ISSN 1392-6195 (print)
ISSN 2029-2058 (online)
JURISPRUDENCIJA
JURISPRUDENCE
2019, 26(2), p. 352–369.

NETEISĖTO DISPONAVIMO ĮRENGINIAIS, PROGRAMINE ĮRANGA, SLAPTAŽODŽIAIS, PRISIJUNGIMO KODAIS IR KITOKIAIS DUOMENIMIS (BAUDŽIAMOJO KODEKSO 198[2] STRAIPSNIS) KVALIFIKAVIMO PROBLEMOS

Renata Marcinauskaitė

Mykolo Romerio universiteto Mykolo Romerio teisės mokyklos
Baudžiamosios teisės ir proceso institutas
Elektroninis paštas: renata.marcinauskaite@gmail.com

Pateikta 2019 m. rugsėjo 9 d., parengta spaudai 2019 m. rugsėjo 23 d.

DOI: 10.13165/JUR-19-26-2-06

Dabar įsibrauti į informacines sistemas nebereikia įgūdžių. Tiesiog atlikite „įsibrovimo priemonių“ paiešką internete <...>. Įveskite kompiuterio, į kurį norite įsibrauti, IP adresą, ir šios priemonės padarys likusį darbą.[1]

Santrauka. *Straipsnyje analizuojami kai kurie neteisėto disponavimo įrenginiais, programine įranga, slaptažodžiais, kodais ir kitokiais duomenimis kriminalizavimo aspektai, aptariamos šios nusikalstamos veikos inkriminavimo problemos. Taip pat nemažas dėmesys skiriamas šios kategorijos baudžiamosiose bylose besiformuojančiai teismų praktikai, joje pateiktiems išaiškinimams. Į šią Lietuvos Respublikos baudžiamojo kodekso 198[2] straipsnyje įtvirtintą nusikalstamą veiką tyrime stengtasi pažvelgti*

1 Robert Schifreen, „Bulletin Interview“, *The Computer Bulletin* 44, 5 (2002): 16.

kiek plačiau, todėl, taikant ekvivalentaus vertinimo principą, ieškota jos atitikmenų fizinėje erdvėje, kriminalizavimo pateisinimo. Straipsnyje telkiamasi į minėtos veikos dalyko apibrėžties problemas, kurių sprendimas yra aktualus aiškinantis Baudžiamojo kodekso 198[2] straipsnio taikymo ribas. Ne mažiau sudėtingas yra ir straipsnyje nagrinėjamas disponavimo dvejopo naudojimo priemonėmis (įrenginiais ar programine įranga) kriminalizavimo klausimas. Atsakant į jį, formuluojami kriterijai, kurie leistų pagrįsti baudžiamosios atsakomybės taikymą tais atvejais, kai baudžiamojoje byloje yra konstatuojamas disponavimas kaip tik tokio pobūdžio priemonėmis.

***Reikšminiai žodžiai**: įrenginiai, programinė įranga, kenkimo programinė įranga, įsibrovimo priemonės, dvejopo naudojimo priemonės, rengimosi stadija.*

Įvadas

Neteisėtas disponavimas įrenginiais, programine įranga, slaptažodžiais, kodais ir kitokiais duomenimis kriminalizuotas Lietuvos Respublikos baudžiamojo kodekso (toliau – BK) 198[2] straipsnyje. Šio straipsnio nuostatos BK įtvirtintos ir pamažu keistos atsižvelgiant į 2004 m. Konvencijos dėl elektroninių nusikaltimų (toliau – 2004 m. Konvencija) 6 straipsnį bei Europos Parlamento ir Tarybos 2013 m. rugpjūčio 12 d. direktyvos 2013/40/ES dėl atakų prieš informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR (toliau – Direktyva 2013/40/ES), 7 straipsnį. Kaip tik pastarojoje direktyvoje, be kita ko, atkreiptas dėmesys į kibernetinių išpuolių atlikimo būdų kitimą, spartų techninės ir programinės įrangos tobulėjimą, pakartotinių didelės apimties išpuolių prieš informacines sistemas didėjimą (ypač kuriant ir naudojant robotizuotų kompiuterių tinklą (angl. *botnet*). Tokios nusikalstamų veikų elektroninėje erdvėje (toliau – e. veikos, kompiuterinės nusikalstamos veikos) tendencijos, šių nusikalstamų veikų padarymo galimybės yra tiesiogiai susijusios, be kita ko, su priemonių, palengvinančių e. veikų padarymą, tobulėjimu, prieigos prie jų galimybėmis. Tinkamo teisinio reguliavimo sukūrimas, reaguojant į atsiradusias grėsmes elektroninėje erdvėje, yra vienas svarbesnių žingsnių užtikrinant šios erdvės saugumą.

Tyrime į neteisėtą disponavimą BK 198[2] straipsnyje nurodytomis priemonėmis – įrenginiais, programine įranga, slaptažodžiais, kodais ir kitokiais duomenimis (toliau – e. veikų priemonės) – siekta pažvelgti iš baudžiamosios teisės pozicijų pirmiausia įvertinant minėtame BK straipsnyje įtvirtinto nusikalstamos veikos dalyko baudžiamąsias teisines problemas. Šių problemų išsprendimas aktualus nustatant galimas neteisėto disponavimo e. veikų priemonėmis nusikalstamos veikos ribas, atitinkamai ir BK 198[2] straipsnio taikymo galimybes. Autorė siekė išspręsti ir mokslinėje literatūroje negausiai nagrinėtą dvejopo naudojimo priemonių (angl. *dual-use*) problemą, analizuojant ją straipsnyje pasiūlomi ir tokių priemonių baudžiamojo teisinio vertinimo kriterijai.

Mokslinės literatūros analizė parodė, kad nusikalstamos veikos, susijusios su neteisėtu disponavimu e. veikų priemonėmis, baudžiamosios teisės prasme nėra plačiai nagrinėtos. Kai kuriuos tokių priemonių juodosios rinkos atsiradimo ir vystymosi aspektus aptarė L. Ablon, lyginamąją Vokietijos ir Kinijos teisinio reguliavimo, susijusio su e. veikų priemonėmis, analizę atliko T. A. Zhang. Dvejopo naudojimo priemonių kai kuriais probleminiais klausimais pasisakė Ch. Walker-Osborn ir S. Fafinski. Etiškam įsibrovimui keliamus reikalavimus apibrėžė A. Česnys, J. Juknius, I. Ronald ir Jr. Raether.

Siekiant tinkamai atskleisti iki šiol mažai nagrinėtą disponavimo e. veikų priemonėmis problematiką, tyrime sistemiškai naudojami dokumentų analizės, loginis, lyginamasis ir apibendrinimo metodai.

1. Apibrėžiant BK 198² straipsnio taikymo ribas

1.1. Nusikalstamos veikos dalyko probleminiai aspektai aiškinant iki 2007 m. galiojusią BK 198² straipsnio redakciją

BK 198² straipsnyje baudžiamoji atsakomybė bendriausia prasme yra nustatytina už e. veikų priemonių gaminimą, gabenimą, importavimą, pardavimą, prieigos prie jų suteikimą ar kitokį platinimą, įgijimą ar laikymą, jei jomis disponuota nusikalstamais tikslais ar kitaip neteisėtai. Šios priemonės – tai: 1) įrenginiai ar programinė įranga, tiesiogiai skirta ar pritaikyta nusikalstamoms veikoms daryti, ir 2) slaptažodžiai, kodai ar kitokie panašūs duomenys, skirti prisijungti prie informacinės sistemos ar jos dalies. Svarbu ir tai, kad, siekiant išvengti pernelyg išplėsto baudžiamosios atsakomybės taikymo, minėtame BK straipsnyje įtvirtinti ir kiti būtini įrodyti – tyčinės kaltės, nusikalstamų tikslų ar kitokio neteisėtumo – požymiai.[2]

Atsižvelgiant į reikšmingą šių dalykų vaidmenį tolimesnių nusikalstamų veikų padarymui, disponavimas jais gali būti priskirtas vienai iš kompiuterinių nusikalstamų veikų – techninės įrangos ir informacijos (duomenų ar programų) kaip nusikalstamos veikos priemonės – kategorijų.[3] Šis supratimas, be kita ko, yra svarbus tuo, kad leidžia į technologijas pažvelgti kaip į nusikalstamos veikos padarymo priemones (įrankius), o ne tik kaip į taikinį ar tikslą.

Iki 2007 m. disponavimas įrenginiais, programine įranga ar prieigos prie informacinės sistemos duomenimis BK 198² straipsnyje buvo laikomas nusikalstamu, jei priemonės buvo skirtos ar pritaikytos konkrečiai šiame BK straipsnyje nurodytoms ir tame pat BK XXX skyriuje esančioms nusikalstamoms veikoms daryti, taip pat asmens susižinojimo neliečiamumo pažeidimui (BK 166 straipsnis). Tuomet su-

2 Šie požymiai BK 198² straipsnyje įtvirtinti atsižvelgiant į 2004 m. Konvencijos 6 straipsnio 1 ir 2 dalis, taip pat Direktyvos 2013/40/ES 7 straipsnį.

3 Eoghan Casey, *Digital evidence and computer crime* (Amsterdam; Boston (Mass.): Elsevier: Academic Press, 2011), 17–18.

kurta nusikalstamos veikos apibrėžtis galėjo būti pateisinama, be kita ko, dėl to, kad atitiko 2004 m. Konvencijos 6 straipsnio nuostatas. Įdomu, kad požiūris, susiaurinantis nusikalstamos veikos dalyko formuluotę iki jo sąsajos su konkrečiomis kompiuterinėmis nusikalstamomis veikomis, yra suderinamas ir su Direktyvos 2013/40/ES 7 straipsniu.[4] Nors, viena vertus, konkrečioms BK 198^2 straipsnyje nurodytoms veikoms padaryti dažnai yra būtinas neteisėtą poveikį elektroniniams duomenims ar informacinėms sistemoms darančių arba prieigą suteikiančių (angl. *hacker tools*) priemonių turėjimas, kita vertus, panaudoto dalyko formuluotė galėjo kelti klausimų, ar įrenginiai (įskaitant programinę įrangą) galėjo būti pasitelkiami kitoms nei BK XXX skyriuje numatytoms nusikalstamoms veikoms padaryti. Tuo labiau, kad į BK 198^2 straipsnyje minimų nusikalstamų veikų sąrašą jau buvo įtraukta kitame – BK XXIV skyriuje esanti ir pirmiausia asmens privataus gyvenimo neliečiamumą pažeidžianti nusikalstama veika (BK 166 str.).

Šį probleminį aspektą anuomet galima buvo netiesiogiai įžvelgti ir teismų praktikoje. Pavyzdžiui, vienoje iš šios kategorijos baudžiamųjų bylų V. B., be kitų nusikalstamų veikų, buvo nuteistas ir pagal BK 198^2 straipsnį dėl to, kad *„per asmenį, nesulaukusį amžiaus, nuo kurio šis atsakytų pagal baudžiamuosius įstatymus, neteisėtai pagamino kompiuterinę programą, skirtą fiksuoti ir kaupti AB (duomenys neskelbtini) klientų elektroninės bankininkystės kodus ir slaptažodžius ir <...> šią kompiuterinę programą neteisėtai laikė anksčiau nurodytais internetiniais adresais, be to, minėtą kompiuterinę programą <...> neteisėtai laikė nešiojamo kompiuterio <...> standžiajame diske; taip pat <...> neteisėtai įgijo prisijungimo prie tarnybinių stočių (duomenys neskelbtini) kodus bei slaptažodžius ir <...> šiuos kodus bei slaptažodžius neteisėtai laikė savo nešiojamo kompiuterio <...> standžiajame diske, turint tikslą daryti nusikalstamas veikas, numatytas Lietuvos Respublikos baudžiamojo kodekso 198^1 straipsnio l dalyje. Šiais veiksmais V. B. padarė nusikaltimą, numatytą Lietuvos Respublikos baudžiamojo kodekso 198^2 straipsnio l dalyje“*[5].

Šioje baudžiamojoje byloje nustatytas nusikalstamos veikos padarymo mechanizmas buvo susijęs su elektroninės bankininkystės vartotojų duomenų neteisėtu gavimu prisidengiant realiai egzistuojančios finansinės institucijos (banko) vardu. Kompiuterinė programa, minima teismo sprendime, bendriausia prasme yra netikras banko internetinis puslapis, kuriame neteisėtai fiksuojami ir kaupiami banko klientų elektroninės bankininkystės kodai ir slaptažodžiai. Tokio pobūdžio tinklalapis yra „sukurtas taip, kad vizualiai niekuo nesiskirtų nuo tikro elektroninės bankininkystės, internetinių mokėjimo paslaugų, elektroninės prekybos įmonės ar kt. instituci-

4 Direktyvos 2013/40/ES 7 straipsnyje nurodoma, kad kompiuterių programos turėtų būti skirtos arba pritaikytos pirmiausia siekiant vykdyti bet kurią iš šios Direktyvos 3–6 straipsniuose nurodytų veikų (neteisėta prieiga prie informacinių sistemų, neteisėtas įsikišimas į sistemą, neteisėtas įsikišimas į duomenis ir neteisėtas duomenų perėmimas).

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

jos tinklalapio“[6]. Ši kompiuterinė programa, atliekanti neteisėtas suvestų duomenų fiksavimo ir jų perdavimo kaltininkui funkcijas, nėra tiesiogiai skirta neteisėtai prisijungti prie informacinės sistemos (BK 198¹ str.), kaip, beje, ir bet kuriai kitai tuo metu BK 198² straipsnyje nurodytai veikai padaryti. Jos paskirtis – neteisėtai fiksuoti ir perduoti (įgyti) elektroninės mokėjimo priemonės naudotojo tapatybės patvirtinimo priemonių duomenis, pakankamus finansinei operacijai inicijuoti, todėl toks tinklalapis yra sukurtas ir skirtas pirmiausia nusikalstamoms veikoms, numatytoms BK 214 straipsnyje, daryti. Be abejo, vėliau tokie duomenys gali būti panaudojami gaunant neteisėtą prieigą prie elektroninės bankininkystės paskyros, tačiau tai nekeičia pačios kompiuterinės programos (suklastoto internetinio tinklalapio) paskirties. Atsižvelgiant į tai, kad BK 198² straipsnio redakcija iki 2007 m. pakeitimų nenumatė platesnės šios nusikalstamos veikos dalyko formuluotės, t. y. kad minėtos priemonės galėtų būti naudojamos kitoms nei BK XXX skyriuje numatytoms nusikalstamoms veikoms daryti (išskyrus BK 166 str.), tokios nusikalstamos veikos požymių aiškinimas, kaip matyti, kėlė nemažai problemų.

Šios problemos kontekste aktualu, kad e. veikos yra kriminalizuotos ne tik BK XXX skyriuje – iš tiesų elektroninėje erdvėje padarytų nusikalstamų veikų sudėčių galime rasti daugelyje kitų BK specialiosios dalies skyrių. Į kompiuterinių nusikalstamų veikų, suvokiamų plačiąja prasme, sąrašą patenka bet kuri tradicinė nusikalstama veika, jei ji gali būti padaryta ne tik fizinėje, bet ir elektroninėje erdvėje (pavyzdžiui, sukčiavimas, turto prievartavimas, disponavimas pornografinio turinio medžiaga). Atitinkamai tokių nusikalstamų veikų padarymą lengvinančių sąlygų sudarymui gali būti suieškomos BK 198² straipsnyje nurodytos priemonės ar įrankiai, skirti ar pritaikyti nusikalstamai veiklai, visiškai arba bent iš dalies susijusiai kaip tik su šia erdve, padaryti. Atsižvelgiant į gana platų minėtos veikos dalyko pritaikomumą, BK 198² straipsnio nuostatos pamažu buvo keičiamos, be kita ko, plečiant ir vėliau tikslinant minėtų požymių turinį. Po 2007 ir 2015 m. BK 198² straipsnio pakeitimų jame kriminalizuotas disponavimas įrenginiais ar programine įranga, tiesiogiai skirta ar pritaikyta *nusikalstamoms veikoms* daryti, taip pat disponavimas slaptažodžiais, kodais ar kitokiais panašiais duomenimis, skirtais prisijungti prie informacinės sistemos ar jos dalies. Taigi šiuo metu įstatymo leidėjo pasirinkta dalyko formuluotė leidžia kalbėti apie disponavimą anksčiau minėtomis priemonėmis, kurios gali būti skirtos tiek nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui (BK XXX skyriaus veikos), tiek ir bet kurios kitos su elektronine erdve susijusios nusikalstamos veikos padarymui palengvinti. Atsižvelgiant į tai teigtina, kad BK 198² straipsnyje kriminalizuotas nusikalstamos veikos padarymą lengvinančių sąlygų sudarymas (kai disponuojama priemonėmis, skirtomis ar pritaikytomis nusikalstamoms veikoms daryti) tam tikra prasme „peržengia“ BK XXX skyriaus ribas.

6 Vaidas Kalpokas ir Renata Marcinauskaitė, „Tapatybės vagystė elektroninėje erdvėje: technologiniai aspektai ir baudžiamasis teisinis vertinimas“, *Teisės problemos* 3, 77 (2012): 34.

1.2. Nusikalstamos veikos dalyko aspektai galiojant 2015 m. BK 198[2] straipsnio redakcijai

Informacinių technologijų panaudojimas „sukūrė įvairios rūšies galimybes ir, nenuostabu, kad kai kurios iš jų yra nusikalstamos prigimties“[7]. Baudžiamosios teisės srityje ši mintis gali būti plėtojama nurodant įvairius to pavyzdžius: kompiuteriniu nusikaltimu pripažintinas ne tik sukčiavimas elektroninėje erdvėje (pavyzdžiui, elektroninės bankininkystės srityje), elektroninių dokumentų klastojimas ar disponavimas pornografinio turinio dalykais, bet ir šioje erdvėje padaromas turto prievartavimas (pavyzdžiui, vertimas suteikti turtinę naudą grasinant panaudoti užkrėstų kompiuterių tinklą (*botnet*) ar net nusikalstamos veikos žmogaus seksualiniam neliečiamumui (pavyzdžiui, ryšių elektroninėje erdvėje mezgimas su vaikais seksualiniais tikslais[8]) ir daugelis kitų. Nusikalstamų veikų elektroninėje erdvėje visumos neapibrėžtumas, kaip minėta, kelia dvejonių sprendžiant, kokioms konkrečiai nusikalstamoms veikoms padaryti gali būti pasitelkiami BK 198[2] straipsnyje nurodyti įrenginiai ar programinė įranga, taigi ir kaip plačiai šis BK straipsnis taikytinas. Bendriausia prasme galima būtų teigti, kad nustačius, jog nusikalstama veika buvo padaryta elektroninėje erdvėje ir radus įrenginius ar programinę įrangą, skirtą tokiai veikai padaryti, spręstina, ar kaltininko veikoje nėra ir BK 198[2] straipsnyje numatytos nusikalstamos veikos sudėties požymių.

Nustačius, kad BK 198[2] straipsnio taikymas po 2007 ir 2015 m. pakeitimų tam tikra prasme „peržengia“ BK XXX skyriaus ribas, aktualu ir tinkamai atskleisti nusikalstamos veikos dalyko požymį. Todėl konkrečios nusikalstamo veikos, kuriai padaryti yra tiesiogiai skirti ar pritaikyti įrenginiai ar programinė įranga, konkretizavimas tokiu atveju tampa esminis. Analizuojant pavojingo disponavimo priemonėmis, lengvinančiomis nusikalstamos veikos padarymą, kriminalizavimo atvejus BK, galima matyti, kad toks nusikalstamos veikos dalykas straipsnio dispozicijoje paprastai yra susietas su veiksmais, kuriuos tiesiogiai leidžia padaryti minėta priemonė. Kaip antai BK 194 straipsnyje, be kita ko, kriminalizuotas disponavimas prietaisais, programine įranga, slaptažodžiais, kodais ar kitokiais panašiais duomenimis, kurie suteikia galimybę pašalinti technines apsaugos priemones. Kitame – BK 302[1] straipsnyje minimos priemonės yra tiesiogiai skirtos ar pritaikytos netikriems antspaudams, spaudams ir kt. klastoti. Įrenginių tiesioginė paskirtis ar pritaikymas sprogstamosioms medžiagoms, sprogmenims ir kt. gaminti nurodoma, pavyzdžiui, ir BK 257[1] straipsnyje. Šios nuostatos leidžia išskirti *tiesioginės paskirties* arba *tiesioginės funkcijos* kriterijų, svarbų formuluojant nusikalstamos veikos dalyką įvairių nusikalstamų veikų sudėtyse. Šio kriterijaus taikymas atskleidžiant BK 198[2] straipsnyje numatyto požy-

---

7 David I. Bainbridge, *Introduction to computer law* (Harlow: Pearson: Longman, 2004), 359.

8 Europos Parlamento ir Tarybos 2011 m. gruodžio 13 d. direktyvos 2011/92/ES dėl kovos su seksualine prievarta prieš vaikus, jų seksualiniu išnaudojimu ir vaikų pornografija, kuria pakeičiamas Tarybos pamatinis sprendimas 2004/68/TVR (OL 2011 L 335, p. 1), 6 straipsnis.

mio – įrenginių ar programinės įrangos, tiesiogiai skirtos ar pritaikytos nusikalstamoms veikoms daryti, – turinį, reikštų, kad pagal bylos aplinkybes konkretizuojant, kokiomis priemonėmis (įrankiais) buvo disponuota, nurodytinas ne visas nusikalstamas sumanymas ar kaltininko siekiamas galutinis rezultatas, o konkreti nusikalstama veika, kurią tiesiogiai leidžia padaryti minėtos priemonės. Pavyzdžiui, vienoje iš baudžiamųjų bylų J. P. buvo nuteistas pagal BK 198² straipsnį, nes pagamino ir perdavė programinę įrangą (netikrą elektroninės bankininkystės paslaugos puslapį), skirtą prisijungimų prie elektroninės bankininkystės paslaugos tarnybinės stoties kodams ir slaptažodžiams fiksuoti, o vėliau jiems persiųsti į konkrečias elektroninio pašto dėžutes:

„Kaltinamasis J. P. veikdamas kartu su M. J. kaip bendrininkų grupė <...> personaliniu kompiuteriu sukūrė netikrą AB bankas (duomenys neskelbtini) internetas bankininkystės paslaugos (duomenys neskelbtini) puslapį, skirtą fiksuoti šio banko klientų prisijungimų prie elektroninės bankininkystės paslaugos tarnybinės stoties kodus ir slaptažodžius, o vėliau – persiųsti juos internetu į M. J. sukurtas elektroninio pašto dėžutes: (duomenys neskelbtini), ir taip pagamino programinę įrangą, skirtą nusikaltimams daryti, o būtent vykdyti nusikalstamas veikas, numatytas LR BK 198¹ str., 214 str., 215 str. ir 182 str. Vėliau, tęsdamas savo nusikalstamą veiką <...> jis minėtą netikrą AB bankas (duomenys neskelbtini) interneto puslapį internetu persiuntė M. J. ir taip neteisėtai jam perdavė programinę įrangą, skirtą nusikaltimams daryti. Šiais veiksmais J. P. padarė nusikalstamą veiką, numatytą LR BK 198² str. 1 d.“[9]

Kaip minėta, tokio pobūdžio programinė įranga, sukurta ir pateikiama taip, kad klaidintų teisėtus elektroninės bankininkystės paslaugos vartotojus, pirmiausia yra skirta BK 214 straipsnyje numatytai nusikalstamai veikai daryti. Tokiu būdu gauti duomenys pagal savo paskirtį gali būti panaudojami neteisėtai prisijungiant prie informacinės sistemos (BK 198¹ str.), vėliau – finansinei operacijai inicijuoti (BK 215 str.), o kaltininkui suklaidinus banko informacinę sistemą, sudaromos galimybės apgaule įgyti svetimą turtinę teisę (turtą) (BK 182 str.). Nors, atsižvelgus į byloje nustatytų aplinkybių visumą, šios nusikalstamos veikos tarpusavyje galėtų sudaryti idealią nusikalstamų veikų sutaptį ir būtų laikomos neatskiriamomis (būtinomis) viso kaltininko sumanymo įgyvendinimo dalimis[10], toks vertinimas, žiūrint baudžiamosios teisės aspektu, neturėtų pakeisti ar itin praplėsti panaudotos programinės įrangos tiesioginės paskirties.

Kaip matyti, įgyvendinus 2004 m. Konvencijos ir Direktyvos 2013/40/ES nuostatas, neteisėto disponavimo įrenginiais, programine įranga, slaptažodžiais, kodais ir kitokiais duomenimis veika BK 198² straipsnyje yra kriminalizuota plačiau. Toks pasirinktas baudžiamosios atsakomybės nustatymo variantas, viena vertus, galėtų

9 Vilniaus miesto 1 apylinkės teismo 2009 m. rugsėjo 14 d. teismo baudžiamasis įsakymas byloje Nr. N1-1470-88/2009.

10 Tokio aiškinimo ištakas galima būtų sieti su Lietuvos Aukščiausiojo Teismo 2012 m. gegužės 8 d. nutartimi baudžiamojoje byloje Nr. 2K-P-78/2012.

būti pateisinamas, ypač atsižvelgus į nacionalinės teisės ypatumus nustatant baudžiamąją atsakomybę už nusikalstamas veikas, susijusias su elektronine erdve. Kaip antai duomenys, kurie yra būtini finansinei operacijai inicijuoti, nelaikytini slaptažodžiais, prisijungimo kodais ar kitais panašiais duomenimis BK 198[2] straipsnio prasme, todėl disponavimas jais kvalifikuojamas pagal BK 214 straipsnį (jis nepatenka į BK XXX skyrių). Be to, pačios Direktyvos 2013/40/ES nuostatos kelia klausimų, pavyzdžiui, kaip vertinti kompiuterinių programų įgijimą, jei jos gali būti panaudojamos kompiuterio slaptažodžiams, prisijungimo kodams ar panašiems duomenims, skirtiems prisijungti prie informacinės sistemos, gauti? Pagal minėtos direktyvos 7 straipsnį disponavimas tokiomis programomis kriminalizuotinas, jei jomis siekiama padaryti šios direktyvos 3–6 straipsniuose numatytas veikas. O disponavimas kompiuterio slaptažodžiais aprašytas šios direktyvos 7 straipsnio b dalyje ir nepatenka į tokių nusikalstamų veikų sąrašą. Atitinkamai nėra aišku, ar pagal direktyvą turėtų būti laikomos nusikalstamomis veikos, jei disponuojama priemonėmis, skirtomis duomenims, būtiniems neteisėtai prisijungti prie informacinės sistemos, t. y. tam tikra prasme toms pačioms nusikalstamos veikos padarymo priemonėms, įgyti. Taigi platesnis veikos kriminalizavimas Lietuvos BK leidžia išvengti pernelyg siauro priemonių supratimo ir problemų atpažįstant, kokia veika turėtų būti laikoma nusikalstama ir kodėl.

Kita vertus, gana plačiai suformuluota nusikalstamos veikos sudėtis gali kelti klausimų ir dėl jos taikymo ribų. Todėl ne mažiau svarbu yra nustatyti kriterijus, leidžiančius identifikuoti, kokių nusikalstamų veikų padarymą lengvinančių priemonių disponavimas kriminalizuotas BK 198[2] straipsnyje. Idėją, kad BK 198[2] straipsnio dispozicijoje nurodyti, pavyzdžiui, įrenginiai yra skirti ne bet kokiai, o kaip tik su elektronine erdve susijusiai nusikalstamai veikai padaryti, leidžia pagrįsti paties įrenginio kaip nusikalstamos veikos dalyko aiškinimas, kaip ir BK skyrius, į kurį ši nusikalstama veika yra įtraukta. Tokia išvada gali būti daroma atsižvelgus taip pat į kitų BK 198[2] straipsnyje nurodytų dalykų – programinės įrangos, slaptažodžių, kodų ar kitų panašių duomenų – paskirtį.

Kaip antai vienoje iš baudžiamųjų bylų V. P. pripažintas kaltu padaręs nusikaltimus, numatytus BK 198[2] straipsnio 1 dalyje, 214 straipsnio 1 dalyje, nes, *„veikdamas bendrininkų grupėje su ikiteisminio tyrimo metu nenustatytu asmeniu, neteisėtai įgijo, laikė ir panaudojo techninę įrangą, t. y. ne mažiau kaip keturis įrenginius, tiesiogiai skirtus svetimų elektroninių mokėjimo priemonių ir jų naudotojų tapatybės patvirtinimo duomenų rinkimui ir kaupimui, tikslu vėliau panaudoti gaminant netikras mokėjimo korteles, <...> bankomatuose, įdėjo mokėjimo kortelių nuskaitymo įrenginius, šios įrangos pagalba įgijo tyrimo metu nenustatytą kiekį svetimų elektroninių mokėjimo priemonių ir jų naudotojų tapatybės patvirtinimo priemonių duomenų, pakankamų finansinei operacijai inicijuoti. <...>*

Specialisto išvadoje <...> nustatyta, kad tyrimui pateiktas įrenginys sudarytas iš neidentifikuotos, pramoniniu būdu pagamintos miniatiūrinės magnetinių juostelių skaityklės ir specialaus, ant bankomato tvirtinamo plastikinio korpuso su plastikinei kortelei skirtu plyšiu ir jos magnetinės juostelės takelių <...> nuskaitymui skirta ma-

gnetine galvute. Įrenginys skirtas plastikinių mokėjimo kortelių magnetinėse juostelėse esančių duomenų rinkimui. Tyrimui pateiktas įrenginys turi galimybę savyje kaupti mokėjimo kortelių duomenis. <...> Tyrimui pateiktas įrenginys neturi galimybės nuotoliniu būdu perdavinėti mokėjimo kortelių duomenis“[11].

Panaudoto įrenginio veikimo ypatumai, pavyzdžiui, tai, kad jis turėjo galimybę kaupti mokėjimo kortelių duomenis, rodo, kad šie suvesti duomenys buvo saugomi elektroninės formos (nesvarbu, kad pats įrenginys neturėjo galimybės nuotoliniu būdu šiuos duomenis perduoti). Atitinkamai darytina išvada, kad BK 214 straipsnyje įtvirtintos nusikalstamos veikos padarymas buvo susijęs su elektronine erdve, t. y. erdve, kurią sukuria informacinės technologijos[12], nes šios veikos dalykas įgavo elektroninę formą.

Įdomu ir tai, kad teismų sprendimuose galima rasti formuluočių, keliančių klausimų, ar BK 198² straipsnyje iš tiesų nėra kriminalizuotas disponavimas tradicinių nusikalstamų veikų padarymą lengvinančiomis priemonėmis (įrankiais). Pavyzdžiui, baudžiamojoje byloje V. G. buvo nuteistas pagal BK 198² straipsnio 1 dalį už tai, kad *„neteisėtai pagamino programinę įrangą ir pardavė ją bei įrenginius, tiesiogiai skirtus daryti nusikaltimus – grobti didelės vertės svetimą turtą (vilkikus <...>), o būtent: <...> gavęs užsakymą iš ginkluoto nusikalstamo susivienijimo vadovo A. B. ir dalyvių V. V., T. T. neteisėtai pagaminti ir jiems parduoti programinę įrangą bei įrenginius, skirtus grobti <...> vilkikus <...>, 2011 m. vasarą savo namuose, esančiuose adresu (duomenys neskelbtini), internetu surinko duomenis apie kompiuterines vilkikų <...> aptarnavimo programas, internetu įgijo nešiojamąjį kompiuterį <...>, prietaisą informacijai įrašyti, kompaktinį diską, jungtis bei tuščius duomenų kaupiklius, neteisėtai pagamino programinę įrangą, tiesiogiai skirtą daryti nusikaltimus – grobti didelės vertės svetimą turtą, t. y. nuskaityti, perprogramuoti ir perrašyti vilkikų <...> kompiuterių duomenis, siekiant pašalinti apsauginius kodus ir variklio užvedimo blokavimą bei pagaminti atsarginius automobilių užvedimo raktus. Neteisėtai pagaminęs programinę įrangą, <...> V. G. <...> pardavė A. B., T. T. ir V. V. nešiojamą kompiuterį <...> su programine įranga, prietaisą informacijai įrašyti, kompaktinį diską, jungtis, tuščius duomenų kaupiklius, tiesiogiai skirtus daryti nusikaltimus – grobti didelės vertės svetimą turtą, t. y. nuskaityti, perprogramuoti ir perrašyti vilkikų <...> kompiuterių duomenis, siekiant pašalinti apsauginius kodus ir variklio užvedimo blokavimą bei pagaminti atsarginius automobilių užvedimo raktus*“[13].

Šiuo aspektu pažymėtina, kad taikant įrenginio ar programinės įrangos *tiesioginės paskirties* arba *tiesioginės funkcijos* kriterijų šioje baudžiamojoje byloje nurodytos priemonės (skirtos kompiuteriniams duomenims nuskaityti, perprogramuoti

11 Kauno apylinkės teismo 2016 m. gruodžio 29 d. teismo baudžiamasis įsakymas byloje Nr. 1-2485-825/2016.

12 Lietuvos Respublikos kibernetinio saugumo įstatymo 2 straipsnio 6 punktas, *TAR*, žiūrėta 2019 m. rugsėjo 4 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee/asr.

13 Šiaulių apylinkės teismo 2013 m. rugsėjo 10 d. teismo baudžiamasis įsakymas byloje Nr. 1-1138-900/2013.

ir perrašyti) pirmiausia buvo skirtos BK XXX skyriuje įtvirtintoms nusikalstamoms veikoms padaryti (pavyzdžiui, neteisėtam poveikiui elektroniniams duomenims, neteisėtam elektroninių duomenų perėmimui ir panaudojimui). Iš padarytos veikos *modus operandi* matyti, kad svetimo didelės vertės turto – vilkikų – pagrobimo veiksmai galėjo būti įvykdyti tik pašalinus apsauginius kodus, variklio paleidimo blokavimą ir pagaminus atsarginius automobilių paleidimo raktus. Toks nusikalstamos veikos padarymo mechanizmas yra klasikinis, jei nusikalstami veiksmai nukreipiami į „išmaniuosius daiktus“[14] – poveikis elektroniniams duomenims ar informacinei sistemai tokiais atvejais dažniausiai neišvengiamas dėl šiuose daiktuose integruotos informacinės sistemos.

2. Kai kurios e. veikų padarymo priemonių kriminalizavimo ir inkriminavimo problemos

2.1. Disponavimo įsibrovimo priemonėmis kriminalizavimo pagrindimo ieškant

Disponavimo e. veikų priemonėmis kriminalizavimo problema yra daugialypė: ji susijusi su nusikalstamų veikų fizinėje ir elektroninėje erdvėje ekvivalenčiu vertinimu, taigi ir kriminalizavimo pusiausvyros išlaikymu, taip pat su bendromis rengimosi stadijos baudžiamojo teisinio vertinimo problemomis.

Nusikalstamų veikų, padarytų elektroninėje ir fizinėje erdvėje, lygiaverčio vertinimo aktualumas gali būti pagrįstas iš ekvivalentaus vertinimo principo kylančiais reikalavimais.[15] Šio principo taikymu užtikrinamas vienodas teisinių vertybių apsaugos lygis šiose erdvėse, taip palaikant baudžiamosios teisės veikimo ribų pusiausvyrą, kai ta pati veika gali būti padaryta ir fizinėje, ir elektroninėje erdvėje. Ieškant BK 198[2] straipsnyje numatyto dalyko – įrenginių, programinės įrangos, slaptažodžių, prisijungimo kodų ir kitokių duomenų – atitikmens fizinėje erdvėje, paprastai išvedama tokių dalykų sąsaja su įsibrauti į patalpas (ketinant padaryti nusikalstamą veiką) naudojamais įrankiais (angl. *burglary tools*) (toliau – įsibrovimo įrankiai). Šiuo palyginimu dažnai bandoma pagrįsti baudžiamosios atsakomybės taikymą už disponavimą priemonėmis, skirtomis nusikalstamoms veikoms elektroninėje erdvėje padaryti: „Precedentai kontroliuojant *tradicines* nusikalstamas veikas egzistuoja, nes kriminalizuojami tokie dalykai kaip *įsibrovimo įrankiai*, ir daugiašaliai teisiniai instrumentai suformulavo analogiškas e. veikas.“[16]

---

14 Somayya Madakam, „Internet of Things: Smart Things“, *International Journal of Future Computer and Communication* 4, 4 (2015): 250–253, http://www.ijfcc.org/vol4/395-ICNT2014-2-203.pdf.

15 Oleg Fedosiuk ir Renata Marcinauskaitė, „Criminalization of Cybercrime and Principle of Equivalence“, *Administratīvā un krimināla justīcija* 2, 63 (2013): 8.

16 „Comprehensive Study on Cybercrime“, 92, žiūrėta 2019 m. rugsėjo 3 d., https://documents.tips/documents/cybercrime-study-210213-56290c8207c33.html.

Ne mažiau svarbu, kad e. veikų padarymo priemonių paklausa veda prie tam tikros rūšies juodosios rinkos (angl. *black market*) tokioms priemonėms gaminti ir platinti sukūrimo. Mokslinėje literatūroje pažymima, kad elektroninėje erdvėje vystosi savotiškas verslas, „paleidžiantis į apyvartą“[17] techninius įgūdžius ir priemones, kurios tampa prieinamos e. veikas darantiems asmenims. Paslaugos, susijusios su nusikalstamos infrastruktūros palaikymu, kenkėjiška programine įranga, įsibrovimu, neteisėtai gauta informacija, pinigų plovimu, kaip nelegalios rinkos kategorijos apibendrintai gali būti vadinamos vienu – „nusikaltimo kaip paslaugos“ (angl. *crime-as-a-service*)[18] terminu. Paskata įsigyti neteisėtai prieigai skirtas (angl. *hacker tools*) ar kitas priemones kyla dėl to, kad jos dažnai būtinos e. veikoms padaryti. Tuo labiau, kad siūlomų produktų ar paslaugų ypatumai (patogūs vartotojui, specializuoti, lengvai naudojami ir pan.) sudaro galimybes daugiau asmenų, nesvarbu, kokie jų techniniai gebėjimai, gauti prieinamas paslaugas – „jie paprasčiausiai sumoka už įdiegimą ir gauna paslaugą, kuri atlieka darbą“[19]. Šios skaitmeninės prekės ir paslaugos aprūpina ir užtikrina „visą atakos gyvavimo ciklą“[20]. Konvencijos dėl elektroninių nusikaltimų aiškinamojoje ataskaitoje, atsižvelgiant į šias elektroninės erdvės *pogrindžio* vystymosi tendencijas, teigiama, kad „kovojant su tokiomis grėsmėmis, baudžiamoji teisė turėtų uždrausti pirmines specifines potencialiai pavojingas veikas prieš tai, kai yra padaromi 2–5 straipsniuose numatyti nusikaltimai“ (71 punktas)[21].

Nors atrodytų, kad šios priežastys kriminalizuoti disponavimą e. veikų priemonėmis yra iš dalies suprantamos, tačiau, žvelgiant nacionalinės baudžiamosios teisės aspektu, toks baudžiamosios atsakomybės numatymas kelia konceptualių abejonių. Pirmiausia dėl to, kad disponavimas įsibrovimo priemonėmis (pavyzdžiui, vagystės ar plėšimo atveju naudojamomis įsibrauti į patalpą (BK 178 ar 180 str. 2 d.)) kaip savarankiška nusikalstama veika Lietuvos BK nėra kriminalizuota. Nesant tiksliausio minėtos e. veikos atitikmens BK, ekvivalentus sudėties požymių vertinimas, išsaugant esmines jų turinio aiškinimo gaires, komplikuojasi.

Tačiau nagrinėjamu aspektu reikėtų atkreipti dėmesį į tai, kad pats požiūris, jog baudžiamoji atsakomybė už disponavimą nusikalstamos veikos padarymą reikšmingai lengvinančiomis priemonėmis yra galima, BK nėra svetimas. Iš tiesų BK specialiojoje dalyje numatyta nemažai nusikalstamų veikų, kurių dalykas yra kitos sumanytai nusikalstamai veikai padaryti skirtos ar pritaikytos priemonės (BK 194, 201, 213, 214, 257[1], 302[1] ir kiti str.). Kaip teigiama mokslinėje literatūroje, šių kriminalizuotų savarankiškų

17 Ting Zhang, „Comparative study of sanction system of cyber aider fom perspectines of German and Chinese criminal law“, *Computer Law & security review* 33 (2017): 98–99.

18 *Ibid*., 98.

19 Lillian Ablon ir kt., „Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar“ (Santa Monica, CA: RAND Corporation, 2014), 9, https://www.rand.org/pubs/research_reports/RR610.html.

20 *Ibid*., 8.

21 „Explanatory Report to the Convention on Cybercrime“, žiūrėta 2019 m. rugsėjo 3 d., http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

nusikalstamų veikų esmę „sudaro rengimasis padaryti kitą nusikalstamą veiką“[22]. Todėl galima būtų teigti, kad e. veikų priemonės (BK 198[2] str.) bendriausia prasme turi panašumų į kitas, nebūtinai įsibrauti naudojamas priemones, nes visų jų paskirtis ta pati – sudaryti lengvinančias sąlygas sumanytai nusikalstamai veikai padaryti.

Šios ekvivalentaus vertinimo paieškos taip pat susijusios su skirtingo rengimosi veiksmų baudžiamojo teisinio vertinimo problema. Disponavimas nusikalstamos veikos padarymą lengvinančiomis priemonėmis ar įrankiais gali atitikti savarankiškos nusikalstamos veikos sudėties požymius (jei taip kriminalizuota), tačiau tokie veiksmai gali būti laikomi ir rengimusi padaryti nusikaltimą (BK 21 str.). Rengimosi stadija rodo daugiau ar mažiau sudėtingą, palaipsniui besivystančią kaltininko veiką, tačiau ja dar nepradedami realizuoti ketinto įvykdyti nusikaltimo sudėties požymiai. *Pasirengimo* terminas tokiais atvejais yra laikomas termino *sąlygų sudarymas* sinonimu.[23] Taigi nors disponavimas *įsibrovimo įrankiais* kaip savarankiška nusikalstama veika BK nėra kriminalizuota, jų suieškojimas ar pritaikymas sudarant lengvinančias sąlygas, pavyzdžiui, vagystei ar plėšimui, gali būti laikomas nusikalstamais rengimosi veiksmais. Be abejo, tokiam teisiniam vertinimui yra svarbios baudžiamosios atsakomybės už rengimosi stadijoje nutrūkusį nusikaltimą sąlygos, kaip antai, kad toks nusikaltimas turi būti sunkus ar labai sunkus (pavyzdžiui, BK 178 str. 3 d., 180 str. 2, 3 d.). Vadinasi, nors disponavimas *įsibrovimo įrankiais* ir *e. veikų priemonėmis* rodo tą patį kaltininko nusikalstamo ketinimo realizavimo lygį, tokių veikų kriminalizavimo „plotis“ skiriasi. Pavyzdžiui, jei disponuojama e. veikos priemonėmis, skirtingai nei įsibrovimo įrankiais fizinėje erdvėje, nebūtina nustatyti, kad ketintas padaryti nusikaltimas yra sunkus ar labai sunkus. Šis skirtingas rengimosi veiksmų vertinimas, kurį iš dalies lėmė ir tarptautinių, ir Europos Sąjungos teisės aktų įgyvendinimo poreikis, rodo vieną iš lygiaverčio fizinėje ir elektroninėje erdvėje padarytų nusikalstamų veikų vertinimo problemų.

2.2. *Dvejopo naudojimo* priemonių ar įrankių baudžiamojo teisinio vertinimo problemos

Disponavimo įrankiais ar priemonėmis veikos tradiciškai reiškia disponavimą akivaizdžiai draudžiamais daiktais, pavyzdžiui, neteisėtas disponavimas šaunamaisiais ginklais, šaudmenimis, sprogmenimis ar sprogstamosiomis medžiagomis (BK 253 str.), nešaunamuoju ginklu (BK 258 str.), narkotinėmis ar psichotropinėmis medžiagomis (BK 260 str.). Nors šios veikos gali kelti jų inkriminavimo problemų, su didesniais sunkumais susiduriama aiškinant tą dalyko kategoriją, į kurią patenka priemonės ar įrankiai, BK įvardyti kaip *tiesiogiai skirti ar pritaikyti* nusikalstamai

22 Gintaras Švedas ir kt., *Lietuvos Respublikos baudžiamojo kodekso bendrosios dalies vientisumo ir naujovių (su)derinimo iššūkiai* (Vilnius: Vilniaus universiteto leidykla, 2017), 141.

23 Anatolij Petrovich Kozlov, *Uchenie o stadijakh prestuplenija* [Teaching about the Stages of the Crime] (Saint Petersburg: Yuridichesky Center Press, 2002), 216.

veikai daryti (pavyzdžiui, BK 213, 214, 257[1], 302[1] str.). Čia teisėkūros ir pasirinktų formuluočių problema kyla bandant atsakyti į klausimą, ar ši frazė nėra „viską pagaunanti“, taigi apimanti ir tas priemones, kurios gali būti naudojamos ir nenusikalstamais tikslais. Pavyzdžiui, nemažai neaiškumų ir pagrįstų baimių užsienio valstybėse kėlė minėtas *įsibrovimo įrankių* kriminalizavimas, nes neteisingai tokią normą supratus, bene kiekvienas įprastas daiktas galėjo būti laikomas šiuo įrankiu.[24] Atsižvelgiant į tai, teismų praktikoje buvo pažymima, kad asmuo negali būti nuteistas už atsarginių raktų, laužtuvo, kabliukų, batų poros, maišo ar kitų daiktų turėjimą savo paties namuose.[25] Šios problemos yra aktualios ir kalbant apie e. veikų padarymo priemones, nes, kaip minėta, kaip tik *įsibrovimo įrankiai* yra bene tiksliausias tokių priemonių atitikmuo fizinėje erdvėje. Dvejopo naudojimo priemonių problema e. veikų srityje kyla keliais aspektais, t. y. kalbant apie: 1) etiško įsibrovimo (angl. *ethical hacking*) priemonių kriminalizavimo pavojų, 2) požymio *tiesiogiai skirtas ar pritaikytas nusikalstamoms veikoms daryti* turinio atskleidimo sunkumus. Todėl aiškinant BK 198[2] straipsnyje numatytus dalykus turėtų būti rasta pusiausvyra, leidžianti išvengti per siauros e. veikų priemonių juodąją rinką skatinančios interpretacijos. Kartu tokia interpretacija neturėtų būti per plati, įtvirtinanti neaiškias teisėto ir nusikalstamo elgesio ribas ir leidžianti kalbėti apie veikų perteklinį kriminalizavimą. Kriterijų paieška yra aktuali atsižvelgiant ir į šios kategorijos baudžiamosiose bylose formuojamą kasacinės instancijos teismo praktiką, pagal kurią *dvejopo naudojimo* priemonės gali būti laikomos BK 198[2] straipsnyje numatytos nusikalstamos veikos dalyku, tačiau tik tuo atveju, jei tokiam disponavimui yra būdingi tam tikri požymiai.[26]

Savo paties informacinės sistemos ar duomenų saugumo patikrinimas naudojant teisėtą testavimą (pavyzdžiui, kontroliuojamus bandymus įveikti saugumo priemones) yra vienas svarbiausių bet kokio efektyvaus duomenų saugumo užtikrinimo mechanizmo elementų.[27] Specialistai, testuodami tinklo ir sistemų saugumą etiško įsibrovimo metu, pasitelkia „tuos pačius įrankius, kuriuos naudoja įsilaužėliai, siekiantys sukompromituoti tinklą“[28]. Šie saugos specialistai[29] gali naudoti daugybę skirtingų

---

24 Paul A. Clark, „Do statutes criminalizing possession of burglary tools reduce crime?“, *Capital University Law Review* 42, 4 (2014): 808. Įdomu tai, kad statutai, draudžiantys disponavimą *įsibrovimo įrankiais*, istoriškai gali būti susieti su dabar, atrodytų, archajiškomis normomis, anuomet draudusiomis būti nusikaltėliu (angl. *rogue*) arba valkata (angl. *vagabond*), o „vienas iš būdų būti nusikaltėliu ar valkata buvo disponuoti įrankiais ar priemonėmis, leidžiančiomis padaryti išvadą apie nusikalstamą ketinimą“ (plačiau žr. *Ibid*., 805).

25 *Ibid*., 808.

26 Lietuvos Aukščiausiojo Teismo 2015 m. gegužės 12 d. kasacinė nutartis baudžiamojoje byloje Nr. 2K-188-489/2015.

27 I. Ronald ir Jr. Raether, „Data Security and Ethical Hacking: Points to Consider for Eliminating Avoidable Exposure“, *Business Law Today* 18, 1 (2008): 55.

28 Plačiau žr. Antanas Česnys ir Jonas Juknius, *Saugumo patikros ir etiško įsilaužimo technologijos* (Kaunas: Kauno technologijos universiteto Informatikos fakultetas, 2011), 7.

29 Literatūroje taip pat vadinami *etiškais programišiais* arba *baltosiomis skrybėlėmis* (plačiau žr. *Ibid*., 7–8).

metodų, taip pat ir daugybę skirtingų priemonių, kuriomis imituojamos tinklų ir sistemų saugumą pažeidžiančios atakos. Todėl sprendžiant dėl disponavimo e. veikų priemonėmis kriminalizavimo apimties, svarbu atkreipti dėmesį į tai, kad egzistuoja ir teisėta priemonių, skirtų sistemos techninei ir programinei įrangai testuoti ar (ir) tikrinti, apyvarta.[30] „Slaptažodžių atkūrimo priemonės sistemos administratoriams yra *slaptažodžių nulaužimo* (angl. *password cracker*) priemonės kaltininkams".[31] Tai vienas iš pavyzdžių, padedančių apibūdinti dvejopo naudojimo priemones – tas, kurios gali būti panaudotos tiek teisėtiems, tiek ir nusikalstamiems tikslams siekti, todėl gali būti laikomos kartu ir teisėtos veiklos, ir nusikalstamos veikos priemone. Tokiais atvejais nustatant šių priemonių statusą yra svarbūs etiško įsibrovimo principai ir tokios veiklos teisiniai aspektai.[32]

Šiuo aspektu pažymėtina, kad baudžiamajai atsakomybei už disponavimą e. veikų priemonėmis kilti pagal BK 198[2] straipsnį, be kita ko, būtina konstatuoti, kad minėtomis priemonėmis disponuota nusikalstamais tikslais ar kitaip neteisėtai. Taip pat ši veika gali būti padaroma tik tiesiogine tyčia, esant atitinkamam psichiniam santykiui su objektyviaisiais sudėties požymiais (BK 15 str. 2 d. 1 p.). Kaip tik šie reikalavimai leidžia išvengti disponavimo e. veikų priemonėmis perteklinio kriminalizavimo, kai priemonės sukuriamos ir pateikiamos prekybai teisėtais tikslais, pavyzdžiui, padedant atremti atakas, nukreiptas prieš informacines sistemas (Konvencijos dėl elektroninių nusikaltimų aiškinamosios ataskaitos 76 p.).[33] Todėl akivaizdu, kad į baudžiamosios teisės veikimo sritį nepatenka etiško įsibrovimo veiksmai, jei buvo laikomasi visų tokių veiksmų atlikimo teisėtumo reikalavimų.[34] Pavyzdžiui, kasacinėje nutartyje baudžiamojoje byloje Nr. 2K-188-489/2015 konstatuotas *DDos atakų* organizavimo neteisėtumas, vadovaujantis tokiais argumentais: „<...> *neteisėtumo požymis nagrinėjamoje byloje gali būti nustatomas atsižvelgiant į tai, kad tinklalapių www.t.lt ir www.tv.lt darbo trikdymo veiksmams nebuvo gautas joks sistemos ar jos dalies savininko (valdytojo) leidimas. Nesant susitarimui dėl sistemos testavimo, A. V. iš kerštо suorganizuotos elektroninės paslaugos trikdymo atakos negali būti laikomos teisėta šių sistemų saugumo patikra. Atsižvelgiant į tai, byloje nustatyti nuteistųjų atlikti DDos atakų organizavimo, atitinkamai ir jų panaudojimo veiksmai sutrikdę tinklalapių www.t.lt ir www.tv.lt darbą, pripažintini neteisėtais.*"

Kita dvejopo naudojimo priemonių teisinio vertinimo problema, kaip minėta, yra susijusi su sunkumais atskleidžiant *tiesiogiai skirtas ar pritaikytas nusikalstamoms veikoms daryti* požymio turinį. Šis disponavimo e. veikų priemonėmis požymis gali būti aiškinamas žvelgiant į jį dviem – objektyviuoju ir subjektyviuoju – aspektu.

---

30 Charlotte Walker-Osborn, „Rules on dual use tools", *ITNOW* 50, 2 (2008): 28.

31 Stefan Fafinski, „Double-edged swords", *ITNOW* 48, 4 (2006): 16.

32 Plačiau žr. Česnys ir Juknius, *supra note*, 28; Ronald ir Raether, *supra note*, 27.

33 „Explanatory Report to the Convention on Cybercrime", *supra note*, 21.

34 Plačiau žr. Ronald ir Raether, *op. cit.*

Požiūrio, pagrįsto objektyviaisiais kriterijais, paprastai yra laikomasi pripažįstant disponavimą minėtomis priemonėmis pavojingu *per se*, todėl toks disponavimas kriminalizuojamas kaip savarankiška nusikalstama veika. Tokiais atvejais nusikalstamos veikos dalykas yra *tiesiogiai skirtas ar pritaikytas nusikalstamoms veikoms daryti*, jei priemonės pagal jų pirminę paskirtį yra skirtos nusikalstamai veikai daryti arba tokiai veikai pritaikytos, nors pirminė jų paskirtis buvo visai kita.[35] Todėl baudžiamoji atsakomybė taikoma už disponavimą ne bet kokiais įrankiais ar priemonėmis, o tik tais, kurie objektyviai pagal savo paskirtį yra tiesiogiai skirti ar pritaikyti nusikalstamai veikai daryti. Laikantis subjektyviojo požiūrio, vadovaujamasi kriterijais, apibūdinančiais ne tiek objektyvią dalyko (priemonės) paskirtį, kiek kaltininko santykį su ta priemone, jo ketinimą šią priemonę panaudoti nusikalstamai veikai padaryti. Laikoma, kad priemonė specialiai nusikalstamai veikai padaryti pritaikyta, jei ja disponuota nusikalstamais tikslais, nors pati priemonė pagal savo prigimtį nėra tam skirta. Šis platus specialaus pritaikymo požymio aiškinimas būdingas tiems atvejams, kai priemonių panaudojimas yra ne savarankiška nusikalstama veika, o sudedamoji kitos veikos dalis – dažniausiai jos kvalifikuojantis požymis. Pavyzdžiui, kasacinėje nutartyje baudžiamojoje byloje Nr. 2K-215-696/2016[36] išaiškintas plėšimo pavojingumą didinantis požymis – kitas specialiai žmogui sužaloti pritaikytas daiktas (BK 180 str. 2 d.), be kita ko, vadovaujantis ir subjektyviuoju požiūriu: „*specialiai pritaikytais žmogui sužaloti laikomi daiktai, kuriuos kaltininkas paruošia ar pritaiko šiam tikslui iš anksto arba plėšimo metu, taip pat daiktai, kurie nors ir nebuvo iš anksto paruošti, tačiau iš anksto parinkti ir pasiimti tais pačiais tikslais.*“

Atitinkamai aiškinantis disponavimo e. veikų priemonėmis, *tiesiogiai skirtomis ar pritaikytomis nusikalstamoms veikoms daryti*, požymį spręstina, kuriuo kriterijumi, o gal jais abiem, turėtų būti vadovaujamasi. Šiuo aspektu aktualu, kad apie subjektyviojo kriterijaus taikymą sprendžiant dėl BK 198² straipsnyje nurodyto nusikalstamos veikos dalyko, be kita ko, leidžia kalbėti Direktyvos 2013/40/ES preambulės 16 punktas: „*atsižvelgiant į skirtingus atakų atlikimo būdus ir spartų techninės ir programinės kompiuterių įrangos tobulėjimą, šioje direktyvoje sąvoka „priemonės“ reiškia priemones, naudojamas šioje direktyvoje nustatytoms nusikalstamoms veikoms vykdyti. Tokios priemonės gali reikšti kibernetinėms atakoms rengti naudojamą žalingą programinę įrangą, įskaitant priemones, kuriomis gali būti kuriami botnetai. Net jeigu tokia priemonė yra tinkama ar netgi specialiai skirta vienai iš šioje direktyvoje nustatytų nusikalstamų veikų vykdymui, gali būti, jog ji pagaminta teisėtu tikslu. Remiantis poreikiu išvengti baudžiamosios atsakomybės taikymo tuo atveju, kai to-*

35 Toks aiškinimas būdingas ir kitoms nusikalstamoms veikoms, pavyzdžiui, atskleidžiant BK 257¹ straipsnyje numatytos nusikalstamos veikos dalyko požymį (plačiau žr. Armanas Abramavičius ir kt., *Lietuvos Respublikos baudžiamojo kodekso komentaras. Specialioji dalis (213–330 straipsniai)* (Vilnius: Registrų centras, 2010), 283.

36 Lietuvos Aukščiausiojo Teismo 2016 m. gegužės 31 d. nutartis baudžiamojoje byloje Nr. 2K-215-696/2016.

kios priemonės yra pagamintos ir pateiktos rinkai teisėtais tikslais, pavyzdžiui, skirtos informacinių technologijų produktų patikimumo arba informacinių technologijų saugumo testavimui, ne tik bendro ketinimo reikalavimas, bet ir tiesioginio ketinimo panaudoti tas priemones šioje direktyvoje nustatytai vienai ar kelioms nusikalstamoms veikoms vykdyti reikalavimas taip pat turi būti išpildytas."

Tokia nuostata yra vadovaujamasi ir kasacinės instancijos teismo praktikoje, kurioje šiuo aspektu pažymima, kad „*BK 198[2] straipsnio 1 dalyje nurodytos priemonės, tinkamos nusikalstamoms veikoms daryti, gali būti pagamintos ir teisėtu tikslu, t. y. jos gali būti dvigubo naudojimo priemonės <...>, kurios gali būti panaudotos tiek teisėtiems, tiek ir nusikalstamiems tikslams. Tačiau siekiant išvengti nepagrįsto baudžiamosios atsakomybės taikymo, kai tokios priemonės yra pagamintos ir pateiktos vartotojams teisėtiems tikslams (pavyzdžiui, skirtos informacinių technologijų produktų patikimumui, saugumui testuoti), būtina nustatyti tiesioginį ketinimą panaudoti tokias priemones nusikalstamai veikai daryti (kasacinė nutartis baudžiamojoje byloje Nr. 2K-188-489/2015). Šiuo aspektu aktualu ir tai, kad pagal <...> direktyvos 2013/40/ES <...> reikalavimus tai reikštų, kad turi būti nustatomas ne tik bendras, bet ir tiesioginis ketinimas panaudoti tokias priemones vienai ar kelioms nusikalstamoms veikoms padaryti (Preambulės 16 punktas)*"[37]. Šie išaiškinimai reikštų, kad dvejopo naudojimo priemonės gali būti laikomos BK 198[2] straipsnyje įtvirtintos nusikalstamos veikos dalyku, jei, be kita ko, pagrindžiamas jų disponavimas tokiomis aplinkybėmis, kurios parodo kaltininko nusikalstamus ketinimus. Vis dėlto tokiais atvejais yra būtina konstatuoti ne bendrą (abstraktų) ketinimą daryti nusikalstamas veikas, o apibrėžtą kaltininko sumanymą realizuoti konkrečios nusikalstamos veikos sudėties požymius. Nors, viena vertus, toks įrodinėjimas iš tiesų yra daug sudėtingesnis, priartinantis BK 198[2] straipsnyje numatytos nusikalstamos veikos aiškinimą prie rengimosi stadijos nustatymo reikalavimų, kita vertus, kaip tik toks sudėties požymių visumos aiškinimas leistų išvengti perteklinio kriminalizavimo pavojaus.

Kadangi nusikalstamas tikslas BK 198[2] straipsnio prasme negali būti pagrįstas vien tik tuo, kad dvejopo naudojimo priemonės gali būti (yra) tinkamos nusikalstamai veikai daryti, tokia išvada turi būti motyvuota byloje surinktų įrodymų visuma: „*apkaltinamasis nuosprendis turi būti grindžiamas ne prielaidomis, o patikimais įrodymais, kurie turi būti neprieštaringi, nuoseklūs, tarpusavyje susiję ir iš kurių analizės turi logiškai išplaukti kaltinamojo kaltę bei kitas svarbias aplinkybes patvirtinančios išvados, o kaltinimui prieštaraujantys duomenys turi būti paneigti.*"[38] Šiuo aspektu kasacinės instancijos teismas neteisėto disponavimo įrenginiais, programine įranga, slaptažodžiais, kodais ir kitokiais duomenimis baudžiamosiose bylose yra pažymėjęs, kad „*padarytos išvados dėl nusikalstamo tikslo turi būti teisiškai motyvuotos ir pagrįstos byloje surinktais įrodymais; kaltininko tikslas programinę įrangą panaudoti kon-*

37 Lietuvos Aukščiausiojo Teismo 2019 m. liepos 2 d. nutartis baudžiamojoje byloje Nr. 2K-199-648/2019.

38 Lietuvos Aukščiausiojo Teismo 2019 m. balandžio 29 d. nutartis baudžiamojoje byloje Nr. 2K-87-719/2019.

krečioms nusikalstamoms veikoms daryti negali būti grindžiamas prielaidomis ar preziumuojamas; dvigubo naudojimo priemonių įgijimas ar laikymas kelia grėsmę elektroninių duomenų ir informacinių sistemų saugumui, jei jomis disponuojama būtent esant minėtam nusikalstamam tikslui“[39]. Tokio tikslo buvimą, taip pat programinės įrangos kenkėjišką prigimtį, be kitų aplinkybių, gali liudyti pačios programinės įrangos ypatumai (tokios programinės įrangos pateikimo forma, jos sandara, funkcionavimo ypatumai), todėl svarbu, ar tokios priemonės yra vienareikšmiškai orientuotos nelegaliam naudojimui (pavyzdžiui, sprendžiant iš jų naudojimo politikos ar gamintojo reklamos), ar jos pagal savo sandaros ypatumus ir veikimo metodus yra sukurtos kaip tik neteisėtiems tikslams siekti ir pan. Jei prieiga prie tokios programinės įrangos suteikiama abejotinuose interneto šaltiniuose, be kitų aplinkybių, įvertinus jos kilmę ir gamintojo nurodytą panaudojimo būdą, papratai gali būti daroma išvada, kad tai yra kenkimo programinė įranga, skirta nusikalstamoms veikoms daryti.

Išvados

1. BK 198² straipsnyje nurodyti įrenginiai ir programinė įranga gali būti naudojami ne tik BK XXX skyriuje nurodytoms nusikalstamoms veikoms padaryti. Vis dėlto, atsižvelgiant į šių e. veikų priemonių ypatumus, nusikalstamos veikos, padarytos jas panaudojus, turėtų pažeisti ir elektroninės erdvės saugumą (turėtų būti visiškai arba bent iš dalies susijusios su elektronine erdve).
2. Kaltininkui inkriminuojant BK 198² straipsnyje numatytą nusikalstamą veiką, įrenginiai ir programinė įranga apibūdintini taikant *tiesioginės paskirties* ar *tiesioginės funkcijos* kriterijų. Todėl, atskleidžiant požymio *tiesiogiai skirtas ar pritaikytas nusikalstamoms veikoms daryti* turinį, nurodytinas ne visas kaltininko sumanymas ar galutinis jo siekiamas nusikalstamas tikslas, o konkreti nusikalstama veika, tiesiogiai padaryta naudojant minėtas e. veikų priemones.
3. Atsakomybei pagal BK 198² straipsnį kilti, be kitų požymių, būtina nustatyti, kad e. veikų priemonėmis disponuota nusikalstamais tikslais ar kitaip neteisėtai, taip pat tyčinę kaltę. Šie sudėties požymiai leidžia išvengti baudžiamosios atsakomybės taikymo, kai priemonės sukuriamos ir pateikiamos prekybai teisėtais tikslais, yra skirtos teisėtam saugumo testavimui vykdyti.
4. Baudžiamoji atsakomybė už disponavimą dvejopo naudojimo priemonėmis yra galima, jei nustatytos aplinkybės, liudijančios kaltininko nusikalstamą tikslą ir priemonės kenkėjišką prigimtį. Tokiais atvejais, be kita ko, vertintini programinės įrangos ypatumai, prieigos prie jos šaltiniai, gamintojo nurodyta jos panaudojimo politika ir kitos šiam klausimui spręsti svarbios aplinkybės.

39 Lietuvos Aukščiausiojo Teismo 2019 m. liepos 2 d. nutartis baudžiamojoje byloje Nr. 2K-199-648/2019.

QUALIFICATION PROBLEMS OF UNLAWFUL DISPOSAL OF INSTALLATIONS, SOFTWARE, PASSWORDS, LOGIN CODES, CODES AND OTHER DATA (ARTICLE 198^2 OF CRIMINAL CODE OF THE REPUBLIC OF LITHUANIA)

Renata Marcinauskaitė
Mykolas Romeris University, Lithuania

Summary. *The article reveals some problematic aspects of unlawful disposition of devices, software, passwords, codes, and other data, as well as the criminalization problem of such offense. The article also devotes considerable attention to the case law that develop in this criminal case category and, moreover, provides the interpretations of it. The offense, enshrined in Article 198^2 of the Criminal Code of the Republic of Lithuania (CC), was analyzed in broader sense: following the principle of equivalence the analogy of such offense in physical space was searched, as well as the justification of its criminalization. The article also focuses on the definition problems of the subject matter of the above-mentioned criminal offense. The solution of such problems is relevant in explaining the application scope of the Article 198^2 of CC. Equally complex is the criminalization issue of the disposal of dual-use tools (devices or software). In response to this, the article formulates criteria that would justify the application of criminal liability when such means are involved.*

Keywords: *devices, software, malicious software, burglary tools, dual-use tools, preparation for commission of a crime.*

Renata Marcinauskaitė, Mykolo Romerio universiteto Mykolo Romerio teisės mokyklos Baudžiamosios teisės ir proceso instituto lektorė, daktarė. Mokslinių tyrimų kryptys: nusikalstamos veikos elektroninėje erdvėje, jurisdikcija.

Renata Marcinauskaitė, doctor of social sciences, lecturer at Mykolas Romeris University, Mykolas Romeris Law School, Institute of Criminal Law and Procedure. Research interests: cybercrime, jurisdiction.