ISSN 2029–2236 (print)
ISSN 2029–2244 (online)
SOCIALINIŲ MOKSLŲ STUDIJOS
SOCIETAL STUDIES
2013, 5(1), p. 367–379.

TECHNOLOGINIO NEUTRALUMO PRINCIPAS IR JO REIKŠMĖ FORMULUOJANT IR AIŠKINANT NUSIKALSTAMŲ VEIKŲ ELEKTRONINIŲ DUOMENŲ IR INFORMACINIŲ SISTEMŲ SAUGUMUI SUDĖTIS

Renata Marcinauskaitė

Mykolo Romerio universiteto Teisės fakulteto
Baudžiamosios teisės ir proceso institutas
Ateities g. 20, LT-08303 Vilnius, Lietuva
Telefonas (+370 5) 271 4584
Elektroninis paštas: renata.marcinauskaite@gmail.com

Pateikta 2012 m. lapkričio 22 d., parengta spausdinti 2013 m. sausio 11 d.

Anotacija. *Informacinių ir komunikacijos technologijų reguliavimo srityje plačiai taikomas technologinio neutralumo principas yra ne mažiau svarbus aiškinant nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumo sudėties požymius. Straipsnyje siekiama atskleisti pagrindinius šio principo įgyvendinimo baudžiamojoje teisėje aspektus, taip pat analizuojama technologijoms neutralaus teisinio reguliavimo atitiktis baudžiamojoje teisėje itin svarbiems legalumo ir teisinio tikrumo principams. Atsižvelgiant į tai, kad gana abstraktus nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui sudėties požymių aprašymas gali kelti baudžiamosios teisės taikymo ribų nustatymo problemų, straipsnyje pateikiami galimi jų sprendimo variantai.*

Reikšminiai žodžiai: *technologinio neutralumo principas, technologinio tikslumo principas, kriminalizavimas, baudžiamosios teisės principai.*

ISSN 2029–2236 (print), ISSN 2029–2244 (online)
http://www.mruni.eu/lt/mokslo_darbai/SMS/
http://www.mruni.eu/en/mokslo_darbai/SMS/

Įvadas

Informacinių ir komunikacijos technologijų reguliavimo srityje plačiai taikomas technologinio neutralumo principas (angl. *technological neutrality*) užtikrina lygiavertį technologijų vertinimą, nes draudžia teikti pirmenybę kuriai nors vienai iš jų. Pagal šį principą prioritetas, aiškinant su technologijomis susijusias sąvokas, turėtų būti teikiamas jų funkcijoms, o ne pačioms konkrečiai įvardijamoms technologijoms. Tai, atsižvelgiant į teisės ir technikos sąveikos perspektyvas, leidžia išvengti teisės normų taikymo apribojimų, kylančių dėl jose vartojamų specifinių terminų.

Kaip vieną iš galimų pavojingų veikų elektroninėje erdvėje kontroliavimo priemonių pasirinkus baudžiamąjį teisinį reguliavimą, šis principas aktualus aiškinant nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui sudėties požymius. Jis baudžiamosios teisės kontekste reikštų, kad nusikalstamos veikos sudėties požymiai, turintys tiesioginę sąsają su informacinėmis ir komunikacijos technologijomis, turėtų būti apibrėžiami taip, kad netaptų priklausomi nuo technologijų pokyčių, jeigu toks priklausomumas nėra įstatymo leidėjo valia.

Tačiau vis dėlto iš pirmo žvilgsnio atrodanti pažangi technologijoms neutralaus teisinio reguliavimo idėja baudžiamosios teisės kontekste galėtų sulaukti ir kritikos dėl tokio reguliavimo neatitikimo legalumo (lot. *nullum crimen, nulla poene sine lege*) ir teisinio tikrumo (angl. *legal cetrainty*) principams. Nors technologinio neutralumo principas laikomas efektyvia priemone derinant greitą informacinių ir komunikacijos technologijų vystymąsi su nustatytu teisiniu reguliavimu, tačiau jis negali užtikrinti nusikalstamos veikos teisiniam apibūdinimui keliamų išsamumo, tikslumo ir aiškumo reikalavimų įgyvendinimo. Kadangi tokia situacija yra tiesiogiai siejama su baudžiamosios teisės funkcijų ir jos ribų nustatymo problema, straipsnyje atkreipiamas dėmesys ne tik į tinkamų sąvokų svarbą, bet taip pat ir į praktinį baudžiamojo įstatymo taikymo lygmenį.

Šio tyrimo tikslas yra atskleisti pagrindinius technologinio neutralumo principo aspektus ir nustatyti šio principo taikymo problemas aiškinant nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui sudėties požymius, taip pat pasiūlyti galimus šių problemų sprendimo variantus.

Tyrimo objektas – technologinio neutralumo principas ir įvairūs jo taikymo aspektai formuluojant bei aiškinant nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui sudėtis.

Technologinio neutralumo principas baudžiamosios teisės aspektu Lietuvos teisės ar kitų sričių mokslininkų darbuose nėra nagrinėtas, tuo tarpu užsienio valstybių mokslinėje literatūroje diskutuojama ne tik apie technologijoms neutralaus teisinio reguliavimo įgyvendinimo galimybes (C. Reed, R. Ali, I. M. van der Haar, P. Ohm, B. J. Koops ir kt.), bet išgryninamos ir pagrindinės šio principo taikymu suponuotos „*perkriminalizavimo*“, „*technologijos ir terminologijos*“ bei kitos problemos (I. Walden, J. Clough ir kt.). Kadangi šiame straipsnyje nagrinėti ir nusikalstamų veikų sudėties požymių aprašymui keliami reikalavimai, todėl jame neapsieita be baudžiamosios teisės principų analizės. Šiuo aspektu reikėtų paminėti, kad Lietuvos baudžiamosios teisės teorijoje

nemažą dėmesį baudžiamosios teisės principams ir pavojingų veikų kriminalizavimo kriterijams skyrė V. Justickis, O. Fedosiukas, G. Švedas ir kt.

Tyrimas atliktas taikant sisteminės analizės, loginį-analitinį, dokumentų analizės ir lyginamąjį metodus.

1. Nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui sudėties požymių turinys ir technologinio neutralumo principas

Nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui (toliau – nusikalstamos veikos EDISS) sudėties požymių aiškinimui įtakos turi informacinių ir komunikacijos technologijų sparti raida. Kadangi šios technologijos nuolat kinta, todėl akivaizdus ir greitas tokio pobūdžio nusikalstamų veikų vystymasis. Atsižvelgiant į tai įvairūs nusikalstamų veikų EDISS kriminalizavimo aspektai kaskart turėtų būti vertinami jų pakankamumo požiūriu, nustatant, ar esamas *status quo* atitinka besikeičiančias aplinkybes.

Būtent su technologijomis ryšį turinčių nusikalstamų veikų sudėties požymių turinys yra gana dinamiškas, kas kelia sudėties požymių apibrėžtumo bei tinkamos terminijos parinkimo problemas. Bendriausia prasme tokie gana keblūs technologiniai-baudžiamieji teisiniai sudėties požymių aiškinimo sunkumai gali būti įvardinti arba kompiuterinėje etikoje suformuluotu „konceptualios painiavos“[1] terminu, arba baudžiamosios teisės moksle minimu „technologijos ir terminologijos klausimu“. Šis klausimas profesoriaus I. Waldeno susietas su „ribų, šviesiosios linijos (angl. *bright line*)[2] nustatymu ir iš to logiškai išvedamu baudžiamojoje sferoje itin svarbiu teisinio tikrumo (angl. *legal certainty*) principu“[3].

Iš esmės sprendimas, kaip turėtų būti suprantami technologinį aspektą turintys nusikalstamų veikų sudėties požymiai, (atitinkamai, kokios yra jų turinio ribos), priklauso nuo pasirinkto vieno iš galimų jų interpretavimo būdų – technologinio neutralumo (angl. *technological neutrality*) arba technologinio tikslumo (angl. *technological specific*). Minėtą technologijų ir terminologijos problemą bene aiškiausiai leidžia suvokti technologinio neutralumo principas, kuris teisėkūros lygmeniu yra pasitelkiamas informacinių ir komunikacijos technologijų kitimo problemoms spręsti (atsižvelgiant į įstatymo leidėjo valią, gali būti taikomas ir baudžiamosios teisės normų aiškinimo, ir taikymo atveju).

---

1 Moor, J. H. What is Computer Ethics [interaktyvus]. [žiūrėta 2012-09-09]. <http://www.cs.ucdavis.edu/~rogaway/classes/188/spring06/papers/moor.html>.

2 „Šviesiąja linija“ vadinama taisyklė (angl. *bright-line rule*), kuri sudaryta iš objektyvių interpretavimo keitimą draudžiančių arba itin ribotas interpretavimo keitimo galimybes leidžiančių kriterijų. Pagrindinis „šviesiosios linijos“ taisyklės, dažniausiai aptinkamos teismų precedentuose, tikslas yra užtikrinti numatomus ir pastovius teisės normų aiškinimo rezultatus.

3 Walden, I. *Computer Crimes and Digital Investigations*. Oxford University Press, 2007, p. 13.

Pirmiausia reikėtų pasakyti, kad šio principo ištakos nėra tiesiogiai siejamos su baudžiamąja teise[4]. Tačiau kaip vieną iš galimų pavojingų veikų reguliavimo elektroninėje erdvėje priemonių pasirinkus baudžiamąjį teisinį reguliavimą, jo aktualumas šioje srityje yra akivaizdus (pavyzdžiui, sprendžiant, kokia prasmė turėtų būti suteikiama tokiems terminams kaip informacinė sistema, kompiuteris, elektroniniai duomenys ir kt., tuo labiau, kad BK autentiškas šių sąvokų išaiškinimas nėra pateikiamas). Žiūrint iš baudžiamosios teisės pozicijų ir įvertinus teisės ir technikos sąveikos perspektyvas, šis principas leidžia išvengti teisės normų taikymo apribojimų, galinčių kilti dėl jose naudojamų su technologijomis susijusių požymių. Iš esmės, jei technologinio neutralumo principas grindžiamas „diskriminavimo“ draudimu[5], jis reiškia ne ką kita kaip draudimą teikti prioritetą vienai technologijai prieš kitą. Todėl pagal jį nusikalstamos veikos sudėties požymiai turėtų būti apibrėžiami taip, kad netaptų priklausomi nuo informacinių ir komunikacijos technologijų pokyčių, specifinių jų savybių, jei toks priklausomumas nėra įstatymo leidėjo valia. Kaip technologiškai specifinių terminų vartojimo atvejį, sukėlusį nepakankamo kriminalizavimo problemą, būtų galima paminėti kaimyninių valstybių (Latvija, Estija ir kt.) ankstesnius bandymus nustatyti baudžiamąją atsakomybę už disponavimą kenkėjiškomis programomis. Šių valstybių kodeksuose įtvirtinus kompiuterinio viruso terminą liko nekriminalizuotas „Trojos arklių“ ir kitų kenkėjiškų programų kūrimas ir platinimas[6]. Tam tikrų nesklandumų neišvengta ir Lietuvos BK nustatant baudžiamąją atsakomybę už nusikalstamas veikas EDISS. 2003 m. įsigaliojusio naujojo BK XXX skyriuje aprašytose nusikalstamose veikose vartotas terminas „kompiuterinė informacija“, tokiu būdu paliekant neaiškumų, ar terminai „informacija“ ir „duomenys“ turėtų būti, anot įstatymo leidėjo, laikomi sinonimais, ar iš tikro tarp jų yra padarytas sąmoningas skirtumas. Kadangi šis terminų atskyrimas yra gana svarbus[7], mokslinėje literatūroje vis dėlto daryta prielaida, kad šių terminų skirtumo įstatymo leidėjas neįžvelgė, atitinkamai jie vartoti kaip sinonimai[8].

---

4 Technologijoms neutralaus teisinio reguliavimo ir teisės normų taikymo aspektas kaip „gerojo“ reguliavimo principas pirmą kartą Europos Sąjungos lygiu daugiausiai dėmesio sulaukė telekomunikacijų reguliavimo peržiūrėjimo metu (nors vėliau minimas ir kitose srityse).

5 Komisijos komunikate Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui „Dėl 1999 metų apžvalgos „Dėl naujųjų elektroninės komunikacijos infrastruktūros ir susijusių paslaugų pagrindų“ COM (1999) 539 siekis, kad būsimi reguliavimai išliktų technologiškai neutralūs, apibūdintas per technologijų diskriminavimo draudimą, t. y. reguliavimas „neturi nei nustatyti, nei diskriminuoti, teikdamas pirmenybę konkrečios rūšies technologijoms, o turi užtikrinti, kad ta pati paslauga būtų reguliuojama lygiaverčiu būdu, neatsižvelgiant į būdus, kuriais ji yra suteikta“.

6 Štitilis, D. *Teisinės atsakomybės pagrindų nustatymo už neteisėtas veikas elektroninėje erdvėje problemos.* Daktaro disertacija. Socialiniai mokslai, teisė. Vilnius: Lietuvos teisės universitetas, 2002, p. 145.

7 Informacinių sistemų naudotojui elektroniniai duomenys gali būti nematomi ir nesuprantami (pavyzdžiui, duomenų apdorojimo ar jų perdavimo procese), todėl jie informacija tampa tuomet, kai įgyja prasmę. Pakeitus duomenis, informacija, kurią suvokia naudotojas, gali ir nekisti. Pavyzdžiui, neteisėtai padarius pakeitimus kompiuterio *host rinkmenoje* (angl. *host file*), naudotojas gali būti nukreipiamas į suklastotus elektroninės bankininkystės puslapius. Atrodytų, kad pakeitus elektroninius duomenis, vaizdo informacija, kurią suvoks naudotojas, patekęs į suklastotą puslapį, taip pat turėtų keistis. Tačiau padaryti pakeitimai *host rinkmenoje* naudotojo dažniausiai nebus suvokiami dėl suklastoto puslapio itin didelio panašumo į tikrąjį. Be to, jis nesupras ir užslėptos šio tinklalapio funkcijos (surinkti asmens tapatybės patvirtinimo priemonių duomenis, persiųsti juos į kaltininko sukurtas elektroninio pašto dėžutes ir pan.).

8 *Informacinių technologijų teisė.* Sauliūnas, D. (red.). Vilnius: NVO Teisės institutas, 2004, p. 529.

Taip pat galimybę baudžiamosios teisės kontekste kalbėti apie technologinio neutralumo principo taikymą, jo privalumus ir trūkumus suteikia Konvencijos dėl elektroninių nusikaltimų aiškinamajame rašte nurodytas nacionalinėje teisėje įgyvendintinų ir su materialine baudžiamąja teise susijusių nuostatų interpretavimo būdas. Konvencijoje, nustačius minimalius nusikalstamų veikų elektroninėje erdvėje sudėties požymiams keliamus reikalavimus, neišvengta su informacinių ir komunikacijos technologijomis susijusios terminijos. Atsižvelgiant į tai Konvencijos aiškinamojo rašto 36 punkte įtvirtintas jos įgyvendinimui nacionalinėje teisėje svarbus išaiškinimas, kad „nors materialinės baudžiamosios teisės nuostatos yra susietos su nusikaltimais, padaromais naudojant informacines technologijas, Konvencija vartoja technologiškai neutralią kalbą, kad teisės pažeidimai, už kuriuos baudžiama pagal baudžiamuosius įstatymus, galėtų būti taikomos abiem – naudojamoms dabartinėms ir būsimosioms, technologijoms“ (36 punktas)[9].

2. Technologinio neutralumo principo taikymo problemos ir galimi jų sprendimo būdai

Nors technologinio neutralumo principas atrodytų galintis išspręsti gana daug tiek teisėkūros, tiek ir baudžiamosios teisės normų aiškinimo problemų, bet iš tikro jis kelia ir nemažai jo praktinio taikymo klausimų. Iš jų bene svarbiausi būtų, kaip užtikrinti technologijoms neutralų nusikalstamos veikos sudėties požymių interpretavimą ir kaip pasiekti, kad toks požymių aiškinimas būtų suderintas su legalumo (lot. *nullum crimen, nulla poene sine lege*) ir teisinio tikrumo principais.

Nagrinėjant pirmąjį klausimą, pirmiausia reikėtų atkreipti dėmesį į tai, kad tinkamų terminų parinkimas, BK aprašant nusikalstamų veikų EDISS sudėtis, ir technologijoms neutralus jų aiškinimas nėra taip paprastai įgyvendinamas tikslas – terminai, turintys ryšį su informacinių ir komunikacijos technologijomis, niekada nebus visiškai technologiškai neutralūs. Be to, reiktų sutikti su L. B Mose‘o išsakyta nuomone, kad „neįmanoma parengti pakankamai tikslų ir aiškų įstatymo projektą, kuris apimtų kiekvieną galimą technologijų pokytį“[10].

Daugelis minėto principo įvairius aspektus nagrinėjusių mokslininkų (I. M. van der Haar, P. Ohm., B. J. Koops ir kt.)[11] neutralumo technologijų atžvilgiu įgyvendinimą pirmiausia siejo su tinkamu jų apibrėžimų konstravimu. Kuriant teisinį reguliavimą, anot I. M. van der Haaro, „turėtų būti pasirenkamos į funkcijas nukreiptos definicijos, kurios,

9 The Explanatory Report to the Convention on Cybercrime [interaktyvus]. [žiūrėta 2012-08-26]. <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>.

10 Reed, C. Taking Sides on Technology Neutrality. *SCRIPTed*. 2007, 4(3): 263–284.

11 Van der Haar, I. M. Technological Neutrality: What Does It Entail? [interaktyvus]. [žiūrėta 2012-09-06]. <http://www.itseurope.org/ITS%20CONF/istanbul2007/downloads/paper/01.08.2007_Haar,%20Ilse%20van%20der_%20technological%20neutralityIstanbul.pdf>; Ohm, P. The Argument Against Technology – Neutral Surveillance Laws. *Texas Law Review*. 2010, 88(7): 1687; Koops, B.-J. Should ICT Regulation be Technology-Neutral? [interaktyvus]. [žiūrėta 2012-09-06]. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=918746>.

į jas neįtraukus užuominų apie pačias technologijas, būtų priklausomos tik nuo funkcijas žyminčių sąvokų.“[12] Į poveikio, funkcijų ir bendriausių požymių, o ne konkrečios rūšies technologijų svarbą taip pat atkreipė dėmesį ir P. Ohm, jis technologinio neutralumo užtikrinimą susiejo su „plačios, atviros tekstūros terminais, kurie nusako tikslus, poveikį, funkcijas ir kitas bendras savybes“[13]. Jei tokie siūlymai būtų vertinami iš baudžiamosios teisės pozicijų, jie reikštų, kad prioritetas formuluojant ir aiškinant su technologijomis susijusius požymius turėtų būti teikiamas technologijų funkcijas, o ne pačias technologijas numatančioms sąvokoms. Būtent tai leistų išvengti galimų baudžiamosios teisės spragų pakitus vienai ar kitai technologijai.

Vienas iš tokios definicijos pavyzdžių – Konvencijos dėl elektroninių nusikaltimų 1 straipsnyje pateiktas kompiuterinės sistemos apibrėžimas. Pagal jį „kompiuterinė sistema – tai įtaisas arba tarpusavyje sujungtų ar susijusių įtaisų grupė, iš kurių vienas ar daugiau pagal programą automatiškai apdoroja duomenis“[14]. Konvencijos aiškinamojo rašto 23 punkte šis apibrėžimas detalizuotas, kad „Konvencijoje kompiuterinė sistema yra prietaisas, sudarytas iš aparatinės įrangos ir programinės įrangos, sukurtos apdoroti skaitmeninius duomenis. Jis gali apimti įvesties, išvesties ir saugojimo priemones. Jis gali būti vienas arba gali būti sujungtas tinklu su kitais panašiais prietaisais“[15]. Kaip matyti, Konvencijoje pateiktu kompiuterinės sistemos sąvokos apibrėžimu nebuvo siekta tiksliai išspręsti šios sąvokos apibrėžties problemą – kompiuterinės sistemos terminas aprašytas gan abstrakčiomis sistemos atliekamomis funkcijomis. Be kita ko, Konvencijos dalyvėms taip pat suteikta diskrecija atsisakyti pažodinio šių nuostatų įgyvendinimo (22 punktas)[16].

Vis dėlto iš pirmo žvilgsnio atrodanti gan pažangi daugelio autorių keliama į technologijų funkcijas orientuoto apibrėžimo idėja baudžiamosios teisės kontekste galėtų sulaukti ir kritikos. Pirma, gana abstrakčios sąvokos neleidžia nustatyti baudžiamosios teisės veikimo ribų, antra, aiškiai neapibrėžto turinio požymiai gali neatitikti legalumo ir teisinio tikrumo principų reikalavimų.

Todėl pereinant prie antrojo klausimo analizės, kaip pavyzdį būtų galima paminėti jau aptartą Konvencijoje dėl elektroninių nusikaltimų pateiktą gana abstraktų ir į sistemos funkciją (automatinį duomenų apdorojimą) orientuotą kompiuterinės sistemos apibrėžimą. Sukonstruotas tokiu būdu jis turi itin daug bendrumų su visomis informacijos apdorojimo technologijomis, nes jos visos yra skirtos apdoroti duomenis ar informaciją – „kelyje nuo pradinių duomenų iki reikiamų rezultatų gavimo visos atliekamos procedūros vienaip ar kitaip apdoroja jiems pateiktus duomenis.“[17] Būtent šis dviprasmiškumas gali lemti, kad nusikalstamų veikų EDISS požymių apimtys ir apskritai jų suvokimas, neatsižvelgus į įstatymo leidėjo tikslus formuluojant vieną ar kitą nusikalstamų veikų sudėtį, gali kaskart skirtis.

---

12 Van der Haar, I. M., *supra* note 11.

13 Ohm, P., *supra* note 11, p. 1687.

14 Europos Tarybos konvencija dėl elektroninių nusikaltimų. *Valstybės žinios*. 2004, Nr. 36-1188.

15 The Explanatory Report to the Convention on Cybercrime, *supra* note 9.

16 *Ibid*.

17 Skyrius, R.; Mikalauskienė, A.; Zalieckaitė, L. *Informacijos ir komunikacijos technologijos*. Vilnius: UAB „Vilniaus spauda“, 2008, p. 166.

Šis vienas iš technologijų ir terminologijos problemos aspektų neliko nepastebėtas ir mokslinėje literatūroje – P. Ohm teigė, kad technologijoms neutralios nuostatos „padeda išvengti pernelyg siauro reguliavimo leisdamos pernelyg platų“[18]. Į technologinio neutralumo principo savybę išplėsti teisinį reguliavimą nors ir artimoms, bet skirtingoms sritims atkreipė dėmesį ir I. M. van der Haar[19].

Baudžiamosios teisės kontekste pernelyg plataus baudžiamojo teisinio reguliavimo problemą šiuo atveju geriausiai atspindi „perkriminalizavimo“ (angl. *over–criminalization*) terminas. Apie „perkriminalizavimą“ iš esmės galima kalbėti, kai „baudžiamoji teisė pradeda veikti už savo teisėtų funkcijų ribų“[20], kas dažniausiai reiškia ir piktnaudžiavimą baudžiamąja teise. Šios ribų problemos analizė yra neatsiejama nuo baudžiamosios teisės principų sistemoje esančių legalumo (lot. *nullum crimen, nulla poene sine lege*) ir kaltės (lot. *nullum crimen, nullum poena sine culpa*) principų. Būtent per jų reikalavimų įgyvendinimą „užtikrinama baudžiamųjų įstatymų leidybos ir jų taikymo atitiktis Konstitucijai ir joje įtvirtintiems bendriesiems teisės principams (teisinės valstybės, humanizmo, teisingumo, lygiateisiškumo, proporcingumo, protingumo ir kt.).“[21]

Kalbant apie „perkriminalizavimo“ pavojų, nusikalstamų veikų EDISS doktrinoje atkreiptas dėmesys į gana įdomią situaciją – didėjant skaičiui asmenų, naudojančių informacines ir komunikacijos technologijas, taip pat įvairovei prietaisų, kurie gali atlikti įvesties, išvesties ir duomenų apdorojimo funkcijas, kyla sunkumų nustatant, kas iš tikro gali būti laikoma kompiuteriu. Pavyzdžiui, mobiliųjų technologijų, galinčių atlikti minėtas funkcijas ir būti tinklo dalimi (sujungus dvi – mobiliojo ryšio ir tinklo, technologijas), prilyginimas kompiuteriams jau neturėtų kelti abejonių. Tačiau mokslinėje literatūroje taikliai pastebima, kad rankiniai bevieliai prietaisai, tokie kaip, pavyzdžiui, išmanieji telefonai, gali neatitikti daugumos žmonių suvokimo, kas yra kompiuteris[22].

Todėl pritarus gana lanksčioms ir besivystančioms technologijoms pritaikomoms sąvokoms, mokslinėje literatūroje vis dėlto pastebėta ir neigiama tokio aiškinimo pusė. Pernelyg lanksčios sąvokos veda prie pernelyg plačios ir dažnai nenuspėjamos jų apimties (angl. *over-inclusiveness*). Todėl, nors ir klasikinėmis funkcijomis apibūdinama, kompiuterio sąvoka[23] gali apimti „įvairius namų apyvokos ar kitus prietaisus, dėl kurių paprastai nebūtų taikomos kompiuterinių nusikaltimų nuostatos. Pavyzdžiui, veiksmai, kuriais paleidžiama saugos signalizacija, <...> gali būti priežastis kompiuteriui atlikti funkciją.“[24] Taip pat kompiuteriu gali būti laikomas nešiojamas skaičiuotuvas, kompiuterinė sistema automobilyje, Mp3 ar DVD grotuvas, net ir tokie namų apyvokos daiktai kaip šaldytuvas, nes jie visi pajėgūs atlikti duomenų apdorojimo funkciją[25]. Todėl, atsižvelgdamas į įvairių prietaisų kompiuterizavimo tendenciją, I. Walden iškėlė idėją, kad

18 Ohm, P., *supra* note 11, p. 1686.

19 Van der Haar, I. M., *supra* note 11.

20 Ashworth, A. Conceptions of Overcriminalization. *Ohio State Journal of Criminal Law*. 2008, 5: 407.

21 Fedosiuk, O. Baudžiamoji atsakomybė kaip kraštutinė priemonė (*ultima ratio*): teorija ir realybė. *Jurisprudencija.* 2012, 19(2): 716.

22 Walden, I., *supra* note 3, p. 16.

23 Blundell, B. G. *Computer Systems and Networks*. Thomson, 2007, p. 2−3.

24 Clough, J. *Principles of Cybercrime*. Cambridge Univercity Press, 2010, p. 55.

25 *Ibid*., p. 56.

„ateitis pranašauja galimybę sukurti namų apyvokos prietaisus su įmontuojamomis sistemomis ir prieiga prie interneto, suteikiančia išplėstas jų nuotolinio valdymo galimybes, kas neišvengiamai leis atsirasti visiškai naujoms nusikalstamo elgesio formoms.“[26]

Kitas svarbus aspektas yra tas, kad teisinis reguliavimas, laikantis technologinio neutralumo principo, yra ne tik abstraktus teisėkūros metu naudojamų technologijų atžvilgiu, bet taip pat siejamas ir su galimomis jų ateities perspektyvomis. Kadangi jis apima ir tas technologijas, kurių išradimas ar vystymasis iš anksto negali būti numatytas, ribiniais technologijų panaudojimo atvejais gali kilti abejonių dėl jo atitikties legalumo ir teisinio tikrumo principams. Mokslinėje literatūroje atkreipiamas dėmesys, kad būtent vienas iš legalumo principo aspektų yra siejamas su maksimaliu nusikalstamos veikos požymių aprašymo tikslumu ir aiškumu[27]. Taip pat išsamaus, tikslaus ir aiškaus nusikalstamos veikos teisinio apibūdinimo reikalavimai kyla iš teisinės valstybės principo[28], kurio įvairūs turinio aspektai ir iš jo išvedamo teisinio saugumo imperatyvai suformuluoti Lietuvos Respublikos Konstitucinio Teismo jurisprudencijoje[29].

Beje, ši galinti kilti problema yra aktuali ne tik tais atvejais, kai įstatymų leidėjas nenumatė autentiško su technologijomis susijusių sąvokų išaiškinimo (kaip tai padaryta Lietuvos BK), bet ir tuomet, kai toks aiškinimas yra pateikiamas įstatymų (statutų) lygmeniu. Sąvokos numatytos įstatymuose (statutuose) dėl technologinio neutralumo principo taikymo vis tiek išlieka gana abstrakčios ir tiksliai neleidžia apibrėžti jų ribų. Kaip tokios problemos kilimo ir jos sprendimo pavyzdį būtų galima paminėti JAV apeliacinio teismo (7-osios apygardos) 2005 m. balandžio 18 d. sprendimą byloje *Jungtinės Amerikos Valstijos prieš Mitrą (US v. Mitra)*[30], kuriuo kaltininkas buvo nuteistas pagal Jungtinių Amerikos Valstijų įstatymų sąvado (angl. *code*) 18 dalies (Nusikaltimai ir baudžiamasis procesas) 1030 paragrafo „a“ dalies 5 punktą (18 U.S.C. § 1030(a)(5)[31] už tyčinį įsikišimą į kompiuterinės sistemos darbą.

Kaltininkas neteisėtam Smartnet II sistemos valdymui, jos veikimo analizei ir signalo, kuris perėmė sistemos kontrolę, siuntimui naudojo aparatinę (angl. hardware) ir programinę (angl. software) įrangą sudarantį prietaisą. Smartnet II kompiuterinė radijo sistema (žinoma kaip „radialinė sistema“ (angl. trunking system) naudota policijos, gaisrinės, greitosios medicinos pagalbos iškvietimo ir kitais kritiniais atvejais. Laikotarpiu tarp 2003 metų sausio – rugpjūčio mėnesių Smartnet II sistema tapo neprieinama jos naudotojams dėl stipraus visus miesto ryšių bokštus „uždengusio“ signalo. Vėliau, nutraukęs sistemos blokavimą, kaltininkas kiekvieną pasibaigusį jos naudotojų pokalbį papildydavo erotine moters dejone.

---

26 Walden, I., *supra* note 3, p. 16.

27 Fedosiuk, O., *supra* note 21, p. 726.

28 Švedas, G. Veikos kriminalizavimo kriterijai: teorija ir praktika. *Teisė*. 2012, 82: 21.

29 Lietuvos Respublikos Konstitucinio Teismo 2001 m. liepos 12 d. nutarimas; Lietuvos Respublikos Konstitucinio Teismo 2003 m. gegužės 30 d. nutarimas; Lietuvos Respublikos Konstitucinio Teismo 2006 m. sausio 16 d. nutarimas ir kt.

30 *United States v. Mitra*, No. 04-2328, April 18, 2005-US 7th Cir. [interaktyvus]. [žiūrėta 2012-09-04]. <http://caselaw.findlaw.com/us-7th-circuit/1031818.html>.

31 The Code of the United States [interaktyvus]. [žiūrėta 2012-09-04]. <http://www.law.cornell.edu/uscode/text/18/1030>.

Nesutikdamas su prokuroro nuomone, kad Smartnet II yra kompiuteris[32], kaltininkas teigė, kad jo veiksmais buvo sutrikdyta tik radijo sistema. Anot jo, jei radijo sistema yra kompiuteris, tuomet kiekvienas telefonas ar „iPod'as", kiekviena bevielio ryšio stotis kavinėse ir daugelis kitų prietaisų turi būti laikoma kompiuteriu. Toks aiškinimas būtų pernelyg platus, taip pat jo tokio nebuvo įmanoma numatyti priimant minėtas nuostatas.

Vis dėlto teismas, akcentuodamas itin spartų technologijų vystymąsi, atmetė tokius kaltininko argumentus. Teismo manymu, nors įstatymų leidėjas galėjo ir nežinoti apie „radialinę sistemą", jis, suvokdamas moderniame pasaulyje vykstančius pokyčius, nustatė bendro pobūdžio normas, o ne konkrečių uždraustų veikų sąrašą. Kuo daugiau prietaisų, teismo nuomone, turės dirbtinį intelektą, tuo labiau plėsis numatytų nuostatų apimtys. Nors tokia tendencija gali būti užuomina peržiūrėti reguliavimą, tačiau tai neįgalina teismo suteikti esamai nuostatai siauresnę apimtį, nei matyti pagal jos formuluotę. Be to, teismo neįtikino kaltininko teiginiai, kad baudžiamosios normos buvo išaiškintos tokiu būdu, kurio nebuvo įmanoma tikėtis. Teismas nesutiko su tuo, kad buvo pažeistas protingo žmogaus (angl. reasonable man) kriterijus, nes iš tikro nuostatos buvo išaiškintos taip, kaip jos suformuluotos, o ne taip, kaip norėjo kaltininkas.

Šioje situacijoje komunikavimui naudota sistema (*Smartnet II*) dėl savo sandaros ir atliekamų funkcijų[33] aiškiai atitiko kompiuterį leidžiančius identifikuoti požymius. Tačiau vis dėlto toks atvejis rodo ateityje galinčias kilti gana rimtas abejones dėl informacinių ir komunikacijos technologijas žyminčių abstrakčių sąvokų išaiškinimo tikslumo ir tinkamo teisės normų taikymo. Kadangi technologijoms neutralūs terminai, kaip minėta, dažniausiai yra bendrojo pobūdžio, todėl ribiniais neteisėtų technologijų panaudojimo atvejais abejonė dėl neaiškios normos tinkamo interpretavimo gali kilti visuomet. Atitinkamai ši abejonė bus siejama su legalumo ir teisinio tikrumo principų reikalavimų pažeidimais.

Kadangi iš tikro nėra paprasta pateikti apibrėžimą, kuris, pavyzdžiui, leistų kalbėti ne apie kišeninį skaičiuotuvą, o apie skreitinį kompiuterį (angl. *laptop computer*)[34], todėl šios problemos sprendimo variantai galėtų būti siejami ne tik su bandymais kiek įmanoma tinkamiau apibrėžti technologijas žyminčias sąvokas. Šiuo aspektu ne mažiau svarbus yra praktinis baudžiamojo įstatymo taikymo lygmuo, t. y. teismų praktika.

Įstatymo leidėjui baudžiamajame įstatyme nepateikus autentiško požymių išaiškinimo, vertinimo kriterijų paieška ir sąvokos turinio bei jos ribų nustatymas paliekamas

32 Jungtinių Amerikos Valstijų įstatymų sąvado 18 dalies 1030 paragrafo „e" dalies 1 punkte kompiuteris yra apibrėžiamas kaip „elektroninis, magnetinis, optinis, elektrocheminis arba kitas greitaeigis duomenų apdorojimo prietaisas, atliekantis logines, aritmetines ar saugojimo (laikymo) funkcijas, apimantis bet kokias duomenų saugojimo (laikymo) ar komunikavimo priemones, tiesiogiai susijusias arba atliekančias veiksmus kartu su šiuo prietaisu. Tačiau šis terminas neapima automatinių rašomųjų mašinėlių arba rinkimo mašinų (angl. *typesetter*), nešiojamų rankinių skaičiuotuvų ar kitų panašių prietaisų". Pagal prokuroro išsakytus argumentus, *Smartnet II* sistema turėtų būti pripažįstama kompiuteriu, nes ją, be kitų dalių, sudaro lustas (angl. *chip*), kuris, valdymo kanalu gavęs signalą, atlieka didelės spartos duomenų apdorojimo funkciją.

33 Kompiuterio aparatinė ir programinė įranga pagal gautus signalus paskirstydavo pokalbius atviriems kanalams, taip pat susiedavo daugybinius vienetus į „komunikavimo grupę," kuri leisdavo pareigūnams tarpusavyje palaikyti bendrą pokalbį.

34 Clough, J., *supra* note 24, p. 54.

teismo diskrecijai – „apibrėždamas įstatymo tekstą tik bendromis sąvokomis, tačiau neatskleisdamas jų turinio ir nenurodydamas apibrėžties kriterijų įstatymų leidėjas neišvengiamai plačiai nubrėžia įstatymo taikymo sferą, taip tarsi išplėsdamas teismo pasirinkimo galimybes <...>.“[35] Tačiau kalbant apie precedentus negalima užmiršti ir teismo, sprendžiančio teisės aiškinimo klausimus, diskrecijos ribų, t. y. kokį turinį teismas gali suteikti su informacinių ir komunikacijos technologijomis susijusiems požymiams, kokiais kriterijais vadovaudamasis turi spręsti, ar padaryta veika turi būti pripažįstama nusikalstama.

Todėl sprendžiant baudžiamosios atsakomybės kilimo klausimą, vienu iš kriterijų galėtų būti laikomos tos aplinkybės, kurios yra vertinamos kriminalizuojant nusikalstamas veikas. Jei veikos pavojingumas, baudžiamosios teisės funkcionavimo sritis ir ribos, baudžiamosios teisės kaip paskutinės priemonės (lot. *ultima ratio*) ir kiti[36] pagrindai leidžia spręsti dėl kriminalizavimo pagrįstumo, tai jie galėtų apibrėžti ir neaiškios baudžiamojo įstatymo normos taikymo ribas. Pavyzdžiui, kalbant apie *ultima ratio* principo praktines taikymo galimybes, mokslinėje literatūroje atkreiptas dėmesys, kad šis principas reikalauja nustatyti tinkamą veikos pavojingumą, nes abstrakčios definicijos kartu su tikrai pavojingu elgesiu gali apimti ir abejotino pavojingumo veikas[37].

Kitas galimas variantas – baudžiamosiose bylose, nustačius neteisėtą informacinių ir komunikacijos technologijų panaudojimo faktą, jų pažinimui pasitelkti specialias žinias turintį ekspertą arba specialistą. Eksperto (specialisto) technikos žinios gali padėti nustatyti ne tik vieno ar kito su informacinių ir komunikacijos technologijomis susijusio termino turinį, bet ir turėti įtakos nusikalstamos veikos kvalifikavimui[38]. Tačiau, vertinant ekspertizės akte (specialisto išvadoje) pateikiamas išvadas, turėtų būti atsižvelgta į tai, kad jos yra tik prielaida teisinei išvadai, nes nusikalstamos veikos sudėties požymių nustatymas yra teismo, o ne ekspertų (specialistų) kompetencija. Tai, kad „ekspertai sprendžia tik techninius klausimus, o teismas – tik teisinius“, ir tai, kad „tik teismo kompetencijoje yra vertinti ekspertų išvadas ir sutikti su jomis pilnai ar iš dalies“[39], nes „įrodymų vertinimas ir jais pagrįstų išvadų byloje sprendžiamais klausimais darymas yra teismo, priimančio baigiamąjį aktą, prerogatyva“[40], ne kartą atkreipė dėmesį ir Lietuvos Aukščiausiasis Teismas. Tokia pozicija yra svarbi ta prasme, kad pagal eksperto (specialisto) išvadą panaudotą prietaisą priskyrus informacinėms ir komunikacijos technologijoms, to neturėtų pakakti sprendimui, kad padaryta nusikalstama veika EDISS. Šis saugiklis siejamas su nusikalstamos veikos sudėties kaip baudžiamosios atsakomybės pagrindo principu (BK 2 straipsnio 4 dalis), įpareigojančiu nustatyti sudėties požymių

35 Pikelis, A. *Baudžiamosios teisėkūros labirintai*. Vilnius: Petro ofsetas, 2011, p. 46.

36 Švedas, G., *supra* note 28, p. 12–24.

37 Fedosiuk, O., *supra* note 21, p. 733.

38 *Baudžiamasis procesas: nuo teorijos iki įrodinėjimo (prof. Eugenijaus Palskio atminimui)*. Mokslo studija. Vilnius: Mykolo Romerio universiteto leidykla, 2011, p. 385.

39 Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2005 m. vasario 22 d. nutartis baudžiamojoje byloje Nr. 2K-187/2005.

40 Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2010 m. spalio 12 d. nutartis baudžiamojoje byloje Nr. 2K-448/2010.

visumą, o ne teikti prioritetą kuriam vienam iš jų. Be abejo, tokiais atvejais išlieka aktualūs ir anksčiau minėti *ultima ratio,* ir kiti tinkamam baudžiamojo įstatymo taikymui svarbūs kriterijai.

Nusikalstamų veikų EDISS kvalifikavimo atveju ne mažiau svarbus ir šių nuostatų priėmimo kontekstas, t. y. pagrindinės priežastys, lėmusios normoje įtvirtintos sąvokos ar požymio nustatymą. Ne veltui mokslinėje literatūroje pabrėžiama, kad tik „tokiu būdu galima kiek įmanoma tiksliau suvokti įstatymo leidėjo ketinimus ir tikslus, įstatymo turinį ir optimaliausias jo veikimo galimybes.“[41]

Todėl apibendrinus būtų galima teigti, kad praktikoje galimos situacijos, kai panaudota priemonė pagal atliekamas funkcijas bus priskiriama informacinėms ir komunikacijos technologijoms, tačiau pati padaryta veika nebus laikoma nusikalstama (nes baudžiamojo įstatymo taikymas neatitiks pagrindinių baudžiamosios teisės principų). Ir atvirkščiai – nustačius visas baudžiamajai atsakomybei kilti būtinas sąlygas, „nėra priežasties veikos nelaikyti nusikalstama vien tik dėl to, kad pagal įprastą suvokimą naudojamas prietaisas nėra apibūdinamas kaip kompiuteris.“[42]

Išvados

1. Nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui sudėties požymių, turinčių technologinį aspektą, turinio ribos priklauso nuo pasirinkto vieno iš galimų šių požymių interpretavimo būdų – technologinio neutralumo (angl. *technological neutrality*) arba technologinio tikslumo (angl. *technological specific*).

2. Nors technologinio neutralumo principo ištakos nėra tiesiogiai siejamos su baudžiamąja teise, tačiau kaip vieną iš galimų pavojingų veikų reguliavimo elektroninėje erdvėje priemonių pasirinkus baudžiamąjį teisinį reguliavimą, jo aktualumas šioje srityje yra akivaizdus. Šis principas, atsižvelgiant į teisės ir technikos sąveikos perspektyvas, leidžia išvengti baudžiamojo įstatymo normų taikymo apribojimų, kylančių dėl jose naudojamų su technologijomis susijusių nusikalstamos veikos sudėties požymių.

3. Technologinio neutralumo principas leidžia užtikrinti teisės ir besivystančių informacinių ir komunikacijos technologijų suderinamumą. Tačiau šio principo suponuotas gana abstraktus baudžiamasis teisinis reguliavimas gali kelti abejonių dėl tokio reguliavimo atitikties legalumo ir teisinio tikrumo principams.

4. Technologinio neutralumo principą taikant baudžiamojoje teisėje, jo taikymo apimtis neišvengiamai siaurina baudžiamosios teisės principai, leidžiantys išvengti pernelyg plataus ir nepagrįsto veikų kriminalizavimo, atitinkamai ir baudžiamosios teisės ribų išplėtimo. Todėl technologinio neutralumo principo tinkamas taikymas galimas tik tuo atveju, jei yra randamas kompromisas tarp šio ir baudžiamojoje teisėje svarbių legalumo ir teisinio tikrumo principų.

---

41 Pikelis, A., *supra* note 35, p. 45.

42 Clough, J., *supra* note 24, p. 57.

Literatūra

Ashworth, A. Conceptions of Overcriminalization. *Ohio State Journal of Criminal Law*. 2008, 5: 407–425.

Baudžiamasis procesas: nuo teorijos iki įrodinėjimo (*prof. Eugenijaus Palskio atminimui*). Mokslo studija. Vilnius: Mykolo Romerio universiteto leidykla, 2011.

Blundell, B. G. *Computer Systems and Networks*. Thomson, 2007.

Clough, J. *Principles of Cybercrime*. Cambridge Univercity Press, 2010.

Europos Tarybos konvencija dėl elektroninių nusikaltimų. *Valstybės žinios*. 2004, Nr. 36-1188.

Fedosiuk, O. Baudžiamoji atsakomybė kaip kraštutinė priemonė (*ultima ratio*): teorija ir realybė. *Jurisprudencija.* 2012, 19(2): 715−738.

Haar van der, I. M. Technological Neutrality: What Does It Entail? [interaktyvus]. [žiūrėta 2012-09-06]. <http://www.itseurope.org/ITS%20CONF/istanbul2007/downloads/paper/01.08.2007_Haar,%20Ilse%20van%20der_%20technological%20neutralityIstanbul.pdf>.

Informacinių technologijų teisė. Sauliūnas, D. (red.). Vilnius: NVO Teisės institutas, 2004.

Koops, B.-J. Should ICT Regulation be Technology-Neutral? [interaktyvus]. [žiūrėta 2012-09-06]. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=918746>.

Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2005 m. vasario 22 d. nutartis baudžiamojoje byloje Nr. 2K-187/2005.

Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2010 m. spalio 12 d. nutartis baudžiamojoje byloje Nr. 2K-448/2010.

Lietuvos Respublikos Konstitucinio Teismo 2001 m. liepos 12 d. nutarimas.

Lietuvos Respublikos Konstitucinio Teismo 2003 m. gegužės 30 d. nutarimas.

Lietuvos Respublikos Konstitucinio Teismo 2006 m. sausio 16 d. nutarimas.

Ohm, P. The Argument Against Technology – Neutral Surveillance Laws. *Texas Law Review*. 2010, 88(7): 1685−1713.

Pikelis, A. *Baudžiamosios teisėkūros labirintai*. Vilnius: Petro ofsetas, 2011.

Reed, C. Taking Sides on Technology Neutrality. *SCRIPTed*. 2007, 4(3): 263–284.

Skyrius, R.; Mikalauskienė, A.; Zalieckaitė, L. *Informacijos ir komunikacijos technologijos*. Vilnius: UAB „Vilniaus spauda“, 2008.

Štitilis, D. *Teisinės atsakomybės pagrindų nustatymo už neteisėtas veikas elektroninėje erdvėje problemos.* Daktaro disertacija. Socialiniai mokslai, teisė. Vilnius: Lietuvos teisės universitetas, 2002.

Švedas, G. Veikos kriminalizavimo kriterijai: teorija ir praktika. *Teisė*. 2012, 82: 12−25.

The Code of the United States [interaktyvus]. [žiūrėta 2012-09-04]. <http://www.law.cornell.edu/uscode/text/18/1030>.

The Explanatory Report to the Convention on Cybercrime [interaktyvus]. [žiūrėta 2012-08-26]. <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>.

United States v. Mitra, No. 04-2328, April 18, 2005-US 7th Cir. [interaktyvus]. [žiūrėta 2012-09-04]. <http://caselaw.findlaw.com/us-7th-circuit/1031818.html>.

Walden, I. *Computer Crimes and Digital Investigations*. Oxford University Press, 2007.

THE TECHNOLOGICAL NEUTRALITY PRINCIPLE AND ITS SIGNIFICANCE IN FORMULATING AND EXPLAINING THE OFFENCES AGAINST THE SECURITY OF ELECTRONIC DATA AND INFORMATION SYSTEMS

Renata Marcinauskaitė

Mykolas Romeris University, Lithuania

Summary. *The article discusses the fundamental aspects of the technological neutrality principle application in explaining the signs of the offences against the security of electronic data and information systems. It also analyses if the legal regulation of being neutral to technologies conforms to the especially important principles of legality and legal certainty in Criminal Law.*

In the sphere of regulation of information and communication technologies, this principle ensures equivalent evaluation of technologies as it forbids giving to any one of them priority over the other. As a result, it helps to avoid restrictions on law application, which arise due to the usage of specific terms related to technologies. If choosing the criminal legal regulation as one of the possible control measures of dangerous acts in cyberspace, this principle becomes relevant when explaining the signs of the offences against the security of electronic data and information systems.

According to the conclusion drawn in the article, the idea of legal regulation being neutral to technologies, which may seem advanced at first sight, in the context of Criminal Law could become open to criticism due to non-conformity of such regulation to the principles of legality and legal certainty. Although the principle of technological neutrality is considered to be an effective instrument when coordinating rapid development of information and communication technologies with the set legal regulation, it cannot guarantee fulfilment of the completeness, accuracy and clarity requirements for legal definition of the criminal act. In the process of resolving the above-mentioned problems, considerable attention is paid not only to the importance of appropriate concepts but also to case law (*court practice). According to the author of the article, the decision to admit or disclaim having committed the criminal act in the case law could be motivated by the criteria of criminalisation* (*decriminalisation*) *and the principles of Criminal Law ensuring appropriate application of Criminal Law.*

Keywords: *technological neutrality principle, technological specific principle, criminalization, the principles of Criminal Law.*

Renata Marcinauskaitė, Mykolo Romerio universiteto Teisės fakulteto Baudžiamosios teisės ir proceso instituto doktorantė. Mokslinių tyrimų kryptys: nusikalstamos veikos elektroninėje erdvėje.

Renata Marcinauskaitė, Mykolas Romeris Univesity, Faculty of Law, Institute of Criminal Law and Procedure, Doctoral Student. Research interests: cybercrime.