikavimo problemų nėra daug. Galima būtų paminėti, kad nusikalstamų veikų, kuriomis pažeidžiamas elektroninių duomenų ir IS konfidencialumas, tematikai yra skirtas R. Marcinauskaitės disertacinis tyrimas. Bendrąja veikų elektroninėje erdvėje problematika tiek galiojant 1961 m. BK, tiek ir įsigaliojus 2000 m., domėjosi D. Štitilis ir R. Petrauskas. Dėl baudžiamojo įstatymo ir tarptautinių teisės aktų suderinamumo elektroninių nusikalstamų veikų reglamentavimo srityje yra pasisakęs D. Sauliūnas. Pavienių nusikalstamų veikų elektroninėje erdvėje aiškinimo atvejų paprastai būna mokomuosiuose leidiniuose (vadovėliuose), taip pat baudžiamojo įstatymo komentare, kuriame pateikiamas glaustas teorinis neteisėto prisijungimo prie IS veikos aiškinimas. Tačiau apžvelgus šios kategorijos baudžiamosiose bylose besiformuojančią teismų praktiką kyla iš tiesų netikėtų, mokslinėje literatūroje neaptartų probleminių klausimų, kurių tinkamas išsprendimas yra būtinas nuoseklios ir technologijų pokyčiams atviros teismų praktikos formavimuisi. Todėl pasirinktas šio straipsnio tikslas − ištirti dažniausiai pasitaikančias neteisėto prisijungimo prie IS inkriminavimo problemas ir pasiūlyti galimų šios veikos aiškinimo variantų. Atsižvelgiant į tarptautinius ir Europos Sąjungos teisės aktus, straipsnyje aptariami šios IS konfidencialumą pažeidžiančios veikos kriminalizavimo ypatumai, taip pat analizuojami teismų praktikoje pasitaikantys jos kvalifikavimo probleminiai aspektai.

3 MCCLURE, S., *et al*. Apsauga nuo hakerių: tinklo saugumo palaikymo paslaptys ir sprendimai. Kaunas: „Smaltijos“ leidykla, 2006.

4 WALDEN, I. Computer Crimes and Digital Investigations. Oxford: Oxford University Press, 2007, p. 1.

5 BARBATSIS, G., *et al*. The Performance of Cyberspace: An Exploration Into Computer-Mediated Reality. Journal of Computer-Mediated Communication, Vol. 5 (1), 1999, <http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.1999.tb00332.x/full>.

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (14), 2016, p. 250-266

1. NETEISĖTO PRISIJUNGIMO PRIE IS KRIMINALIZAVIMO YPATUMAI

Neteisėto prisijungimo prie IS kriminalizavimo BK 198[1] straipsnyje ištakos sietinos su tarptautinių ir Europos Sąjungos teisės aktų nuostatų įgyvendinimu. Analizuojant šią veiką, visų pirma aktuali 2001 m. Europos Tarybos konvencija dėl elektroninių nusikaltimų[6] (toliau – Konvencija), kurioje numatyta plačiausia elektroninės erdvės saugumą pažeidžiančių ar jam grėsmę keliančių nusikalstamų veikų apibrėžtis. Joje prie materialiosios baudžiamosios teisės priemonių, kurių turėtų būti imamasi nacionaliniu lygmeniu (II skyriaus 1 skirsnis), nurodomi kriminalizuotini nusikaltimai, be kita ko, darantys žalą ir kompiuterinių duomenų bei sistemų *konfidencialumui, vientisumui* ir *prieinamumui.* Šie elementai padeda atskleisti techninio kompiuterių saugumo turinį ir mokslinėje literatūroje bendrai vadinami konfidencialumo, integralumo ir prieinamumo triada (CIA triada)[7]. Ji, beje, yra tinkama ir BK XXX skyriuje nurodytai baudžiamojo įstatymo saugomai vertybei – elektroninių duomenų ir informacinių sistemų saugumui – atskleisti, šiame skyriuje numatytoms nusikalstamoms veikoms struktūrizuoti. Kalbant apie savarankiškus CIA triados elementus pritartina, kad neteisėto prisijungimo veika pirmiausia turėtų būti siejama su IS konfidencialumo pažeidimais[8].

Be minėtos Konvencijos, šios nusikalstamos veikos analizei ne mažiau svarbūs yra ir Europos Sąjungos teisės aktai: 2005 m. vasario 24 d. Tarybos pamatinis sprendimas 2005/222/TVR dėl atakų prieš informacines sistemas (toliau – Sprendimas 2005/222/TVR)[9] ir 2013 m. rugpjūčio 12 d. Europos Parlamento bei Tarybos direktyva 2013/40/ES dėl atakų prieš informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR (toliau – Direktyva 2013/40/ES)[10]. Kadangi Sprendimo 2005/222/TVR 2 straipsnyje ir Direktyvos 2013/40/ES 3 straipsnyje suformuluota panaši neteisėtos prieigos apibrėžtis, apibendrinant galima būtų teigti, kad ši veika pasireiškia „prieiga prie visos IS arba bet kurios jos dalies neturint tam teisės, jei tai padaryta tyčia, <...> pažeidžiant apsaugos priemonę, bent tais atvejais, kurie nėra mažareikšmiai“. Tačiau tikslumo dėlei reiktų paminėti ir jų skirtumą – IS apsaugos priemonių pažeidimas Direktyvoje 2013/40/ES laikomas būtinu sudėties požymiu, o Sprendime 2005/222/TVR jis minimas tik kaip vienas iš variantų sprendžiant padarytos veikos perteklinio kriminalizavimo problemą. Šiuo aspektu aktualu tai, kad Lietuvoje 2004 m. nustačius baudžiamąją atsakomybę už šią veiką ir vėliau (2007-aisiais) keičiant jos sudėties požymius, neteisėtas prisijungimas visada buvo siejamas su IS apsaugos priemonių pažeidimu. Todėl pastarieji 2015 m. BK 198[1] straipsnio pakeitimai, kuriais į nacionalinę teisę buvo perkeltos Direktyvos 2013/40/ES 3 straipsnio nuostatos, didesnių šios veikos pertvarkų nepadarė.

6 Konvencija dėl elektroninių nusikaltimų. Valstybės žinios, 2004, Nr. 36-1188.

7 MARCINAUSKAITĖ, R. Nusikalstamomis veikomis elektroninėje erdvėje pažeidžiamos pagrindinės baudžiamojo įstatymo saugomos vertybės nustatymo problema. Socialinių mokslų studijos, Nr. 3(3), 2011.

8 ABRAMAVIČIUS, A., *et al*. Lietuvos Respublikos baudžiamojo kodekso komentaras. Specialioji dalis (99−212 straipsniai). Vilnius: Registrų centras, 2009, p. 435.

9 2005 m. vasario 24 d. Tarybos pagrindų sprendimas 2005/222/TVR dėl atakų prieš informacines sistemas. OL L 69, 2005, p. 67.

10 2013 m. rugpjūčio 12 d. Europos Parlamento ir Tarybos direktyva 2013/40/ES dėl atakų prieš informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR. OL L 218, 2013, p. 8.

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (14), 2016, p. 250-266

Pakeitimais patikslintas nusikalstamos veikos dalykas – sudėtyje numatyta ne tik IS, bet ir jos dalis, atitinkamai prisijungimas prie IS laikomas nusikalstamu gavus prieigą tiek prie visos, tiek ir prie dalies IS; taip pat sugriežtinta bausmė už BK 198[1] straipsnio 1 dalyje numatytas veikas pakeliant viršutinę laisvės atėmimo bausmės ribą iki dvejų metų.

Šios nusikalstamos veikos dalyko tikslinimo poreikis iš tiesų kilo ne tik dėl Direktyvos 2013/40/ES 3 straipsnio nuostatų, bet ir dėl IS apibrėžties problemų bei jos funkcionavimo ypatumų. Įgyvendinant technologinio neutralumo principą[11], Direktyvos 2013/40/ES 2 straipsnio a punkte IS apibūdinama abstrakčiai kaip „prietaisas arba tarpusavyje sujungtų ar susijusių prietaisų grupė, iš kurių vienas arba daugiau pagal programą vykdo automatinį kompiuterinių duomenų tvarkymą, taip pat kompiuteriniai duomenys, saugomi, tvarkomi, išrenkami arba perduodami to prietaiso ar grupės prietaisų jo ar jų eksploatacijos, naudojimo, apsaugos ir priežiūros tikslais“. Toks sąvokos „neutralumas technologijoms“, viena vertus, padeda užtikrinti požymių atvirumą elektroninės erdvės pokyčiams, kita vertus, sukelia problemų sprendžiant, kas yra, o kas nėra IS. Kaip matyti, IS sąvoka konstruojama nurodant atskirus prietaisus ar grupes tarpusavyje susijusių prietaisų, kurie ir sudaro šias sistemas. Akivaizdu, kad IS paprastai funkcionuoja kaip vienetas, sudarytas iš įvairių sudedamųjų dalių derinių. Atsižvelgiant į tai, neteisėtas poveikis IS konfidencialumui gali būti padaromas tiesiogiai veikiant ne tik visą sistemą, bet ir vien tam tikrus specifines funkcijas atliekančius jos komponentus (IS dalis). Baudžiamosios teisės srityje dėl to gali kilti neaiškumų, − ar gali būti konstatuotas prisijungimas prie visos IS, jei prieiga gauta tik prie kurio nors vieno įrenginio? Pavyzdžiui, A. Venčkauskas ir J. Toldinas pastebi, kad „konfidencialumo, prieinamumo ir vientisumo sąvokos taikomos ne tik informacijai (duomenims), bet ir kitiems tinklo ištekliams, pavyzdžiui, išoriniams įrenginiams arba priedams. Yra daugybė sisteminių išteklių, kurių „neteisėto“ panaudojimo galimybė gali sudaryti sąlygas pažeisti sistemos saugumą“[12]. Siekiant išvengti galimų nesusipratimų aiškinant BK 198[1] straipsnyje numatyto dalyko požymį, minėtais pakeitimais buvo išspręsta neteisėto prisijungimo inkriminavimo problema byloje nustačius būtent tokią aptartą situaciją (pavyzdžiui, kaltininkui prisijungus prie išorinio įrenginio, kai kurių tinklo infrastruktūros įrenginių ir pan.).

Kitas galintis kilti klausimas, įstatymų leidėjui kriminalizavus šią veiką, – ar aiškinantis elektroninėje erdvėje kylančias grėsmes konfidencialumui (privatumui) nebūtų įmanoma fizinėje erdvėje rasti bent abstraktaus neteisėtos prieigos prie IS atitikmens? Nors dėl BK XXX skyriuje numatytų veikų specifikos tokių analogų ieškoti yra sudėtinga, tačiau į fizinėje ir elektroninėje erdvėse padaromų veikų skirtumus neturėtų būti žvelgiama pernelyg supaprastintai. Neteisėtas prisijungimas prie IS iš pirmo žvilgsnio gali pasirodyti sunkiai paaiškinamas, tačiau kai kurie aspektai vis dėlto leis pamatyti tokios veikos panašumų su tradicinėmis nusikalstamomis veikomis. Čia aktualu, kad informacinių ir komunikacijos technologijų srityje prieiga prie IS dažnai apibrėžiama nevengiant tų posakių, kurie vartojami veiksmams fizinėje erdvėje apibūdinti: priėjimo prie duomenų ar IS gavimas[13], galimybė įeiti ir

11 MARCINAUSKAITĖ, R. Technologinio neutralumo principo taikymo problemos aiškinant nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui sudėties požymius. Socialinių mokslų studijos, Nr. 5 (1), 2013, p. 367.

12 VENČKAUSKAS, A.; TOLDINAS, J. Kompiuterių ir operacinių sistemų sauga. Kaunas: Vitae Litera, 2008, p. 9.

13 A Dictionary of Computing. 5-asis leidimas. Ats. red. Daintith, J. Oxford: Oxford University Press, 2004, p. 5.

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (14), 2016, p. 250-266

naudotis sistema[14] arba galimybė pasiekti sistemos išteklius[15]. Panašiai prieiga apibūdinama ir Konvencijos aiškinamojoje ataskaitoje[16] teigiant, kad ji yra „įėjimas į visą arba dalį kompiuterinės sistemos“ (46 punktas). Kaip matyti, šis prieigos aiškinimas „sukelia buvimo kompiuterio „viduje“ arba „išorėje“ įsivaizdavimą“[17], o pati prieiga tampa panaši į neteisėtą įėjimą į fizinėje erdvėje esančią vietą. Todėl galima ne tik suformuluoti elektroninės erdvės kaip vietos palyginimą, bet taip pat pastebėti tradicinės neteisėto įsibrovimo į svetimą valdą doktrinos raidą. Ji dažnai laikoma logišku atspirties tašku aiškinant neteisėto prisijungimo veiką ir vadinama elektroninio įsibrovimo į svetimą virtualią erdvę terminu (angl. *cybertrespass)*[18]. Šiame kontekste įdomu tai, kad Lietuvos Respublikos Konstitucinis Teismas, ne kartą pasisakydamas dėl Lietuvos Respublikos Konstitucijos 22 straipsnyje numatytos asmens teisės į privatų gyvenimą, pabrėžė, kad pagal Konstituciją privatus žmogaus gyvenimas – tai individo asmeninis gyvenimas, kuris, *inter alia*, yra susijęs ir su jo gyvenamąja aplinka, namų gyvenimu (Konstitucinio Teismo 2002 m. spalio 23 d., 2003 m. kovo 24 d. nutarimai). Gyvenamąją aplinką, pagal Lietuvos Respublikos visuomenės informavimo įstatymo[19] 2 straipsnio 45 punktą, sudaro fizinio asmens gyvenamoji patalpa, jai priklausanti privati teritorija ir kitos privačios patalpos, kurias fizinis asmuo naudoja savo ūkinei, komercinei ar profesinei veiklai. Už teritorinio privatumo pažeidimus, vertinant juos baudžiamosios teisės požiūriu, atsakomybė kyla pagal BK 165 straipsnį, kuriame kriminalizuoti neteisėti asmens būsto neliečiamumo pažeidimai. Analizuojant „įsibrovimą“ elektroninėje erdvėje, galima būtų išsakyti idėją, kad tam tikra elektroninės erdvės kaip vietos privatumo apsauga, *mutatis mutandis* įgyvendinant žmogaus būsto neliečiamumo principą, yra užtikrinta ir BK 198[1] straipsnyje, numatančiame baudžiamąją atsakomybę už neteisėtą prisijungimą prie IS. Šis kontekstas svarbus, nes leidžia aiškiau suvokti tokios veikos prigimtį ir jos santykį su kitomis elektroninėje erdvėje padaromomis nusikalstamomis veikomis.

2. NETEISĖTO PRISIJUNGIMO PRIE IS KVALIFIKAVIMO PROBLEMOS

Dėl technologijų panaudojimo plėtros pakitus nusikalstamų veikų padarymo galimybėms, atsirado esminių tokių veikų kriminalizavimo pakankamumo problemų, kurios bandytos spręsti įvairiai; antai baudžiamajame įstatyme įtvirtintos naujos nusikalstamų veikų sudėtys, teismų praktikoje išplėstas senųjų sudėčių aiškinimas. Tačiau šie bandymai sukūrė ir visai kitų, t. y. baudžiamojo įstatymo normų tarpusavio santykio, problemų. Ne išimtis būtų ir BK 198[1] straipsnyje numatyta nusikalstama veika, kurios taikymas teismų praktikoje yra nevienareikšmis: neteisėto prisijungimo veika ne visada pastebima tarp kitų kaltininko elektroninėje erdvėje padarytų nusikalstamų veikų; BK ieškoma normų, kurios galėtų apimti šią

14 Dictionary of information science and technology. I tomas. Ats. red. Khosrow-Pour, M.; Hershey, P. *et al*.: Idea Group Reference, 2007, p. 2.

15 DAGIENĖ, V., *et al*. Enciklopedinis kompiuterijos žodynas. Vilnius: TEV, 2008, p. 369.

16 Convention on Cybercrime Explanatory Report, <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>.

17 CLOUGH, J. Principles of Cybercrime. Cambridge: Cambridge University Press, 2010, p. 59.

18 WALDEN, I. Computer Crimes and Digital Investigations. Oxford: Oxford University Press, 2007, p. 163.

19 Lietuvos Respublikos visuomenės informavimo įstatymas. Valstybės žinios, 1996, Nr. 71-1706.

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (14), 2016, p. 250-266

veiką, taip išvengiant papildomo BK 198[1] straipsnio taikymo; nenuosekliai aiškinami neteisėto prisijungimo prie IS sudėties požymiai, būtini konstatuojant šios veikos padarymą.

2.1. Neteisėtas prisijungimas prie IS kaip atskira nusikalstama veika

Vienas iš aktualesnių Direktyvos 2013/40/ES 3 straipsnio nuostatų įgyvendinimo BK aspektų yra susijęs su neteisėto prisijungimo prie IS koncepcija, tiksliau − su tuo, kad įstatymų leidėjas, kaip ir anksčiau, šią veiką kriminalizuoja kaip pavojingą savaime, t. y. be tiesioginės sąsajos su paskesnėmis kaltininko sistemoje padaromomis nusikalstamomis veikomis. Todėl atsakomybei pagal BK 198[1] straipsnį atsirasti yra pakankami vien tik kaltininko neteisėti prisijungimo prie IS veiksmai (jei pažeidžiamos IS apsaugos priemonės), nepriklausomai nuo to, ar po prieigos gavimo buvo padarytos kitos nusikalstamos veikos. Toks baudžiamosios atsakomybės nustatymo būdas gali būti siejamas su Konvencijos aiškinamojoje ataskaitoje minimomis priemonėmis, kurių turėtų būti imtasi „ankstyvajame etape“, kol nėra įvykdytos kitos nusikalstamos veikos sistemoje (45 punktas). Kaip teigia J. Clough, taip kriminalizuota veika yra „baudimo už „nutolusią“ žalą, kurios kilimas priklauso nuo kaltinamojo ar kito asmens būsimo sprendimo padaryti nusikaltimą, pavyzdys“[20]. Konvencijos aiškinamojoje ataskaitoje pabrėžiama, kad įsibrovimas gali suteikti prieigą „prie konfidencialių duomenų (įskaitant slaptažodžius, informaciją apie sistemą) ir paslapčių, sudaryti galimybę nemokamai naudotis sistema arba paskatinti programišius padaryti daug pavojingesnius su kompiuteriais susijusius nusikaltimus, tokius kaip sukčiavimas ar klastojimas“ (44 punktas).

Kadangi neteisėtas prisijungimas BK kriminalizuotas kaip pavojingas pats savaime ir nėra įtrauktas į kitų nusikalstamų veikų sudėtį, tai ši veika turėtų būti inkriminuojama kiekvieną kartą nustačius visus BK 198[1] straipsnyje aprašytus sudėties požymius. Iš tiesų įstatymo leidėjo pasirinktas toks šios veikos kriminalizavimo būdas sukuria gana įdomią visų kaltininko padarytų veikų kvalifikavimo situaciją: paprastai galimybių padaryti įvairias nusikalstamas veikas pačioje IS suteikia pirminiai neteisėto prisijungimo veiksmai, todėl kvalifikuojant visas kaltininko padarytas nusikalstamas veikas neturėtų stebinti itin dažnas neteisėto prisijungimo prie IS inkriminavimas. Palyginant galima būtų aptarti neteisėto įsibrovimo į svetimą fizinėje erdvėje esančią teritoriją atvejį, jei nustatoma, kad tokie įsibrovimo veiksmai sudarė galimybes, pavyzdžiui, pagrobti patalpoje ar saugomoje teritorijoje esantį materialų turtą. Iš BK 165 ir 178 bei 180 straipsnių 2 dalių matyti, kad neteisėto asmens būsto neliečiamumo pažeidimo ir svetimo turto pagrobimo derinimo problema fizinėje erdvėje išspręsta vagystės ir plėšimo sudėtyse numačius šias veikas kvalifikuojantį įsibrovimo į patalpą, saugyklą ar saugomą teritoriją požymį. Vadinasi, tokios veikos papildomai ir pagal BK 165 straipsnį nekvalifikuojamos. Deja, panašiu būdu nebuvo bandyta spręsti neteisėto prisijungimo prie IS ir, pavyzdžiui, neteisėto elektroninių duomenų perėmimo ir panaudojimo (BK 198 straipsnis), neteisėto poveikio elektroniniams duomenims (BK 196 straipsnis) sąryšio problemos[21].

20 CLOUGH, J. Data Theft? Cybercrime and the Increasing Criminalization of Access to Data. Criminal Law Forum, No. 22, 2011, p. 161.

21 Tik iš dalies su neteisėtu prisijungimu prie IS gali būti siejamas 2015 m. BK 196 ir 197 straipsniuose numatytas požymis „pasinaudodamas svetimais asmens duomenimis“ (plačiau žr. ir Direktyvos 2013/40/ES 9 straipsnio 5 dalį).

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (14), 2016, p. 250-266

Analizuojant teismų praktiką matyti, kad dažniausiai užuominų dėl BK 198[1] straipsnio taikymo gali būti randama sukčiavimo ir privataus gyvenimo neliečiamumo pažeidimų baudžiamosiose bylose. Pavyzdžiui, Lietuvos Aukščiausiojo Teismo 2012 m. birželio 26 d. nutartyje baudžiamojoje byloje Nr. 2K-375/2012 atkreiptas dėmesys į tai, kad „veiksmai neteisėtai prisijungus prie internetinės bankininkystės sistemos, panaudojant svetimus vartotoją identifikuojančius duomenis, galėtų būti kvalifikuojami ir pagal 198[1] straipsnį kaip neteisėtas prisijungimas prie informacinės sistemos <...>“. Ne mažiau aktuali aptariamos nusikalstamos veikos aiškinimui yra ir Lietuvos Aukščiausiojo Teismo 2015 m. sausio 6 d. kasacinė nutartis baudžiamojoje byloje Nr. 2K-138-976/2015, kurioje pasisakyta dėl BK 198[1] straipsnio inkriminavimo kaltininkui neteisėtai prisijungus prie kito asmens elektroninio pašto paskyros. Kadangi šioje byloje taip pat buvo iškelta BK 198[1] ir 198 straipsnių santykio problema, kasacinės instancijos teismas ją spręsdamas nurodė, kad neteisėtas elektroninių duomenų perėmimas ir panaudojimas neapima neteisėto prisijungimo prie IS, todėl kaltininko veikai kvalifikuoti, be kitų, turi būti taikomas ir BK 198[1] straipsnis: „Neteisėtas prisijungimas prie IS BK 198[1] straipsnyje numatytas atsižvelgiant į 2001 m. lapkričio 23 d. Konvencijos dėl elektroninių nusikaltimų 2 straipsnį ir 2005 m. vasario 24 d. Tarybos pamatinio sprendimo 2005/222/TVR dėl atakų prieš informacines sistemas <...> 2 straipsnį. Įgyvendinant šiuos teisės aktus neteisėtas prisijungimas BK 198[1] straipsnyje kriminalizuotas kaip savarankiška nusikalstama veika, t. y. be tiesioginio ryšio su kitomis jau sistemoje padaromomis veikomis. Be to, BK 198[1] straipsnyje numatytos veikos inkriminavimui būtina nustatyti, kad prie IS buvo prisijungta pažeidžiant šios sistemos apsaugos priemones. Nagrinėjamos bylos kontekste aktualu tai, kad vartotoją elektroninio pašto sistemoje leidžianti nustatyti autentiškumo patvirtinimo procedūra gali būti laikoma viena iš šios sistemos saugumo (taip pat ir konfidencialumo) užtikrinimo priemonių. O teisėto vartotojo tapatybę patvirtinančių duomenų neteisėtas įvedimas, suklaidinant sistemą, laikytinas šios sistemos apsaugos priemonių pažeidimu ir atitinka tik neteisėto prisijungimo prie IS veikos padarymo būdą. Taigi byloje nustatyto neteisėto prisijungimo prie elektroninio pašto paskyros *j@yahoo.de* vertinimui taikant tik BK 198 straipsnį, iš baudžiamosios teisės pozicijų liktų neįvertintas pats neteisėto prisijungimo prie paskyros veiksmas. Todėl, priešingai nei teigiama kasaciniame skunde, BK 198[1] straipsnio 1 dalies, o ne BK 198 straipsnio 1 dalies norma pripažintina norma-visuma ir taikytina kvalifikuojant neteisėtą prisijungimą prie informacinės sistemos, šiuo atveju − prie elektroninio pašto paskyros.“

Neaiškumų vertinant BK 198[1] straipsnio taikymo galimybes, jei byloje nustatytas įdiegtos autentifikavimo procedūros apėjimo faktas, gali kelti kitų (žemesniosios instancijos) teismų praktika. Nors ir nereti atvejai, kai neteisėti kaltininko prisijungimo, pavyzdžiui, prie internetinės bankininkystės veiksmai teismų sprendimuose kvalifikuoti atskirai pagal BK 198[1] straipsnį[22], tačiau praktikoje būta ir diskutuotinų aiškinimų. Antai Kauno apygardos teismo 2015 m. gegužės 7 d. nutartyje baudžiamojoje byloje Nr. 1A-432-594/2015 teigiama, kad IS apsaugos priemonių pažeidimu yra laikomi veiksmai, kuriais priėjimas prie IS resursų yra gaunamas apeinant informacinės sistemos saugumo politikos nustatytas procedūras ir

22 Pavyzdžiui, Klaipėdos miesto apylinkės teismo 2015 m. birželio 11 d. nuosprendis baudžiamojoje byloje Nr. 1-430-606/2015, Kauno apylinkės teismo 2015 m. kovo 19 d. nuosprendis baudžiamojoje byloje Nr. 1-754-738/2015, Trakų rajono apylinkės teismo 2015 m. balandžio 17 d. teismo baudžiamasis įsakymas byloje Nr. 1-164-424/2015.

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (14), 2016, p. 250-266

procesus. Tačiau byloje tokių priemonių pažeidimu nepripažintas prisijungimas prie banko IS panaudojus apgaulę, atitinkamai šie veiksmai pagal BK 198[1] straipsnį nekvalifikuoti: „M. V. pirmiausia iš M. M. neteisėtai įgijo jo tapatybės patvirtinimo priemonių duomenis, pakankamus finansinei operacijai inicijuoti (BK 214 str. 1 d.), po to, neteisėtai naudodamas tuos įgytus duomenis, inicijavo atitinkamas finansines operacijas (BK 215 str. 1 d.) ir taip apgaule įgijo turtinę teisę į M. M. turtą (BK 182 str. 1 d.). Priešingai prokuroro apeliacinio skundo argumentams, byloje nenustatyta, kad M. V., įgyvendindamas savo nusikalstamą sumanymą, teikdamas paraiškas juridiniams asmenims dėl kreditų, prisijungdamas prie AB (duomenys neskelbtini) informacinės sistemos – elektroninės bankininkystės, atlikdamas kitas kaltinime nurodytas finansines operacijas, būtų pažeidęs kažkokias informacinės sistemos apsaugos priemones, jas sugadinęs, pakenkęs apsaugos priemonių režimui, sutrikdęs informacinės sistemos darbą ir pan. M. V. prie informacinių sistemų neteisėtai jungėsi naudodamasis tikrais, nors ir neteisėtai gautais elektroninių mokėjimo priemonių naudotojo tapatybės patvirtinimo duomenimis ir informacinių sistemų apsaugos priemonių nepažeidė.“

Pritarus, kad elektroninio sukčiavimo, privataus gyvenimo neliečiamumo elektroninėje erdvėje pažeidimų ir kt. baudžiamosiose bylose neteisėto prisijungimo prie IS veikai turėtų būti suteikta savarankiška reikšmė, aktualiu tampa nusikalstamų veikų sutapties (realiosios ar idealiosios) nustatymo klausimas. Kaip žinia, realioji sutaptis paprastai yra konstatuojama, jei kelios savarankiškos veikos (numatytos tiek skirtinguose, tiek tuose pačiuose BK specialiosios dalies straipsniuose ar jų dalyse) yra padarytos esant tarp jų laiko tarpui[23]. Tačiau čia reikėtų paminėti svarbų idealiosios nusikalstamų veikų sutapties plėtojimo teismų praktikoje aspektą. Antai Lietuvos Aukščiausiasis Teismas yra konstatavęs, kad „nusikalstamų veikų sutaptis yra ideali ir tuo atveju, jei įgyvendinant vieningą sumanymą padarytos kelios veikos, kurios iš esmės yra neatskiriamos (būtinos) visos kaltininko veikos dalys, šios veikos padarytos viena po kitos, per trumpą laiko tarpą“ (pavyzdžiui, kasacinės nutartys baudžiamosiose bylose Nr. 2K-355/2009, Nr. 2K-P-78/2012, Nr. 2K-207/2013). Nors toks idealiosios nusikalstamų veikų sutapties aiškinimas dar tebeplėtojamas, tačiau teismų praktikoje galima pastebėti bandymų šią sutaptį įžvelgti ir neteisėto prisijungimo prie IS baudžiamosiose bylose[24]. Be abejo, šios kiek pakitusios idealiosios sutapties taikymas turėtų būti pagrįstas aplinkybių visumos analize, motyvuojant, kad padarytos nusikalstamos veikos yra tarpusavyje neatsiejamos, padaromos įgyvendinant vieningą kaltininko tyčią ir tik kartu geriausiai atspindi visą jo nusikalstamą sumanymą. Šį aiškinimą perimant IS konfidencialumo pažeidimų baudžiamosiose bylose, idealioji sutaptis paprastai galėtų būti inkriminuojama, jei neteisėtai prisijungdamas prie IS kaltininkas yra aiškiai suvokęs, kokius paskesnius veiksmus sistemoje jis rengiasi atlikti, ir palaipsniui šį sumanymą įgyvendina. Tai, priklausomai nuo sistemos teikiamų paslaugų, gali būti neteisėtų mokėjimo operacijų atlikimas (pervedant pinigus į kitas sąskaitas, sumokant už

23 PIESLIAKAS, V. Lietuvos baudžiamoji teisė. Antroji knyga. Vilnius: Justitia, 2008, p. 129; GIRDENIS, T. Nusikalstamų veikų daugetas Lietuvos baudžiamojoje teisėje. Socialiniai mokslai: teisė (01 S). Vilnius: Mykolo Romerio universitetas, 2010, p. 105.

24 Pavyzdžiui, Panevėžio miesto apylinkės teismo 2015 m. spalio 1 d. teismo baudžiamajame įsakyme byloje Nr. 1-637-334/2015 kaltininkui už BK 214 straipsnio 1 dalyje, 215 straipsnio 1 dalyje, 198[1] straipsnio 1 dalyje, 182 straipsnio 1 dalyje numatytų veikų padarymą paskirtos bausmės subendrintos jas apimant, nes konstatuota idealioji visų jo padarytų nusikalstamų veikų sutaptis (BK 63 straipsnio 5 dalies 1 punktas).

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (14), 2016, p. 250-266

pirkinius, pasinaudojus internetine bankininkyste gaunant greituosius kreditus[25] ir kt.), privataus gyvenimo neliečiamumo pažeidimai, socialinės inžinerijos metodų taikymas renkant kitų asmenų konfidencialius duomenis, komercinės informacijos įgijimas, elektroninių dokumentų klastojimas, neteisėtas poveikis pačiai IS ir daugelis kitų. Priešingu atveju, pagal bylos aplinkybes nustačius, kad po prisijungimo prie IS susiformavo nauja kaltininko tyčia, kurią įgyvendinant buvo padarytos iš pradžių nenumatytos veikos, jos galėtų sudaryti realiąją sutaptį. Pavyzdžiui, nusikalstamų veikų sutapčių klausimas spręstas jau minėtoje Lietuvos Aukščiausiojo Teismo 2015 m. sausio 6 d. nutartyje baudžiamojoje byloje Nr. 2K-138-976/2015, kurioje nustatyta, kad kaltininkas, neteisėtai prisijungęs prie elektroninio pašto paslaugą teikiančios sistemos, vėliau pažeidė ir asmens privataus gyvenimo neliečiamumą. Šioje byloje kasacinės instancijos teismas priėjo prie išvados, kad L. B. padarytos nusikalstamos veikos sudaro ne idealiąją, o realiąją sutaptį, iš esmės dėl to, kad jos tarpusavyje nebuvo sujungtos idealiajai sutapčiai būdingu vieningo sumanymo požymiu (tyčia): „Byloje nenustatyta, kad L. B. veiksmais neteisėtai prisijungiant prie elektroninio pašto paskyros *j@yahoo.de*, gaunant privataus pobūdžio D. J. ir D. Č. susirašinėjimą elektroniniu paštu ir vėliau šį susirašinėjimą išsiunčiant šešiais elektroninio pašto adresais buvo siekta vieno pagrindinio tikslo – viešai paskleisti informaciją apie asmens privatų gyvenimą, ir kad juos jungė vieningas sumanymas. Priešingai, iš bylos medžiagos darytina išvada, kad neteisėto prisijungimo prie D. J. elektroninio pašto dėžutės tikslas buvo patikrinti, kokio turinio susirašinėjimas yra jos pašto dėžutėje. Kitas savarankiškas sumanymas ir tyčia atskleisti tretiesiems asmenims išsaugotas nuotraukas ir susirašinėjimą kilo tada, kai L. B. atsitiktinai pastebėjo minėtas nuotraukas ir perskaitė D. J. ir D. Č. susirašinėjimą. Taigi šioje situacijoje, teisėjų kolegijos nuomone, visos L. B. padarytos nusikalstamos veikos nebuvo susijusios viena ta pačia paskata (motyvu), susiformavusia viena tyčia, taigi ir nebuvo neatskiriamos jo padarytos veikos dalys.“

2.2. Neteisėtas prisijungimas prie IS ir neteisėtas elektroninės mokėjimo priemonės ar jos duomenų panaudojimas (BK 215 straipsnis)

Paplitus elektroninės komercijos paslaugoms, jų teikimas tapo neatsiejamas nuo asmens tapatybės nustatymo elektroninėje erdvėje, įvairių vartotojo atliekamų veiksmų patvirtinimo reikalavimų. Ši teikiamų e. paslaugų funkcionavimo specifika, be kita ko, gali lemti nusikalstamų veikų kvalifikavimo problemas, pavyzdžiui, nustačius, kad prieiga prie atitinkamų e. paslaugų buvo gauta neteisėtai ir padaryta žala tikrajam IS bei jos teikiamų paslaugų naudotojui.

Apžvelgus teismų praktiką matyti, kad aktualus klausimas kvalifikuojant neteisėtos prieigos prie internetinės bankininkystės veiksmus yra susijęs su BK 198[1] ir 215 straipsniuose aprašytų nusikalstamų veikų santykiu. Vienas iš praktikoje pateikiamų aiškinimo variantų būtų tas, kad neteisėta prieiga yra sudėtinė BK 215 straipsnyje numatytos nusikalstamos veikos

25 Šiuo aspektu, be kita ko, aktualios Lietuvos Aukščiausiojo Teismo nutartys atnaujintose administracinių teisės pažeidimų bylose Nr. 2AT-6-942/2015, Nr. 2AT-23-303/2015, Nr. 2AT-44-2014, kuriose pripažinta, jog 1 cento pavedimo iš kliento banko sąskaitos gavimas pažeidžia kliento ir naudos gavėjo tapatybės nustatymo priemonių įgyvendinimo tvarką.

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (14), 2016, p. 250-266

dalis, todėl prisijungimo veiksmų kvalifikavimas ir pagal BK 198[1] straipsnį yra perteklinis[26]. Pavyzdžiui, Klaipėdos apygardos teismo 2015 m. balandžio 15 d. nuosprendyje baudžiamojoje byloje Nr. 1A-19-557/2015 nurodoma, kad „<...> neteisėtai inicijuoti ar atlikti bent vieną finansinę operaciją, neteisėtai panaudojant bent vienos svetimos elektroninės mokėjimo priemonės naudojo tapatybės patvirtinimo priemonių duomenis, <...> buvo galima tik neteisėtai prisijungiant prie informacinės sistemos, pažeidžiant informacinės sistemos apsaugos priemones – panaudojant neteisėtai gautus I. B. prisijungimo prie banko sąskaitos elektroninės bankininkystės duomenis. Taigi šiuo atveju kvalifikuojant atliktas veikas, konstatuotina ne idealioji nusikalstamų veikų sutaptis, o kitas reiškinys, baudžiamosios teisės teorijoje vadinamas visumos ir dalies konkurencija, kur visuma yra BK 215 str. 1 d., o dalis – BK 198[1] str. 1 dalis. Esant visumos ir dalies konkurencijai, taikoma bendra visumą nustatanti norma, nes ji atitinka visus padarytos veikos požymius, išskyrus atvejį, kai nusikalstamos veikos dalis, įeinanti į visumą, yra pavojingesnė nei pati visuma ir reikalauja sutapties taikymo.

BK 215 str. 1 d. nustatyta griežčiausia bausmė yra laisvės atėmimas iki šešerių metų (apysunkis nusikaltimas pagal BK 11 str. 4 d.), o BK 198[1] str. 1 d. – laisvės atėmimas iki vienerių metų (nesunkus nusikaltimas pagal BK 11 str. 3 d.). Taigi BK 215 str. 1 d. numatytas neteisėtas elektroninės mokėjimo priemonės ar jos duomenų panaudojimas (visuma) yra pavojingesnė veika nei BK 198[1] str. 1 d. numatytas neteisėtas prisijungimas prie informacinės sistemos (dalis), todėl A. Š. veika turėjo būti kvalifikuota tik pagal BK 215 str. 1 d., o jos kvalifikavimas dar ir pagal BK 198[1] str. 1 d. yra perteklinis.“

Su šiuo nuosprendyje pateiktu išaiškinimu sutikti nesinorėtų dėl kelių priežasčių. Svetimi elektroninių mokėjimo priemonių naudotojų tapatybės patvirtinimo duomenys prisijungiant prie internetinės bankininkystės ir vėliau inicijuojant ar atliekant finansinę operaciją yra panaudojami skirtingais veiksmais. Neabejotina, kad tokie duomenys yra pateikiami autentiškumo patvirtinimo procedūros metu suklaidinant IS, tačiau pasinaudojant apgaule prisijungimas prie internetinės bankininkystės paprastai neturėtų būti laikomas finansine operacija, kurią numato BK 215 straipsnio dispozicija. Techninės kliūtys, kaip antai minėtos autentiškumo patvirtinimo procedūros (loginės prieigos kontrolės sistemos)[27] yra naudojamos elektroninės atpažinties procese, o pirminė jų paskirtis, be kita ko, yra užtikrinti IS saugumą (konfidencialumą), tai yra kad prie jos galės prisijungti tik teisėtą prieigą turintys vartotojai. Tik po tapatybės įrodymo ir patikrinimo procedūros asmeniui yra suteikiamos galimybės atlikti tolimesnius veiksmus pačioje sistemoje, naudotis jos teikiamomis paslaugomis (kurios, beje, ne visada yra susijusios su finansinių operacijų inicijavimu ar atlikimu). Nors pradedant neteisėtas mokėjimų operacijas kaltininkui yra būtina prieš tai neteisėtai prisijungti prie internetinės bankininkystės, vien tik tai nesudaro prielaidų teigti, kad kuri nors vėliau padaroma veika turėtų visada apimti pirminius IS konfidencialumo pažeidimo veiksmus – tiek BK 198[1], tiek 215 straipsniuose numatytos veikos yra atskiros, todėl siūlytina jas ir kvalifikuoti atskirai.

Čia reikėtų atkreipti dėmesį į tai, kad tokia teismų praktika nėra absoliuti, nes taip pat galima rasti pavyzdžių[28], kai kvalifikuojant sukčiavimą, padarytą pasinaudojus internetine

26 Kauno apygardos teismo 2015 m. liepos 31 d. nuosprendis baudžiamojoje byloje Nr. 1A-644-634/2015; Šiaulių apygardos teismo 2015 m. liepos 2 d. nutartis baudžiamojoje byloje Nr. 1A-299-309/2015.

27 Milinis, A., et al. Lietuvos baudžiamoji teisė. Specialioji dalis. Pirmoji knyga. Vilnius: Justitia, 2013, p. 483.

28 Vilniaus apygardos teismo 2014 m. gegužės 12 d. nuosprendis baudžiamojoje byloje Nr. 1A-294-195/2014; Kauno apygardos teismo 2015 m. balandžio 16 d. nutartis baudžiamojoje byloje Nr. 1A-301-

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (14), 2016, p. 250-266

bankininkyste, kaltininkui, be kitų veikų, atskirai inkriminuotos ir BK 198[1] bei 215 straipsniuose numatytos veikos. Pavyzdžiui, Kauno apygardos teismo 2015 m. balandžio 16 d. nutartyje baudžiamojoje byloje Nr. 1A-301-478/2015 teigiama, kad neteisėtas prisijungimas prie IS kriminalizuotas „kaip savarankiška nusikalstama veika, t. y. be tiesioginio ryšio su kitomis jau sistemoje padaromomis veikomis (Lietuvos Aukščiausiojo Teismo nutartis Nr. 2K-138/2015). Nagrinėjamu atveju, S. B., S. B. ir L. D., veikdami grupėje ir su kitais įrodymų tyrimo metu nenustatytais asmenimis, iš nukentėjusiosios J. R. apgaulės būdu įgijo elektroninės bankininkystės duomenis, kurie leido prisijungti prie elektroninės bankininkystės sistemos <...> vartotoją elektroninės bankininkystės sistemoje leidžianti nustatyti autentiškumo patvirtinimo procedūra gali būti laikoma viena iš šios sistemos saugumo (taip pat ir konfidencialumo) užtikrinimo priemonių. O teisėto vartotojo tapatybę patvirtinančių duomenų neteisėtas įvedimas, suklaidinant sistemą, laikytinas šios sistemos apsaugos priemonių pažeidimu ir atitinka neteisėto prisijungimo prie informacinės sistemos veikos padarymo būdą, todėl nuteistųjų veiksmai atitinka BK 198[1] straipsnio 1 dalies dispoziciją. <...> BK 215 straipsnio 1 dalyje numatytų nusikalstamų veikų objektyvieji požymiai pasireiškė tuo, kad S. B., S. B. ir L. D., veikdami grupėje ir su kitais įrodymų tyrimo metu nenustatytais asmenimis, neteisėtai panaudodami svetimos elektroninės mokėjimo priemonės ir jos naudotojos J. R. tapatybės patvirtinimo priemonės duomenis, tai yra atsiskaitomosios sąskaitos numerius, internetinės bankininkystės prisijungimo kodus bei slaptažodžių kortelės kodus, neteisėtai, apgaule, nukentėjusiosios J. R. vardu, pasinaudoję G. B. pagalba, inicijavo ir atliko finansines operacijas – sudarė paskolos sutartis“.

2.3. Kai kurios neteisėto prisijungimo prie IS veikos sudėties požymių aiškinimo problemos

Neteisėto prisijungimo prie IS padarymo būdas – šios sistemos apsaugos priemonių pažeidimas − yra vienas iš kriterijų, apibrėžiančių neteisėto prisijungimo prie IS inkriminavimo ribas; šio požymio aiškinimas gali rodyti gana siaurą arba, priešingai, platesnį, įvairius prisijungimo variantus apimantį suvokimą. Minėta, kad, pagal Direktyvos 2013/40/ES 3 straipsnį, IS apsaugos priemonių pažeidimas yra būtinas nusikalstamos veikos sudėčiai inkriminuoti, o baudžiamoji atsakomybė už šią nusikalstamą veiką turėtų kilti bent tais atvejais, kurie nėra mažareikšmiai. Pati direktyva šio požymio turinio neatskleidžia, mažareikšmiškumo klausimus palieka spręsti nacionalinei teisei ir praktikai, pateikdama tik kai kurių gana abstrakčių vertinamųjų kriterijų: „Atvejis gali būti laikomas mažareikšmiu <...> kai nusikalstama veika padaryta žala ir (arba) dėl jos kylanti grėsmė viešiesiems arba privatiesiems interesams, pvz., kompiuterių sistemos arba kompiuterinių duomenų vientisumui arba asmens neliečiamumui, teisėms ir kitiems interesams, yra menka arba tokio pobūdžio, kad nėra būtina skirti baudžiamąją sankciją laikantis teisės aktuose nustatytų ribų arba nustatyti baudžiamąją atsakomybę“ (Direktyvos 2013/40/ES preambulės 11 punktas).

Nors neteisėtas prisijungimas prie IS Lietuvos BK 198[1] straipsnyje visada buvo siejamas su sistemos apsaugos priemonių pažeidimu, tačiau per visą šio straipsnio taikymo laikotarpį taip ir nesusiformavo vienoda minėto požymio aiškinimo praktika. Bene pagrindinė šioje srityje

478/2015.

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (14), 2016, p. 250-266

kylanti technologijų ir terminologijos problema gali būti nusakyta klausimu – ar IS apsaugos priemonių pažeidimas turėtų būti konstatuojamas tik tada, kai toms apsaugos priemonėms yra padaryta žala? Ar vis dėlto tokia nusikalstamos veikos padarymo būdo formuluotė interpretuotina ir kitaip – kaip apsaugos priemonėmis nustatytų apribojimų (reikalavimų) pažeidimas? Bene akivaizdžiausi atvejai, kai žala pačioms IS apsaugos priemonėms nėra padaroma, yra kai kaltininkas pažeidžia elektroninės atpažinties procese taikomų priemonių nustatytus prisijungimo prie IS apribojimus (pavyzdžiui, kito asmens duomenimis neteisėtai jungiasi prie elektroninio pašto paskyros, socialinių tinklų, internetinės bankininkystės, elektroninės parduotuvės).

Šiame kontekste aktualu, kad paplitusi vartotoją elektroninių paslaugų sistemoje leidžianti nustatyti autentiškumo patvirtinimo procedūra (loginė prieigos kontrolės sistema) gali būti laikoma viena iš šios sistemos saugumo užtikrinimo priemonių. Šios priemonės padeda nustatyti asmens, siekiančio naudotis sistema, tapatybę ir, jei funkcionuoja sklandžiai, užtikrina, kad sistema bus prieinama tik tokią teisę turintiems asmenims ar kitoms sistemoms. Kadangi elektroninėje erdvėje tapatybę paprasčiausiu atveju gali atstoti, pavyzdžiui, vartotojo vardas (ar ID) ir slaptažodis[29], kaltininkas šiais neteisėtai įgytais duomenimis jungdamasis prie sistemos tiesioginės žalos jos apsaugos priemonėms nepadaro. Tačiau būtina diskusija, ar iš tiesų tokie atvejai turėtų būti pašalinami iš BK 198[1] straipsnio taikymo srities? Pirma, žalos padarymas apsaugos priemonėms (pavyzdžiui, jų sugadinimas) objektyviai nėra būtinas, jei prieiga prie IS yra gaunama autentifikavimo procedūros metu panaudojus apgaulę, t. y. IS pateikiant teisėto vartotojo duomenis ir taip ją suklaidinant; antra, dėl apgaulės IS suteikus prieigą kaltininkui yra pažeidžiami apsaugos priemonėmis (paprastai ir privatumo politika bei sutartimis pagrįsti) nustatyti apribojimai, turėję užtikrinti, kad sistema galės naudotis tik tam teisę turintis vartotojas; trečia, ne mažiau svarbu tai, kad po tokio neteisėto prisijungimo kaltininkas įgyja galimybių sistemoje įgyvendinti kitus nusikalstamus ketinimus, taigi tokie veiksmai neturėtų būti vertinami kaip nereikšmingi baudžiamosios teisės požiūriu. Atsižvelgiant į tai vertėtų svarstyti, ar BK 198[1] straipsnyje nurodytas požymis *apsaugos priemonių pažeidimas* neturėtų būti aiškinamas atsižvelgiant į galimų neteisėtų prisijungimų prie IS būdų įvairovę ir bendriausia prasme reikšti minėtomis priemonėmis nustatytų apribojimų pažeidimus. Taip būtų išspręstos BK 198[1] straipsnio taikymo problemos, byloje nustačius, kad prie IS buvo prisijungta pasinaudojus apgaule ar sistemos saugumo spragomis, pavyzdžiui, taikant SQL komandos įterpimo ataką, pasinaudojus buferio perpildymo spraga ir pan.

Kaip matyti, teismų praktikoje kol kas ši technologijų ir terminologijos problema sunkiai išsprendžiama. Smarkiai besiskiriantys aiškinimai leidžia kalbėti apie du skirtingus požiūrius. Pirmuoju atveju lanksčiau ir plačiau atskleidžiamas IS apsaugos priemonių pažeidimo turinys. Pavyzdžiui, Lietuvos Aukščiausiojo Teismo 2015 m. gruodžio 8 d. nutartyje baudžiamojoje byloje Nr. 2K-555-788/2015 nurodoma, kad „<...> kasacinio teismo praktikoje, aiškinant informacinės sistemos apsaugos priemonių pažeidimo požymį, <...> atkreiptas dėmesys, jog vartotoją informacinėje sistemoje leidžianti nustatyti autentiškumo patvirtinimo procedūra gali būti laikoma viena iš šios sistemos saugumo (taip pat ir konfidencialumo) užtikrinimo priemonių. O teisėto vartotojo tapatybę patvirtinančių duomenų neteisėtas įvedimas, suklaidinant sistemą, laikytinas šios sistemos apsaugos priemonių pažeidimu ir atitinka neteisėto prisijungimo prie informacinės sistemos veikos padarymo būdą (kasacinės nutartys

29 ŠTITILIS, D.; LAURINAITIS, M. Tapatybės vagystė elektroninėje erdvėje. Informacijos mokslai, Nr. 50, 2009, p. 241.

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (14), 2016, p. 250-266

baudžiamosiose bylose Nr. 2K-375/2012, Nr. 2K-138/2015). Toks neteisėto prisijungimo prie informacinės sistemos (be kita ko, ir internetinės bankininkystės sistemos) atvejis pasireiškia autentifikavimo priemonėmis nustatytų prisijungimo prie informacinės sistemos apribojimų (reikalavimų) pažeidimu, kuris šios bylos kontekste negali būti laikomas nereikšmingu vertinant jį iš baudžiamosios teisės pozicijų. Nagrinėjamoje byloje M. V. neteisėtai jungdavosi prie AB (duomenys neskelbtini), tik M. M. buvo suteiktos internetinės bankininkystės paslaugos, leidžiančios naudotis banko paslaugų teikimu internetu, be kita ko, atlikti mokėjimo operacijas. Ne mažiau svarbu tai, kad M. V. padaryti neteisėti prisijungimai prie internetinės bankininkystės leido neteisėtai sudaryti kredito sutartis ir taip apgaule įgyti jam nepriklausantį (svetimą) turtą“.

Kitas teismų praktikos taikomas apsaugos priemonių pažeidimo interpretavimo variantas yra daug siauresnis, pabrėžiantis šių priemonių sugadinimą, jų funkcionavimo sutrikdymą. Šiuo aspektu galima būtų paminėti Panevėžio apygardos teismo 2015 m. sausio 29 d. nuosprendį baudžiamojoje byloje Nr. 1A-23-366-2015, kuriame, be kitų nusikalstamų veikų, spręstas ir neteisėto prisijungimo prie internetinės bankininkystės klausimas. Byloje teismas pasisakė, kad pažeidimas gali būti nustatomas kaltininkui „naudojant ne savo slaptažodį, panaudojant nusikaltimams daryti tiesiogiai skirtus ar pritaikytus įrenginius ar kompiuterines programas, išvengiant identifikacijos, apeinant užkardas ir pan., taip pat išnaudojant silpnas vietas sistemos apsaugoje“. Nors, kaip matyti, nusikalstamos veikos padarymo būdas teismo buvo apibrėžtas plačiai (įskaitant ir svetimų slaptažodžių panaudojimą), tačiau byloje kaltininkai pagal BK 198[1] straipsnio 1 dalį išteisinti kaip nepadarę veikos, turinčios šio nusikaltimo požymių. Kaip nurodoma nuosprendyje, „iš byloje nustatytų aplinkybių visumos matyti, kad nuteistųjų J. T. ir V. D. tikslas buvo pasisavinti svetimus pinigus. Neteisėtai įgiję V. Č. banko mokėjimo kortelę ir tikrąjį jos PIN kodą, informacinėje banko sistemoje prisijungė prie sąskaitos Nr. (duomenys neskelbtini) įvesdami tikrąjį PIN kodą ir atliko finansines operacijas, kuriomis išgrynino pinigus arba atsiskaitė už prekes. Kadangi byloje nenustatyta, kad nuteistieji būtų siekę pamatyti informacinėje sistemoje laikomas duomenų bylas, susipažinti su duomenų turiniu, atlikti kitus veiksmus (juos keisti, trinti, kopijuoti ir t. t.), kad jų veiksmai būtų buvę nukreipti prieš elektroninių duomenų ir informacinių sistemų saugumą, kad jie prie informacinės sistemos prisijungė pažeisdami apsaugos priemones, t. y. jas sugadindami ar pakenkdami apsaugos priemonių režimui, konstatuojama, kad jų veiksmuose nėra BK 198[1] straipsnio 1 dalyje numatyto nusikaltimo sudėties, todėl dėl kaltinimo pagal BK 198[1] straipsnio 1 dalį J. T., taip pat <...> V. D. išteisintini kaip nepadarę veikos, turinčios nusikaltimo ar baudžiamojo nusižengimų požymių (BPK 329 straipsnio 1 punktas)“. Toks neteisėto prisijungimo prie IS požymių aiškinimas yra probleminis, be kita ko, ir todėl, kad inkriminuojant šią veiką reikalaujama nustatyti siekį atlikti kitus veiksmus sistemoje, nors pati BK 198[1] straipsnio dispozicija to nenumato. Iš tiesų šis kaltininko siekis byloje galėtų būti vertinamas sprendžiant, pavyzdžiui, padarytos veikos mažareikšmiškumo, bausmės skyrimo klausimus, bet ne konstatuojant nusikalstamos veikos sudėties požymių buvimą. Taip pat svarbu paminėti, kad neteisėtu prisijungimu prie internetinės bankininkystės yra pažeidžiamas vienas iš IS saugumo elementų – IS konfidencialumas, turėjęs užtikrinti, kad teikianti šias paslaugas sistema bus prieinama tik prieigos teisę turintiems vartotojams.

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (14), 2016, p. 250-266

IŠVADOS

1. Neteisėto prisijungimo prie IS, kaip ir kitų elektroninių duomenų bei informacinių sistemų saugumą pažeidžiančių veikų, kriminalizavimas yra pagrįstas tarptautiniais ir Europos Sąjungos teisės aktais. 2015 m. įgyvendinant Direktyvos 2013/40/ES nuostatas, BK 198[1] straipsnyje patikslintas dalyko požymis, sugriežtinta baudžiamoji atsakomybė, tačiau pati neteisėtos prieigos koncepcija nepakito. Atsakomybei pagal BK 198[1] straipsnį, kaip ir anksčiau, yra pakankami vien tik kaltininko neteisėti prisijungimo prie IS veiksmai (pažeidus IS apsaugos priemones), nepriklausomai nuo to, ar po prieigos gavimo sistemoje buvo padarytos kitos nusikalstamos veikos.
2. Elektroninio sukčiavimo, privataus gyvenimo neliečiamumo pažeidimų ir kitose elektroninių nusikalstamų veikų baudžiamosiose bylose neteisėto prisijungimo prie IS veika turėtų būti laikoma atskira, t. y. ji inkriminuotina kartu su kitomis, pavyzdžiui, BK 215, 182, 166, 168 straipsniuose numatytomis ir kaltininko sistemoje padarytomis nusikalstamomis veikomis. Sprendžiant šių padarytų veikų sutapties klausimą, neatmestinos teismų praktikos išplėstos idealiosios sutapties taikymo galimybės.
3. Neteisėtas elektroninės mokėjimo priemonės ar jos duomenų panaudojimas inicijuojant ar atliekant finansinę operaciją neapima neteisėto prisijungimo prie IS veikos – BK 198[1] ir 215 straipsniuose numatytų normų santykis paprastai neturėtų būti vertinamas pagal normos visumos ir normos dalies konkurencijos įveikimo taisykles.
4. IS apsaugos priemonių pažeidimas konstatuotinas ne tik tada, kai apsaugos priemonėms padaroma žala, bet ir nustačius, kad buvo pažeisti jų nustatyti apribojimai nesukeliant žalos pačioms apsaugos priemonėms.

LITERATŪROS SĄRAŠAS

I. Teisės aktai

1. Lietuvos Respublikos Konstitucija. Valstybės žinios, 1992, Nr. 33-1014.
2. Lietuvos Respublikos baudžiamasis kodeksas. Valstybės žinios, 2000, Nr. 89-2741.
3. Lietuvos Respublikos visuomenės informavimo įstatymas. Valstybės žinios, 1996, Nr. 71-1706.
4. Konvencija dėl elektroninių nusikaltimų. Valstybės žinios, 2004, Nr. 36-1188.
5. 2005 m. vasario 24 d. Tarybos pagrindų sprendimas 2005/222/TVR dėl atakų prieš informacines sistemas. OL L 69, 2005, p. 67.

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (14), 2016, p. 250-266

6. 2013 m. rugpjūčio 12 d. Europos Parlamento ir Tarybos direktyva 2013/40/ES dėl atakų prieš informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR. OL L 218, 2013, p. 8.

II. Specialioji literatūra

1. ABRAMAVIČIUS, Armanas, *et al*. Lietuvos baudžiamojo kodekso komentaras. Specialioji dalis (99−212 straipsniai). Vilnius: Registrų centras, 2009.
2. A Dictionary of Computing. 5-asis leidimas. Atsak. redaktorius John Daintith. Oxford: Oxford University Press, 2004.
3. BARBATSIS, Gretchen, *et al*. The Performance of Cyberspace: An Exploration Into Computer-Mediated Reality. Journal of Computer-Mediated Communication, Vol. 5 (1), 1999. Prieiga per internetą: <http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.1999.tb00332.x/full>.
4. CLOUGH, Jonathan. Principles of Cybercrime. Cambridge: Cambridge University Press, 2010.
5. CLOUGH, Jonathan. Data Theft? Cybercrime and the Increasing Criminalization of Access to Data. Criminal Law Forum, No. 22, 2011.
6. Convention on Cybercrime Explanatory Report. Prieiga per internetą: <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>.
7. DAGIENĖ, Valentina, *et al*. Enciklopedinis kompiuterijos žodynas. Vilnius: TEV, 2008.
8. Dictionary of information science and technology. I tomas. Atsak. redaktorius KHOSROW-POUR, Medhi. HERSHEY, Pa, *et al*.: Idea Group Reference, 2007.
9. GIRDENIS, Tomas. Nusikalstamų veikų daugetas Lietuvos baudžiamojoje teisėje. Socialiniai mokslai: teisė (01 S). Vilnius: Mykolo Romerio universitetas, 2010.
10. MARCINAUSKAITĖ, Renata. Nusikalstamomis veikomis elektroninėje erdvėje pažeidžiamos pagrindinės baudžiamojo įstatymo saugomos vertybės nustatymo problema. Socialinių mokslų studijos, Nr. 3(3), 2011.
11. MARCINAUSKAITĖ, Renata. Technologinio neutralumo principo taikymo problemos aiškinant nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui sudėties požymius. Socialinių mokslų studijos, Nr. 5(1), 2013.
12. MCCLURE, Stuart, *et al*. Apsauga nuo hakerių: tinklo saugumo palaikymo paslaptys ir sprendimai. Kaunas: Smaltijos leidykla, 2006.
13. MILINIS, Albertas, *et al*. Lietuvos baudžiamoji teisė. Specialioji dalis. Pirmoji knyga. Vilnius: Justitia, 2013.
14. ŠTITILIS, Darius; LAURINAITIS, Marius. Tapatybės vagystė elektroninėje erdvėje. Informacijos mokslai, Nr. 50, 2009.
15. VENČKAUSKAS, Algimantas; TOLDINAS, Jevgenijus. Kompiuterių ir operacinių sistemų sauga. Kaunas: Vitae Litera, 2008.
16. PIESLIAKAS, Vytautas. Lietuvos baudžiamoji teisė. Antroji knyga. Vilnius: Justitia, 2008.
17. WALDEN, Ian. Computer Crimes and Digital Investigations. Oxford: Oxford University Press, 2007.

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (14), 2016, p. 250-266

III. Teismų praktika

1. Lietuvos Respublikos Konstitucinio Teismo 2002 m. spalio 23 d. nutarimas. Valstybės žinios, 2002, Nr. 104-4675.
2. Lietuvos Respublikos Konstitucinio Teismo 2003 m. kovo 24 d. nutarimas. Valstybės žinios, 2003, Nr. 29-1196.
3. Lietuvos Aukščiausiojo Teismo 2012 m. birželio 26 d. nutartis baudžiamojoje byloje Nr. 2K-375/2012.
4. Lietuvos Aukščiausiojo Teismo 2015 m. sausio 6 d. nutartis baudžiamojoje byloje Nr. 2K-138-976/2015.
5. Lietuvos Aukščiausiojo Teismo 2015 m. gruodžio 8 d. nutartis baudžiamojoje byloje Nr. 2K-555-788/2015.
6. Kauno apygardos teismo 2015 m. balandžio 16 d. nutartis baudžiamojoje byloje Nr. 1A-301-478/2015.
7. Kauno apygardos teismo 2015 m. gegužės 7 d. nutartis baudžiamojoje byloje Nr. 1A-432-594/2015.
8. Kauno apygardos teismo 2015 m. liepos 31 d. nuosprendis baudžiamojoje byloje Nr. 1A-644-634/2015.
9. Kauno miesto apylinkės teismo 2015 m. kovo 19 d. nuosprendis baudžiamojoje byloje Nr. 1-754-738/2015.
10. Klaipėdos apygardos teismo 2015 m. balandžio 15 d. nuosprendis baudžiamojoje byloje Nr. 1A-19-557/2015.
11. Klaipėdos miesto apylinkės teismo 2015 m. birželio 11 d. nuosprendis baudžiamojoje byloje Nr. 1-430-606/2015.
12. Panevėžio miesto apylinkės teismo 2015 m. spalio 1 d. teismo baudžiamasis įsakymas byloje Nr. 1-637-334/2015.
13. Panevėžio apygardos teismo 2015 m. sausio 29 d. nuosprendis baudžiamojoje byloje Nr. 1A-23-366-2015.
14. Šiaulių apygardos teismo 2015 m. liepos 2 d. nutartis baudžiamojoje byloje Nr. 1A-299-309/2015.
15. Trakų rajono apylinkės teismo 2015 m. balandžio 17 d. teismo baudžiamasis įsakymas byloje Nr. 1-164-424/2015.
16. Vilniaus apygardos teismo 2014 m. gegužės 12 d. nuosprendis baudžiamojoje byloje Nr. 1A-294-195/2014.

SUMMARY

The development of information technologies and electronic networks created preconditions for different types of large-scale dissemination of information, new accesses to information, and information exchange at the national and international levels. Information technologies have in

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (14), 2016, p. 250-266

one way or the other pervaded almost every aspect of human activities. These developments have given rise to an unprecedented changes, but they also determined the emergence of new types of crime as well as the commission of traditional crimes by means of information technologies. The paper analyses one of the offences against the security of information systems (IS) – unlawful access to IS, which is criminalized in Lithuanian CC Article 1981, and presents various aspects of its interpretation and qualification. This analysis is based on international and European Union legal documents, also Lithuanian case-law practice. It is important that the last changes of the CC Article 1981 were determined by the Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. The author also agrees, that a criminal prohibition of unauthorized access is able to give additional protection to the system and the data at an early stage, but it is important to avoid over-criminalization of such offence.

The author draws attention, that the breach of confidentiality of IS was criminalized a decade ago in Lithuania, but real incrimination problems of such offence emerged recently. Considering quite different qualification practice, unlawful access to IS problem solving options are suggested in the paper. For example, it is offered to qualify the perpetrator's actions of unlawfully connecting to e-banking or e-mail as an independent criminal act, provided in CC Article 1981. It is concluded that violation of security measures should be interpreted, inter alia, as a violation of determined restrictions (requirements), when damage for these security measures was not caused. The analysis also revealed that the separation of criminal offence against confidentiality of IS from similar criminal offences against the financial system and crimes against inviolability of a person's private life is problematic.

Keywords: criminal law, unlawful access, information system, criminalization