Jurisprudencija, 2003, t. 47(39); 59–69

KAI KURIE NETEISĖTOS PRIEIGOS PRIE KOMPIUTERINĖS INFORMACIJOS KRIMINALIZAVIMO ASPEKTAI

Dr. Darius Štitilis

Lietuvos teisės universiteto Valstybinio valdymo fakulteto Teisinės informatikos katedra
Ateities g. 20, 2057 Vilnius
Telefonas 271 45 71
Elektroninis paštas stitilis@ltu.lt

Pateikta 2003 m. rugpjūčio 27 d.
Parengta spausdinti 2003 m. gruodžio 15 d.

Recenzavo Lietuvos teisės universiteto Teisės fakulteto Kriminalistikos katedros lektorius dr. ***Rolandas Krikščiūnas*** *ir šio Universiteto Policijos fakulteto Policijos teisės katedros lektorius dr.* ***Raimundas Kalesnykas***

Pagrindinės sąvokos: kompiuteriniai nusikaltimai, neteisėta prieiga prie kompiuterinės informacijos, neteisėtos prieigos kriminalizavimas

Keywords: computer crimes, illegal access to computer data, criminalisation of illegal access to computer data

Santrauka

Šio straipsnio objektas – neteisėta prieiga prie kompiuterinės informacijos, dalykas – kai kurie tokios veikos kriminalizavimo aspektai. Straipsnio tikslas – išanalizuoti kai kurias pagrindines neteisėtos prieigos prie kompiuterinės informacijos kriminalizavimo problemas ir numatyti baudžiamosios atsakomybės už tokią veiką tobulinimo būdus Lietuvoje. Straipsnio uždaviniai: apibūdinti pagrindinius neteisėtos prieigos prie kompiuterinės informacijos požymius; atskleisti kai kurias pagrindines problemas, susijusias su tokios prieigos vertinimu; pateikti neteisėtos prieigos prie kompiuterinės informacijos kriminalizavimo Lietuvoje galimus variantus.

Straipsnyje taikomos lyginamosios analizės, lyginamasis bei kiti metodai, remiamasi užsienio valstybių doktrina bei periodine literatūra. Straipsnį sudaro įvadas, keturi skyriai bei išvados. *Pirmajame* skyriuje apibūdinama neteisėta prieiga prie kompiuterinės informacijos, atskleidžiamos teisinės problemos, susijusios su šios veikos vertinimu. *Antrajame* skyriuje nagrinėjamos tarptautinių (regioninių) dokumentų nuostatos, susijusios su neteisėta prieiga prie kompiuterinės informacijos. *Trečiajame* skyriuje analizuojama tokios prieigos kriminalizavimo praktika užsienyje. *Ketvirtajame* skyriuje aptariamos naujojo Lietuvos Respublikos baudžiamojo kodekso nuostatos dėl neteisėtos prieigos prie kompiuterinės informacijos, taip pat galimybė už tokią veiką nustatyti administracinę atsakomybę. Straipsnio pabaigoje pateikiamos išvados.

Įvadas

Kuriant žinių visuomenę, visose žmogaus veiklos srityse sparčiai plinta šiuolaikinės informacinės technologijos, kurios elektroninę erdvę padaro prieinamą. Nepaisant teigiamų elektroninės erdvės aspektų, neišvengiamai susiduriama ir su didėjančiu pavojingų veikų naudojantis šia erdve skaičiumi [1, p. 5]. Elektroninė erdvė suteikia naujų galimybių padaryti nusikaltimus [2], sudaro sąlygas naujiems nusikaltimų būdams atsirasti [3, p. 64] bei galimybes padaryti naujas, iki šiol teisinėje praktikoje [4] nežinomas veikas. Viena iš tokių veikų – neteisėta prieiga prie kompiuterinės informacijos.

I. Neteisėta prieiga prie kompiuterinės informacijos

Siekiant išsiaiškinti kai kuriuos neteisėtos prieigos prie kompiuterinės informacijos kriminalizavimo aspektus pirmiausia reikia aptarti pačią neteisėtą prieigą prie kompiuterinės informacijos. Neteisėtą prieigą prie kompiuterinės informacijos iš kitų kompiuterinių nusikaltimų informatikai[1] išskiria bei tokios prieigos kai kurias kriminalizavimo problemas nagrinėja U. Sieberis, C. Gringras, N. Nathansonas, D. Baibridge'as ir kt. D. Baibridge'as teigia, kad neteisėta prieiga yra prieiga prie kompiuterių sistemos be savininko leidimo [5, p. 307]. Tačiau tokia samprata yra labai nekonkreti, neatskleidžiami prieigos požymiai. U. Sieberis nurodo, kad neteisėta prieiga suprantama kaip prasiskverbimas į kompiuterių sistemas, kai tikslas yra ne manipuliacija, sabotažas ar šnipinėjimais, o pasitenkinimas, susijęs su kompiuterinės sistemos apsaugos priemonių įveikimu. Šiuo atveju autorius prieigą išskiria kaip neteisėtą veiksmą, kai nekyla jokios pasekmės (išskyrus grėsmę padaryti žalą). Toliau nagrinėdamas kai kuriuos neteisėtos prieigos prie kompiuterinės informacijos aspektus U. Sieberis vis dėlto pažymi, jog neteisėta prieiga gali būti dvejopa:

1) prasiskverbiant į kompiuterių sistemą, kai jokia žala nepadaroma, tik sukeliamas pavojus (tačiau tokiais atvejais pažeidžiamos kompiuterių sistemos, kompiuterinės informacijos slaptumas arba su tuo susijęs integralumas), ir
2) prasiskverbiant į kompiuterių sistemą, kai padaroma žala (pvz., gauti duomenys panaudojami įvykdyti sukčiavimui, pasisavinama kompiuterinė informacija ar pan.) [6, p. 41].

Specialioje literatūroje mokslininko V. V. Krylovo neteisėta prieiga prie kompiuterinės informacijos taip pat suprantama kaip neteisėtas susipažinimas su informacija (duomenimis), esančia kompiuteryje [7, p. 40]. Šiai sampratai iš esmės pritaria ir V. S. Komisarovas ir nurodo trūkumą – terminas „susipažinimas“ su informacija neapima tokių neteisėtos prieigos atvejų, kai asmuo, jau žinodamas informacijos turinį iš kitų šaltinių, šią informaciją tik kopijuoja arba trina [8, p. 14]. Dėl to autorius pažymi, kad neteisėta prieiga prie kompiuterinės informacijos reikėtų laikyti veiksmus, kurių metu asmuo neteisėtai gauna galimybę susipažinti su kompiuterine informacija arba tokio asmens tam tikri veiksmai, atliekami su tokia informacija neturint savininko leidimo [8, p. 14]. Taip pat nurodoma, jog neteisėtos prieigos prie kompiuterinės informacijos būdai gali skirtis: svetimo vardo ir/ar slaptažodžio panaudojimas, kompiuterinės sistemos apsaugos priemonių pažeidimas ir t. t.

Pažymėtina, jog Elektroninės erdvės nusikaltimų konvencijos (ang. – *Cybercrime convention*)[2] (toliau – Konvencija) aiškinamajame rašte nurodoma, jog neteisėta prieiga apima veikas, kai kompiuterinės informacijos saugumui sukeliama žalos grėsmė, taip pat veikas, pažeidžiančias kompiuterinės informacijos saugumą (t. y. prieinamumą, konfidencialumą ar vientisumą) [9, p. 44]. Šiuo atveju išskiriama neteisėta prieiga, nesukelianti žalingų pasekmių (kyla tik žalos grėsmė), ir prieiga, dėl kurios kyla žalingos pasekmės (pvz., neteisėtai pakeičiama kompiuterinė informacija).

Taigi nepaisant skirtingų apibūdinimų galima išskirti dvi neteisėtos prieigos prie kompiuterinės informacijos rūšis:

[1] Terminai „nusikaltimai informatikai“ bei „kompiuteriniai nusikaltimai“ šiame straipsnyje suprantami kaip sinonimai, nors dėl šių sąvokų apimties mokslininkai diskutuoja.

[2] Konvencija rengiant šį straipsnį dar nebuvo įsigaliojusi.

1) prieigą, kai žala nepadaroma, o kyla tokios žalos grėsmė, bei

2) prieigą, kai padaroma reali žala.

Vis dėlto autorius, nagrinėdamas neteisėtos prieigos prie kompiuterinės informacijos kriminalizavimo aspektus, laikysis pozicijos, jog neteisėta prieiga prie kompiuterinės informacijos laikytina tokia neteisėta veika, kurios metu įveikiant apsaugos priemones prieinama prie kompiuterinės informacijos ir pažeidžiamas laikomos informacijos slaptumas. Prie tokios nuomonės prieita ir kai kuriuose tyrimuose kompiuterinių nusikaltimų tema, pavyzdžiui, Honkongo darbo grupės ataskaitoje dėl kompiuterinių nusikaltimų [10, p. 35] (t. y. kyla realios žalos grėsmė), o dėl neteisėtos prieigos metu vykdomas šnipinėjimas, sabotažas, sukčiavimas, neteisėtas autorių teisėmis apsaugotų kūrinių kopijavimas, kompiuterinės informacijos pakeitimas ir pan., autoriaus nuomone, laikytini savarankiškomis pavojingomis veikomis.

II. Tarptautinių (regioninių) dokumentų nuostatos dėl neteisėtos prieigos prie kompiuterinės informacijos kriminalizavimo

1983–1985 m. Ekonominio bendradarbiavimo ir plėtros organizacijos (EBPO) valstybėms narėms buvo pateiktas minimalus kriminalizuotinų pavojingų veikų, susijusių su kompiuteriais, sąrašas. Prie tokių veikų buvo priskirta ir neteisėta prieiga, t. y. patekimas į kompiuterį arba kompiuterio ir/ar telekomunikacijos sistemos perėmimas be asmens, atsakingo už šią sistemą, leidimo pažeidžiant apsaugos priemones arba dėl kitų nesąžiningų ar žalingų paskatų [11, p. 25]. Kaip matome, prieigos aprašymas nereikalauja materialių pasekmių, t. y. pati veika apibrėžiama tik kaip įsilaužimas į kompiuterinę sistemą. Tačiau reikalaujama nustatyti objektyviosios pusės požymį – saugumo priemonių pažeidimą.

Užbaigus Ekonominio bendradarbiavimo ir plėtros organizacijos (EBPO) ataskaitą, 1989 m. Europos Tarybos Ministrų kabinetas taip pat priėmė rekomendaciją R89(9) Europos Sąjungos šalių vyriausybėms, kurioje siūloma iš naujo svarstant ar kuriant įstatymus atsižvelgti į Europos komiteto nusikaltimų problemoms tirti pranešimą apie kompiuterinius nusikaltimus [12]. Šiame pranešime pateiktame minimaliame sąraše minima ir neteisėta prieiga prie kompiuterinės sistemos: prieiga prie kompiuterinės sistemos arba kompiuterinio tinklo neturint tam teisės bei pažeidžiant saugumo priemones. Galima teigti, kad nusikalstamų pasekmių atžvilgiu šios neteisėtos prieigos požymių aprašymas yra panašus į anksčiau minėtą neteisėtos prieigos aprašymą.

Neteisėta prieiga prie kompiuterinės informacijos aptariama ir Konvencijoje[1]. Konvencijos 2 straipsnyje numatyta, jog „turi būti priimtos įstatymų normos, pagal kurias būtų nustatyti baudžiamosios atsakomybės pagrindai už tyčinę prieigą prie kompiuterinės sistemos, neturint tam teisės“ [13; 2 str.]. Šia nuostata siekiama, kad būtų nustatyta baudžiamoji atsakomybė už veikas, keliančias pavojų kompiuterinių sistemų ir duomenų saugumui (t. y. konfidencialumui, integruotumui ir prieinamumui). Tame pačiame Konvencijos straipsnyje nurodoma, jog nustatant baudžiamosios atsakomybės pagrindus gali būti reikalaujama, jog nusikaltimas būtų padaromas pažeidžiant saugumo priemones siekiant gauti kompiuterinę informaciją arba turint nesąžiningą tikslą, arba kai veika yra susijusi su kompiuterine sistema, kuri sujungta su kita kompiuterine sistema. Anksčiau minėta formuluotė valstybėms narėms palieka tam tikrą veikimo laisvę nustatant baudžiamosios atsakomybės pagrindus už neteisėtą prieigą. Galima konstatuoti, jog Konvencijoje laikomasi nuostatos, kad tyčinė prieiga prie kompiuterinės sistemos neturint tam teisės (kai nekyla žalingos pasekmės) turi būti įvardijama kaip neteisėta veika [14, p. 3]. Paminėtina, jog Konvencijos aiškinamajame rašte nurodoma, jog teisinės apsaugos reikalingumą lemia asmenų interesai valdyti bei kontroliuoti jų informacines sistemas. Neteisėta prieiga (kai nekyla žalingos pasekmės) turėtų būti iš principo neteisėta, nes sudaro galimybę pakeisti, sunaikinti vertingą kitiems asmenims priklausančią kompiuterinę informaciją arba vykdyti kitas neteisėtas veikas [9, p. 44].

[1] Artimiausiu metu Lietuva rengiasi šią Konvenciją ratifikuoti.

2002 m. balandžio 19 d. Europos Komisijos siūlyme Tarybai dėl sprendimo, susijusio su veiksmais prieš informacines sistemas, buvo konstatuota, jog atakos prieš informacines sistemas kelia grėsmę saugiai informacinei visuomenei, saugumui ir justicijai, todėl reikia imtis tam tikrų priemonių Europos Sąjungos lygiu [15]. Pasiūlymo 3 straipsnyje nurodoma, jog valstybės narės turi užtikrinti, kad tyčinė prieiga prie visos arba dalies informacinės sistemos neturint tokios teisės turi būti laikoma nusikalstama, jei veika padaryta:

1) per bet kokią informacinės sistemos dalį, kuri yra saugoma specialiomis saugumo priemonėmis, ar
2) siekiant padaryti žalą fiziniam ar juridiniam asmeniui ar
3) siekiant gauti ekonominę naudą [16; 3 str.].

Šiomis nuostatomis norima nustatyti atsakomybės pagrindus už neteisėtą prieigą prie informacinių sistemų (ang. – *hacking*). Tačiau šalys narės, įgyvendindamos šias nuostatas savo nacionaliniuose įstatymuose, gali nenustatyti baudžiamosios atsakomybės už nereikšmingus pažeidimus [15, 3 str.].

Apibendrinant tarptautinių (regioninių) dokumentų nuostatas galima teigti, jog nepaisant to, kad šiuose dokumentuose siūloma kriminalizuoti neteisėtą prieigą (kai kyla žalingos pasekmės), pavojinga veika laikoma ir neteisėta prieiga prie kompiuterinės informacijos, kai kyla tiktai žalos grėsmė (bet ne žalingos pasekmės). Tačiau neteisėtos prieigos požymiai skiriasi (pvz., objektyviosios pusės požymiai ir kt.). Pažymėtina, jog tarptautiniai (regioniniai) dokumentai nenustato specialių reikalavimų dalykui, t. y. kompiuterinei informacijai – rekomenduojama apsaugoti bet kokią informaciją elektronine forma.

III. Neteisėtos prieigos prie kompiuterinės informacijos kriminalizavimas užsienyje

Yra kelios nuomonės apie baudžiamosios atsakomybės pagrindų nustatymą už neteisėtą prieigą prie kompiuterinės sistemos. Teisės komisijos baudžiamosios teisės srityje (angl. – *The Law Commission on Criminal Law*) buvo pabrėžta, jog nustatant atsakomybės pagrindus už neteisėtą prieigą pirmiausia siekiama apsaugoti ne informaciją, o kompiuterinių sistemų vientisumą bei saugumą. Todėl siūlyta kriminalizuoti dvi atskiras veikas: pirma, nustatyti atsakomybę už paprastą neteisėtą prieigą prie kompiuterinės sistemos, ir, antra, nustatyti atsakomybę (sankcija turi būti sunkesnė) už neteisėtą prieigą siekiant įvykdyti ar palengvinti kito sunkaus nusikaltimo padarymą [17, p. 346]. Panašios pozicijos buvo laikomasi 1994 m. Kriminalinės policijos tarptautinėje apžvalgoje kompiuterinių nusikaltimų srityje. Šioje apžvalgoje pabrėžta ne tik specialios kompiuterinės informacijos (pvz., komercinių paslapčių) apsaugos nuo neteisėtos prieigos būtinybė, tačiau ir būtinybė saugoti bet kokią kompiuterinę informaciją [18, p. 19]. Taigi pabrėžiama, jog neteisėtos prieigos atveju neturi būti reikalaujama prieiti prie įstatymų saugomos informacijos kitaip nei kompiuterinės informacijos pasisavinimo atveju [18, p. 22]. Už neteisėtos prieigos kriminalizavimą yra ir M. Mohrenschlageris. Jo teigimu, argumentai už baudžiamosios atsakomybės pagrindų nustatymą vis dėlto vyrauja [14, p. 3]. Tarptautinėje kriminalinės policijos apžvalgoje dėl kompiuterinių nusikaltimų taip pat nurodoma, jog neteisėta prieiga turi būti įvardyta nusikaltimu, nes sudaro galimybę sunaikinti kompiuterinius duomenis, sutrikdyti kompiuterinės sistemos darbą [18, p. 74]. Šiek tiek kitos nuomonės yra P. J. Schickis ir G. Schmolzeris. Pasak jų, už neteisėtą prieigą, kai nekyla žala (sukeliama tiktai grėsmė teisiniams gėriams), nustatytina ne baudžiamoji, o administracinė atsakomybė [19, p. 137].

Kai kurių autorių (U. Sieberio ir kitų) buvo konstatuota tokia padėtis, susijusi su įstatymų nuostatomis dėl neteisėtos prieigos. Kai kuriose valstybėse (Anglijoje, Australijoje, Graikijoje, daugumoje JAV valstijų ir kt.) kriminalizuojama vien tiktai neteisėta prieiga prie kompiuterinių sistemų. Tokiomis normomis siekta apsaugoti formalią slaptumo, privatumo sritį [6, p. 70]. Kitose valstybėse veika yra baudžiama tik tada, kai prie kompiuterinių sistemų prieinama pažeidžiant saugumo priemones (Vokietijoje, Nyderlanduose, Norvegijoje) arba turint tikslą pagrobti, modifikuoti ar sunaikinti kompiuterinę informaciją (Kanadoje, Prancūzijoje, Izraelyje, Naujojoje Zelandijoje, Škotijoje ir kt.) arba kai kyla tokie žalingi padariniai

(Ispanijoje ir kt.) [6, p. 71]. Kai kurios valstybės (Suomija, Nyderlandai, Jungtinė Karalystė ir kt.) yra sujungusios šiuos du požiūrius į vieną straipsnį ir nustačiusios atsakomybę už „paprastą“ neteisėtą prieigą. Prieigą siekiant padaryti kitą pažeidimą (arba tam tikrų pasekmių kilimą) jos traktuoja kaip kvalifikuojantį požymį [18, p. 19; 6, p. 71]. Kai kuriose valstybėse veika, kai įsilaužiama į kompiuterinę sistemą, bet žala nepadaroma, kol kas nelaikoma nusikalstama. Tačiau reikia pažymėti, jog vis dėlto dauguma valstybių ėmėsi saugoti formalią privatumo, slaptumo sritį nuo neteisėtos prieigos, nes tradiciniai įstatymai tokios apsaugos garantuoti negalėjo. Tai pažymima ir Tarptautinėje kriminalinės policijos apžvalgoje dėl kompiuterinių nusikaltimų [18].

Keleto valstybių baudžiamieji įstatymai nagrinėtini išsamiau. Štai Rusijos Federacijos baudžiamojo kodekso (toliau – Rusijos BK) 272 straipsnyje nustatyta atsakomybė už tyčinę neteisėtą prieigą prie įstatymo saugomos kompiuterinės informacijos, jei tai sukėlė kompiuterinės informacijos sunaikinimą, blokavimą, modifikavimą ar kopijavimą, taip pat sutrikdė kompiuterinės sistemos darbą [20; 272 str.]. Iš šių nuostatų susidaro įspūdis, jog Rusija bent jau kol kas pasirinko neteisėtos prieigos kriminalizavimo būdą, kai nusikalstama veika įvardijama tik tokia veika, dėl kurios kyla nustatytos pasekmės (žala). Tokią poziciją patvirtina ir Rusijos mokslininkas V. S. Komisarovas. Jo teigimu, dėl neteisėtos prieigos turi kilti žalingos pasekmės [8, p. 14]. Tuo tarpu neteisėta prieiga prie kompiuterinės informacijos, kai nekyla jokių pasekmių, dažnai nelaikoma nusikalstama veika. Kitokios nuomonės yra D. V. Čepčugovas. Anot šio rusų autoriaus, Rusijos BK 272 straipsnis apima visus neteisėtos prieigos atvejus [21]. Tam, kad kiltų baudžiamoji atsakomybė dėl neteisėtos prieigos, turi kilti įstatymo nustatytos pasekmės, t. y. informacija turi būti sunaikinta, blokuota, modifikuota arba nukopijuota. D. Čepčugovo nuomone, kai kompiuterinėje sistemoje esantys duomenys pasirodo pažeidėjo kompiuterio ekrane, įvyksta informacijos perkėlimas. Kadangi elektroniniai impulsai per ryšių linijas atsiranda pažeidėjo kompiuteryje ir apdorojami šio kompiuterio procesoriaus bei „išvedami“ į ekraną, tokie veiksmai gali būti laikomi informacijos kopijavimu ir patenka į Rusijos BK 272 straipsnio veikimo sritį [21]. Taigi neteisėtos prieigos metu kopijuojant informaciją įsikišti į šios informacijos apdorojimo procesą nebūtina, nes tokiu atveju kiltų kita šiame straipsnyje nurodyta pasekmė – informacijos modifikavimas. Tačiau kai kurie kiti Rusijos autoriai nesutinka su nuomone, jog visi neteisėtos prieigos atvejai Rusijos BK yra kriminalizuoti. Šių autorių nuomone, turint omenyje, kad 272 straipsnio (bei 274 str.) dispozicija reikalauja tam tikrų pasekmių (žalos teisiniams gėriams), kai kurios pavojingos veikos, susijusios su neteisėta prieiga prie kompiuterinės informacijos, lieka nekriminalizuotos [22].

Kaip kitokios neteisėtos prieigos kriminalizavimo apimties pavyzdį galima pateikti Latviją – jos Baudžiamojo kodekso 241 straipsnyje nustatyta atsakomybė už savavališką prieigą prie kompiuterinių sistemų. Šio straipsnio 1 dalyje nurodyta, jog baudžiamojon atsakomybėn traukiamas asmuo, kuris savavališkai prieina prie kompiuterinės sistemos, jei dėl tokių veiksmų atsiranda galimybė pasiekti informaciją, esančią šioje kompiuterinėje sistemoje [23; 241 str.]. Straipsnio 2 dalyje nustatyta atsakomybė už tą pačią veiką, jei atliekant neteisėtą prieigą pažeidžiamos kompiuterio programinę įrangą apsaugančios sistemos arba prieinama prie ryšių linijų.

Kroatijos baudžiamojo kodekso 223 straipsnyje nurodyta, jog nusikaltimas yra neteisėta prieiga prie kompiuterinės informacijos arba kompiuterių programų pažeidžiant apsaugos priemones [24; 223 str.]. Taigi šia norma siekiama apsaugoti kompiuterinę informaciją bei kompiuterių programas. Baudžiamajai atsakomybei kilti užtenka vien neteisėtos prieigos, tačiau kompiuterinė informacija arba kompiuterių programos turi būti apsaugotos specialiomis apsaugos priemonėmis [25; 1 d. 4 p.].

Panaši neteisėtos prieigos kriminalizavimo praktika yra ir kai kuriose bendrosios teisės tradicijos valstybėse. Pavyzdžiui, Didžiojoje Britanijoje, remiantis 1990 m. Piktnaudžiavimo naudojantis kompiuteriais įstatymo 1 skyriumi „Neteisėta prieiga prie duomenų kompiuterine forma“, asmuo pripažįstamas kaltu, jei jis:

1) atlieka veiksmus siekdamas prieiti prie bet kokios kompiuterinės programos arba kompiuterinių duomenų, esančių kitame kompiuteryje;
2) jei prieiga, kuriai rengiamasi, yra neteisėta;

3) asmuo supranta, jog jis atlieka veiksmus stengdamasis vykdyti neteisėtą prieigą.

Pažymėtina, jog šios normos taikymas veikoms elektroninėje erdvėje gali pasireikšti tuo, jog net nesėkmingas įsilaužėlio (ang. – *hacker*) bandymas neteisėtai įsilaužti į kompiuterinę sistemą gali būti įvertintas kaip nusikaltimas [5, p. 315]. Pasak M. Wasiko, remiantis straipsnio dispozicija, panašu, jog tam, kad kiltų baudžiamoji atsakomybė, nereikia įveikti jokių kompiuterinės sistemos apsaugos priemonių – jų gali ir nebūti [26, p. 275]. Tuo šio įstatymo nuostatos skiriasi nuo kai kurių kitų valstybių baudžiamųjų įstatymų nuostatų, kuriose reikalaujama, kad būtų pažeistos saugumo priemonės. Jungtinės Karalystės teisės komisija yra konstatavusi, jog neteisėtos prieigos kriminalizavimas tik apsaugotos informacijos atžvilgiu būtų prilygintas absurdiškai situacijai, pavyzdžiui, jei neužrakinto automobilio vagystė nebūtų pripažįstama nusikaltimu [26, p. 277]. Tačiau ši nuostata yra ir kritikuojama teigiant, jog neteisėta prieiga kriminalizuota netikslingai, nes neteisėtas įsibrovimas į namus nėra nusikaltimas, o prieigą elektroniniu būdu galima prilyginti tokiems veiksmams [27, p. 629]. Nepaisant to, autoriaus nuomone, nagrinėjamu atveju baudžiamosios teisės normomis yra apsaugomas privatumas, kompiuterinės sistemos integralumas, todėl tokios normos įtvirtinimas baudžiamuosiuose įstatymuose yra tikslingas.

Autoriaus nuomone, nagrinėjant neteisėtos prieigos prie kompiuterinės informacijos kriminalizavimo klausimą svarbus ir dar vienas aspektas – neteisėtos prieigos dalykas, jo apimtis. Pavyzdžiui, kai kuriose užsienio valstybėse (Rusijoje ir kt.) neteisėtos prieigos dalykas yra ne visa informacija, o tik įstatymo saugoma informacija (pvz., konfidenciali informacija, informacija, sudaranti valstybės paslaptį ir pan.). Tačiau nemažai valstybių savo baudžiamuosiuose įstatymuose nuo neteisėtos prieigos saugo bet kokią informaciją, kuri gali būti elektroninės formos.

Apibendrinant tai, kas šioje dalyje išdėstyta, galima daryti išvadą, jog užsienio valstybėse neteisėta prieiga prie kompiuterinės informacijos kriminalizuojama skirtingai: skiriasi nusikaltimo sudėčių rūšys (materiali, formali), dalyko ypatumai (pvz., specialūs reikalavimai dalykui), taip pat kai kurie objektyviosios pusės požymiai (pvz., reikalavimas pažeisti saugumo priemones). Nepaisant to, pastebėtinos neteisėtos prieigos prie kompiuterinės informacijos (kai nepadaroma žala) kriminalizavimo tendencijos.

IV. Kai kurie neteisėtos prieigos prie kompiuterinės informacijos kriminalizavimo aspektai Lietuvoje

Baudžiamoji atsakomybė už neteisėtą prieigą prie kompiuterinės informacijos (su tam tikromis realiomis pasekmėmis (žala)) gali kilti pagal kelis Lietuvos Respublikos baudžiamojo kodekso (toliau – BK) straipsnius. Nustatydamas baudžiamąją atsakomybę už neteisėtą prieigą, Lietuvos įstatymo leidėjas pasirinko tokį veikos elektroninėje erdvėje kriminalizavimo būdą – reikalaujama realios žalos [28, p. 83], t. y. kompiuterinės informacijos sunaikinimo, pakeitimo ar sugadinimo (BK 196 str.), kompiuterinės programos sunaikinimo, pakeitimo ar sugadinimo (BK 197 str.) arba kompiuterinės informacijos pasisavinimo (BK 198 str.). Tačiau už neteisėtą prieigą, kai reali žala nepadaroma, baudžiamoji atsakomybė BK nėra nustatyta. Ar tokia veika iš tikrųjų nėra pavojinga? Pažymėtina, jog kėsinantis į įstatymo saugomus teisinius gėrius gali būti ne tik daroma reali žala, bet ir kilti tos žalos grėsmė. Tais atvejais, kai reali žala neatsiranda, o yra tiktai tokios žalos grėsmė, objekte irgi vyksta tam tikri pakeitimai [29, p. 177]. Pavojingumo pobūdį paprastai apibūdina kėsinimosi objekto vertingumas [30, p. 15].

Nusikaltimo objekto, į kurį kėsinamasi atliekant neteisėtą prieigą, – visuomeninių santykių saugant, apdorojant kompiuterinę informaciją vertingumą yra pabrėžę U. Sieberis, D. Baibridge'as ir kt. Šio objekto apsaugos baudžiamosiomis normomis praktika (kai reali žala nepadaroma) yra nustatyta ne vienoje valstybėje[1]. Be to, jau minėta, kad kriminalizuoti neteisėtą prieigą, kai nepadaroma reali žala, rekomenduojama ir tarptautiniuose (regioniniuose)

[1] Tačiau reikia pažymėti, jog už šią veiką numatomos sankcijos paprastai yra lengvesnės nei už kitus nusikaltimus elektroninėje erdvėje (aut. pastaba).

dokumentuose. Vis dėlto į kokius teisinius gėrius kėsinamasi vykdant neteisėtą prieigą prie kompiuterinės informacijos (kai nekyla reali žala)?

Autoriaus manymu, neteisėta prieiga pažeidžiant saugumo priemones sukelia realią grėsmę visuomeniniams santykiams saugant ir apdorojant informaciją, pažeidžia nukentėjusiųjų slaptumo sritį. Kompiuterinė informacija yra labiau pažeidžiama, jos kopijavimo, susipažinimo mastai, kitaip nei informacija materialiuose objektuose, yra neribojami, todėl ši informacija turi būti labiau saugoma teisinėmis normomis. Autoriaus nuomone, Lietuvos įstatymo leidėjui reikėtų imtis priemonių apsaugoti šiuos visuomeninius santykius baudžiamosios teisės normomis. Ši veika galėtų būti įvardijama baudžiamuoju nusižengimu turint omenyje mažesnį jos pavojingumą, palyginti su veikomis, kai padaroma žala. Numatant baudžiamąją atsakomybę už neteisėtą prieigą, kai kyla grėsmė saugomiems teisiniams santykiams, baudžiamąją normą autorius siūlytų formuluoti taip: „*Tas, kas pažeisdamas saugumo priemones neteisėtai įsilaužė į kompiuterinę sistemą, padarė baudžiamąjį nusižengimą ir* <…>“.

Neatmestina ir neteisėtos prieigos prie kompiuterinės informacijos įvardijimo administraciniu teisės pažeidimu galimybė. Užkertant kelią teisės pažeidimams plačiai taikomos visų teisinės atsakomybės rūšių priemonės. Čia labai svarbus administracinės atsakomybės vaidmuo [31, p. 7]. Deja, tenka konstatuoti, jog šiuo klausimu užsienio teisinės literatūros beveik nėra. Tokią padėtį lemia ir tai, jog administracinių teisės pažeidimų kodeksų, kaip atskirai egzistuojančių teisės aktų, nustatančių teisinę atsakomybę už administracinės teisės pažeidimus, daugelyje užsienio valstybių iš viso nėra. Kai kuriose iš tokių valstybių nusižengimai inkorporuoti į šių valstybių baudžiamuosius įstatymus. Antai Vokietijos baudžiamajame kodekse visos nurodytos veikos skirstomos į nusikaltimus ir nusižengimus [30, p. 30]. Anglijoje, Skandinavijoje ir JAV nusikaltimais laikomi visi teisės pažeidimai, taigi ir, mūsų supratimu, administraciniai teisės pažeidimai [32, t. 1, p. 40–41].

Tiesa, šalių, kuriose atskirai galioja administracinių teisės pažeidimų kodeksai, yra. Pavyzdžiui, Latvijoje, Rusijoje ir kt. Šių valstybių teisės literatūroje bei praktikoje daug dėmesio skiriama baudžiamajai atsakomybei už nusikaltimus, susijusius su kompiuteriais, nustatyti, tačiau administracinės atsakomybės nustatymo už mažesnio pavojingumo pažeidimus problemos kol kas nesprendžiamos, nors kai kurie mokslininkai jau siūlo tam tikras veikas įvardyti administraciniais teisės pažeidimais.

Pažymėtina, jog administracinė atsakomybė, kaip alternatyva baudžiamosioms sankcijoms, buvo iškelta Kriminalinės policijos tarptautinėje apžvalgoje, susijusioje su kompiuteriniais nusikaltimais, kur nurodyta, jog kompiuterinė informacija turi būti apsaugota ir administracinės teisės priemonėmis, tačiau pažymėta, jog nuomonės dėl apsaugos skirtingų teisės šakų normomis laipsnio skiriasi iš esmės [18, p. 29]. Tokiai nuomonei pritarė ir U. Sieberis. Jis nurodė, jog pavojingos veikos turi būti ne tik kriminalizuotos – galima nustatyti ir administracinės atsakomybės pagrindus [6, p. 204]. Konvencijoje taip pat yra nuostatos – tokios kaip „*turi būti nustatyta baudžiamoji atsakomybė arba imtasi kitų teisinių priemonių atsakomybei nustatyti“*, iš kurių galima daryti išvadą, jog valstybėms narėms paliekama teisė ne tik nustatyti baudžiamąją atsakomybę už nusikaltimus, susijusius su kompiuteriais, tačiau tam tikras veikas elektroninėje erdvėje įvardyti administracinės teisės pažeidimais.

Atskirose užsienio valstybėse šiuo metu beveik neskiriama dėmesio administracinei atsakomybei nustatyti už neteisėtą prieigą prie kompiuterinės informacijos. Tačiau kaip išimtis paminėtina Latvija. Atsižvelgiant į Konvencijos nuostatas šioje šalyje imamasi aktyvių veiksmų keisti ne tik Baudžiamąjį kodeksą – parengti ir atitinkami Latvijos administracinių teisės pažeidimų kodekso pakeitimai [33; 34]. Apie galimybę administraciniais pažeidimais įvardyti tokias pavojingas veikas kaip neteisėtą prieigą užsimena ir Rusijos autoriai *(V. O.* Černišova [35] bei kt.).

Autoriaus nuomone, atsižvelgiant į Lietuvoje egzistuojančią teisinę sistemą, Konvencijos nuostatas, paliekančias tam tikrą laisvę valstybėms pačioms spręsti atsakomybės už neteisėtą prieigą nustatymo klausimus, nagrinėtina administracinės atsakomybės nustatymo galimybė. Administracinės atsakomybės nustatymas galėtų „subalansuoti“ atsakomybės taikymą už neteisėtą prieigą prie kompiuterinės informacijos (ypač nagrinėjamu atveju, kai

įstatymo leidėjas tokios prieigos nepripažįsta tiek pavojingos, jog ji turėtų užtraukti baudžiamąją atsakomybę) bei įgyvendintų Konvencijos nuostatas, susijusias su teisinės atsakomybės nustatymu už neteisėtą prieigą. Be to, administracinė atsakomybė taikoma daug operatyviau ir paprasčiau negu baudžiamoji atsakomybė [31, p. 29], todėl kai kuriais atvejais administracinės atsakomybės taikymas padėtų greičiau, efektyviau įvertinti neteisėtą prieigą. Tokios atsakomybės taikymas vietoje baudžiamosios atsakomybės valstybei kainuotų ir mažiau lėšų.

Gali kilti klausimas, kas ir kokiais pagrindais remdamasis sprendžia, kokie teisei priešingi ir visuomenei pavojingi veiksmai turi būti laikomi administraciniais teisės pažeidimais. P. Petkevičius nurodo, jog šį klausimą sprendžia įstatymo leidėjas, atsižvelgdamas į atitinkamas vietos, laiko, politines, socialines, ekonomines sąlygas ir kitas konkrečias aplinkybes. Vis dėlto egzistuoja tam tikri požymiai, kuriais remiantis galima tam tikras veikas priskirti prie nusikaltimų arba administracinių teisės pažeidimų (padariniai, žala; pažeidimo mastas; kaltės forma ir žalos dydis; pakartotinumas; pažeidimo padarymo būdas, įrankiai ir priemonės bei kiti požymiai, kuriuos įvertina įstatymų leidėjas [31, p. 70]. Autoriaus šiame darbe išdėstyti samprotavimai paremti užsienio autorių diskusijomis dėl veikų, rodančių tam tikrų veikų mažesnį pavojingumą, kriminalizavimo bei vidiniu įsitikinimu, pagrįstu išvardytų požymių buvimu.

Taigi, autoriaus nuomone, už mažiau pavojingą veiką – įsilaužimą į kompiuterių sistemą, kai informacija nepasisavinama, taip pat nėra kitų būtinų kvalifikuojančių požymių, tačiau pažeidžiamos saugumo priemonės, įstatymo leidėjo pasirinktinai gali būti nustatyta ir administracinė atsakomybė (kaip baudžiamosios atsakomybės alternatyva). Toks administracinės atsakomybės pagrindo nustatymas padėtų „išbalansuoti“ atsakomybę už neteisėtą prieigą prie kompiuterinės sistemos. Kaip baudžiamosios atsakomybės alternatyvą autorius siūlo šią administracinio teisės pažeidimo sudėtį: „*Neteisėta prieiga prie kompiuterinės informacijos pažeidžiant saugumo priemones, užtraukia* <…>“.

Svarbūs ir kiti neteisėtos prieigos prie kompiuterinės informacijos kriminalizavimo aspektai (pvz., saugomos informacijos apimtis), tačiau dėl darbo apimties reikalavimų smulkiau šie klausimai nebus nagrinėjami.

Išvados ir pasiūlymai

1. Neteisėta prieiga prie kompiuterinės informacijos laikytina neteisėta veika, kurios metu įveikiant apsaugos priemones prieinama prie kompiuterinės informacijos ir pažeidžiamas laikomos informacijos slaptumas bei privatumas.

2. Tarptautiniuose (regioniniuose) dokumentuose neteisėtą prieigą prie kompiuterinės informacijos (kai nekyla žalingos pasekmės) rekomenduojama laikyti pavojinga veika, nes sukeliamas pavojus laikomos kompiuterinės informacijos slaptumui bei konfidencialumui. Tačiau neteisėtos prieigos požymiai skiriasi (pvz., objektyviosios pusės požymiai ir kt.), išskyrus dalykui, t. y. saugomai informacijai, keliamus reikalavimus.

3. Nepaisant to, kad dalies užsienio valstybių baudžiamuosiuose įstatymuose neteisėta prieiga prie kompiuterinės informacijos (kai nepadaroma reali žala) iš viso nėra įvardijama nusikaltimu (nusižengimu), pastebėtinos neteisėtos prieigos prie kompiuterinės informacijos (kai nepadaroma žala) kriminalizavimo tendencijos.

4. Užsienio valstybėse neteisėta prieiga prie kompiuterinės informacijos kriminalizuojama skirtingai: skiriasi nusikaltimo sudėčių rūšys (materiali, formali), dalyko ypatumai (pvz., specialūs reikalavimai dalykui), taip pat kai kurie objektyviosios pusės požymiai (pvz., reikalavimas pažeisti saugumo priemones).

5. Nusikalstama veika tikslinga įvardyti neteisėtą prieigą (kai nepadaroma žala), Lietuvos Respublikos baudžiamąjį kodeksą papildant tokia nusikaltimo sudėtimi: „*Tas, kas pažeisdamas saugumo priemones neteisėtai įsilaužė į kompiuterinę sistemą, padarė baudžiamąjį nusižengimą ir* <…>“.

6. Kaip baudžiamosios atsakomybės alternatyvą autorius siūlo pildyti Lietuvos Respublikos administracinių teisės pažeidimų kodeksą – nustatyti administracinės atsakomybės

pagrindus už neteisėtą prieigą, pažeidimo sudėtį formuluojant taip: „*Neteisėta prieiga prie kompiuterinės informacijos, pažeidžiant saugumo priemones, užtraukia <…>*“.

♦♦♦

LITERATŪRA

1. **Petrauskas R., Štitilis D.** Kompiuteriniai nusikaltimai ir jų prevencija. – Vilnius: Lietuvos teisės akademijos Leidybos centras, 2000.
2. **Grabosky P.** Computer Crime: A Criminological Overview. Australian Institute of Criminology // http://www.aic.gov.au/conferences/other/compcrime/index.html (paskutinį kartą prieita: 2002 m. spalio 8 d.).
3. **Klingys V., Morkūnaitė L., Vaitiekūnas V.** Nusikaltimų, susijusių su interneto panaudojimu, kompiuteriniai tyrimai // Jurisprudencija. 1999. T. 14(6).
4. **Bylenchuk P. D.** Organized transnational computer crime: the global problem of the new millenium // http://www.crime–research.org/eng/library/Bileng.htm (paskutinį kartą prieita: 2002 m. liepos 4 d.).
5. **Baibridge D.** Introduction to Computer Law / Fourth edition. – Pearson Education Limited, 2000.
6. **Sieber U.** Legal Aspects of Computer–Related Crime in the Information Society. Comcrime study, prepared for European Commission // 1998. http://europa.eu.int/ISPO/legal/en/comcrime/sieber.html (paskutinį kartą prieita: 2002 m. kovo 11 d.).
7. **Крылов В. В.** Информационные компьютерные преступления. – Москва, 1997.
8. **Комисаров В. С.** Преступления в сфере компьютерной информации: понятие и ответстенность // Юридический мир. 1998, февраль.
9. **Explanatory** Memorandum of Cyber–Crime Convention // http://conventions.coe.int (paskutinį kartą prieita: 2003 m. kovo 11 d.).
10. **Inter–departmental** Working Group on Computer Related Crime Report // Hong Kong, September, 2000. http://www.info.gov.hk/itbb/english/it/doc/iiac6–2000.doc (paskutinį kartą prieita: 2003 m. kovo 19 d.).
11. **Sabaliauskas G.** Informacijos saugumas internete: teisininkų ir informatikų problema // Justitia. 2001. Nr. 2.
12. **Council** of Europe. Computer–related crime. Recomendation No. R(89)9, adopted by Committee of Ministers of the Council of Europe on 13 September 1989 // Strasbourg, 1990. http://cm.coe.int/ta/rec/1989/89r9.htm (paskutinį kartą prieita: 2003 m. kovo 9 d.).
13. **Convention** on Cybercrime // Strasbourg, 19.09.2001. http://conventions.coe.int (paskutinį kartą prieita: 2003 m. kovo 1 d.).
14. **Mohrenschlager M.** Criminal Offences and Other Substantive Criminal Law Provisions in the Convention // Conference on Cybercrime. Budapest, 22 November 2001. http://www.legal.coe.int (paskutinį kartą prieita: 2003 m. balandžio 28 d.).
15. **Explanatory** Memorandum of Proposal of a Council Framework Decision on attacks agains information systems // Brussels, 19.04.2002. COM(202) 173 final. 202/0086 (CNS). http://europa.eu.int (paskutinį kartą prieita: 2003 m. balandžio 29 d.).
16. **Proposal** of a Council Framework Decision on attacks agains information systems // Brussels, 202/0086 (CNS). http://europa.eu.int (paskutinį kartą prieita: 2002 m. balandžio 29 d.
17. **Rowland D., Macdonald E.** Information Technology Law. – Cavendish Publishing Limited, 1997.
18. **United Nations** Manual on Computer–Related Crime. International Review of Criminal Policy Nos. 43/44 // http://www.uncjin.org/Documents/EighthCongress.html (paskutinį kartą prieita: 2003 m. kovo 3 d.).
19. **Schick P. J., Schmolzer G.** Computer Crimes and other Crimes against Information Technology in Austria. International Review of Penal Law: Computer Crimes and Other Crimes Against Information Technology. – Wurzburg, Germany, 1992.
20. **Уголовный** кодекс Российской Федерации // http://www.d–sign.com/uk/uk.htm (paskutinį kartą prieita: 2003 m. kovo 12 d.).
21. **Čerpčugov D.** MVD Onlain // InterNet magazine, 2001. No. 14. http://www.gagin.ru/internet/14/3.htm (paskutinį kartą prieita: 2003 m. kovo 5 d.).
22. **Отечественное** законодательство в борьбе с компьютерными преступлениями // http://www.russianlaw.net/law/doc/a01.htm (paskutinį kartą prieita: 2003 m. kovo 7 d.).

23. **Criminal** Code of Latvia // 1961. http://www.nais.dati.lv/ (paskutinį kartą prieita: 2003 m. kovo 11 d.).
24. **Criminal** Code of Croatia // http://www.law.cornell.edu/world/europe.html#croatia (paskutinį kartą prieita: 2003 m. birželio 20 d.).
25. **Croatia**: National Report // Conference on Cybercrime. Budapest, 22 November 2001. http://www.legal.coe.int (paskutinį kartą prieita: 2003 m. balandžio 28 d.).
26. **Akdeniz Y., Walker C., Wall D.** The Internet, Law and Society. – Pearson Education Limited, 2000.
27. **Wasik M.** Computer Crimes and other Crimes against Information Technology in United Kingdom // International Review of Penal Law: Computer Crimes and Other Crimes against Information Technology. – Wurzburg, Germany, 1992.
28. **Petrauskas R., Štitilis D.** Lietuvos Respublikos baudžiamasis kodeksas Nusikaltimų elektroninėje erdvėje konvencijos kontekste // Jurisprudencija. 2002. T. 24(16).
29. **Abramavičius A., Čepas A. ir kt.** Baudžiamoji teisė: bendroji dalis. – Vilnius: Eugrimas, 1998.
30. **Piesliakas V.** Mokymas apie nusikaltimą ir nusikaltimo sudėtį. – Vilnius: Lietuvos policijos akademija, 1996.
31. **Petkevičius P.** Administracinė atsakomybė. – Vilnius: Justitia, 1996.
32. **Piesliakas V.** Ekonominiai nusikaltimai Europos valstybių bei JAV teisėje // Lietuvos policijos akademijos mokslo darbai. 1993.
33. **Kinis U.** Threats on e–business // The Third International Conference „Infobalt“. http://www.infobalt.lt/common/pranesimai/D_Kinis.ppt (paskutinį kartą prieita: 2003 m. vasario 21 d.).
34. **The Following** Countries Are in the Process of developing laws to Prosecute Cyber Crime // http://www.mcconnellinternational.com (paskutinį kartą prieita: 2003 m. vasario 21 d.).
35. **Чернишова В. О.** Интернет и преступность. // Computer Crime Research Center. http://www.crime–research.org/library/Chernish1.htm (paskutinį kartą prieita: 2003 m. kovo 4 d.).

♦ ♦ ♦

Criminalization of Illegal Access to Computer Information

Dr. Darius Štitilis

Law University of Lithuania

SUMMARY

The main purpose of the article – to analyze legal problems related to the criminalisation of illegal access to computer information. The developments of cyberspace have given rise to an unprecedent economic and social changes, but they also have other side: the emergence of new forms of crimes. The present work deals with some legal regulation problems of illegal access to computer information, as one of the forms of computer crimes.

The importance of private, economic and political information, stored in or transmitted by computers, then required the extension of such a „formal sphere of secrecy“ at least to certain computer–stored data. The legal protection of specific computer–stored data can also be regarded as a new analogy in the information society to age–old notions of breaking, entering and trespassing. However, in most countries, a protection of this „formal sphere of secrecy“ against illegal access to computer–stored data and computer communication could not be guaranteed by traditional criminal provisions.

In the first part of the present work legal problems, related to the conception of illegal access to computer information are briefly discussed, also the foreign experience are studied.

In the second part the provisions of international (regional) documents related to illegal access to computer information are studied. A corresponding criminal offence would be desirable in accordance with existing international recommendations.

In the third part the foreign experience are studied. In response to the new cases of „hacking“, many states developed new statutes protecting a „formal sphere of secrecy“ for computer data by

criminalising the illegal access to or use of a third person's computer or computer data. The new laws which have been enacted or proposed demonstrate various approaches, which range from provisions criminalising „mere" access to computer systems, to those punishing access only in cases where the accessed data are protected by security measures, where the perpetrator has harmful intentions, where information is obtained, modified or damaged or where a minimum damage is caused. On the other hand, however, there are still some countries that do not have special criminal law provisions against hacking (i.e. the mere penetration into foreign computer systems).

In the fourth part the provisions of Criminal code of the Republic of Lithuania related to illegal access to computer information are studied.

At the end of the article the conclusions are presented.