LIETUVOS TEISĖS UNIVERSITETAS
VALSTYBINIO VALDYMO FAKULTETAS
TEISINĖS INFORMATIKOS KATEDRA

RIMAS VALENTA
INFORMATIKOS TEISĖS STUDIJŲ PROGRAMA

NUSIKALTIMAI ELEKTRONINIŲ RYŠIŲ SEKTORIUJE

Mokslinis tiriamasis darbas

Darbo vadovas –
dr. Darius Štitilis

Vilnius, 2004

TURINYS

ĮVADAS

Įžengėme į XXI amžių, kuris jau prieš du dešimtmečius buvo pavadintas kompiuterių ir ryšių amžiumi. Jų dėka visuomenė perėjo į aukštesnįjį raidos etapą – informacinę visuomenę.

Daugeliui atrodo, kad komunikacijos, kurios lietuviškai reiškia ryšius, yra kažkas nauja. Nors kompiuterinių ryšių tinklų menas iš tikrųjų yra naujas, tačiau jų koncepcija gana sena. Ji gimė XIX amžiuje. Šiuolaikinei kompiuterinių ryšių tinklų technologijai padėjo atsirasti trys dideli išradimai: telegrafas, telefonas ir teletaipas. Prisiminkime komunikacijų ištakas.

Samuelis Morzė, telegrafo ir jo vardu pavadinto kodo tėvas, neatpažintų kompiuterio, bet atpažintų kompiuterinių ryšių logiką ir paprastumą, savo kodo kompiuterinį alfabetą. Morzės telegrafas elektros impulsais siuntė laiškus ir skaičius iš vienos vietos į kitą. Dabartiniai kompiuteriai daro tą patį, tik kur kas greičiau. Telegrafas iš tikrųjų buvo pirmoji skaitmeninių ryšių priemonė.

Aleksandras Belas taip pat neatpažintų modemo, bet atpažintų savo telefoninio ryšio sietuvą (interfeisą), kurie iki šiol jungia daugelį telefonų su centrinėmis telefonų stotimis. Pasaulinis telefoninių ryšių tinklas labai pasikeitė, bet laidai tarp mūsų namų ar įstaigų bei telefono stoties nedaug pakito nuo Belo laikų. Išradėjai daug padarė sujungdami skaitmeninius kompiuterius su analogiškomis telefonų linijomis.

Emilio Bodo (Baudot) išradimas labai neišgarsino jo autoriaus, bet jo daugkartinio spausdinimo telegrafas buvo kompiuterių spausdinimo ir galinio įrenginio (terminalo) pirmtakas. Kiti išradėjai patobulino Bodo išradimą, ir gimė teletaipas. Teletaipai sujungė pasaulį TELEX tinklais, kuriais tarp šalių ir žemynų siunčiami spausdinti dokumentai. Šie trys išradimai yra telekomunikacijų (teleryšių) pagrindas. Jie atvėrė duris kompiuterių ir elektroninių ryšių amžiui.

Girdėdami žodį „komunikacijos“, įsivaizduojame vietinių telefonų, kabelinės, palydovinės televizijos ir kompiuterių ryšių tinklus bei radijo signalus. Pirmosios elektroninių ryšių linijos buvo telefono linijos tarp dviejų taškų. Didėjant šių taškų skaičiui, ryšių tinklas XX amžiuje virto Žemės rutulį apgaubusiu tinklu. Didėjant perduodamos informacijos kiekiui, reikėjo naudoti vis didesnius dažnius. Taip tas tinklas tapo sudarytas ne tik iš laidų, kurie jau nebegalėjo patenkinti visų poreikių, bet ir kabelių, mikrobangų radiorėlinių linijų ir bangolaidžių, nutiestų tarp miestų ir valstybių, optinio ryšio linijų ir ryšių palydovų.

Iki 1990 metų daugiau dėmesio buvo skiriama informacijos teisei, o pastarąjį dešimtmetį daugiau problemų kelia elektroninė informacijos pateikimo forma, naujos informacijos apdorojimo, perdavimo ir saugojimo technologijos. Pastaruoju metu ypač paspartėjo informatikos, komunikacijų, žinių technologijų plėtra. Informatikos priemonių ir paslaugų, teikiamų tuo pačiu tinklu, susiliejimas turi netikėtų pasekmių ir iš esmės provokuoja juridinius

pamąstymus. Internetas nuo šiol turi daugiau kaip tris šimtus milijonų vartotojų ir platina korespondenciją, duomenis, balsą, vaizdą, radiją, televiziją, spaudą. Sparčiai auga elektroninė komercija, elektroninė bankininkystė, kuriamos elektroninės balsavimo sistemos, o web tampa masine rinka. Vis daugiau žmonių veiklos yra susieta su elektroniniais ryšiais, kai tuo tarpu kiekvienas internautas-vartotojas yra vis mažiau apsaugotas. Toks spartus informacinių technologijų įsiveržimas į šiuolaikinės visuomenės gyvenimą, be teigiamų poslinkių, sukėlė ir daugybę problemų, visų pirma informacijos apsaugos srityje. Nors šios problemos egzistavo ir „klasikinėse“ telekomunikacinėse sistemose – telegrafo, telefono, radijo ryšio, tačiau, atsiradus pasauliniam tinklui – internetui, jos įgavo visai kitokį pobūdį, mastą bei naujas formas. Kita priežastis – komunikuojamos informacijos vertingumas. Todėl natūralu, kad informacijos apsauga turėtų būti teisiškai reglamentuojama. Tam būtina nustatyti apsaugos priemones visose srityse, susijusiose su elektroninių ryšių panaudojimu, nes šiai veiklai kyla vis didesnė grėsmė dėl šioje srityje daromų nusikaltimų.

Pažymėtina, kad tema „Nusikaltimai elektroninių ryšių sektoriuje“ yra novatoriška. Visuose iki šiol rašytuose darbuose buvo nagrinėjami tik kompiuteriniai nusikaltimai ir informaciniai nusikaltimai, o nusikaltimai elektroninių ryšių sektoriuje nebuvo aptariami:

-S.Gudmonas. Pavojingų veikų naudojant kompiuterinę įrangą tyrimo problemos: diplominis darbas.- 1996; 343.533: 681.3(04).

-R.Čėsna. Nusikaltimai kompiuteriniuose tinkluose: diplominis darbas.- 1997; 343.533:681.3 (04).

-D.Štitilis. Nusikaltimai kompiuterinėse sistemose: diplominis darbas.- 1997; 343.533:681.3 (04).

-V.Urbonavičius. Neteisėta prieiga prie kompiuterinės informacijos : kriminalizavimo aspektai : diplominis darbas.- 2003; 343.533: 681.3(04).

-A.Vosylienė. Telekomunikacijų rinkos teisinis reguliavimas Lietuvos Respublikoje: magistro baigiamasis darbas.- 2003; 347.725(474.5)(04).

Tačiau iki šiol neišnagrinėti klausimai: nusikaltimai elektroninių ryšių sektoriuje; nusikaltimų elektroninių ryšių sektoriuje objektai, klasifikavimas ir požymiai; precedentai, nagrinėjant bylas, susijusias su nusikaltimais elektroninių ryšių sektoriuje; pasaulinė ir Europos Sąjungos valstybių narių patirtis reglamentuojant nusikaltimus elektroninių ryšių sektoriuje; Lietuvos teisinės bazės, reglamentuojančios nusikaltimus elektroninių ryšių sektoriuje, lyginamasis įvertinimas ir kt.

Šio darbo objektas – nusikaltimai elektroninių ryšių sektoriuje ir jų reglamentavimas (įskaitant atsakomybės už tokius nusikaltimus nustatymą).

Darbo tikslas – išanalizuoti nusikaltimų elektroninių ryšių sektoriuje rūšis ir požymius bei pabandyti nustatyti, kokia baudžiamoji atsakomybė už nusikaltimus elektroninių ryšių sektoriuje būtų racionaliausia ir atitiktų šiuolaikinės baudžiamosios teisės tendencijas.

Norint pasiekti užsibrėžtą tikslą, reikia *(pagrindiniai uždaviniai)*:

- apibūdinti elektroninių ryšių sektorių, suformuluoti elektroninių ryšių sampratą, išsiaiškinti „elektroninės erdvės“ sąvoką ir nustatyti jos santykį su „elektroniniais ryšiais“;
- išanalizuoti nusikaltimus elektroninių ryšių sektoriuje, atskleisti jų rūšis ir požymius;
- apžvelgti nusikaltimų elektroninių ryšių sektoriuje precedentus;
- palyginamuoju aspektu apžvelgti nusikaltimų elektroninių ryšių sektoriuje reglamentavimą tarptautiniu (regioniniu) mastu ir kai kuriose užsienio valstybėse;
- išanalizuoti nusikaltimų elektroninių ryšių sektoriuje reglamentavimą Lietuvoje ir pateikti pasiūlymus dėl teisinės bazės tobulinimo.

Tokia užduotis nėra lengva jau vien todėl, kad autoriaus pasirinkta tema yra novatoriška, ir literatūros apie nusikaltimus elektroninių ryšių sektoriuje tiek lietuvių kalba, tiek ir kitomis kalbomis nėra. Todėl šios studijos pagrindas – internete rasti straipsniai, diskusijų ir konferencijų medžiaga, naujų įstatymų projektai, žinomų mokslininkų darbai.

Rašant šį darbą buvo naudojamas aprašomasis, sisteminės analizės, dokumentų analizės, loginis, lyginamasis bei statistinės analizės metodai.

Pažymėtina, kad nusikaltimai elektroninių ryšių sektoriuje pasauliniu mastu uždraudžiami tarptautinių sutarčių, dažniausiai – konvencijų pagalba. Europos Sąjungos mastu – rekomendacijų, sprendimų ir iš dalies direktyvų pagalba. Lietuvoje baudžiamoji atsakomybė už nusikaltimus elektroninių ryšių sektoriuje yra nustatyta tik Baudžiamajame kodekse.

Rašant šį darbą naudojami žemiau nurodyti terminai, kitų terminų sąvokos atitinka įstatymuose nurodytas sąvokas:

1. *Elektromagnetinis, akustinis, mechaninis arba kitoks įrenginys (pranc.* dispositif electromagnetique, acoustique, mecanique ou autre) – reiškia bet kokį įrenginį arba aparatą, kuris yra naudojamas arba gali būti naudojamas perimti privatų ryšį, išskyrus garsinį aparatą.
2. *Privačios komunikacijos* – reiškia bet kokį žodinį ryšį arba bet kokį telefoninį ryšį (telekomunikaciją), kuriuo vienas asmuo perduoda informaciją kitam asmeniui, pagrįstai tikėdamas, kad ši informacija nebus prieinama pašaliniam asmeniui, įskaitant bet kokį telefoninį ryšį radijo ryšio pagrindu.

1.Elektroninių ryšių sektoriaus apibūdinimas ir elektroninių ryšių samprata

Telekomunikacijų sektoriaus specialistai vienareikšmiškai pastebi, kad tokia sparti kelių pastarųjų metų technologinė pažanga šiame sektoriuje didžiąja dalimi sąlygota vieno veiksnio – konkurencijos, kaip pagrindinio ekonominės veiklos variklio, principų pritaikymo jame.

Kita konkurencijos principų įdiegimo ir technologinio vystymosi išdava – technologinė telekomunikacijų, informacinių technologijų ir televizijos konvergencija. Konvergencija - „[lot.convergens (kilm.convergentis) – susieinantis; suartėjantis], (su) panašėjantis, (su) artėjantis“.[1] Jos pasekmė yra ta, kad skaitmeninės technologijos leidžia teikti tradicines ir naujas komunikacijų paslaugas – balso, duomenų, garso ar vaizdo įvairiais skirtingais tinklais. Pavyzdžiui, balso telefonijos paslaugos gali būti teikiamos tiek tradiciniais fiksuotais telekomunikacijų tinklais, tiek internetu, tiek kabeliniais tinklais. Pati konvergencijos sąvoka šiuo atveju yra daugialypė, t.y. ji apima tiek technologinę konvergenciją arba skaitmeninių technologijų naudojimą įvairiuose komunikacijų sektoriuose, tiek komunikacijų konvergenciją. Jei anksčiau tam tikro tipo tinklas buvo naudojamas specifinei informacijos rūšiai perduoti, tai dabartinės technologijos iš esmės bet kuriuo tinklu leidžia perduoti bet kokią informaciją. Visa tai lemia tiek naujų paslaugų atsiradimą, tiek ir pačių rinkų susiliejimą.

Atsižvelgiant į telekomunikacijų rinkos plėtrą ir spartų technologijų vystymąsi ir siekiant užtikrinti tolesnę jų plėtrą Europos Bendrijoje, XX amžiaus paskutinio dešimtmečio pabaigoje buvo suformuluotas pagrindinis tikslas – nustatyti teisės sistemą, kuri užtikrintų pasikeitusius rinkos poreikius atitinkančią technologijų plėtrą, skatintų kuo įvairesnes paslaugas kuo įvairesniais tinklais. Po ilgų konsultacijų 2000 m. viduryje Europos Komisija Europos Sąjungos lygmeniu pateikė visiškai naują teisės aktų projektų, naujai sureguliuosiančių šią rinką, rinkinį, t.y. pasiūlymus direktyvų pagrindu dėl reguliavimo elektroninių ryšių ir paslaugų, dėl elektroninių ryšių ir aptarnavimo paslaugų, dėl duomenų apdorojimo ir saugumo elektroninių ryšių sektoriuje ir kt. [2]. 2002 metais visos šešios direktyvos buvo priimtos, o 2003 metais Europos Sąjungos šalys narės šių direktyvų nuostatas inkorporavo į savo teisines sistemas. Plačiau neanalizuojant visų aukščiau minėtų direktyvų, būtina pažymėti, kad jos visiškai nesprendžia baudžiamosios atsakomybės problemų.

Pažymėtina, kad naujoje Europos Sąjungos elektroninių ryšių reguliavimo sistemoje sąvoka „elektroniniai ryšiai“ neapibrėžta, paliekant galimybę valstybėms narėms savaip interpretuoti šią sąvoką. Tiesa, visiškos laisvės interpretacijai nesuteikiama. Pateikiama tik elektroninių ryšių tinklo sąvoka, kuri apima tiek visus šiuo metu žemėje naudojamus tinklus

[1]Kvietkauskas V. Tarptautinių žodžių žodynas.-Vilnius: VER, 1985.p.265.
[2]1999 Communications Review for electronic communications infrastructure and associated servines// http://europa.eu.int/ISPO/infosoc/telecompolicy/review99/review99.htm

(fiksuoto ir judriojo ryšio, palydovinio ryšio, elektros perdavimo kabelinių sistemų, kabelinės televizijos), tiek ir radijo, optines ar elektromagnetines priemones bei kitas priemones signalams perduoti, tuo pačiu paliekant terpę naujoms technologijoms. Pagal Europos Parlamento ir Tarybos direktyvas 2002/21/EB ir 2002/77/EB[3] „elektroninių ryšių tinklas“ – perdavimo sistemos ir atitinkamais atvejais komutavimo ar maršruto parinkimo įranga bei kiti ištekliai, kurie leidžia perduoti signalus laidais, radijo, optinėmis ar kitomis elektromagnetinėmis priemonėmis, įskaitant palydovinius tinklus, fiksuoto (komutuojamą ir paketinį duomenų perdavimą, įskaitant internetą) ir judriojo ryšio antžeminius tinklus, elektros perdavimo kabelines sistemas, tokiu mastu, kokiu jos yra naudojamos signalams perduoti; radijo ir televizijos programų transliavimui naudojami tinklai ir kabelinės televizijos tinklai, neatsižvelgiant į perduodamos informacijos pobūdį. Iš to darytina išvada, kad sąvoka „elektroniniai ryšiai“, be tradicinių telekomunikacijų, apima ir informacijos turinio perdavimo technologinę dalį tinkluose, skirtuose transliavimui ir retransliavimui. Autoriaus manymu, naujoji Europos Sąjungos elektroninių ryšių reguliavimo sistema leidžia daryti išvadą, kad „elektroniniai ryšiai“ apima visą informacijos (signalų) perdavimą nuotolinio perdavimo ir maršruto parinkimo laidinėmis, radijo, optinėmis ar kitokiomis elektromagnetinėmis priemonėmis, išskyrus perdavimo tinklais, perduodamos informacijos turinį.

Analizuodamas JAV, Didžiosios Britanijos, Rusijos, ir Prancūzijos teisės aktus, autorius pastebėjo, kad sąvoka „elektroniniai ryšiai“ aiškiai suformuluota ne visose valstybėse.

Siekdama inkorporuoti Europos Sąjungos elektroninių ryšių sistemą į savo teisės sistemą, Didžioji Britanija 2003 metais priėmė Slaptumo ir Elektroninių komunikacijų (ES direktyva) instrukciją[4]. Tačiau ši instrukcija nepateikia „elektroninių ryšių (komunikacijų)“ sąvokos apibrėžimo. Apibrėžiant „elektroninių komunikacijų sistemos“ sąvoką, pateikiama nuoroda į 2003 metų Komunikacijų aktą[5]. Šio akto 2 dalies „Tinklai, paslaugos ir radijo spektras“ 1 skyriuje „Elektroninių komunikacijų sistemos ir paslaugos“ „elektroninių komunikacijų sistema“:

a) perdavimo sistema, elektrine, magnetine arba elektromagnetine energija, perduodanti bet kokio pobūdžio signalus; ir
b) dėl to naudojama asmens, aptarnaujančio sistemą ir bendradarbiaujančio su ja signalų perdavimui, kai:
    1) aparatas jungiamas į sistemą;
    2) aparatas naudojamas perjungimui ir signalų nukreipimui ; ir

[3]Directive (2002/21/EC) on a Common Regulatory Framework// http://europa.eu.int/information_society/topics/telecoms/regulatory/new_rf/index_en.htm#reg
[4] The Privacy and Electronics Communications (EC Directive) Regulations 2003// http://www.hmso.gov.uk/si/si2003/n12#n12
[5] Communications Act 2003 // http://www.hmso.gov.uk/acts/acts2003/30021--c.htm

3) programinės įrangos ir duomenų išsaugojimui.

Iš šio aiškinimo „elektroninių ryšių“ sąvoką galime apibrėžti, kaip bet kokio pobūdžio signalus, perduodamus elektrine, magnetine arba elektromagnetine energija. Tačiau 2000 metais priimtas Elektroninių komunikacijų aktas[6] pateikia iš dalies kitokį „elektroninių ryšių“ apibrėžimą. Jame „elektroninės komunikacijos (ryšiai)“ reiškia perduotą ryšį (ar nuo vieno asmens kitam asmeniui, ar nuo vieno įrenginio kitam arba nuo vieno asmens įrenginiui arba atvirkščiai):

a) telekomunikacijų sistema (1984 metų Telekomunikacijų akto apimtyje);
b) kitomis priemonėmis, tik elektronine forma.

Telekomunikacijų sistema reiškia bet kurią sistemą (įskaitant įrenginį įjungtą į ją), kuri egzistuoja (arba visiškai, arba dalinai Didžiojoje Britanijoje, arba kitoje vietoje) komunikacijų perdavimui palengvinti, naudojant elektrinę arba elektromagnetinę energiją. Lyginant abu apibrėžimus, autoriaus nuomone, galima įžvelgti tam tikrus sąvokų neatitikimus, nes viename iš jų vartojama sąvoka „signalas“, o kitame – „ryšys“. Tačiau ir be to abu „elektroninių ryšių“ apibrėžimai yra painūs, o toks būdas, kaip sąvokos suformulavimas su nuoroda į kitą teisės aktą, iš esmės yra nepatogus ir teisiniu požiūriu nepriimtinas.

Prancūzijoje „elektroninių ryšių“ sąvoka galiojančiuose teisės aktuose nevartojama. Vietoje to Pašto ir telekomunikacijų kodekse[7] vartojama sąvoka „telekomunikacija“, kuri suprantama kaip bet kokio telekomunikavimo perdavimą, perdavimą arba gavimą ženklų, signalų, rankraščių, vaizdų, garsų arba duomenų bet kokio pobūdžio laidine linija, vaizdavimu, radijo technika arba kitomis elektromagnetinėmis sistemomis. Toks telekomunikacijos apibrėžimas visiškai atitinka „elektroninių ryšių“ sąvoką. Tai patvirtina ir tas faktas, kad Elektroninių komunikacijų įstatymo[8] projekte nurodyta, kad priėmus šį įstatymą, sąvoka „telekomunikacijos“ bus pakeista sąvoka „elektroniniai ryšiai“. Pažymėtina, kad Prancūzijos teisės aktuose suformuluota „telekomunikacijų“ („elektroninių ryšių“) sąvoka yra trumpa, konkreti, logiška, apimanti visus šiuo metu techniškai įmanomus perdavimo būdus ir visus perdavimo objektus (vaizdus, garsus, ženklus, signalus ir kt.), ir galėtų būti naudojama kaip pavyzdys ir kitoms valstybėms.

Pažymėtina, kad panaši tendencija vyrauja ir kitose pasaulio valstybėse. Štai JAV sąvoka „elektroniniai ryšiai“ vartojama skirtingai tiek lokaliu, tiek ir regioniniu mastu. Elektroninių ryšių slaptumo įstatyme[9] „elektroniniai ryšiai“ reiškia bet kokį perdavimą signalų, laiškų, vaizdų,

[6] Electronics Communications Act 2000// http://www.hsmo.gov.uk/acts/acts2000/20000007.htm
[7] CODE DES POSTES ET TELECOMMUNICATIONS// http://lexinter.net/servpub/code des postes et telecommunications.htm
[8] 2003 Projet de loi sur les communications electroniques// http://dess droit-internet.univ paris1.fr/biblioteque/IMG/doc/2003-04 Avant projet loi Ctn lq.doc
[9] Interception and disclosure of wire, oral, or electronic communications prohibited// http://www4.law.cornell.edu/uscode/18/2511.html

garsų, duomenų arba žinių, perduotų visiškai arba dalinai laidine, radijo, elektromagnetine arba fotooptine sistema, kuri susijusi su ryšiais tarp valstijų arba su vidaus prekyba, išskyrus:

1. bet kokį laidinį ar žodinį ryšį;
2. bet kokį toninį pranešimą;
3. bet kokį ryšį su sekimo įranga arba
4. kai elektroniniai fondai perduoda informaciją, kurią finansų įstaigos saugo komunikacinėje sistemoje, skirtoje informacijos saugojimui ir fondų perdavimui.

Kiek kitaip šią sąvoką interpretuoja JAV Konektikuto komunikacijų koledžas. Palaikomas Konektikuto valstijos koledžų asociacijos Konektikuto komunikacijų koledžas išleido teisės aktą „Elektroninių komunikacijų politika“[10], kuriame „elektroniniai ryšiai“ apibrėžti kaip bet kokie ryšiai, kuriais naudojantis galima informaciją pasiųsti, išsiųsti, atsakyti, perduoti, išsaugoti, palaikyti, nukopijuoti, užkrauti, parodyti, peržiūrėti, skaityti arba atspausdinti viena arba keliomis elektroninių komunikacijų paslaugomis, įtraukiant, pavyzdžiui, elektroninį paštą ar telefoną. Kalifornijos universiteto 2000-11-17 „Elektroninių komunikacijų politikoje“[11] elektroniniai ryšiai reiškia bet kokius ryšius, kuriais naudojantis galima informaciją pasiųsti, išsiųsti, atsakyti, perduoti, išsaugoti, palaikyti, nukopijuoti, užkrauti, parodyti, peržiūrėti, skaityti arba atspausdinti viena arba keliomis elektroninių komunikacijų sistemomis arba paslaugomis. Nežiūrint sąvokų įvairovės, autoriaus nuomone, Jungtinėse Amerikos Valstijose vartojama sąvoka „elektroniniai ryšiai“ apima visus šiuo metu įmanomus signalų perdavimo būdus.

Rusijoje „elektroninių ryšių“ sąvoką pateikia 1995-02-16 Rusijos federalinis įstatymas Nr.15-F3 „Apie ryšius“[12]. 2 straipsnyje „Pagrindinės sąvokos, vartojamos šiame federaliniame įstatyme“ pateikiama tokia „elektroninių ryšių“ sąvoka: elektroniniai ryšiai – bet koks ženklų, signalų, balsinės informacijos, rašytinio teksto, vaizdo, garso arba bet kokio asmens pranešimo išspinduliavimas, perdavimas arba priėmimas per radijo sistemą, laidine, optine ir kitomis elektromagnetinėmis sistemomis. Taigi sąvoka apima bet kokios rūšies signalo perdavimą bet kuria ryšio sistema.

Iki 2004-05-01 Lietuvoje, visuomeninius santykius, apimančius elektroninius ryšius ir su jais susijusią veiklą, reglamentavo Lietuvos Respublikos telekomunikacijų įstatymas (žin.,1998, Nr.56-1548; 2002, Nr.75-3215) ir Lietuvos Respublikos visuomenės informavimo įstatymas (žin., 1996, Nr.71-1706; 2000, Nr.75-2272). Juose sąvoka „elektroniniai ryšiai“ nevartojama.

Nuo 2004-05-01 Lietuvoje įsigaliojo Lietuvos Respublikos elektroninių ryšių įstatymas[13]. Įstatyme „elektroniniai ryšiai“ – signalų perdavimas laidinėmis, radijo, optinėmis ar kitomis

[10] Electronic communications policy// http://www.commnet.edu/it/policy/electronic-communications.html
[11] Electronic Communications Policy – University of California//
http://www.ucop.edu/ucophome/policies/ec/html/welcome.htm
[12] Новый Федеральный закон „О связях“// http://www.medialaw.ru/laws/russian laws/telecom/
[13] Elektroninių ryšių įstatymas // http://www3.lrs.lt/cgi-bin/preps2?Condition1=232036&Condition2

elektromagnetinėmis priemonėmis. Autoriaus manymu, tokia elektroninių ryšių sąvoka trumpa ir ganėtinai konkreti bei tikslesnė, lyginant su kitų šalių pateiktomis sąvokomis. Analizuojant Lietuvos Respublikos elektroninių ryšių įstatymo pateikiamą „elektroninių ryšių“ sąvoką, galima išskirti du jos segmentus:

1. signalai. „Signalas [pranc. signal < lot.signum – ženklas]:1.fizinė informacijos išraiška; susideda iš informacijos nešiklio ir turinio; pagal nešiklio prigimtį būna mechaniniai, garso, šviesos, elektriniai, elektromagnetiniai (radijo) ir kt.; ...“[14] ir
2. jų perdavimas bet kokiomis priemonėmis (laidinėmis, radijo, optinėmis ar kitomis elektromagnetinėmis). Pažymėtina, kad sąvokoje paminėtų perdavimo priemonių skaičius nėra baigtinis ir tai palieka galimybę taikyti ir kitas perdavimo priemones.

Analizuojant pirmąjį segmentą, atrodytų, kad vietoje žodžio „signalai“ galima vartoti žodį „informacija“, nes signalas – fizinė informacijos išraiška. Tačiau 1985 metų Tarptautinių žodžių žodyne nurodyta, kad „informacija [lot. informatio – išaiškinimas, pranešimas], mokslinės, visuomeninės, politinės, techninės žinios, perduodamos vienų asmenų kitiems žodžiu, raštu arba masinės komunikacijos priemonėmis (per spaudą, radiją, televiziją, kiną).“[15] Tačiau vadovaujantis Didžiosios Britanijos Elektroninių Komunikacijų akte suformuluota sąvoka, informacija neapims tų atvejų, kai perdavimas vyks tarp elektroninių įrenginių ar tarp elektroninio įrenginio ir žmogaus. Šiuo atveju žodis „signalas“ yra tikslesnis, nes apima ne tik tuos atvejus, kai perdavimas vyksta tarp dviejų ir daugiau žmonių, bet ir perdavimo atvejus tarp elektroninių įrenginių arba tarp vieno ar kelių žmonių bei vieno ar kelių elektroninių įrenginių.

Kalbant apie antrąjį segmentą, būtina pastebėti, kad jis apima visas šiuo metu pasaulyje naudojamas elektronines perdavimo priemones ir kitas priemones, kurios, nors šiuo metu ir nenaudojamos, tačiau bet kada gali būti atrastos ir pradėtos naudoti.

Atsižvelgiant į tai, kas išdėstyta, autoriaus manymu, Lietuvos Respublikos elektroninių ryšių įstatyme suformuluota „elektroninių ryšių“ sąvoka laikytina tinkamiausia.

Pažymėtina, kad sąvoka „elektroniniai ryšiai“ teisinėje literatūroje, analizuojančioje nusikaltimus, sutinkamas retai. Tačiau to negalima pasakyti apie sąvoką „elektroninė erdvė“ (sinonimai – kiber erdvė, kibernetinė erdvė). Tolesniam nusikaltimų elektroninių ryšių sektoriuje nagrinėjimui būtina išsiaiškinti „elektroninės erdvės“ sąvoką ir nustatyti jos santykį su „elektroniniais ryšiais“.

Sąvoką „elektroninė erdvė“ pirmą kartą pavartojo Viljamas Gibsonas (Williams Gibson) 1984 metų romane apie mokslinę fantastiką „Neuromancer“[16]. Knygoje elektroninė erdvė aprašoma kaip įsivaizduojama karalystė, kur vyrauja kompiuterinė informacija. Vėliau nuo 1989

[14] Kvietkauskas V. Tarptautinių žodžių žodynas.-Vilnius: VER, 1985.p.446.
[15] Kvietkauskas V. Tarptautinių žodžių žodynas.-Vilnius: VER, 1985.p.213.
[16] What is Cyberspace? // http://www.nutball.com/classes/mrshowell/dewitt/Whatis.html

metų šią sąvoką imta vartoti aiškinant kompiuterines sistemas. Nežiūrint to , kad nuo 1990 metų praėjo jau 14 metų, tačiau iki šiol sąvoka „elektroninė erdvė“ aiškinama nevienodai. Štai keletas pavyzdžių. Elektroninė erdvė:

1. apima milijonus personalinių kompiuterių, sujungtų modemais per telefoninę sistemą į kompiuterines dialogines paslaugas, taip pat elektroninio pašto sistemas ir internetą[17];
2. - bioelektrinė erdvė, kuri egzistuoja visur, kur yra telefonai, koaksialiniai kabeliai, optinio pluošto linijos arba elektromagnetinės bangos[18];
3. - kompiuterinis tinklas, susidedantis iš Pasaulinio tinklo kompiuterinių tinklų, naudojančių TCP/IP tinklų protokolus duomenų perdavimui ir duomenų apsikeitimui palengvinti[19];
4. – aplinka, kurioje bendraujama per į tinklą sujungtus kompiuterius. Fiziniai atstumai tarp bendraujančiųjų neturi reikšmės. Pavyzdys – internetas[20].

Iš pateiktų pavyzdžių nesunkiai galima pastebėti, kad sąvokos „elektroninė erdvė“ ir „elektroniniai ryšiai“ yra panašios. Visų pirma tiek elektroniniams ryšiams, tiek ir elektroninei erdvei yra bendra tai, kad jų pagrindas – Pasaulinis tinklas, susidedantis iš daugybės kompiuterių tinklų. Antra, jau anksčiau buvo nustatyta, kad elektroniniai ryšiai yra signalų perdavimas laidinėmis, radijo, optinėmis ar kitomis elektromagnetinėmis priemonėmis, o elektroninė erdvė – bioelektroninė erdvė, egzistuojanti visur, kur yra telefonai, koaksialiniai kabeliai, optinio pluošto linijos arba elektromagnetinės bangos. Apjungus šias dvi sąvokas gaunama, kad elektroniniai ryšiai – signalų perdavimas elektroninėje erdvėje. Šiuo atveju elektroninė erdvė – tik vieta, erdvė, aplinka, kurioje galimas bet kokio signalo perdavimas. Tai patvirtina ir 1998 metais profesoriaus Džerio Kango (Jerry Kang) pateiktas Elektroninės erdvės slaptumo įstatymo projektas[21], kuriame jis suformulavo ir elektroninės erdvės sampratą. Jame „elektroninė erdvė“ reiškia bet kokį naudojimąsi ryšiais ar sistema, kuri, tarpininkaujant kompiuteriui, per elektroninius ryšius užtikrina prieigą prie kompiuterinio serverio. „Elektroninė erdvė“ be apribojimų apima bet kokį naudojimąsi ryšiais arba sistema, kuri užtikrina arba leidžia elektroninius ryšius per internetą[22], t.y. erdvė, kuri leidžia bet kokį signalų perdavimą.

Apibendrindamas visa tai, kas išdėstyta, autorius tinkamiausiu laiko tokį „elektroninių ryšių“ ir „elektroninės erdvės“ santykį: elektroninė erdvė – vieta, erdvė, aplinka, kurioje galimi bet kokie elektroniniai ryšiai.

---

[17] Ten pat.
[18] Cybercrime // htp://faculty.ncwc.edu/toconnor/315/315lect12.htm
[19] Cyberspace // http://www.thefreedictionary.com/cyberspace
[20] Kibernetinė erdvė // http://aldona.mii.lt/pms/terminai/term/z2odynas.html
[21] Proposed Cyberspace Privacy Act // http://www1.law.ucla.edu/~kang/Scholarship/Cyberspace/CyberspacePrivacyAct/cyberspaceprivacyact.htm
[22] Ten pat.

2.Nusikaltimų elektroninių ryšių sektoriuje specifika:

2.1.Nusikaltimų elektroninių ryšių sektoriuje samprata, rūšys ir požymiai

Dar visai neseniai didžiausias dėmesys buvo skiriamas neteisėtoms veikoms, susijusioms su kompiuterinėmis technologijomis ir tarptautinėmis kompiuterinėmis sistemomis – kompiuteriniams nusikaltimams ir iš dalies nusikaltimams telekomunikacijų sektoriuje. Spartus technologijų vystymasis sąlygojo technologinę telekomunikacijų, informacinių technologijų ir televizijos konvergenciją, elektroninių ryšių atsiradimą ir plėtrą. Todėl konvergavo ir patys nusikaltimai. Dabar tos pačios rūšies nusikaltimus galima atlikti naudojantis ir laidinėmis linijomis, ir radijo ar optinėmis linijomis ar net keliomis iš jų vienu metu. Atsižvelgiant į tai, kad vis daugiau tiek atskirų žmonių, tiek ir žmonių grupių veikla yra susijusi su elektroninių ryšių panaudojimu (elektroninės žinutės, duomenų ar laiško siuntimas, interaktyvus bendravimas, elektroninė komercija, elektroninė bankininkystė, viešosios elektroninės paslaugos, elektroninis balsavimas ir kt.), todėl šiai veiklai kyla vis didesnė grėsmė dėl šioje srityje daromų nusikaltimų, kurių įvairovė išties įspūdinga. Didžiąja dalimi tai sąlygojama interneto – globalaus laisvai prieinamo kompiuterinio tinklo, suteikiančio ne tik daug gerųjų galimybių, bet lygiai tiek pat ir blogųjų galimybių.

Siekiant tinkamai suformuluoti nusikaltimo elektroninių ryšių sektoriuje sąvoką, būtina suskirstyti visus nusikaltimus elektroninių ryšių sektoriuje į atskiras rūšis, grupes. Apskritai nusikaltimų skirstymas į tam tikras grupes, rūšis pagal tam tikrus kriterijus, požymius yra vadinamas klasifikacija. Pagrindinis uždavinys klasifikuojant nusikaltimus – tinkamai nustatyti klasifikacijos pagrindą. Klasifikacijos pagrindu gali būti kėsinimosi objektas, kaltės forma, veikos pavojingumo visuomenei laipsnis, nusikaltimo atlikimo būdas, priemonės ir panašiai.

Pirma ir vienintelė daugelio valstybių pripažinta klasifikacija, susijusi su nusikaltimais elektroninių ryšių sektoriuje, buvo atlikta tik šiame tūkstantmetyje. Tačiau jos pagrindu buvo klasifikuoti ne nusikaltimai elektroninių ryšių sektoriuje, o nusikaltimai elektroninėje erdvėje, t.y. erdvėje, kurioje galimi elektroniniai ryšiai. Tai padaryta 2001 metais, kai buvo priimta Nusikaltimų elektroninėje erdvėje konvencija[23]. Konvencijos I dalyje, kuri susijusi su materialine teise, pasiūlytas toks pavojingų veikų rūšių klasifikavimas:

1) konfidencialumo, duomenų vientisumo, kompiuterinių duomenų ir sistemų pažeidimai (neteisėta prieiga, neteisėtas perėmimas, įsikišimas į duomenų apdorojimo procesą, įsikišimas į kompiuterinių sistemų darbo procesą, piktnaudžiavimas kompiuterinėmis priemonėmis (įrenginiais));
2) su kompiuteriais susiję pažeidimai (sukčiavimas, susijęs su kompiuteriais; klastojimas, susijęs su kompiuteriais);
3) pažeidimai, susiję su turiniu (pažeidimai, susiję su pornografine medžiaga apie vaikus);

[23] Convention on Cybercrime // http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

4) pažeidimai, susiję su autorių teisėmis ar gretutinėmis teisėmis.

Nežiūrint šios klasifikacijos išsamumo ir paprastumo, ji neapima visų neteisėtų veikų, atliekamų elektroninių ryšių sektoriaus aplinkoje – elektroninėje erdvėje. Autoriaus manymu, prie pažeidimų, susijusių su turiniu, reikėtų priskirti įžeidžiančios medžiagos platinimą ir kiber persekiojimus.

Australas Piteris Graboskis (Piter Grabosky) siūlo kitokią klasifikaciją. Nusikaltimus elektroninėje erdvėje jis klasifikuoja į devynis tipus, įtraukiančius informacines sistemas kaip nusikaltimo priemones ir/arba tikslą[24]:

1. Informacinių paslaugų vagystė. Pavyzdžiui, mobiliųjų telefonų klonavimas, apmokėjimo už telekomunikacijų paslaugas klastojimas, neteisėta prieiga prie įmonės telefoninės paskirstymo spintos.
2. Komunikacijos, palengvinančios kitų nusikaltimų atlikimą. Pavyzdžiui, nusikalstamos veiklos planavimui ir vykdymui – organizuojant narkotinių medžiagų platinimą, ginklų prekybą ir kt.
3. Informacinis piratavimas ir padirbinėjimas. Pavyzdžiui, bet koks autorinių teisių pažeidimas naudojant kompiuterį.
4. Įžeidžiančios medžiagos platinimas. Elektroninėje erdvėje egzistuoja daugybė nepageidaujamos informacijos. Pavyzdžiui, aiškiai seksualinio pobūdžio medžiaga, rasistinė propaganda, informacija apie uždegamųjų ir sprogstamųjų įtaisų pasigaminimą. Informacinės sistemos taip pat gali būti naudojamos bauginimui, nepadoriems telefoniniams skambučiams ar kiber persekiojimams.
5. Elektroninis pinigų plovimas. Pavyzdžiui, siekiant paslėpti ir perduoti (persiųsti) neteisėtu būdu įsigytas pinigines lėšas.
6. Elektroninis vandalizmas ir terorizmas. Teigiama, kad keičiasi tradicinė karo samprata. Visame pasaulyje apsaugos planuotojai didžiausią dalį kapitalo skiria informaciniam karui: priemonėms, kurios sunaikina infrastruktūros technines apsaugos priemones.
7. Komercinis ir investicinis sukčiavimas. Elektroninėje erdvėje egzistuoja daugybė siūlymų komerciniam ir investiciniam sukčiavimui. Pavyzdžiui, interneto naudojimo augimas užtikrina beprecedentinius atvejus nusikalstamam eksploatavimui.
8. Neteisėtas informacijos perėmimas. Pavyzdžiui, šiandieninės technologijos suteikia ne tik naujas galimybes, bet ir naujo tipo nusikaltimus. Elektromagnetiniai signalai, kuriuos skleidžia kompiuteriai, gali būti perimti; kabeliai gali veikti kaip antenos, taip sudarydamos galimybę radijo signalo perėmimui.

[24] Crime in the Cyberspace // http://www.abc.net.au/rn/science/ockham/stories/s45008.htm

9. Elektroninis sukčiavimas perduodant (siunčiant) fondus. Pavyzdžiui, nusikaltimai, susiję su elektronine komercija.

Tokia klasifikacija, autoriaus manymu nėra išbaigta, nes toks nusikaltimas kaip pinigų „plovimas“ gali būti priskirtas tiek prie antro, tiek prie penkto tipo aukščiau išvardintų nusikaltimų, o nusikaltimai, susiję su elektronine komercija (devintas tipas) gali būti priskiriami ir septintam tipui. Nežiūrint to, šios klasifikacijos privalumai dvejopi:

- ji apima praktiškai visas neteisėtas veikas, atliekamas elektroninių ryšių sektoriaus aplinkoje;
- joje neišskiriami kompiuteriniai nusikaltimai, nes naudojantis kompiuteriu ir bet kuriais komunikavimo tinklais galima atlikti bet kurį, iš klasifikacijoje nurodytų, nusikaltimų tipų.

Nusikalstamą veiką, atliktą informacinių technologijų (*informacinės technologijos – internetas, telekomunikacijos ir skaitmeninės technologijos* [25] - autoriaus pastaba) srityje, galima apibrėžti naudojantis JAV Federalinio tyrimų biuro (toliau – FTB) atskirai įsteigto padalinio kovai su kompiuteriniais nusikaltimais (FBI NATIONAL Computer Crime Squad‘s (NCCS))[26] pateikta formuluote. Išskiriamos šios informacinių technologijų sferoje atliekamos nusikalstamos veikos:

1) įsiveržimas į viešųjų komutatorių/operatorių tinklus (telefoninės kompanijos);
2) įsiveržimas į kompiuterinius tinklus;
3) privatumo pažeidimai;
4) gamybinis špionažas;
5) programinės įrangos piratavimas;
6) kiti nusikaltimai, kuriems atlikti kompiuteris buvo panaudotas kaip pagrindinis įrankis.

Nesunku pastebėti, kad visi tiek FTB klasifikacijoje išvardinti nusikaltimai, tiek ir Piterio Graboskis ar Nusikaltimų elektroninėje erdvėje konvencijoje išvardinti nusikaltimai gali būti ir dažniausiai yra atliekami naudojant kompiuterį. Atrodytų galima teigti, kad absoliuti dauguma nusikaltimų, atliekamų elektroninių ryšių aplinkoje – elektroninėje erdvėje, gali būti įvardinti kaip kompiuteriniai nusikaltimai. Tačiau nusikaltimams elektroninių ryšių sektoriuje priskirtini tik tokie kompiuteriniai nusikaltimai, kurie „išeina“ už vieno kompiuterio veiklos ribų, t.y. tik tokie kompiuteriniai nusikaltimai, kurių vykdymas susijęs su perdavimu vienokio ar kitokio neteisėto signalo.

Kalbant apie kompiuterinius nusikaltimus, susiduriama su dvejopo pobūdžio problematika:

[25] Meškauskaitė L. Naujųjų informacinių technologijų teisinis reguliavimas. – Vilnius: Jurisprudencija, 2002.t.32 (34).p.106.
[26] Computer Crimes & Cyberspace Cases // http://www.massachusetts-lawyers.com/pages/criminal/computercrime.html

1) sąvokų, susijusių su kompiuterių panaudojimu, problema – naudojamų sąvokų (sampratų) įvairovė: „kompiuterinis nusikaltimas“, „su kompiuteriais susijęs nusikaltimas“, taip pat „informacinis nusikaltimas“, „informatikos nusikaltimas“, “elektroninis nusikaltimas“ ir kt.;
2) nėra aiškaus kompiuterinio nusikaltimo apibrėžimo[27]:
   - JAV teisės specialistas Donas Parkeris – „visos tyčinės veikos, vienaip ar kitaip susijusios su kompiuteriais, dėl kurių nukentėjusysis patyrė ar galėjo patirti žalą, o nusikaltimo subjektas turėjo ar galėjo gauti iš to naudos“;
   - Europos ekonominės plėtros ir vystymo organizacija (OECD) – „bet koks neteisėtas, neetiškas, savavališkas elgesys duomenų apdorojimo ar siuntimo procese“;
   - Jungtinėse Amerikos valstijose – „bet koks baudžiamosios teisės pažeidimas, kuriam padaryti arba ištirti naudojamos kompiuterinių technologijų žinios“;

Kai kurie teisės specialistai Rusijoje laikosi nuomonės, kad prie kompiuterinių nusikaltimų turi būti priskiriami ir telekomunikaciniai nusikaltimai. Panašios nuomonės laikomasi ir kitose šalyse. Pavyzdžiui, Kanadoje - „Kompiuterinis nusikaltimas – bet kokia neteisėta veika, kuri įtraukia kompiuterinę sistemą, nepriklausomai nuo to, ar kompiuteris buvo nusikaltimo objektas ar paprasčiausiai įrankis nusikaltimui atlikti ar kaip nusikaltimo akivaizdumo įrodymas. Telekomunikacinis nusikaltimas – bet kokio telefono, mikrobanginio įrenginio, palydovo ar kitos telekomunikacinės sistemos naudojimas sukčiaujant. Dauguma pačių telekomunikacinių sistemų – kompiuteriai, ir todėl kai kuriais atvejais į pažeidimus prieš telekomunikacijų sistemas galima žiūrėti kaip į kompiuterinius nusikaltimus.“[28] Tas pats pasakytina ir apie informacinių technologijų nusikaltimus.

Praktikoje konkretaus nusikaltimo, atlikto informacinėmis technologijomis, negalima priskirti vienam kokiam nors informacinių technologijų tipui. Elementai, esantys vieno nusikaltimo sudėtyje, yra persipynę, todėl nusikalstamo veiksmo procese dažniausiai atrandama keletas jo sudėtinių dalių – vagystė, asmeninio privatumo pažeidimas, terorizmas, šantažas ir t.t. Nusikaltimai, kuriuose informacinės technologijos yra kaip nusikaltimo objektas, dažniausiai apjungia tokius pažeidimus, kaip:

1. vagystė – intelektualios nuosavybės, rinkos informacijos, klientų sąrašas, duomenys apie kainas arba rinkodaros planai, gamybinis špionažas;

[27] Petrauskas R., Štitilis D. Kompiuteriniai nusikaltimai ir jų prevencija. Mokomasis leidinys. – Vilnius: LTA Leidybos centras, 2000.p.5.
[28] Computer Crime - Can it affect you?? // http://www3.sk.sympatico.ca/rcmpccs/cpu-crim.html

2. šantažas – informacija, gauta vagiant kompiuterinius duomenis, kurioje galima rasti informaciją apie asmens sveikatos būklę, seksualines orientacijas, asmenines istorijas ir informaciją, naudojamą asmeniniams tikslams;
3. diversija – rinkos, kainų politikos, intelektualios nuosavybės. Pavogus informaciją, galima sabotuoti operacines sistemas, kompiuterines programas ir sukelti chaosą visuomenėje arba privačioje sferoje;
4. techno-vandalizmas – pasireiškia tada, kai neteisėtu priėjimu prie kompiuterio duomenų, operacinių sistemų, kompiuterinių programų jos yra sulaužomos, sugadinamos, siekiant ne kažkokios konkrečios naudos, o asmeninio pasitenkinimo. Toks nusikaltimas gali būti atliktas tiek sąmoningai, tiek ir nesąmoningai;
5. techninis piktnaudžiavimas – pasireiškia privatumo pažeidimo forma. Asmuo neteisėtai įsibrauna į kito asmens kompiuterį, tiesiog po jį naršo, nieko negadina, bet pažeidžia jo privatumą;
6. privatumo pažeidimas – šis pažeidimas dažniausiai siejasi su visomis penkiomis aukščiau išvardintomis nusikaltimų rūšimis ir yra viena iš dažniausiai pasitaikančių nusikaltimo rūšių;
7. neteisėtas informacijos bei duomenų pakeitimas ir manipuliavimas jais. Tai viena iš pavojingiausių nusikaltimų pasireiškimo formų. Pakeitus galiojančius vyriausybinius įrašus, galima suklastoti įvairius dokumentus: vairavimo teisių licenziją, paso duomenis ir t.t. Šis nusikaltimas įtraukia visas kitas aukščiau išvardintų nusikaltimų formas.

Visos aukščiau išvardintos klasifikacijos tik iš dalies tinka autoriaus nagrinėjamai temai. Klasifikacijos nusikaltimų elektroninių ryšių sektoriuje autoriui nepavyko rasti. Autorius, vadovaudamasis bendraisiais klasifikavimo reikalavimais, pateikia savo siūlomą klasifikaciją, sudarytą pagal šios studijos pirmame skyriuje suformuluotą elektroninių ryšių sampratą. Atsižvelgiant į tai, pagal nusikaltimo atlikimui naudojamas priemones, nusikaltimai elektroninių ryšių sektoriuje skirstomi į :

1) atliekamus laidinėmis priemonėmis;
2) atliekamus radijo priemonėmis;
3) atliekamus optinėmis priemonėmis;
4) atliekamus elektromagnetinėmis priemonėmis.

Tokių nusikaltimų pavyzdžiai – kompiuteriu laidiniu tinklu prisijungus prie interneto, neteisėtai perimamos privačios komunikacijos ar kompiuterinė informacija, įsikišama į duomenų apdorojimo procesą; radijo imtuvu neteisėtai perimama saugoma informacija arba apribojama

prieiga prie jos; elektromagnetiniu įrenginiu neteisėtai perimama informacija išspinduliuojamos energijos pavidale ir panašiai. Pažymėtina, kad visi nusikaltimai elektroninių ryšių sektoriuje gali būti atliekami tiek viena, tiek ir keliomis iš minėtų priemonių. Pavyzdžiui, toks Lietuvoje neretai pasitaikantis nusikaltimas, kaip melagingas pranešimas apie visuomenei gresiantį pavojų ar ištikusią nelaimę, gali būti atliekamas:

1) kompiuteriu (naudojantis kompiuteriu pasiunčiama žinutė);
2) telefonu (paskambinant ir pranešant žodžiu);
3) faksimiliniu aparatu (pasiunčiant melagingai surašytą informaciją);
4) skaitmeniniais įrenginiais (konferencijos realiame laike metu).

Visgi aukščiau minėtas nusikaltimų elektroninių ryšių sektoriuje klasifikavimas nėra išsamus ir aiškus. Nusikaltimo elektroninių ryšių sektoriuje sąvokos suformulavimui tikslinga aptarti galimas nusikaltimų elektroninių ryšių sektoriuje rūšis.

Iki tol, kol bet kokios informacijos, signalo perdavimas yra teisėtas ir nėra pažeisti kieno nors interesai, nusikaltimo nėra. Pavyzdžiui, draugui elektroniniu paštu siunčiamas pranešimas, duomenys apdorojami teisėtai prisijungus per nutolusį kompiuterį, teisėtai naudojamasi telekomunikacijų paslaugomis, persiunčiamos kompiuterinės bylos ir panašiai. Tačiau kai perdavimas yra neteisėtas, tai jau yra nusikaltimas. Neteisėtas signalų perdavimas gali pasireikšti žmogaus turtinių interesų ar komunikavimo privatumo pažeidimu, neteisėtu įvairių programų įvedimu, modifikavimu, apribojimu teisėtai naudotis tam tikromis elektroninėmis priemonėmis ir panašiai. Todėl neteisėtą signalų perdavimą galima laikyti viena iš nusikaltimų elektroninių ryšių sektoriuje rūšių. Prie šios rūšies nusikaltimų galima priskirti šiuos nusikaltimus elektroninėje erdvėje (pagal Nusikaltimų elektroninėje erdvėje konvenciją):

1) konfidencialumo, duomenų vientisumo, kompiuterinių duomenų ir sistemų pažeidimai;
2) su kompiuteriais susiję pažeidimai.

Šios rūšies nusikaltimų, atliekamų elektroninių ryšių sektoriuje esmė – neteisėtas perdavimas, t.y. neteisėtas aktyvus veiksmas. Šiuo atveju perduodamo signalo teisėtumas neturi reikšmės.

Tačiau be šių nusikaltimų elektroninių ryšių sektoriaus aplinkoje – elektroninėje erdvėje – dar egzistuoja daug kitų nusikaltimų, pavyzdžiui, informacinis piratavimas ir padirbinėjimas, platinimas įžeidžiančios ar draudžiamo turinio medžiagos (informacijos) ir panašiai. Visus šiuos nusikaltimus elektroninių ryšių sektoriuje galima priskirti prie nusikaltimų, kurie atliekami teisėtais būdais – perdavimas, siuntimas, platinimas ir kt., tačiau jų turinys – neteisėtas. Todėl neteisėtų signalų perdavimą taip pat reikia laikyti viena iš nusikaltimų elektroninių ryšių

sektoriuje rūšių. Prie šios rūšies nusikaltimų galima priskirti šiuos nusikaltimus elektroninėje erdvėje (pagal Nusikaltimų elektroninėje erdvėje konvenciją):

1) pažeidimai, susiję su turiniu;
2) pažeidimai, susiję su autorių teisėmis ar gretutinėmis teisėmis.

Šios rūšies nusikaltimų, atliekamų elektroninių ryšių sektoriuje esmė – perdavimas neteisėto signalo, kai tuo tarpu pats perdavimas, bet kuriuo iš būdų – teisėtas.

Atsižvelgiant į tai, kas išdėstyta, autorius daro išvadą, kad nusikaltimai elektroninių ryšių sektoriuje gali būti atliekami dviejų rūšių neteisėtomis veikomis:

- signalai laidinėmis, radijo, optinėmis ar kitomis elektromagnetinėmis priemonėmis yra perduodami neteisėtai. Pavyzdžiui:
  - neteisėtai perimama kompiuterinė informacija, siunčiant ją elektroniniu paštu, persiunčiant kompiuterines bylas (failus) ir kt.;
  - prisijungus per nutolusį kompiuterį, neteisėtai sunaikinama, ištrinama, pakeičiama, sugadinama kompiuterinė informacija;
  - sutrikdomas kompiuterinės sistemos darbas, kuris pasireiškia kompiuterinės informacijos įvedimu, perdavimu, sunaikinimu, ištrynimu, sugadinimu, pakeitimu;
  - bet kokiu būdu neteisėtai įsikišama į duomenų apdorojimo procesą;
  - neteisėtas privačių komunikacijų perėmimas;
  - telekomunikacinių paslaugų vagystė;
  - apribojamas priėjimas prie elektroninių ryšių ir kt.
- laidinėmis, radijo, optinėmis ar kitomis elektromagnetinėmis priemonėmis yra perduodami neteisėti signalai. Pavyzdžiui:
  - ✓ neteisėtas medžiagos, susijusios su vaikų pornografija, padarymas prieinama (taip pat siūlymas), platinimas ar siuntimas, „tiekimas“ (angl. Procuring) per kompiuterinę sistemą sau ar kitam;
  - ✓ įžeidžiančių pranešimų siuntimas;
  - ✓ melagingas pranešimas apie visuomenei gresiantį pavojų ar ištikusią nelaimę;
  - ✓ sukčiavimai, susiję su prekyba (elektroninės parduotuvės, skelbimų lentos), ir kt.

Pirmame šios studijos skyriuje jau buvo minėta, kad pats signalų perdavimas elektroninių ryšių sektoriuje nėra nusikaltimas. Nusikaltimas baudžiamojoje teisėje suprantamas kaip teisės saugomų vertybių pažeidimas, pasisavinimas ar visiems priimtinų teisės normų nesilaikymas. Atsižvelgiant į autoriaus pateiktą nusikaltimų elektroninių ryšių sektoriuje klasifikaciją, nusikaltimu elektroninių ryšių sektoriuje laikysime tokius veiksmus, kurie pažeidžia teisėtą, saugų ir priimtiną signalų naudojimą, perdavimą ir kitokį skleidimą elektroninėje erdvėje, t.y.

nusikaltimas elektroninių ryšių sektoriuje – bet koks neteisėtas visiškas ar dalinis signalų perdavimas (tiek teisėtų signalų, perduodant neteisėtai, tiek neteisėtų signalų, perduodant teisėtai) laidinėmis, radijo, optinėmis ar kitomis elektromagnetinėmis priemonėmis. Pažymėtina, kad nusikaltimu dažniausiai pažeidžiama tam tikra tvarka, kuri vyrauja tam tikroje srityje, sektoriuje, regione ir kt. Pažeidimo forma gali būti įvairi : perėmimas, pakeitimas, pasiuntimas (nusiuntimas), įvedimas, ištrynimas, naudojimas, kopijavimas, platinimas ir kiti aktyvūs veiksmai, kuriais gali būti siunčiami signalai. Atsižvelgiant į tai, autorius bet kokį nusikaltimą elektroninių ryšių sektoriuje teisiškai siūlo apibrėžti taip – *tai neteisėta veika, kuria pažeidžiama* (perimama, pakeičiama, siunčiama, įvedama, ištrinama, naudojama, kopijuojama, platinama ir kt.) *teisėta signalų perdavimo laidinėmis, radijo, optinėmis ar kitomis elektromagnetinėmis priemonėmis tvarka.* Visos tos tvarkos pažeidimo formos yra pavojingos tiek vienam asmeniui, tiek grupei asmenų ar visai visuomenei ir kriminalizuojamos baudžiamosios teisės normomis.

Nusikaltimų elektroninių ryšių sektoriuje požymiai

Kalbant apie nusikaltimus (teisės pažeidimus), visų pirma reikėtų apibrėžti, kad nusikaltimas (teisės pažeidimas) – tai teisės saugomų vertybių pažeidimas, pasisavinimas ar jų nesilaikymas. Būtent nusikaltimais yra pažeidžiama viena iš svarbiausių žmogaus teisių – privataus gyvenimo neliečiamumas. Kiekvienoje valstybėje ši teisė ginama įvairiomis teisinėmis priemonėmis.

Nusikaltimams elektroninių ryšių sektoriuje, kaip ir visų kitų rūšių nusikaltimams, būdingi šie požymiai:

1) veika;
2) pavojinga veika;
3) priešinga teisei veika.

Nusikaltimu elektroninių ryšių sektoriuje gali būti laikoma tik sąmoninga ir valinga *veika*. Nei įsitikinimai, nei mintys, nei „pavojinga asmens būsena“, nei asmens neigiamos subjektyvios elgsenos savybės, kol jos nėra realizuojamos žmogaus išorinėje veikloje, negali būti laikomos nusikaltimu. Tai sąmoninga veika, nes žmogus valdo tam tikras priemones ir panaudoja jas nusikaltimui. Kalbant apie nusikaltimus elektroninių ryšių sektoriuje, tos priemonės gali būti tokios:

1) kompiuteris;
2) fiksuoto laidinio ryšio telefonas ar faksimilinis aparatas;
3) judriojo ryšio telefonas;
4) skaitmeninės televizijos įrenginiai ir pan.

Pažymėtina, kad priemonių sąrašas nėra baigtinis. Prie minėtų priemonių turi būti priskiriamos visos priemonės, kuriomis galima perduoti signalus.

Tačiau nusikaltimu elektroninių ryšių sektoriuje yra pripažįstama ne bet kokia veika, bet tik pavojinga veika. Taigi antruoju nusikaltimo elektroninių ryšių sektoriuje požymiu reiktų laikyti jo *pavojingumą*.

Įstatymo leidėjas privalo iš veikų rato išsirinkti tokias veikas, kurios yra pavojingos ir tai įtvirtinti baudžiamosios teisės normose. Veikos pavojingumas, ypač elektroninių ryšių sektoriuje, yra dinamiškas, kintantis požymis. Visuomeninių santykių raidą lemia tai, kad vienos veikos, kurios buvo laikomos pavojingomis, praranda savo pavojingumą, o kartais tampa net nenaudingomis, o kitos veikos, kurios nebuvo pavojingos, pasidaro tokiomis.

Veikos pavojingumas elektroninių ryšių sektoriuje yra apibūdinamas dviem rodikliais:

- pavojingumo pobūdžiu;
- pavojingumo laipsniu.

Pavojingumo pobūdis – tai kokybinė veikos charakteristika. Jis daugiausiai priklauso nuo nusikaltimo objekto, t.y. nuo teisinių gėrių, į kuriuos kėsinamasi, vertingumo. Pavojingumo pobūdžiu skirsis nusikaltimai, sukeliantys materialinę, moralinę, fizinę žalą.

Pavojingumo laipsnis išreiškia kiekybinę veiklos charakteristiką. Jei pavojingumo pobūdis rodo, koks yra pavojingumas, t.y. jo turinys, tai pavojingumo laipsnis parodo, kokio dydžio yra šis pavojingumas. Pavyzdžiui, Lietuvos Respublikos Baudžiamojo kodekso 179 straipsnio „Neteisėtas naudojimasis energija ir ryšių paslaugomis“ telekomunikacinių paslaugų vagystė , dėl ko kitam asmeniui padaryta turtinė žala yra mažiau pavojinga, negu ta pati veika, tik padariusi kitam asmeniui didelės turtinės žalos. Pavojingumo laipsniui įtakos turi ir nusikaltimo padarymo būdas, nusikaltimo padarymo motyvai, tikslai, kitos aplinkybės. Veikos pavojingumą elektroninių ryšių sektoriuje galime vadinti materialiu nusikaltimo požymiu, nes jis parodo tokio nusikaltimo esmę, paaiškina, dėl ko toks žmogaus poelgis laikomas nusikaltimu.

Pažymėtina, kad nusikaltimo elektroninių ryšių sektoriuje pavojingumo pobūdį lemia šie požymiai:

1) kėsinimosi objekto vertingumas;
2) nusikaltimo dalykas;
3) veikos padarymo būdas;
4) veikos padarymo pasekmės;
5) nusikaltimo subjekto ypatumai;
6) kaltės forma;
7) veikos padarymo motyvas;
8) veikos tikslas.

Tačiau pavojingos veikos padarymas elektroninių ryšių sektoriuje dar nereiškia, kad tokia veika bus laikoma nusikaltimu, o kaltas asmuo bus traukiamas baudžiamojon atsakomybėn. Vien

veikos pavojingumo nepapanka, kad būtų galima laikyti ją nusikaltimu. Minėta veika turi būti *priešinga teisei*. Nusikaltimu elektroninių ryšių sektoriuje laikoma tik tokia pavojinga veika, kuri numatyta baudžiamajame įstatyme. Šiuo atveju vadovaujamasi tarptautiniu mastu pripažinta nuostata, kad niekas negali būti nuteistas už veiksmus ar neveikimą, kurie pagal galiojusius jų įvykdymo momentu valstybės vidaus įstatymus arba tarptautinę teisę nebuvo laikomi nusikaltimais.

Visi trys požymiai yra tarpusavyje susiję. Nusikaltimo elektroninių ryšių sektoriuje pavojingumas ir priešingumas teisei pasireiškia veika. Jei nėra bent vieno iš būtinųjų nusikaltimo požymių, nėra ir nusikaltimo. Nusikaltimo požymių nebuvimas paprastai pasireiškia tuo, kad veikoje trūksta vieno iš įstatyme įtvirtintų nusikaltimo elektroninių ryšių sektoriuje požymių:

1) padaryta veika pripažįstama pavojinga vyraujančioms vertybėms, tačiau nėra priešinga baudžiamajai teisei;
2) veika priešinga baudžiamajai teisei, tačiau nėra pavojinga vertybių sistemai, nedaro jai žalos.

Su pirmosios rūšies situacijomis, kalbant apie nusikaltimus elektroninių ryšių sektoriuje, susiduriama gan dažnai. Gyvenimas keičiasi: keičiantis socialinėms-ekonominėms sąlygoms, keičiasi ir veikų pavojingumas. Tačiau nepalyginamai greičiau keičiasi padėtis elektroninių ryšių sektoriuje. Galima netgi teigti, kad šiame sektoriuje vyksta pastovūs pokyčiai su pastaruoju metu vis didėjančiu pagreičiu, dėl ko atsiranda vis naujų veikų, keliančių pavojų visuomenei. Šių veikų kriminalizavimas aiškiai atsilieka. Taip susidaro spragos tarp veikų pavojingumo ir jų teisinio įvertinimo. Pavyzdžiui, šiuo metu pasaulyje vykdomi bandymai, siekant turimais elektros tinklais perduoti ne tik elektros signalus, bet ir kitus signalus. Todėl dabar sunku net prognozuoti, kokios naujos pavojingos veikos atsiras pradėjus naudotis šia nauja technologija.

Be minėtų nusikaltimo požymių, baudžiamosios teisės teorijoje prie nusikaltimo požymių dar priskiriami veikos *baudžiamumas* ir *kaltumas*. Šie požymiai neturi savarankiškos reikšmės, nes, pavyzdžiui, priešingumas teisei apima ir kaltumą. Nei viena veika pagal baudžiamąjį įstatymą nebus laikoma nusikaltimu, jei ji bus padaryta nekaltai.

Plačiau nenagrinėjant, būtina pažymėti, kad aukščiau buvo paminėti visi būtinieji visų nusikaltimų, tarp jų ir nusikaltimų elektroninių ryšių sektoriuje, požymiai. Juos galima laikyti bendrais visiems nusikaltimams. Todėl jie nėra labai svarbūs žiūrint per šios analizės prizmę. Šios studijos tikslas – nustatyti tuos specifinius nusikaltimų elektroninių ryšių sektoriuje požymius, kurie leistų išskirti šiuos nusikaltimus iš visų kitų.

Šiandieninės informacinės technologijos sukūrė visiškai naują, iki tol neegzistavusią terpę, aplinką, kurioje įmanoma globali komunikacija, informacijos kaupimas bei perdavimas. Internetas – laisvai prieinamas globalus elektroninių ryšių tinklas. Jam būdinga tai, kad:

1) jame kaupiama bet kokio pobūdžio informacija;
2) didžioji dalis informacijos prieinama bet kuriuo metu;
3) galimas priėjimas prie informacijos tais pačiais telekomunikacijų tinklais tiek civiliams, tiek juridiniams asmenims;
4) informacija gali būti gaunama ir siunčiama bei talpinama iš bet kurios ir į bet kurią pasaulio vietą (erdvės ir laiko apribojimai tampa minimalūs).

Todėl pirmas išskirtinis nusikaltimų elektroninių ryšių sektoriuje požymis – *aplinka*, kurioje atliekami nusikaltimai elektroninių ryšių sektoriuje. Ta aplinka, terpė, sritis – elektroninė erdvė. Ji yra čia pat regima, pasiekiama, bet iš tiesų nežinia kur. Virtualus pasaulis yra jos vieta, o kompiuteris – tik vienas iš galimų tarpininkų, norint patekti į ją. Elektroninė erdvė, pasak G.Willet, išreiškia globalios komunikacijos idėją : suteikia galimybę įvykdyti efektyvų veiksmą per atstumą[29]. Dėl tos priežasties nebereikia, kad koks nors žmogus būtų šalia, jei jis yra ten, kur susikerta virtualios erdvės ir to žmogaus akiračiai.

Nusikaltimai, kurie atliekami naujomis informacinėmis technologijomis, nėra visiškai nauja nusikalstama veika. Tai tradiciniai nusikaltimai – vagystė, terorizmas, šantažas, asmens teisių pažeidimai ir t.t., kurie informacinių technologijų įtakoje įgavo naują formą. Todėl *naujos formos tradicinius nusikaltimus* galima laikyti kitu išskirtiniu šių nusikaltimų požymiu. Tokiems nusikaltimams atlikti reikia naujų įgūdžių ir žinių. Pačios nusikaltimo priemonės, tokios kaip kompiuteris, mobilios ryšio priemonės, orgtechnika (skaneriai, lazeriniai spausdintuvai, kopijavimo aparatai) šiuo metu tampa lengvai prieinamomis kone kiekvienam individui. Netgi informacija, reikalinga nusikaltimui atlikti, dėl informacinių technologinių priemonių yra lengvai pasiekiama. Interneto svetainėse gausu pradedantiesiems įstatymų pažeidėjams detalizuotos medžiagos, kurioje išsamiai išdėstyti algoritmai, programų „nulaužimui“, svetainių ar asmeninių skaitmeninių dokumentų kodai. Interneto tinklapiuose galima surasti organizacijas, kurių narius jungia vienas bendras interesas - sugebėjimas apeiti apsaugos sistemas.

Kaip jau buvo minėta, elektroninių ryšių sektoriuje atliekami nusikaltimai nėra nauji, nauja yra tik atlikimo technologija, reikalaujanti specializuoto žinojimo. Pasauliniame globaliame tinkle – internete – tarp nuolatinių jo vartotojų jau yra susiformavusi specifinė terminija. Ne išimtis šiame procese yra ir nusikaltimų sfera. Dažniausiai pasitaikančiai nusikaltimo atlikimo technikai jau yra pritaikytas žargonas. Jis yra plačiai paplitęs ir dažnai naudojamas ne tik oficialiose, bet ir neoficialiose sferose. Žargono įvedimas palengvina bendravimą ir susikalbėjimą tarp pačių įstatymų laužytojų. Bruceas T.Fraseris išskiria tokius pagrindinius terminus, apibrėžiančius populiariausius nusikaltimo atlikimo metodus[30]:

[29] Willet G. Global Communications: a modern myth? // http://www.unisa.ac.za/dept/press/comca/212/willet.html
[30] Informacinės technologijos ir nusikaltimai // http://www.infovi.vu.lt/ivs.biblioteka/temos/nusikaltimai.htm

a) (data diddling) duomenų trynimas, gadinimas, nelegalus talpinimas – tokiu atveju asmenys, neteisėtai prasibraudami prie tam tikros informacijos, ją gadina, nelegaliai keičia ar tiesiog ištrina;
b) (Trojan horse) Trojos arklys – šiuo atveju į vartotojo kompiuterį be jo žinios ir sutikimo įrašoma kompiuterinė programa, kuri suteikia prieigą prie kompiuteryje saugomos informacijos;
c) (trap door) klastingos durys – prie kompiuterinės programos būna iš anksto nelegaliai prijungta papildoma programa, kuria suteikiama prieiga prie kompiuteryje saugomos informacijos;
d) (saliami) vagystės iš sąskaitų – šiuo atveju nusikaltėliai, naudodamiesi kompiuteriniais tinklais, pralaužia apsaugos sistemas ir prasibrauna prie piniginių sąskaitų, iš kurių tiesiog pervedami pinigai;
e) (pirating) piratavimas - nelegalus programinės įrangos kopijavimas ir platinimas be leidėjo sutikimo.

Specifinė terminija – dar vienas šių nusikaltimų išskirtinių požymių.

Kitas požymis – šio sektoriaus nusikaltimų *latentiškumas*, kuris atspindi šalyje tą realią padėtį, kai dalis nusikaltimų lieka neužregistruoti. Praktiškai visose valstybėse faktinis nusikaltimų skaičius yra didesnis, lyginant su užregistruotais. Taip Federalinio tyrimų biuro[31] duomenimis nuo 85% iki 97% kompiuterinių kėsinimųsi net nėra nustatomi. Kitų ekspertų vertinimu kompiuterinių nusikaltimų latentiškumas Jungtinėse Amerikos Valstijose siekia 80%, Didžiojoje Britanijoje – 85%, Vokietijoje – 75%, Rusijoje – net 90%. Pažymėtina, kad nusikaltimų, atliekamų elektroninių ryšių sektoriuje, latentiškumo priežasčių yra keletas:

1) nukentėjusios šalies (įmonės, įstaigos, organizacijos arba atskiro individo) nenoras pranešti apie nusikalstamą kėsinimąsi. Priežastys gali būti įvairios: baimė prarasti savo autoritetą, teisminio nagrinėjimo metu organizacijos saugumo sistemos trūkumų paviešinimas, baimė, kad bus išaiškinta neteisėta nukentėjusios šalies veikla;
2) konfliktų tarp organizacijų sprendimas savo jėgomis;
3) nukentėjusi šalis nėra įsitikinusi, kad kaltininkai bus nubausti, o prarastos piniginės lėšos ar kitas turtas bus grąžintas;
4) žemas žmonių teisinės sąmonės lygis, nežinojimas savo teisių ir nenoras ginti savo teisių ir teisėtų interesų teisiniais metodais;
5) nepakankamos personalo, atsakingo už kompiuterinės sistemos ar kitokios sistemos informacijos apsaugą, žinios apie nusikaltimus šioje srityje ir kt.

[31]Проблемы латентности комьютерной преступности // http://www.crime-research.ru

Didelis latentiškumas tam tikroje aplinkoje sukuria psichologinę nebaudžiamumo nuostatą už visuomenei pavojingas veikas, skatina nusikaltėlius atlikti naujas nusikalstamas veikas, kurti pastovius nusikalstamus susivienijimus, mažina baudžiamojo įstatymo prevencinę vertę, blogina moralinį klimatą valstybėje ir pan.

Nusikaltimai, kurie atliekami naudojant informacines technologijas, tokias kaip mobilios ryšio priemonės, nešiojami bei stacionarūs kompiuteriai, profesionali orgtechnika ir skaitmeniniai įrenginiai minimizuoja laiko ir erdvės sąnaudas. Jų pagalba sudėtingus nusikaltimus gali atlikti vienas individas. Tokie nusikaltimai, kaip pinigų vagystės iš sąskaitų, pinigų „plovimas“, piktnaudžiavimas telekomunikacijų ryšiais, atliekami globaliu mastu per komunikacijos tinklus. Galima teigti, kad informacinės technologijos iš esmės pakeitė kai kuriuos socialiniams reiškiniams būdingus bruožus. Pagrindiniai iš jų - tai erdvė, laikas ir identitetas. Laiko ir erdvės sąnaudos, norint pasiekti reikiamą objektą, tapo minimalios. Identifikacijos procese, identifikuojamas nebe konkretus asmuo, o tiesiog skaičių kombinacija, interneto protokolas. Todėl galima išskirti ir tokius bruožus (požymius), būdingus nusikaltimui, kuris virtualioje erdvėje atliekamas per komunikacijos tinklus:

1) *kontaktas su nusikaltimo objektu vyksta tiesiogiai, realiame laike;*
2) *bet kuri sistema, prijungta prie globalaus ryšio tinklo, pasiekiama iš bet kurios pasaulio vietos;*
3) *anonimiškumas* – anonimu tampa tiek nusikaltėlis, tiek ir auka.

Išskirtiniu nusikaltimų elektroninių ryšių sektoriuje požymiu laikytina sąmoninga ir valinga *veika*, kuri pasireiškia tik aktyvia elgesio forma, tam tikrų veiksmų ar jų komplekso atlikimu. Pavyzdžiui, perėmimas, pakeitimas, siuntimas, įvedimas, ištrynimas, naudojimas, parūpinimas, pateikimas, siūlymas, reklamavimas ir kitoks platinimas.

Dar vienas išskirtinis nagrinėjamų nusikaltimų požymis – *nusikalstamos pasekmės*. Lietuvoje dauguma nusikaltimų elektroninių ryšių sektoriuje sudėčių yra materialios, todėl nusikaltimui nustatyti būtinas nusikaltimo rezultatas – pasekmės, kurios nurodo, kokie pakitimai įvyko nusikaltimo objekte. Pasekmės gali būti:

1. turtinės – turtinė žala arba didelė turtinė žala, pavyzdžiui, Lietuvos Respublikos BK 179 straipsnio 1,2 ir 3 dalys; 196 straipsnio 1 dalis; 197 straipsnio 1 dalis; 285 straipsnio 1 dalis ir kt.;
2. organizacinės;
3. moralinės – pavyzdžiui, Lietuvos Respublikos BK 166 straipsnio 1 dalis; 191 straipsnio 1 ir 2 dalys; 198 straipsnio 1 dalis ir kt.

Išimtis - kai pažeidžiamos konstitucinės teisės ar ypač saugomi teisiniai gėriai, pavyzdžiui, privačių komunikacijų perėmimas. Tai rodo, kad jau pati veika, kai įsikišama į privatų

komunikavimą, yra pavojinga, ir kad bausti reikia jau už tokią nusikalstamą veiką (įsikišimą), nesvarbu, ar kils žalingos pasekmės.

Panaši padėtis ir kitose pasaulio valstybėse. Štai JAV Sukčiavimo ir piktnaudžiavimo, panaudojant kompiuterius, įstatymas[32], nustatydamas nusikalstamas veikas formuluoja joms ir nusikalstamas pasekmes, kurios yra gana specifinės:

- pasisavinama įstatymo saugoma ar valstybinė informacija;
- pasisavinama finansinė informacija;
- paveikiamas vyriausybės institucijos naudojimasis kompiuteriu ir pan.

JAV Elektroninių ryšių slaptumo įstatyme[33] numatyta, kad baudžiamas už nusikaltimą tas, kas neteisėtai prieina prie įrenginio ir pasisavina ar pakeičia kompiuterinę informaciją arba apriboja priėjimą prie elektroninių ryšių.

Kiek kitokia padėtis Kanadoje. Pagal Kanados Baudžiamąjį kodeksą[34] dauguma nusikaltimų elektroninių ryšių sektoriuje sudėčių formalios, kriminalizuojančios tik pavojingas veikas:

- privačių komunikacijų perėmimas (184 straipsnio 1 dalis);
- telekomunikacinių paslaugų vagystė (326 straipsnio 1 dalies b punktas);
- neteisėtas tiesioginis ar netiesioginis naudojamasis kompiuterinėmis paslaugomis (342 straipsnio 1 dalies a punktas);
- neteisėtai naudojantis elektromagnetiniu, akustiniu, mechaniniu ar kitu įrenginiu tiesiogiai ar netiesiogiai perimamos kompiuterinės sistemos funkcijos (342 straipsnio 1 dalies b punktas) ir kt.

Didžiosios Britanijos 1990 metų Piktnaudžiavimo, panaudojant kompiuterius, įstatymu[35] taip pat kriminalizuotos tik pavojingos veikos: neteisėta prieiga prie kompiuterinės medžiagos ir neteisėta prieiga, kurios tikslas - atlikti ar palengvinti kitus nusikaltimus.

Apibendrinant valstybių praktiką, būtina pažymėti, kad pavojingų veikų kriminalizavimas atskirose valstybėse skiriasi. Tinkamiausias jis Kanadoje, kur dauguma nusikaltimo sudėčių – formalios, o nusikalstamos pasekmės neįvardijamos. Esmė ta, kad vienas iš nusikaltimų elektroninių ryšių sektoriuje požymių yra tai, kad jau pačios veikos, kai įsikišama į signalų perdavimą ar trukdoma perduoti signalus, yra pavojingos ir baustinos. Tai sąlygoja šio sektoriaus specifika:

- spartus informacinių technologijų vystymasis;

[32] Fraud and related activity in connection with computers // http://www.usdoj.gov/criminal/cybercrime/fedcode.htm
[33] Interception and disclosure of wire, oral, or electronic communications prohibited // http://www4.law.cornell.edu/uscode/18/2511.html
[34] Canadian Criminal Code // http://www.digitaldefence.ca/Kanada CriminalCode.htm
[35] Computer Misuse Act 1990 In United Kingdom // http://www.hmso.gov.uk/acts/acts1990/Ukpga 19900018 en 1.htm

- interneto, kaip globalaus pasaulinio tinklo, visuotinumas;
- visų šiuo metu pasaulyje esančių tinklų konvergencija;
- didelis besinaudojančiojo elektroniniais ryšiais anonimiškumas ir kt.

Tai, kad Kanadoje dauguma nusikaltimų elektroninių ryšių sektoriuje sudėčių yra formalios, paaiškinama dar viena priežastimi. Kaip nurodoma baudžiamojoje teisėje, jei nusikaltimo sudėtis yra formali, tai nusikaltimo vieta bus ta vieta, kur buvo atlikta neteisėta veika, o jei nusikaltimo sudėtis materiali – vieta, kur atsirado pasekmės. Esmė ta, kad šiandieninės informacinės technologijos leidžia atlikti nusikalstamas veikas iš bet kurios pasaulio vietos, o visų kilusių pasekmių nustatyti praktiškai neįmanoma.

Vietos problema iškyla ir tiriant bei nustatant asmenį, padariusį nusikaltimą. Nusikaltimo elektroninių ryšių sektoriuje tyrimo metu, jei pavyksta, yra nustatomas kompiuteris, iš kurio yra įvykdytas nusikaltimas, tačiau tai ne visada nurodo asmenį, padariusį nusikaltimą. Gerai, jei asmenys, dirbantys kompiuteriu, yra registruojami nurodant laiką, nuo kada iki kada asmuo dirbo, tačiau jei tai neregistruojama, o su kompiuteriu gali dirbti daugelis žmonių? Tada kaltininko nustatymas pasidaro dar sunkesnis. Bet tai jau yra ikiteisminio tyrimo problema - iš asmenų, galėjusių dirbti su kompiuteriu, rato išskirti asmenį, padariusį nusikaltimą, ir įrodinėjimo problema, nes asmens kaltumą reikia įrodyti remiantis Baudžiamojo proceso kodekso normomis.

Pažymėtina, kad tam tikra specifika nusikaltimų elektroninių ryšių sektoriuje būdinga ir subjektyviosios nusikaltimo sudėties pusei. Subjektyvioji nusikaltimų darymo pusė susideda iš *kaltės, motyvų ir tikslų*. Visų pirma iškyla tokių problemų, kaip: ar galima nusikaltimus elektroninių ryšių sektoriuje atlikti neatsargiai ar tik tyčia? Tyčia – tai tokia kaltės forma, kai kaltininkas supranta daromos veikos pavojingumą, numato jos pasekmes ir jų siekia arba, jei ir nenori tokių pasekmių, sąmoningai leidžia joms kilti. Analizuojant Nusikaltimų elektroninėje erdvėje konvenciją[36], nesunku pastebėti, kad visose pavojingose veikose, susijusiose su signalų perdavimu, valstybių kriminalizavimui siūloma kaltės forma – tyčia. Tyčia akcentuojam ir kituose ankstesniuose teisės aktuose, reglamentuojančiuose kompiuterinius nusikaltimus. Tas pats pasakytina ir apie atskirų valstybių įstatymus. Tiek autoriaus nagrinėtų Europos Sąjungos šalių – Didžiosios Britanijos ir Vokietijos, tiek ir JAV, Kanados ir Rusijos bei Lietuvos teisės aktuose akcentuojama tyčia. Todėl *tyčia* yra nusikaltimų elektroninių ryšių sektoriuje subjektyviosios pusės išskirtinis požymis.

Kaip nustatyti, ar asmens veiksmai buvo tyčiniai? Jeigu teigtume, kad įsikišimas į signalų perdavimą galimas tik tyčia, tai kaip vertintume žmogaus veiksmus, kai jis į signalų perdavimą įsijungia dėl programinės įrangos gedimų ar kitų klaidų arba dėl kito žmogaus veiksmų, kai yra

[36] Convention on Cybercrime // http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

paliekamas kelias (galimybė) visiems norintiesiems. Ar veiksmai tyčiniai, galime nustatyti iš nusikaltimo rengimosi stadijos, kurios vienokie ar kitokie pėdsakai visada pasilieka vykdant nusikaltimą. Pavyzdžiui, slaptažodžio parinkimas pasinaudojant specialia programa. Dažniausiai tokios programos sukūrimas ar tiesiog įsigijimas jau rodo rengimąsi įsilaužti. Būtent rengimosi ir kėsinimosi stadijos įmanomos tik tyčiniuose nusikaltimuose.

Įsikišimas į signalų perdavimą atliekamas dėl įvairių paskatų, motyvų, siekiant pačių įvairiausių tikslų ir rezultatų, tokių kaip:

- savanaudiškumo (kai tikimasi pasipelnyti);
- politinių motyvų (kai siekiama gauti tam tikrą informaciją ir paskui pasiekti tam tikrų politinių sprendimų);
- noras ištirti, kas paslėpta;
- noras parodyti savo sugebėjimus;
- kerštas ir kt.

Teisinėje literatūroje motyvai, atsižvelgiant į objektą, skirstomi taip:

- karinės ir žvalgybos atakos;
- biznio atakos;
- finansinės atakos;
- teroristinės atakos;
- neapykantos atakos;
- pasilinksminimo atakos.

Lyginant nusikaltimų elektroninių ryšių sektoriuje motyvus ir tikslus su nusikaltimų elektroninėje erdvėje ar visų kompiuterinių nusikaltimų tikslais ir motyvais, nesunkiai galime pastebėti, kad jie yra labai panašūs.

Tam tikrą specifiką turi ir nusikaltimų elektroninių ryšių sektoriuje objektas, kuris autoriaus nagrinėjamas kitame studijos poskyryje.

2.2. Nusikaltimų elektroninių ryšių sektoriuje objektai

Daugelio šiandieninių nusikaltimų objektas yra nustatomas gan nesunkiai, pavyzdžiui, tokių tradicinių nusikaltimų, kaip vagystė ar žmogžudystė, atitinkamai – nuosavybė ir žmogaus gyvybė. Tačiau koks nusikaltimo objektas, kokie teisiniai gėriai pažeidžiami, kai neteisėta veika bet kuriuo iš būdų yra neteisėtai įsikišama į signalų perdavimą laidinėmis, radijo, optinėmis ar kitomis elektromagnetinėmis priemonėmis arba laidinėmis, radijo, optinėmis ar kitomis elektromagnetinėmis priemonėmis yra perduodami neteisėti signalai? Vienareikšmiškai į tai atsakyti nėra lengva, nes nusikaltimais elektroninių ryšių sektoriuje gali būti pažeidžiama daugybė įstatymų saugomų gėrių. Pavyzdžiui, pagal Lietuvos Respublikos Baudžiamąjį kodeksą, tokiais saugomais gėriais yra :

- privataus gyvenimo neliečiamumas;
- viešoji tvarka;
- informatika;
- intelektinė ir pramoninė nuosavybė;
- nuosavybė, turtinės teisės ir turtiniai interesai ir kt.

Logiškai kyla klausimas, koks požymis vienija nusikaltimus, kuriais pažeidžiami skirtingi saugomi gėriai ir kurie yra priskiriami prie nusikaltimų elektroninių ryšių sektoriuje? Siekiant išsiaiškinti visus objekto požymius, toliau bus nagrinėjami kompiuteriniai nusikaltimai, apimantys telekomunikacinius nusikaltimus ir sudarantys didžiąją dalį nusikaltimų elektroninių ryšių sektoriuje.

Teisinėje literatūroje nurodoma, kad nusikaltimo objektas – tai teisiniai gėriai, kurie pažeidžiami padarant nusikaltimą. Nusikaltimo dalykas – materiali išraiška, kuria pažeidžiamas objektas. Kriminalistinėje literatūroje pateikiama tokia objektų klasifikacija :

- bendrasis – visi teisiniai gėriai. Bendras objektas yra vieningas visiems nusikaltimams;
- rūšinis – vienarūšių ar tapačių teisinių gėrių dalis;
- tiesioginis – teisinis gėris, į kurį kėsinamasi konkrečiu nusikaltimu.

Kalbant apie kompiuterinių nusikaltimų objektą, būtina paminėti, kad pasaulyje susiformavo dvi skirtingos nuomonės :

1) viena tyrėjų grupė prie kompiuterinių nusikaltimų priskiria veiksmus, kuriuose kompiuteris yra arba kėsinimosi objektas, arba įrankis;
2) kitos grupės tyrėjai, prie kompiuterinių nusikaltimų priskiria tik neteisėtus veiksmus informacijos apdorojimo procese. Pagrindinis kvalifikuojantis požymis, leidžiantis priskirti šiuos nusikaltimus prie nurodytos grupės, - kėsinimosi būdų, įrankių, objektų

bendrumas. Kitais žodžiais tariant, kėsinimosi objektu yra informacija, apdorojama kompiuterinėse sistemose, o kompiuteris tarnauja tik kaip kėsinimosi įrankis.

Pažymėtina, kad daugelio šalių įstatymų leidyba pasuko šiuo antruoju keliu.

Analogiškai, nusikaltimų elektroninių ryšių sektoriuje, kėsinimosi objektu, autorius siūlo laikyti informaciją, nes dažniausiai šios rūšies nusikaltimuose kėsinimosi įrankiu tampa kompiuteris.

Visų kompiuterinių nusikaltimų *bendruoju objektu* laikomi visuomeniniai santykiai, saugomi baudžiamojo įstatymo.

Tam, kad apibūdintume rūšinį objektą, būtina išsiaiškinti informacinio saugumo sąvoką. Teigiama, kad kompiuterinių nusikaltimų objektu galima laikyti informacinį saugumą, t.y. visuomeninius santykius, atsirandančius informacinės aplinkos funkcionavimo sferoje ir užtikrinančius saugumo būseną. Tuo tarpu informacinis saugumas – tai asmens, visuomenės, valstybės gyvybiškai svarbių interesų informacinėje terpėje saugumo būsena, apsauganti nuo vidinių ir išorinių grėsmių, užtikrinanti jos formavimą, naudojimą ir vystymą vardan žmonių, visuomenės, valstybės interesų. Informacinio saugumo sąvokos išsiaiškinimui tikslinga nustatyti, išanalizuoti ir klasifikuoti visas grėsmes.

Literatūroje yra pateikiama daug informacinio saugumo grėsmių klasifikacijų. Autoriaus nuomone, informatyviausios, atsižvelgiant į klasifikavimo objektą, yra šios:

1.Pagal grėsmių atsiradimo šaltinį:

- išorinės – grėsmės, susijusios su stichinėmis nelaimėmis, politiniais, socialiniais faktoriais, informacinių ir komunikacinių technologijų vystymusi, jau minėta tinklų konvergencija ir pan.;
- vidinės – grėsmės, susijusios su informacinių komunikacinių technologijų gedimu ir programavimo klaidomis.

2.Pagal atsiradimo pobūdį:

- objektyvios – tai grėsmės, atsirandančios stichiškai ir nepriklausančios nuo žmogaus valios;
- subjektyvios – tai grėsmės, atsiradusios dėl poveikio informacinei žmogaus sferai. Šios grėsmės savo ruožtu dar gali būti skirstomos į atsitiktines ir tyčines.

3.Pagal poveikio pobūdį : naudojantis teisėta prieiga ir naudojantis paslėptais kanalais.

4.Pagal įvykdymo tikslą : konfidencialumo pažeidimai, vientisumo pažeidimai, pasiekiamumo pažeidimai ir k.t.

5.Pagal poveikio pobūdį : aktyvūs ir pasyvūs.

Iš pateiktos klasifikacijos matyti, kad pagrindinės informacinio saugumo problemos susijusios su žmonių veiksmais, nes būtent jie yra visų nusikaltimų ir pažeidimų pagrindinė priežastis.

Atsižvelgiant į tai, kas išdėstyta, kompiuterinių nusikaltimų *rūšiniu objektu* galime laikyti visumą visuomeninių santykių, užtikrinančių kompiuterinės informacijos saugumą, t.y. teisėtą ir saugų kompiuterinės informacijos, informacinių sistemų, informacinių resursų, informacinių technologijų ir aprūpinimo priemonių kūrimą, platinimą ir naudojimą. Savo ruožtu *rūšiniu objektu* nusikaltimų elektroninių ryšių sektoriuje turėtume laikyti *visumą visuomeninių santykių, užtikrinančių informacijos saugumą*, t.y. teisėtą ir saugų informacijos, informacinių sistemų, informacinių resursų ir informacinių technologijų naudojimą ir platinimą.

Šių nusikaltimų dalyku yra *informacinė aplinka*, t.y. subjektų veikla, susijusi su informacijos sukūrimu, keitimu ir vartojimu. Tolesniam nagrinėjimui būtina įvertinti, kad, jeigu informacija yra ne objektas, o pasikėsinimo priemonė į kitą baudžiamosios teisės saugomą objektą, tai būtina išsiaiškinti, ar tai buvo mašininė informacija, t.y. informacija, kuri yra produktas, pagamintas su kompiuterine technika arba kompiuterinei technikai, ar ji turėjo kitą „nekompiuterinį“ požymį. Pirmuoju atveju nusikaltimai priskiriami kompiuteriniams nusikaltimams, antruoju – ne kompiuteriniams nusikaltimams.

Pažymėtina, kad mašininė informacija suprantama kaip informacija, cirkuliuojanti kompiuterinėje sistemoje, fiziniame informacijos nešėjuje užfiksuota formoje, kurią galima priimti elektronine skaičiavimo mašina arba perduoti telekomunikaciniais kanalais, t.y. ji suformuota kompiuterinėje aplinkoje ir persiunčiama iš vieno kompiuterio kitam, iš vieno kompiuterio į periferinį įrenginį arba į įrangos valdymo daviklį elektromagnetiniais signalais. Kitais žodžiais tariant, mašininė informacija yra ne kas kita, kaip signalai. Tolesniam nagrinėjimui būtina išsamiai išsiaiškinti informacijos sąvoką, kilmę ir jos svarbą šiandienos ir rytojaus žmonių gyvenime.

Pats žmonių visuomenės atsiradimas ir egzistavimas iš pat pradžių yra pagrįstas galimybe informacinių mainų, egzistuojančių pačiomis įvairiausiomis formomis nuo protingo bendravimo kalba, laiškais iki apsikeitimo veikla, technologijomis, mokslo žiniomis, darbo rezultatais ir produktais. Tačiau maždaug iki XX amžiaus vidurio terminas „informacija“ buvo vartojamas kaip žinių, pranešimų, signalų sinonimas. Pati informacijos samprata buvo traktuojama ganėtinai paprastai – kaip kažkokia realybė, objektyviai egzistuojanti greta daiktų arba pačiuose daiktuose[37].

Vystantis duomenų perdavimo techninėms priemonėms ir ypač atsiradus kompiuteriams, kurių dėka tapo įmanomas apsikeitimas duomenimis ne tik tarp žmonių, bet ir tarp žmogaus ir

[37] Батурин Ю. М. Проблемы компьютерного права - М.: Юридическая литература, 1991.с.14-15.

technikos (kompiuterio), „informacinis sprogimas“ labai pakeitė požiūrį į informacinės veiklos produktus.

Šiandien informacija suprantama ir laikoma vienu iš svarbiausių visuomenės vystymosi resursų. Informacijos paradigmos rėmuose pažymima, kad įvairių socialinių-ekonominių reiškinių ir procesų substancija yra informacija. Įvairūs politiniai, socialiniai, psichologiniai ir ekonominiai reiškiniai (procesai) turi informacinę aplinką arba informacijos užduotą genetinį pagrindą. Informacinę aplinką turi ir ekonominė dinamika ir socialinių procesų dinamika. Tinkamiausiu patvirtinimu, kad vidine sudėtimi ekonominių reiškinių yra informacija, tarnauja didelis informacijos paplitimas ir praktinis tokio šiuolaikinio finansinio instrumento, kaip elektroniniai pinigai, pritaikymas labiausiai išsivysčiusiose šalyse. Būtent elektroniniai pinigai labiausiai išryškina vertybių informacinius požymius. Elektroniniuose piniguose vertybė labiausiai visapusiškai realizuoja savo esmę, kai pinigų informacinis turinys išreiškia save adekvačioje (skaitmeninėje) formoje, nusimesdamas taip įprastus auksinius, sidabrinius ir popierinius rūbus. Informacinėje visuomenėje su informacinio tipo ekonomika visi socialiniai-ekonominiai fenomenai (resursai, vertybės, turtas) realizuoja save labiausiai adekvačia, visuotine forma – informacine forma (informacinių resursų, elektroninių resursų, informacijos turto).

Pažymėtina, kad nors samprata „informacija“ yra abstrakti, ji visada pasireiškia materialiai-energetinėje formoje, dažniausiai signalų pavidalu. Signalas informavimo procese atlieka informacijos nešėjo funkciją nuo šaltinio iki imtuvo ir toliau iki gavėjo. Priklausomai nuo konkrečių sąlygų, informacijos perdavimo procesas gali būti daugiapakopis. Pats informacinis procesas prasideda tam tikrame šaltinyje esančios informacijos paėmimu ir baigiasi signalo suformavimu, kurio dėka perduodama informacija. Tai tapo įmanoma dėl to, kad signalas, turintis materialinę išraišką (elektros srovės impulsas, elektromagnetinis virpesys, kvapas, garsas ir t.t.), charakterizuojamas tam tikra struktūra, kurią galima išreikšti tam tikra diskrecine forma.

Tokiu būdu informacijos perdavimas reiškia informacijos perdavimą per atstumą, jos judėjimą laike ir erdvėje vienokio ar kitokio signalo pavidalu.

Mašininės informacijos, kaip nepriklausomo baudžiamosios teisės normomis saugomo gėrio, išskyrimas yra pagrįstas jos specifinėmis savybėmis. Literatūroje išskiriami tie požymiai, kurie turi vienokią ar kitokią reikšmę teisei:

1) apibrėžtas informacijos savarankiškumas santykyje su jos nešėju;
2) galimybė tą pačią informaciją naudoti daug kartų;
3) informacijos išsilaikymas ją naudojant;
4) fizinis informacijos nesidėvėjimas;
5) galimybė išsaugoti ir suspausti;
6) informacijos kiekybinis apibrėžtumas;

7) informacijos sistemiškumas.

Nusikaltimams prieš nuosavybę Baudžiamojoje teisėje yra priimta nustatyti tris požymius: fizinį, ekonominį ir juridinį. Tokių požymių nustatymas kompiuterinei informacijai yra labiausiai priimtinas iš būdų, nustatant ją kaip nusikaltimo dalyką.

Fizinis požymis. Kompiuterinės informacijos, kaip nusikaltimo dalyko, specifika pasižymi negalėjimu priskirti jos prie materialių ar nematerialių dalykų. Informacija, kaip nematerialus dalykas, į visuomeninių santykių sistemą įtraukiama dėka materialaus informacijos nešėjo, t.y. fizinis kompiuterinės informacijos, kaip nusikaltimo dalyko, požymis apima informacijos nešėją, kuris dažniausiai suprantamas kaip dalykas, daiktas, kurio požymiai naudojami informacijos perdavimui, saugojimui ir apdorojimui. Kompiuterinės informacijos nešėjais yra diskeliai, optiniai ir kietieji diskai ir pan. Kalbant apie kompiuterinę informaciją taip pat būtina įvertinti, kad viena iš šiandieninės kompiuterizacijos etapo charakteristikų yra elektroninių ryšio priemonių vystymasis. Informacija ryšio kanalais perduodama dėka signalų, kurie taip pat yra materialūs informacijos nešėjai. Pavyzdžiui, elektroniniai signalai telefoninio ryšio linijose gali būti informacijos nešėjais kompiuteriniuose tinkluose. Būtent tokia kompiuterinės informacijos samprata leidžia mums kompiuterinės informacijos sunaikinimą arba iškraipymą traktuoti ne tik kaip poveikį kompiuterio įrenginiams, bet ir signalams, perduodamiems tarp kompiuterių.

Tokiu būdu kompiuterinės informacijos, kaip nusikaltimo dalyko, fizinis požymis yra nešėjas – kaip daiktas arba signalas, kurio fiziniai, cheminiai arba kitokie požymiai naudojami informacijos perdavimui ir apdorojimui bei atpažįstami elektroninės skaičiavimo mašinos.

Informacija, kaip nusikaltimo dalykas, turi ir ekonominį požymį, kainą, kurią apsprendžia turinys ir vartotojo suinteresuotumas ją įsigyti. Pabrėžiama, kad kaip prekė informacija turi labai daug specifinių savybių: yra nesunaikinama vartojimo procese; perduodamas vartotojui gamintojas jos nepraranda; informacijos nauda subjektyvi ir neapibrėžta; ypatingas jos senėjimo procesas – ji ne sunaudojama, o praranda aktualumą. Informacijos svarba įvairi: ji gali būti svarbi iš esmės (kaip ilgo darbo rezultatas) arba pagal paskirtį (tam tikros užduoties atlikimui).

Kompiuterinės informacijos juridinis požymis reiškia tai, kad ji turi būti svetima kaltinamajam ir turėti savininką.

Tokiu būdu, apibendrinant tai, kas išdėstyta, ir vadovaujantis šioje studijoje suformuluotu teiginiu, kad kompiuteriniai nusikaltimai sudaro didžiąją dalį visų nusikaltimų elektroninių ryšių sektoriuje, informaciją elektroninių ryšių sektoriuje kaip nusikaltimo dalyką galima apibūdinti taip: tai žinios apie objektyvųjį pasaulį ir jame vykstančius procesus, kurių visapusiškumas, konfidencialumas ir prieinamumas užtikrinamas dėka kompiuterinės, telekomunikacinės, radijo, optinės ir kitos elektroninės technikos, ir kurios turi kainą ir savininką.

2.3. Nusikaltimų elektroninių ryšių sektoriuje precedentai

Kompiuteriais ir komunikaciniais tinklais yra saugomos ir perduodamos didelės apimties materialinės ir intelektualios vertybės. Informacija, susijusi su medicinos klausimais, draudimu, moksliniais tyrimais, socialiniu aprūpinimu, teisėtvarka ir šalies gynyba, iš spintų ir darbo stalų persikelia į virtualias darbo vietas. Kartu kompiuteriniai tinklai, elektroninis paštas ir kitos komunikacijos priemonės tampa politikos instrumentu: šalies Prezidento administracijos elektroninio pašto adresai plačiai žinomi ir intensyviai naudojami. Apskrities ir vietos savivaldos administracijų valstybiniai institutai taip pat yra prisijungę prie kompiuterinių tinklų.

Nusikaltimai elektroninių ryšių sektoriuje išsidėstę nuo katastrofiškai didelio iki paprasčiausiai erzinančio lygio. Paprasčiausias kompiuterinio špionažo atvejis gali smarkiai paveikti nacionalinį saugumą. Vienas kompiuterinės vagystės atvejis gali pašalinti konkurentę kampaniją iš verslo. Paprasti krakerio pajuokavimai faktiškai jokių nuostolių nepadaro, tačiau video kampanijoms, interneto svetainėms arba bet kuriam kompiuterio naudotojui gali sukelti susierzinimą. Dalis nusikaltimų atliekami juokais dėl socialinių ar poltinių priežasčių; kiti – profesionalių nusikaltėlių verslas. Nėra kito tokios formos nusikaltimo, kuris turi tiek rūšių nusikaltėlių ir atliekamų nusikalstamų veikų.

Nusikalstamos veikos, atliekamos elektroninių ryšių sektoriuje, pasižymi ypač dideliu įvairiapusiškumu. Kai kurios iš jų yra žinomos (klasikinės), tačiau aplinka, kurioje jos atliekamos – nauja, kitos – iš esmės naujos. Siekiant atskleisti jų savitumą ir pavojingumą, toliau pateikiami nusikaltimų elektroninių ryšių sektoriuje precedentai.

A. Kiber sukčiavimas ir kiber vagystė.

*Kevinas Mitnikas - vienas iš žinomiausių hakerių. Jis tapo pasaulio „įžymybe“ po to, kai 1994 metais buvo nubaustas 5-rių metų laisvės atėmimo bausme. Neteisėtą veiką K.Mitnikas pradėjo dar 1982 metais, kaip telefoninis frikeris (phreaking), kai naudodamasis metodu whick ahcker galėjo laisvai prieiti prie firmų Motorolla, Intel, IBM, At*T ir kt. duomenų. Federalinių tyrimų biuro (toliau – FTB) duomenimis, K.Mitnikas padarė daugiau kaip 100 milijonų JAV dolerių nuostolių vien per 1982 – 1990 metus[38]. Nuo 1990 metų jis buvo vienas iš labiausiai FTB ieškomų asmenų ir beveik du metus buvo priverstas slapstytis. Penkeri metai laisvės atėmimo už tokio masto nusikalstamą veiką tikrai nedaug, tačiau, kaip nurodoma literatūroje, viena iš priežasčių – pritrūkta įrodymų.*

Vis labiau augant elektroninei komercijai, Pasaulinis tinklas – internetas dėl patogumo ir pigumo suteikia naudingas galimybes investavimui. Greta to, internetas tampa pagalbininku nusikaltėliams kiber sukčiavimuose. Pasikėsinimų į biržų fondus ir bankų finansinius aktyvus

[38] Danko Vukovic „Computer Crime“ // http://www.elitesecurity.org/tema/477/

skaičius pastebimai didėja, o sukčiavimo būdu pasisavinamų lėšų suma auga. To geras pavyzdys, *nusikalstamas susitarimas tarp Vladimiro L.Levino ir daugybės pagalbininkų, kurie neteisėtai įsilaužė į „Citibank“ banko kompiuterius ir elektroniniu būdu „pasiėmė“ iš banko klientų sąskaitų apie 10 milijonų JAV dolerių.*[39] *Klientų sąskaitos buvo „Citibank“ banko filialuose JAV Kalifornijos valstijoje, Suomijoje, Vokietijoje, Olandijoje, Šveicarijoje ir Izraelyje. V.Levinas, matematikos ir kompiuterių specialistas, naudodamas personalinį kompiuterį ir pavogtus slaptažodžius bei identifikavimo kodus, daugiau kaip keturiasdešimt kartų gavo neteisėtą prieigą prie „Citibank“ banko valdymo sistemos. V.Levinas 1995 metais buvo sulaikytas Londone ir išduotas JAV. 1998 m. vasario 24 dieną jis buvo nuteistas trejų metų laisvės atėmimo bausme ir įpareigotas sumokėti „Citibank“ bankui 240 tūkstančių JAV dolerių.*

Pažymėtina, kad sukčiavimas elektroninių ryšių sektoriuje gali pasireikšti:

1) sukčiavimu prekyboje, pvz., elektroniniai aukcionai;
2) sukčiavimu kreditinėmis kortelėmis;
3) finansiniu sukčiavimu, pvz., internete paskelbus melagingą informaciją, dirbtinai sumažinama kampanijos akcijos kaina.

Po sukčiavimų elektroninių ryšių sektoriuje ne mažiau populiarios yra kiber (elektroninės) vagystės. Kiber vagys gali vogti iš kiber bankų arba neteisėtai gauti prieigą prie intelektinės nuosavybės. Pavyzdžiui, *2003 metais spaudoje pasirodė pranešimas, kad FTB atlieka tyrimą, kurio metu nežinomi hakeriai neteisėtai pagrobė kompanijos, kurios veikla susijusi su pinigų pervedimu, 8 milijonų kreditinių kortelių numerius.*[40] *Pasaulyje garsi kompanija Data Processors International, kuri atlieka transakcijas su VISA, MASTERCARD, American Express ir Discover Financial Service kortelėmis, pranešė apie įsilaužimą į jos sistemą. Įmonėms, kurios užsiima kreditinių kortelių gamyba, teks sumokėti po 4 – 5 JAV dolerius už kiekvienos plastikinės kortelės, kurios numeris buvo pavogtas, pakeitimą. Atsižvelgiant įtai, bendra nuostolių suma išaugs iki 32 – 40 milijonų JAV dolerių*.

Minėti atvejai parodo, kad sukčiavimas ir vagystė, naudojantis kompiuterinėmis sistemomis ir tinklais, tampa vis labiau pavojingi, o jų daroma žala skaičiuojama milijonais. Kovoti su šios rūšies nusikaltimais labai sunku dėl šioje studijoje įvardintų priežasčių. Teisinėje literatūroje nurodoma, kad JAV gauna apie 250 skundų per dieną dėl įtarimų kiber sukčiavimu. Tai sudaro daugiau nei 54000 skundų per metus. Bandymai nuspėti būsimus nusikalstamos veikos pasireiškimus sudėtingi, o rezultatai – minimalūs. Tam įtakos dalinai turi interaktyvios

[39]Statement for the Record of Louis J. Freeh, Director Federal Bureau of Investigation On Cybercrime Before the Senate Committee on Judiciary Subcommittee for the Technology, Terrorism, and Government Informatikon Washington, D.C.,March 28, 2000 // http://4uth.gov.ua/usa/english/tech/crimesip/freeh328.htm

[40] ФБР расследует беспрецедентный взлом систем кредитных карт.Похищено 8 млн номеров // http://palm.newsru.com/world/19may2003/rus hackers.html

(elektroninės) prekybos augimas. Dauguma tokios prekybos dalyvių nesusipažinę su elektroninės prekybos ypatumais ir tokiu būdu linkę į sukčiavimą.

B. Elektroniniai ryšiai, padedantys atlikti kitus nusikaltimus.

Retai, tačiau vis dar pasitaiko taip vadinamų telefoninio arba radijo piratavimo atvejų. Vienas iš tokių atvejų buvo aprašytas spaudoje. Piktybinį radijo piratą, kuris ganėtinai ilgą laiką sukeldavo avarines situacijas prie Maskvos „Šeremetjevo“ aerouosto, pavyko sulaikyti Federalinės saugumo tarnybos darbuotojams.[41] *Nustatyta, kad sulaikytasis, naudodamasis pietų Korėjoje pagamintu radijo bangų siųstuvu, uždraustu naudotis Rusijos teritorijoje, sugebėjo prisijungti telefoną sode. Siųstuvą jis sumontavo ant nedidelės vilos, esančios netoli tarptautinio aerouosto, stogo ir nukreipė signalą į mieste esantį butą. Tokiu būdu buvo prisijungiama prie telefono, esančio Maskvoje, net neįtariant, kad tokiu būdu aerouosto lėktuvų ekipažams ir keleiviams sukeliamas mirtinas pavojus. Esmė ta, kad dėl stipraus radijo siųstuvo signalo neveikdavo kai kurie lėktuvų navigaciniai prietaisai, tarp jų - ir aukščio matuoklis. Neveikiant aukščio matuokliui, lėktuvo pilotai negalėdavo nustatyti, kiek metrų juos skiria nuo žemės, kada išleisti šasi (*važiuoklę – aut. pastaba*) ir pan.*

Elektroninių ryšių sektoriuje svarbiausias vaidmuo tenka kompiuteriams ir kompiuterizuotoms sistemoms, nesvarbu, ar tai būtų personalinis kompiuteris ar skaitmeninės technologijos, kuriomis veikia telekomunikacijų operatoriai ir kiti įvairias sistemas reguliuojantys techniniai įrengimai. Tokios gyvybiškai svarbios operacinės sistemos, kurios reguliuoja traukinių eismą, lėktuvų skrydžius ar net gynybinius įrenginius, dažnai yra prijungtos prie globalaus kompiuterinio tinklo. Tokiu būdu jos tampa pasiekiamos ne tik tiems asmenims, kurie jas prižiūri ir reguliuoja, bet ir civiliams piliečiams. Todėl individų išmanymas apie kompiuterinių tinklų administravimą, kuris suteikia prieigą prie operacinės sistemos, kelia pavojų, nes, pakenkus tokioms sistemoms, kyla grėsmė civiliams gyventojams. Pavyzdžiui, *2004 metų rugpjūčio 20 d. SecurityFokus išspausdino informaciją apie įsilaužimą į JAV antarktinę stotį „Amundsenas-Skotas“, kuri yra pietų ašigalyje.*[42] *Praėjusių metų gegužės mėnesį stoties kompiuterinio tinklo administratoriai gavo anoniminį elektroninį laišką, kuriame pasakojama apie įsilaužimą į kompiuterius, kurie atsakingi už gyvenimo sąlygų užtikrinimą stotyje bei svarbios informacijos saugojimą. Hakeriai pareikalavo iš amerikiečių tyrinėtojų pinigų, prigrasinę perduoti pagrobtą informaciją „kitai šaliai“. Kaip pavyzdys buvo atsiųstas pagrobtos informacijos fragmentas. Tačiau kompiuteriai buvo išjungti, o FTB pradėjo tyrimą. Tyrimo metu nustatyta, kad elektroninis laiškas buvo išsiųstas iš interneto kavinės Rumunijoje. Įtariamasis buvo sulaikytas. Vėliau į tą pačią stotį vėl buvo įsibrauta. Tada hakeris Poizon Box įsilaužė į*

[41] Правовой анализ отдельных действий, наносящих потерпевшим ущерб в сфере высоких технологий // http://sm.aport.ru/scripts/template.dll?r...

[42] Киберпреступность в зарубежных странах, концепция ее детерминации и предупреждения // http://www.crime-research.ru/articles/Sabadash0904/

pagrindinius ir rezervinius kompiuterius, valdančius interferometrą DASI, kuris tyrinėja Visatos foninį mikrobanginį spinduliavimą.

Iš patektų atvejų matyti, kad nusikaltimais elektroninių ryšių sektoriuje galima padaryti ne tik didelės materialios žalos, tačiau ir sukelti grėsmę žmonių gyvybėms. Tokių neteisėtų ir pavojingų veikų pasekmės gali būti įvairios: žmonių žūtis, jų suluošinimas, tarptautinis konfliktas, materialiniai nuostoliai, pasitikėjimo oro transporto priemonėmis sumažėjimas ir pan.

C. Kiber prievarta (kiber persekiojimai, grasinimai ir neapykantos tinklapiai).

Šiandien naudojantis elektroniniais ryšiais galima lengvai susidurti su medžiaga (informacija), kuri yra nepageidaujama. Makulatūros pavidalu gautas elektroninis paštas gali turėti pornografinio ar kitokio nepageidaujamo turinio. Bet kuris interneto vartotojas gali gauti daugkartinius grasinančius pranešimus, nepadorius siūlymus ar neapykantos elektroninį paštą. Paskalos gali būti paskleistos interaktyviai tiek siekiant įžeisti asmenį, tiek ir dėl šantažavimo. Pavyzdžiui, *vienas vyras, kaip įtariama, pavogė intymias savo buvusios žmonos ir jos draugo fotografijas ir paskelbė (išsiuntinėjo elektroniniu paštu) jas internete, kartu su vardais, adresu ir telefono numeriu.*[43] *Vėliau pora iš Viskonsino gavo daug „pasiūlymų“ telefonu ir elektroninu paštu net iš Danijos, teigdami kad jie matė fotografijas internete. Tyrimo metu nustatyta, kad įtariamasis kompiliavo ir teikė informaciją apie buvusios žmonos šeimą.*

Dažnai elektroninės komunikacijos naudojamos ir įvairaus pobūdžio grasinimams. Šios rūšies nusikaltimų galima rasti diskusijų svetainėse internete, telekonferencijose. Taip *1998 metais buvęs Kalifornijos universiteto studentas naudojo elektroninį paštą tam, kad sukeltų nerimą penkioms studentėms.*[44] *Internete jis nusipirko informaciją apie moteris naudojančias kreditines korteles ir pasiuntė 100 įvairių pranešimų, tarp jų - mirtinus grasinimus, grafinius seksualinius aprašymus ir rekomendacijas dėl jų kasdienės veiklos. Manoma, kad jis tikriausiai grasino atsakydamas į nuolatinį erzinimą dėl jo išvaizdos.*

Tai tik keletas neteisėtų veikų, kurių gausu elektroninių ryšių sektoriuje, pavyzdžių. Be jų dar yra daugybė piratavimo rūšių. Bet kokia medžiaga, kuri gali būti laikoma skaitmeninėje formoje, yra atvira neteisėtam kopijavimui ir platinimui. Tam dažniausiai naudojamas internetas ir skelbimų lentos.

D. Nauji nusikalstamos veikos pasireiškimai.

Neseniai spaudoje[45] *paskelbta informacija, kad Oslo universiteto magistrantas sukūrė metodą, kuris leidžia keisti SMS žinučių siuntėjo duomenis. Anderso Svenssono sukurta paslauga reiškia, jog gavęs SMS žinutę žmogus negalės 100 % būti įsitikinęs, kad gavo ją nuo savo draugo, viršininko ar kito jam žinomo asmens, t.y. SMS žinutės gavėjas negalės nustatyti, kad*

[43] Компьютерное преступление в мире без границ http://www.crime-research.org/library/peter.htm
[44] Ten pat.
[45] http://www.delfi.lt/news/economy/ITbussines/article.php?id=5150802

žinutė yra „padirbta“: pavyzdžiui, vardas, telefono numeris bei kiti identifikavimo duomenys. Aišku gavėjas bus įsitikinęs, kad šią žinutę atsiuntė jam žinomas asmuo. Tačiau gavėjui žinomas asmuo niekada ir nesužinos, kad buvo pasinaudota jos ar jo numeriu. A.Svenssono teigimu, kad nebūtų galima klastoti SMS žinučių, reikės pakeisti GSM standartą. Mobiliojo ryšio operatorės „Telenor Mobil“ informacijos skyrius nurodo, kad bus ieškoma būdų, kaip užkirsti kelią suklastotų SMS žinučių siuntimui. Tuo tarpu Norvegijos pašto ir ryšių tarnybos atstovė Anne Marie Storli teigia, kad šiuo metu kovoti su šiuo reiškiniu trūksta teisinės bazės.

Apibendrinant būtina pastebėti, kad išnagrinėti atskirų nusikaltimų rūšių precedentai patvirtina šios studijos 2 skyriuje suformuluotą teiginį, kad daugelis nusikaltimų elektroninių ryšių sektoriuje yra atliekami naudojantis bet kuriomis signalų perdavimo priemonėmis, t.y. bet kuriomis sistemomis: internetu, skelbimų lentomis, elektroniniu paštu ir kt. Praktiškai bet koks nusikaltimas dabar gali būti atliktas elektroninių ryšių aplinkoje – elektroninėje erdvėje. Joje gausu tradicinių nusikaltimų – sukčiavimų, vagysčių, pornografijos, neapykantos nusikaltimų, autorių teisių pažeidimų. Yra ir naujo tipo nusikaltimų, kurie yra unikalūs internete, pavyzdžiui, neteisėta prieiga, neteisėtas naršymas ir kt. Neteisėtos veikos elektroninių ryšių sektoriuje išsiskiria dideliu įvairiapusiškumu ir pavojingumu, o jų pasekmės – asmens privatumo pažeidimas, dideli materialiniai nuostoliai, grėsmė civiliams gyventojams, tarptautinis konfliktas ir kt. Kol kas neturima pakankamai patirties visų šių nusikaltimų užkardymui ir dėl to kompiuterinės sistemos ir komunikacijos daugeliu atvejų neapsaugotos. Varžymasis dėl masinės kompiuterizacijos ir komunikacijos nepaliko laiko sukurti tinkamai veikiančią apsaugos sistemą. Šios sistemos trūkumai ir pastangos jas tobulinti nagrinėjamos kitame studijos skyriuje.

3.Nusikaltimų elektroninių ryšių sektoriuje reglamentavimo praktika:

3.1.Nusikaltimų elektroninių ryšių sektoriuje reglamentavimas tarptautiniu (regioniniu) mastu

Tarptautiniu mastu nemažai organizacijų koordinuoja ir derina atskirų valstybių veiksmus, siekdamos užkirsti kelią pavojingoms veikoms elektroninių ryšių sektoriuje : Europos Taryba, Europos Sąjunga, Europos ekonominio bendradarbiavimo ir plėtros organizacija, Interpolas, Jungtinės tautos, G8 ir kt. Tačiau visų jų indėlis nevienodas, ir kiekvienos iš jų pastangos nukreiptos kriminalizavimui tam tikros rūšies nusikaltimų, kurie, įvertinus šiandieninių komunikavimo priemonių galimybes, kelia grėsmę visuomenei tiek lokaliai, tiek ir globaliai.

Pirmąkart kompleksiškai įvertinti sunkumus, susijusius su dalimi nusikaltimų, įvykdomų elektroninių ryšių sektoriuje - kompiuteriniais nusikaltimais - pabandė Europos ekonominio bendradarbiavimo ir plėtros organizacija. 1983-1985 metais Europos ekonominio bendradarbiavimo ir plėtros organizacijos specialiai tam sudarytas komitetas atliko tyrimą dėl baudžiamųjų įstatymų, susijusių su kompiuteriniais ir telekomunikaciniais nusikaltimais. Atlikus tyrimą, buvo pateiktas minimalus pavojingų veikų, susijusių su kompiuteriais ir telekomunikacijomis, sąrašas[46]. Valstybėms buvo pasiūlyta užtikrinti, kad jų baudžiamieji įstatymai būtų pataisyti pagal išvardintų veikų sąrašą. Tačiau minėtas sąrašas neišvengė kritikos, nes jis neapėmė visų nusikalstamų veikų.

Europos Taryba. Užbaigus Europos ekonominio bendradarbiavimo ir plėtros organizacijos ataskaitą, Europos Taryba, įvertinusi kompiuterinių nusikaltimų pavojingumą, iniciavo savo tyrimą. 1989 metais Europos Tarybos (toliau – ET) pateikė rekomendaciją R 89(9) apie nusikaltimus, susijusius su kompiuteriais[47]. Valstybėms ET narėms buvo siūloma, peržiūrint ar kuriant įstatymus, atsižvelgti į Europos komiteto nusikaltimų problemoms tirti pranešimą apie susijusius su kompiuteriais nusikaltimus. Pažymėtina, kad šiame dokumente nustatyti bendri principai valstybių ET narių įstatymų leidžiamajai valdžiai. Atsižvelgiant į tai, nustatytas konkretus piktnaudžiavimų, susijusių su kompiuterių naudojimu, sąrašas ir fakultatyvus išvardinimas bei neteisėtų veikų aprašymas. Šiame pranešime pateikiami du, susijusių su kompiuteriniais nusikaltimais, veikų sąrašai: minimalus ir papildomas. Minimaliame išvardintos 8 pavojingesnės veikos, susijusios su kompiuterinėmis technologijomis :

1) sukčiavimas, susijęs su kompiuteriu;
2) klastojimas naudojant kompiuterį;
3) kompiuterinių duomenų ar programų sunaikinimas ar sugadinimas ir kt.

[46] Computer-related crime: Anglysis Of Legal Policy, Paris: OECD, 1986.p.86.
[47] Recommendations no. R (89)9 on Computer-related crime // http://cm.coe.int/ta/rec/1989/89r9.htm

Papildomas sąrašas apima keturias mažiau pavojingas veikas, kurios įtraukiamos į įstatymų leidybą, bet nėra privalomos: kompiuterinių duomenų ar programų pakeitimas, kompiuterinis špionažas, neteisėtas kompiuterio naudojimas, neteisėtas apsaugotų kompiuterinių programų naudojimas. Šioje rekomendacijoje buvo išvardintos praktiškai visos veikos susijusios su kompiuterinėmis technologijomis. Tačiau dokumentas nebuvo privalomo pobūdžio ir atskirų valstybių buvo įvertintas nevienodai.

Susirūpinusi, kad kompiuterių tinklai ir elektroninė informacija gali būti naudojama vykdyti baudžiamiesiems nusikaltimams, ir įvertinusi būtinybę, jog valstybėms ir privačiam verslui būtina bendradarbiauti kovojant su nusikaltimais elektroninėje erdvėje, šio tūkstantmečio pradžioje ET paruošė vieną svarbiausių dokumentų - Nusikaltimų elektroninėje erdvėje konvenciją. Ši Konvencija buvo suderinta su daugeliu valstybių, tarp jų JAV ir Kanada. 2001 metų Nusikaltimų elektroninėje erdvėje konvencija yra kompleksinis dokumentas, susidedantis iš imperatyvių normų, kurių paskirtis - įtakoti daugelį įvairių teisės šakų: baudžiamosios, baudžiamojo proceso, autorių, civilinės ir kt. Jos pagrindą sudaro pagrindiniai tarptautinės teisės principai: žmogaus teisių gerbimas, bendradarbiavimas ir geranoriškas įsipareigojimų vykdymas. Konvencijos I dalyje, kuri susijusi su materialine teise, siūloma nustatyti teisinės atsakomybės pagrindus už šias pavojingų veikų rūšis:

1) konfidencialumo, duomenų vientisumo, kompiuterinių duomenų ir sistemų pažeidimus (neteisėta prieiga, neteisėtas perėmimas, įsikišimas į duomenų apdorojimo procesą, įsikišimas į kompiuterinių sistemų darbo procesą, piktnaudžiavimas kompiuterinėmis priemonėmis (įrenginiais));
2) su kompiuteriais susijusius pažeidimus (sukčiavimas, susijęs su kompiuteriais; klastojimas, susijęs su kompiuteriais);
3) pažeidimus, susijusius su turiniu (pažeidimai, susiję su pornografine medžiaga apie vaikus);
4) pažeidimus, susijusius su autorių teisėmis ir gretutinėmis teisėmis.

Plačiau neanalizuojant aukščiau nurodytų neteisėtų veikų, būtina pastebėti, kad Konvencija pateikia dar dvi naujoves:

- joje nepateikiamas sąvokos „nusikaltimai kompiuterinės informacijos srityje“ apibrėžimas. Jis pakeičiamas sąvoka „nusikaltimas elektroninėje erdvėje“, kuris iš Konvencijos konteksto suprantamas kaip:
  - veikos, nukreiptos prieš kompiuterinę informaciją (kompiuterinė informacija yra nusikaltimo dalykas), ir veikos, kai kompiuterinė informacija yra nusikaltimo įrankis, ir

- veikos, kur nusikaltimo dalykas yra kiti baudžiamojo įstatymo saugomi gėriai, o informacija, kompiuteriai, komunikacijos ir kt. yra tik vienas iš nusikaltimo sudėties objektyviosios pusės elementų, pavyzdžiui, nusikaltimo įvykdymo įrankis.

- atsižvelgiant į skirtingą valstybių praktiką, Konvencija reikalauja nustatyti ir juridinių asmenų atsakomybę už joje išvardintas nusikalstamas veikas.

Siekiant kriminalizuoti veikas, susijusias su rasinės ir tautinės neapykantos kurstymu pasitelkiant kompiuterines sistemas, 2002 m. lapkričio 7 d. buvo priimtas ET Nusikaltimų elektroninėje erdvėje konvencijos papildomas protokolas (2002)24[48]. Protokole rasinę ir tautinę neapykantą kurstanti informacija apibrėžiama kaip bet koks rašytinis, vizualinis ar kitoks minčių ir teorijų, propaguojančių diskriminaciją ar smurtą prieš individą ar jų grupes, išsiskiriančias dėl savo rasės, tikėjimo, politinių pažiūrų ir pan. pateikimas. Prie Protokolo prisijungusios valstybės skatinamos priimti reikiamus teisės aktus, siekiant kriminalizuoti minėtų veikų vykdymą kompiuterinėse sistemose, sudaryti sąlygas taikyti atitinkamas priemones, kurių gali prireikti konkrečių nusikaltimų tyrimui, įrodymų, esančių elektroniniame pavidale surinkimui.

Apibendrinant ET iniciatyvas, būtina pažymėti, kad jos apima beveik visas nusikalstamas veikas, kurios gali būti atliekamos elektroninių ryšių sektoriaus aplinkoje – elektroninėje erdvėje. Visos jos įvardijamos Nusikaltimų elektroninėje erdvėje konvencijoje, kurią ratifikavusios ar prie jos prisijungusios valstybės privalo nustatyti fizinių ir juridinių asmenų baudžiamąją atsakomybę už visas konvencijoje nustatytas neteisėtas veikas. Tačiau nei viename ET priimtame teisės akte nesuformuluota „nusikaltimo elektroninėje erdvėje“ sąvoka, paliekant galimybę ją interpretuoti kiekvienai valstybei savaip.

Pažymėtina, kad ***Europos Sąjunga*** (toliau – ES) ilgą laiką nenagrinėjo nei kompiuterinių nusikaltimų, nei nusikaltimų elektroninių ryšių sektoriuje problematikos. Iki 2002 metų visos jos iniciatyvos iš esmės buvo nukreiptos prieš neteisėtą interneto turinį. Vienas svarbesnių dokumentų yra Europos Parlamento ir Tarybos 1999 m. sausio 25 d. sprendimas Nr.276/1999/EB, kuriuo patvirtintas ilgalaikis Bendrijos veiksmų planas, kaip skatinti saugiau naudotis internetu kovojant su neteisėtu ir žalingu tarptautinių tinklų turiniu[49], tačiau nei jame, nei kituose teisės aktuose (komunikatuose, rekomendacijose) baudžiamosios atsakomybės klausimai nenagrinėjami.

Kaip jau buvo minėta šios studijos pradžioje, 2002 metais ES lygiu dėl elektroninių ryšių sektoriaus buvo priimta visa eilė direktyvų. Jose buvo pažymėta, kad lengvai prieinamos interneto paslaugos atveria naujas galimybes, bet sukelia naują grėsmę privatumui ir saugumui.

[48] Additional Protocol to the Council of Europe Convention on Cyber-crime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems // http://www.era.int/www/gen/f 16632 file en.pdf

[49] Action Plan on promoting safer use of the Internet // http://europa.eu.int/ISPO/iap/decision/en.html

Nežiūrint to, direktyvose neteisėtos veikos elektroninių ryšių sektoriuje nenagrinėjamos, nesprendžiami ir baudžiamosios atsakomybės klausimai.

2002 m. balandžio 19 d. EB Komisija pateikė Siūlymą Tarybai dėl atakų prieš informacines sistemas[50] sprendimo. Šiame Siūlyme buvo konstatuota, jog atakos prieš informacines sistemas kelia grėsmę saugiai informacinei visuomenei, saugumui ir justicijai, ir todėl reikia imtis tam tikrų priemonių Europos Sąjungos lygiu. Komisija pasiūlė kriminalizuoti veikas, susijusias su neteisėta prieiga prie informacinių sistemų ir neteisėtu įsikišimu į informacinių sistemų darbą.

Pasiūlymo 3 straipsnyje nustatyta, kad valstybės narės turi užtikrinti, kad tyčinė prieiga, neturint tam teisės, prie visos ar dalies informacinės sistemos turi būti laikoma nusikalstama, jei veika yra įvykdyta:

a) per bet kokią informacinės sistemos dalį, kuri yra saugoma specialiomis saugumo priemonėmis, ar
b) siekiant padaryti žalą fiziniam ar juridiniam asmeniui, ar
c) siekiant gauti ekonominę naudą.

Šiomis nuostatomis norima nustatyti atsakomybės pagrindus už neteisėtą prieigą prie informacinių sistemų (Hacking). Tačiau šalys narės, įgyvendindamos šias nuostatas savo nacionaliniuose įstatymuose, gali nenustatyti baudžiamosios atsakomybės už nereikšmingus pažeidimus. Pastebėtina, kad paminėtos nuostatos daugiausiai skirtos vadinamosioms DOS atakoms (Denial of service attacks) kriminalizuoti, kai apgalvotai siekiama apkrauti („užversti“) informacinę sistemą duomenimis kompiuterine forma. Nuostatos taip pat paliečia įvairių atakų rūšis, kai tokie veiksmai skirti sutrikdyti ar pertraukti informacinės sistemos darbą, bei su WWW puslapių „sugadinimu“.

Apibendrinant ES praktiką, būtina pažymėti, kad nusikaltimų elektroninių ryšių sektoriuje reglamentavimas vykdomas toje srityje, kurioje tarptautinis reglamentavimas nevykdomas arba nepakankamas.

Tam tikrą indėlį, reglamentuojant kompiuterinius nusikaltimus pateikė ir **Jungtinių Tautų Organizacija**. Vienas svarbesnių jos priimtų dokumentų – Tarptautinė nusikaltimų politikos apžvalga – rekomendacija dėl su kompiuteriais susijusių nusikaltimų užkardymo ir kontrolės[51]. Joje pabrėžiama, kad tiek atskiri įstatymai, tiek ir tarptautinis bendradarbiavimas vystėsi daug lėčiau nei naujosios technologijos. Tik kai kurios šalys yra priėmusios baudžiamuosius įstatymus, adekvačius šiandienos neteisėtoms veikoms, susijusioms su

[50] COUNCIL FRAMEWORK DECISION on attack against informatikon systems // http://europa.eu.int/eur-lex/en/com/pdf/2002/com2002_0173en01.pdf
[51] International review of criminal policy „United Nations Manual on the prevention and control of computer-related crime“ // http: // www.uncjin.org/Documents/EighthCongress.html

kompiuterių panaudojimu. Atsižvelgiant į tai, rekomendacijoje apibūdintos visos neteisėtos veikos, susijusios su kompiuterių panaudojimu, pateikta kompiuterinio nusikaltimo samprata, tarptautinio bendradarbiavimo sąlygos ir kt., tačiau jame baudžiamosios atsakomybės klausimai nenagrinėjami, o ir pats dokumentas yra daugiau pažintinio-rekomendacinio pobūdžio ir valstybėms neprivalomas.

Apibendrinant pasaulinę praktiką nustatant atsakomybę už pavojingas veikas elektroninių ryšių sektoriuje, būtina pastebėti, kad būtinybė efektyviai kovoti su nusikaltimais šio sektoriaus aplinkoje buvo plačiai pripažinta tarptautiniu lygiu. Įvairios organizacijos koordinavo arba bandė derinti veiksmus šioje srityje. Dėl to priimta nemažai norminių dokumentų, numatančių baudžiamąją atsakomybę beveik už visas neteisėtas veikas elektroninių ryšių sektoriuje. Daugelyje išnagrinėtų teisės aktų vyrauja tendencija, kai privalomojo ar rekomendacinio pobūdžio teisės aktais apibrėžiamos tam tikros pavojingos veikos, paliekant pačioms valstybėms nustatyti atsakomybės dydį. Vienu svarbiausių dokumentų, autoriaus manymu, laikytina Nusikaltimų elektroninėje erdvėje konvencija, kurios nuostatos buvo suderintos su tokiomis valstybėmis kaip JAV ir Kanada. Konvenciją ratifikavusios ar prie jos prisijungusios valstybės privalėjo nustatyti baudžiamąją atsakomybę už visas, Konvencijoje nustatytas neteisėtas veikas. Kaip tai atsispindi atskirų valstybių praktikoje, autorius nagrinėja toliau.

3.2.Nusikaltimų elektroninių ryšių sektoriuje reglamentavimas kai kuriose užsienio valstybėse

Pastaruoju metu, dėl vis didėjančio nusikaltimų, atliekamų elektroninių ryšių sektoriuje, pavojaus pradedama reikalauti atitinkamų adekvačių nacionalinių priemonių jų užkardymui. Daugelyje pasaulio šalių, deja, esantys baudžiamieji įstatymai yra neefektyvūs kovojant su tokiais nusikaltimais. Šalys, kuriose baudžiamoji atsakomybė neadekvati, taps vis mažiau ir mažiau konkurencingomis naujoje ekonomikoje. Kad to išvengtų, valstybės privalo peržiūrėti galiojančius baudžiamuosius įstatymus ir įvertinti, ar jie pakankami, kovojant su naujo tipo nusikaltimais. Atskirų veikų kriminalizavimui galima remtis kitų valstybių - JAV, Kanados, Didžiosios Britanijos ir Vokietijos - praktika. Daugelio teisės specialistų nuomone, būtent šiose valstybėse baudžiamoji atsakomybė yra nustatyta beveik už visas veikas elektroninių ryšių sektoriaus aplinkoje – elektroninėje erdvėje.

Jungtinės Amerikos Valstijos

Literatūroje nurodoma, jog JAV – viena iš pirmaujančių veikų, susijusių su kompiuteriniais nusikaltimais, kriminalizavimo srityje. Atsakomybė už *neteisėtą signalų perdavimą* elektroninių ryšių sektoriuje, JAV nustatyta keliuose teisės aktuose. Visų pirma – Jungtinių valstijų kodekso Sukčiavimo ir piktnaudžiavimo naudojant kompiuterius įstatymas[52]. Pavyzdžiui, pagal šį įstatymą yra neteisėta ir baudžiama:

- prieiga neturint tam teisės (ar viršijant nustatytas teises) prie bet kokios kompiuterinės sistemos, kai dėl to pasisavinama informacija, susijusi su valstybės saugumu, tarptautiniais santykiais, atomine energetika;
- prieiga neturint tam teisės (ar viršijant nustatytas teises) prie bet kokios kompiuterinės sistemos, kai dėl to pasisavinama finansinė informacija, laikoma finansų institucijoje, taip pat informacija apie paskolas ar informacija, susijusi su kreditinėmis kortelėmis;
- tyčinė prieiga, neturint tam teisės prie JAV departamento ar agentūros kompiuterio, jei kompiuteris skirtas išimtinai šioms institucijoms naudoti, taip pat jei kompiuteris nėra skirtas išimtinai šioms institucijoms naudoti, kai dėl to yra paveikiamas vyriausybinės institucijos naudojimasis kompiuteriu;
- prieiga prie kompiuterio sukčiavimo kėslais, siekiant gauti bet kokią naudą, įskaitant ir neteisėtą kompiuterio tinklų naudojimą (laiko vagystė), jeigu per kalendorinius metus buvo padaryta didesnė nei 5000 JAV dolerių žala;
- kenkimas apsaugotiems kompiuteriams tyčia ar dėl neatsargumo;

[52] Fraud and related activity in connection with computers // http://www.usdoj.gov/criminal/cybercrime/fedcode.htm

- slaptažodžių ar kitos informacijos, kuria pasinaudojus galima neteisėtai patekti į kompiuterį, platinimas (siekiant apgaulės), jei dėl tokio platinimo yra paveikiama užsienio komercija arba komercija tarp valstijų ar tokia informacija yra naudojama JAV vyriausybės;
- grasinimas, turto prievartavimas, šantažas ir kitos neteisėtos veikos padarytos panaudojant kompiuterius.

Pažymėtina, kad minėti nusikaltimai yra viename 1030 skirsnyje, kuris sudarytas taip, kad už šias neteisėtas veikas gali būti baudžiamas tiek fizinis, tiek ir juridinis asmuo. Aukščiau minėtas skirsnis yra skirtas tik daliai nusikaltimų elektroninių ryšių sektoriuje -neteisėtai prieigai ir kompiuteriniams nusikaltimams. Už sukčiavimo veikas elektroninių ryšių sektoriuje nustatyta atsakomybė 1343 skirsnyje. Pagal šį skirsnį neteisėtas (ir baudžiamas) bet koks neteisėtas laiškų, signalų, paveikslų arba garsų perdavimas arba pastangos perduoti laidinėmis, radijo arba televizijos komunikacijomis.

Atsakomybė už privačių komunikacijų perėmimą yra nustatyta 1362 skirsnyje „Ryšio linijos, stotys arba sistemos“. Pagal šį skirsnį baudžiama yra ne tik bet kokia neteisėta veika privačios informacijos komunikavimo metu, bet net ir kėsinimasis ar susitarimas tai daryti.

Be abejo, yra ir kitų JAV įstatymų, kriminalizuojančių veikas elektroninių ryšių sektoriuje. Vienas iš jų – Elektroninių ryšių slaptumo įstatymas.[53] Remiantis šiuo įstatymu, bet kas, kas neteisėtai prieina prie įrenginio, per kurį tiekiamos elektroninių ryšių paslaugos, arba viršija įgaliojimus ir tokiu būdu prieina prie įrenginio bei pasisavina ar pakeičia kompiuterinę informaciją arba apriboja priėjimą prie elektroninių ryšių, yra baudžiamas už nusikaltimą. Be to, įstatymo 2511 skirsnyje „Perėmimas ir atskleidimas uždraustų laidinių, žodinių arba elektroninių komunikacijų“ nustatyta, kad bus baudžiamas už nusikaltimą bet koks žmogus, kuris:

- bando perimti, užtikrina perėmimą bet kuriam kitam žmogui arba perima bet kokias laidines, žodines arba elektronines komunikacijas (2511(1)(a);
- atskleidžia arba bando atskleisti bet kokiam kitam žmogui bet kokios laidinės, žodinės arba elektroninės komunikacijos turinį, žinodamas arba turėdamas žinoti, kad informacija buvo gauta perimant laidines, žodines arba elektronines komunikacijas (2511(1)(c).

Minėto teisės akto 2701 straipsnyje nustatyta atsakomybė už neteisėtą prieigą prie išsaugotų komunikacijų, o 2702 straipsnyje – už išsaugotų komunikacijų turinio atskleidimą.

Pažymėtina, kad Elektroninių ryšių slaptumo įstatyme įvardinta daug atvejų, kai minėtos veikos nebus pripažįstamos nusikalstamomis, pavyzdžiui, perėmimas ar turėjimas priėjimo prie

[53] Interception and disclosure of wire, oral, or electronic communications prohibited // http://www4.law.cornell.edu/uscode/18/2511.html

elektroninio ryšio, jeigu toks ryšys yra prieinamas plačiam asmenų ratui, nebus traktuojamas kaip nusikaltimas.

Atsakomybė už *neteisėtų signalų perdavimą* elektroninių ryšių sektoriuje JAV nustatyta visų pirma 1996 metų Kongreso priimtame Vaikų pornografijos prevencijos įstatyme.[54] Jame be kitų veikų kriminalizuotas ir mechaninis ar elektroninis pornografinės medžiagos, susijusios su vaikais, skelbimas ir platinimas. Tuo pat metu, atsižvelgiant į tai, kad tiek visuomenei, tiek jai atstovaujantiems politikams kėlė susirūpinimą nevaržomas pornografijos platinimas, 1996 metais buvo priimtas Komunikacijų padorumo įstatymas (CDA).[55] Pagal šį įstatymą yra neteisėta ir baudžiamas tas, kas buvo pripažintas kaltu dėl transliavimo ar padarymo prieinamu nepilnamečiams komentaro, kvietimo, siūlymo ar kitos informacijos, kuri yra nepadori, nešvanki ar įžeidžianti arba kuri pabrėžtinai drastiškai visuomenės gyvenimo normų požiūriu pristato arba aprašo seksualų veiksmą ar lyties organus. JAV laikomasi nuomonės, kad prie žalingos informacijos, kuri kenkia ne tik nepilnamečiams, bet ir visai visuomenei, reikėtų priskirti nevaržomą pornografiją, smurtą, ekstremizmą ir terorizmą, rasinę diskriminaciją ir net vulgarią kalbą, kuri atitinkamai pažeidžia žmogaus orumą ir pagarbą žmogui.

Be to jau minėto Jungtinių valstijų kodekso 2314 skirsnyje nustatyta baudžiamoji atsakomybė už neteisėtai įgytų vertybių judėjimą, perdavimą kompiuteriniais tinklais

Apibendrinant tai, kas išdėstyta, autorius pastebi, kad federalinių įstatymų šioje srityje yra tikrai nepapankamai. Atsižvelgiant į tai, kad federaliniai įstatymai baudžiamąją atsakomybę nustato ne už visas neteisėtas veikas, likusios neteisėtos veikos skirtingai reglamentuojamos atskirų valstijų lygmeniu. Štai Aidacho (Idaho) valstijos baudžiamojo statuto 18 skyriaus „Nusikaltimai ir bausmės“ 67 dalies „Komunikacijų saugumas“ 18-6713 skirsnyje „Telekomunikacijų paslaugų vagystė“, be telekomunikacijų paslaugų vagystės, nusikaltimu laikoma ir viena iš naujausių neteisėtų veikų – mobiliųjų telefonų klonavimas.[56] Įstatyme nustatyta galimybė telekomunikacijų paslaugų teikėjui gauti kompensaciją dėl kai kurių neteisėtų veikų. Telekomunikacijų paslaugų teikėjas, kurį tiesiogiai paveikė bet kuri iš įstatyme nustatytų neteisėtų veikų, neatsižvelgiant į tai, ar nusikaltėlis buvo nubaustas, turi teisę į protingą nuostolių atlyginimą, atsižvelgiant į nusikaltimo sunkumą.

Savotiškas yra 1972 metų JAV Misisipės valstijos kodeksas.[57] Šio kodekso 45 skyrius „Kompiuteriniai nusikaltimai“ skirtas kompiuteriniams nusikaltimams, prie kurių be tradicinių kompiuterinių nusikaltimų priskiriami:

[54] Certain activities relating to material involving the sexual exploitation of minors // http://www4.law.cornell.edu/uscode/18/2252.html
[55] Communications Decency Act of 1996 // http://www.fcc.gov/Reports/tcom1996.txt
[56] 18-6713. THEFT OF TELECOMMUNICATION SERVINES // http://www3.state.id.us/cgi-bin/newidst?sctid=180670013.K
[57] Mississippi Code of 1972 // http://www.mscode.com/free/statutes/97/025/0054.htm

- „Kiber persekiojimas“ , t.y. elektroninio pašto arba elektroninių komunikacijų naudojimas bet kokio pobūdžio bauginimui ar melagingam pranešimui;
- pranešimų, įžeidžiančių bet kurį žmogų, siuntimas. Draudžiama siųsti pranešimą, kuris įžeistų bet kurį žmogų, naudojantis bet kuria ryšio priemone, įskaitant internetą arba kompiuterį, kompiuterinę programą, kompiuterinę sistemą arba kompiuterinį tinklą, arba kitą elektroninę ryšio priemonę be aukos sutikimo.

Abi neteisėtos veikos, autoriaus manymu, taip pat priskiriamos prie nusikaltimų elektroninių ryšių sektoriuje, t.y. prie nusikaltimų siunčiant neteisėtus signalus, kurie čia vis dėlto traktuojami kaip pranešimai.

JAV įstatymuose kriminalizuotos praktiškai visos neteisėtos veikos elektroninių ryšių sektoriuje, apibrėžtos kai kurios sąvokos, susijusios su elektroniniais ryšiais. Tačiau nei viename federaliniame ar federacijos teisės akte nesuformuluota nusikaltimo elektroninių ryšių sektoriuje ar elektroninėje erdvėje sąvoka, neapibrėžta, kokios pavojingos veikos sudaro nusikaltimus elektroninių ryšių sektoriuje, neapibrėžta, kas laikoma „neteisėta prieiga“, dėl ko gali atsirasti interpretavimo problemų, o kai kurios veikos gali nepatekti į federalinių ar federacinių įstatymų veikimo sritį.

Kanada

Pažymėtina, kad Kanadoje praktiškai už visas šiuo metu įmanomas neteisėtas veikas baudžiamoji atsakomybė nustatyta viename teisės akte – Baudžiamajame kodekse. Teisinėje literatūroje nurodoma, kad Kanada buvo viena iš pirmųjų valstybių, dar 1985 metais nustačiusi atsakomybę už neteisėtas veikas, susijusias su kompiuteriniais nusikaltimais. 2000 metais firma McConnell[58] atliko devyniolikos šalių baudžiamųjų įstatymų, nustatančių atsakomybę už nusikaltimus elektroninėje erdvėje, tyrimą. 2001 metų pradžioje McConnell pranešime nurodė, kad Kanados baudžiamieji įstatymai nustato atsakomybę už beveik visas pavojingas veikas elektroninėje erdvėje. Jos Baudžiamajame kodekse [59] atsakomybė už *neteisėtą signalų perdavimą* elektroninių ryšių sektoriuje, nustatyta keliuose straipsniuose:

1. Komunikacijų perėmimas (184.(1)). Pagal minėtą straipsnį yra neteisėta ir baudžiamas kiekvienas, kuris, naudodamasis bet kokiu elektromagnetiniu, akustiniu, mechaniniu arba kitokiu įrenginiu, tyčia perima privačią komunikaciją.

Kituose skirsnio straipsniuose yra išdėstytos išimtys, kai privačių komunikacijų perėmimas nelaikomas nusikaltimu, pavyzdžiui:

- perėmimas, siekiant išvengti bet kokio kenkimo (184.1(1));
- perėmimas, esant sutikimui (184.2(1));

[58] Cyber crime ... and punishment? // http://www.mcconnellinternational.com/services/cybercrime.htm
[59] Canadian Criminal Code // http://www.digitaldefence.ca/Kanada CriminalCode.htm

- perėmimas, esant išimtinėms aplinkybėms (184.4) ir kt.

Kanados Baudžiamajame kodekse atskirais straipsniais nustatyta atsakomybė :

- kai privačios komunikacijos perimamos naudojantis radijo komunikacijomis (184.5(1));
- už įrangos, skirtos privačių komunikacijų perėmimui, turėjimą (191 (1));
- kai atskleidžiama informacija, kuri gauta neteisėtai perėmus privačias komunikacijas (193.1(1)).

Pažymėtina, kad neteisėtas privačių komunikacijų perėmimas Kanados Baudžiamajame kodekse reglamentuotas labai išsamiai. Nežiūrint to, niekur nėra minimi elektroniniai ryšiai ir iš viso ši sąvoka nesuformuluota.

2. Telekomunikacijų paslaugų vagystė (326. (1)) – bet koks neteisėtas telekomunikacijų priemonių naudojimas arba neteisėtas paslaugų gavimas. Telekomunikacijos reiškia bet kokį perdavimą, emisiją arba priėmimą požymių (parašų), signalų, laiškų, vaizdų arba garsų arba duomenų bet kokios kilmės laidine, radijo, vizualine arba kita elektromagnetine sistema. Nesunkiai galima pastebėti, kad sąvoka „Telekomunikacijos“ neapima visų šiuo metu įmanomų signalų perdavimo būdų, pvz.: perdavimo optinėmis priemonėmis. Todėl lieka galimybė, kad tam tikros veikos lieka nebaudžiamomis.

3. Neteisėtas kompiuterio naudojimas (342.1 (1)). Remiantis 1985 metų Kanados Baudžiamojo kodekso 342.1 (1) straipsnio pakeitimais, nusikaltimu laikoma veika, kai neteisėtai arba siekiant apgauti:

a) tiesiogiai arba netiesiogiai naudojamasi kompiuterinėmis paslaugomis;
b) tiesiogiai arba netiesiogiai naudojantis elektromagnetiniu, akustiniu, mechaniniu arba kitokiu įrenginiu perimamos kompiuterinės sistemos funkcijos;
c) tiesiogiai arba netiesiogiai a) ir b) atvejais naudojama kompiuterinė sistema.

Be to, Kanados Baudžiamajame kodekse nustatyta atsakomybė ir už įrenginio, skirto neteisėtai naudotis kompiuterinėmis paslaugomis, turėjimą.

4. Kenkimas (430. (1)). Straipsnyje nustatyta, kad baudžiamos yra veikos, susijusios su kenkimu duomenims, kai:

- tyčia sunaikinami ar pakeičiami duomenys;
- tyčia pakeičiamas duomenų turinys, reikšmė;
- tyčia įsiterpiama į duomenų apdorojimo procesą ir pan.

Kanados Baudžiamajame kodekse baudžiamoji atsakomybė nustatyta ir už *neteisėtų signalų perdavimą* elektroninių ryšių sektoriuje:

1.Neteisėtos informacijos perdavimas. Šio rūšies neteisėtos veikos kriminalizuotos keliose srityse : laivų navigacijoje (78.1.(3)), priešgaisrinės gelbėjimo tarnybos darbe (437) ir

žmogaus privačiame gyvenime (372.(1)). Pažymėtina, kad kai kuriose srityse neteisėtos informacijos perdavimas apima tik tradicinius telekomunikacijos tinklus. Pavyzdžiui, Kanados Baudžiamajame kodekse yra du straipsniai, kuriuose kriminalizuotos neteisėto įsikišimo į asmens privatumą veikos:

- nepadorūs telefoniniai skambučiai (372. (2));
- varginantys telefoniniai skambučiai (372. (3)).

Abiejuose straipsniuose nustatyta atsakomybė, kai neteisėtais telefoniniais skambučiais įsikišama į asmens privatumą. Būtina pastebėti, kad minėtos neteisėtos veikos neapims atvejų, kai, pavyzdžiui, elektroniniu būdu bus siuntinėjami nepadorūs, įžeidžiantys, grasinantys ar nuolat pasikartojantys nepageidautini pranešimai. Todėl minėti straipsniai turi būti tobulinami.

2. Pornografinės medžiagos apie vaikus platinimas (163.1(3)). Platinimas apima daug nusikalstamų veikų : pornografinės medžiagos perdavimas, padarymas prieinamos, paskirstymas, pardavimas, importavimas, eksportavimas ir kt. Pažymėtina, kad medžiagos platinimas internete, t.y. naujienų grupėse, interneto puslapiuose ar susirašinėjimo sąrašuose, prilyginamas paskelbimui.

3. Kanados baudžiamajame kodekse yra nustatyta atsakomybė ir už veikas, susijusias su neskelbtinos informacijos platinimu. Prie jų priskirtinos: kurstymas asmens, kuris priešiškas Kanadai (50. (1) (a)), grasinimas Parlamentui (51.str.), maišto kurstymas (53.str.) ir kt.

Būtina paminėti dar vieną Kanados Baudžiamojo kodekso privalumą. Jame išspręsta sąvokų traktavimo problema. Praktiškai kiekviename skyriuje yra pateikiamas tame skyriuje vartojamų sąvokų išaiškinimas.

Pažymėtina, kad elektroninių ryšių sektoriaus veikla Kanadoje reglamentuojama daugeliu teisės aktų : įstatymų, instrukcijų ir taisyklių.[60] Kai kuriuose iš jų taip pat nustatyta atsakomybė už neteisėtas veikas. Pavyzdžiui, Radijo komunikacijų įstatymas.[61] Šio įstatymo skyriuje „Nusikaltimai (pažeidimai) ir bausmės“ nustatyta, kad yra neteisėta ir baudžiama, kai:

- perduodamas arba pasiunčiamas melagingas arba apgavikiškas pagalbos signalas;
- neteisėtai apsunkinamas bet koks radijo ryšys;
- neteisėtai iššifruojama užšifruota informacija ir kt.

Atskiri straipsniai, nustatantys atsakomybę už veikas, kai neteisėtai įsikišama į signalų perdavimą arba perduodami neteisėti signalai, yra nustatyti ir kituose komunikacijų veiklą reglamentuojančiuose įstatymuose.

Atsižvelgiant į šiandienos įvykius Lietuvoje, būtina pastebėti, kad asmens privatumas, kaip teisinis gėris, ypač saugomas Kanadoje. Jau buvo minėta, kad Kanados Baudžiamajame kodekse yra nustatytos išimtys, kai leidžiama pažeisti žmogaus komunikacijų privatumą, tačiau

[60] Canadian Radio-television and Telecommunications Commission // http://www.crtc.gc.ca/eng/statutes.htm
[61] Ten pat.

tik siekiant apsaugoti kitus svarbius teisinius gėrius. Be to, privačių komunikacijų perėmimas atliekamas laikantis tam tikrų taisyklių, direktyvų ir panašiai. Pavyzdžiui, Specialaus įgaliotinio direktyva „Privačių komunikacijų, susijusių su aptarnavimu nustatyto saugumo, perėmimas“.[62] Nurodyta, kad šio teisės akto tikslas – garantuoti įstaigose saugią aplinką, vykdant komunikacijų perėmimą baudžiamojo įstatymo ribose. Skyriuje „Perėmimo sąlygos ir teisiniai reikalavimai“ išdėstytos sąlygos ir reikalavimai, kurių privaloma laikytis perimant privačias komunikacijas. Pavyzdžiui, privačių komunikacijų perėmimas turi būti sąlygojamas įrašymo į vaizdo, garso juostą ir galimas tik esant šioms sąlygoms:

- tai reikalinga saugumui užtikrinti;
- tai vykdoma laikantis įstatymo; ir
- tai daroma dėl ypatingų priežasčių.

Specialaus įgaliotinio direktyvoje taip pat nustatyta perėmimo sistemų kontrolė, požymių registracija, įrašymo juostų, kaip įrodymų, naudojimas ir ataskaita apie perimtas komunikacijas. Pastarojoje nurodyta, kad kiekvieną kartą, kai žmogaus komunikacijos perimamos, ataskaita apie tai turi būti išsaugota.

Apibendrinant Kanados nusikaltimų elektroninių ryšių sektoriuje reglamentavimo praktiką, galima teigti:

1. Kanadoje atsakomybė už beveik visas pavojingas veikas elektroninių ryšių sektoriuje nustatyta Baudžiamajame kodekse.

2. Kanados Baudžiamajame kodekse išspręsta sąvokų traktavimo problema.

3. Bet kuriam asmeniui ypač didelę žalą darantis privačių komunikacijų perėmimas galimas tik įstatymo nustatyta tvarka ir tais atvejais, kurie reglamentuoti Kanados Baudžiamajame kodekse ir kituose teisės aktuose.

Didžioji Britanija

Šios šalies baudžiamajai teisei būdingi ypatumai, kurie nebūdingi kitų išsivysčiusių šalių įstatymų leidybai. Visų pirma tai atskirų teisės šakų kodeksų nebuvimas. Šiandieninėje Didžiojoje Britanijoje pagrindiniu teisės šaltiniu yra statutai ir teisminiai precedentai, kurių visuma sudaro taip vadinamą bendrąją teisę. Nežiūrint to, vis dėlto galima išskirti keletą įstatymų, kurie kodifikuota forma turi baudžiamosios teisės požymių nagrinėjamu klausimu.

Didžiojoje Britanijoje baudžiamoji atsakomybė už *neteisėtą signalų perdavimą* elektroninių ryšių sektoriuje visų pirma nustatyta 1990 metais priimtame Piktnaudžiavimo,

[62] Interception of communications related to the maintenance of institutional security // http://www.csc-scc.gc.ca/text/plcy/cdshtm/575-cde e.s.html

panaudojant kompiuterius, įstatyme.[63] Jame baudžiamosios atsakomybės pagrindai nustatyti už šiuos nusikaltimus elektroninių ryšių sektoriuje:

- neteisėtą prieigą prie kompiuterinių sistemų (1 str.);
- neteisėtą prieigą siekiant įvykdyti ar palengvinti kitų nusikaltimų įvykdymą (2 str.);
- neteisėtą kompiuterinių duomenų pakeitimą (3 str.).

Remiantis minėto įstatymo 1 straipsniu, asmuo gali būti pripažintas kaltu įvykdęs neteisėtą prieigą prie kompiuterinių sistemų, tik jo veikoje nustačius tris būtinus požymius, pavyzdžiui, prieiga yra neteisėta.

Remiantis minėto įstatymo 2 straipsniu, asmuo gali būti pripažintas kaltu įvykdęs neteisėtą prieigą siekiant įvykdyti ar palengvinti kitų nusikaltimų įvykdymą, jeigu jis įvykdo nusikaltimą, nurodytą šio įstatymo 1 straipsnyje, siekdamas įvykdyti kitą nusikaltimą, ar palengvina kito nusikaltimo įvykdymą. Šio straipsnio nuostatos apima ir tokius veiksmus, kaip „kenkėjiškų“ programų įvedimas į kompiuterinę sistemą.

Aukščiau minėto įstatymo 3 straipsnyje nustatyta atsakomybė asmeniui, įvykdžiusiam neteisėtą kompiuterinių duomenų pakeitimą, jeigu jis :

- įvykdo neteisėtą veiką, ir dėl to modifikuojamas bet kokio kompiuterio turinys, ir
- veikos vykdymo metu asmuo turi reikiamą ketinimą bei reikiamų žinių.

Įstatyme „reikiamas ketinimas“ apibrėžiamas kaip ketinimas modifikuoti bet kokio kompiuterio turinį ir kartu susilpninti kompiuterio darbą, apriboti prieigą prie bet kokios programos ar duomenų bet kokiame kompiuteryje, pabloginti bet kokios programos darbą ar bet kokių duomenų patikimumą. Kai kurie teisės specialistai teigia, kad ši norma apima ir tuos atvejus, kai asmuo siekia blokuoti priėjimą prie informacijos ar programų ir panašiai.

Šis įstatymas ypatingas dar vienu aspektu. Tai įstatymo normos, išdėstytos skirsnyje „Jurisdikcija“. Šių normų dėka kompetentingų institucijų ir Didžiosios Britanijos teismų jurisdikcija taikoma bet kuriai iš minėtų neteisėtų veikų, jeigu, atliekant tokią veiką, bent vienas iš nusikaltimo sudėties elementų buvo Didžiojoje Britanijoje, t.y. tais atvejais, kai Didžiosios Britanijos teritorijoje buvo atlikta neteisėta veika arba dėl neteisėtos veikos kitoje šalyje atsirado žalingų pasekmių Didžiojoje Britanijoje.

Autoriaus nuomone, tokios įstatymo nuostatos yra tiesiog būtinos, kai nusikaltimas atliekamas naudojantis kompiuteriu, esančiu šalyje, nenustačiusioje atsakomybės už tokius nusikaltimus, arba kai baudžiamasis įstatymas yra materialaus charakterio, nustatydamas, kad nusikaltimas yra baigtas, kai nusikalstamos pasekmės atsiranda ten, kur buvo atlikta neteisėta veika .

[63]Computer Misuse Act 1990 In United Kingdom // http://www.hmso.gov.uk/acts/acts1990/Ukpga 19900018 en 1.htm

Nežiūrint to, kad šiame įstatyme išspręsta daug klausimų, kai kurie autoriai kritikuoja Piktnaudžiavimo, panaudojant kompiuterius įstatymą, nes jame neapibrėžtos sąvokos „kompiuteris“, „kompiuterinė programa“, „duomenys“ ir kt.

Be to, už sukčiavimo veikas, panaudojant kompiuterį, atsakomybė nustatyta 1968 metų Vagystės įstatymo (Theft Act) skirsnio „Sukčiavimas ir šantažas“ 15-20 skyriuose.[64] Pavyzdžiui, 20 skyriaus (2) poskyryje nustatyta, kad kiekvienas žmogus, kuris nesąžiningai apgaulės būdu padaro netektį kitam, gali būti nubaustas, remiantis šiuo įstatymu, laisvės atėmimu iki 7 metų. Toliau nurodoma, kad šis poskyris turi būti taikomas prieš neteisėtą sukūrimą, priėmimą, patvirtinimą, pakeitimą, atšaukimą arba dalinį arba visišką sunaikinimą saugios informacijos ir atitinkamai prieš pasirašymą arba užantspaudavimą bet kokio dokumento arba kitokios medžiagos, kad tai būtų atlikta paverčiant dokumentu.

1978 metais priimtas kitas vagystės įstatymas, kurio 1 ir 2 skyriuose vėlgi atitinkamai kriminalizuotos sukčiavimo veikos panaudojant kompiuterį:[65]

- nesąžiningas paslaugų gavimas apgaulės būdu;
- nesąžiningas atsakomybės vengimas apgaulės būdu.

Pavyzdžiui, minėto įstatymo 1 skyriaus (1) poskyryje nustatyta, kad baudžiamojon atsakomybėn traukiamas asmuo, kuris nesąžiningai apgaulės būdu naudojosi kito asmens paslaugomis.

Už kai kurias sukčiavimo veikas, kai neteisėtai siunčiami signalai, atsakomybė nustatyta 1984 metų Telekomunikacijų įstatyme:[66]

- sukčiavimas, naudojantis telekomunikacijų sistema (42 skyrius);
- netinkamas naudojimasis visuomenine telekomunikacijų sistema (43 skyrius);
- neteisėtas informacijos atskleidimas (101 skyriaus (5) poskyris).

Pažymėtina, kad sukčiavimu naudojantis telekomunikacijų sistema yra kriminalizuota telekomunikacijų paslaugų vagystė. Įstatymo 43 skyriuje nustatyta, kad netinkamas naudojimasis telekomunikacijų sistema, kai:

- naudojantis visuomenine telekomunikacijų sistema pasiunčiamas pranešimas arba informacija, kuri yra ypatingai įžeidžianti, nepadori arba bauginančio pobūdžio;
- naudojantis visuomenine telekomunikacijų sistema turint tikslą sukelti susierzinimą, nepatogumą arba bereikalingą susirūpinimą kitu pasiunčiamas pranešimas, žinant jį esant melagingu.

Privatumo apsaugai Didžiojoje Britanijoje skiriamas ypač didelis dėmesys. 1998 metais priimtas žmogaus teisių įstatymas, o kiek anksčiau, siekiant apsaugoti žmones nuo persekiojimų,

[64] Theft Act 1968 // http://www.vanuatu.usp.ac.fj/Paclawmat/UK legislation/UK Theft.html
[65] Theft Act 1978 http://www.sixthform.info/law/06 miscellaneous originals/statutes/theft act 1978.htm
[66] Telecommunications Act 1984 // http://www.communicationsbill.gov.uk/legislation/Telecommunications Act 1984.doc

1997 metais priimtas Apsaugos nuo persekiojimo įstatymas[67]. Kaip pažymi kai kurie teisės specialistai, tai labai svarbi įstatyminė sritis, kuri gali užtikrinti apsaugą rasinio persekiojimo, išvarginimo darbe, persekiojimo elektroninėmis priemonėmis, paštu ar telefoniniais skambučiais bylose. Būtina pastebėti, kad persekiojimo sąvoka neapibrėžta Apsaugos nuo persekiojimo įstatyme, ir tai turės būti įvertinta kiekvienu atveju. Tačiau keli netinkami straipsniai laikraštyje dar nesudaro persekiojimo. Persekiojimą turi sudaryti du požymiai: pavyzdžiui, daugiau nei vienas telefoninis skambutis, ir žmogaus sąmoningai pasirinktas tikslas - persekioti.

Kriminalizavimas veikų, susijusių su *neteisėtų signalų perdavimu* (siuntimu) elektroninių ryšių sektoriuje.

Neapykantos paštas dažniausiai yra anoniminis, tačiau jeigu jis gali būti nustatytas, tai asmuo gali būti traukiamas baudžiamojon atsakomybėn, remiantis 1988 metų Piktavališkų komunikacijų įstatymu.[68] Jame nustatyta baudžiamoji atsakomybė bet kuriam žmogui, pasiuntusiam:

a) laišką arba bet kokį kitą paštą, kuris perduoda:

(i) pranešimą, kuris yra nepadorus arba ypač agresyvus;

(ii) grasinimą; arba

(iii) informaciją, kuri yra melaginga, apie tai žinant siuntėjui; arba

b) bet kokį kitą paštą, kuris visas arba dalinai nepadorus arba ypač agresyvus.

Būtina sąlyga, kad aukščiau minėti veiksmai sukelia varginimą arba nerimą gavėjui arba bet kuriam kitam žmogui. 1988 metų Piktavališkų komunikacijų įstatymo kategorija 2001 metais išplėsta ir dabar apima ir elektronines komunikacijas arba bet kokio pobūdžio pranešimą. Ši nauja kategorija apima neapykantos telefoninius skambučius, elektroninį paštą arba teksto perdavimą.[69]

Kalbant apie interneto turinio reguliavimą, Didžiojoje Britanijoje vyrauja nuomonės, kad turi būti taikytini tie patys įstatymai kaip ir kitoms informacijos priemonėms. Vadovaudamasi šiuo požiūriu, Didžiosios Britanijos vyriausybė visų pirma papildė jau galiojančius įstatymus, išplėsdama jų taikymo sritį elektroninėms komunikacijoms. 1959 ir 1964 metų Nepadorių publikacijų, 1978 metų Apsaugos bei 1988 metų Kriminalinės justicijos įstatymai, parašyti tradiciniams leidėjams 1994 metais buvo papildyti Kriminalinė justicijos ir viešosios tvarkos įstatymu (Criminal Justine and Public Order Act)[70], kad būtų pritaikyti elektroninėms komunikacijoms, o „fotografijos“ sąvoka šiuose teisės aktuose apimtų kompiuterinius vaizdus. Pavyzdžiui, pakeista sąvoka „skelbimas“ dabar gali būti pritaikyta ir tiems atvejams, kai vienas

[67] Police (health and safety) Act 1997 // http://www.hmso.gov.uk/acts/acts1997/1997042.htm
[68] Malicious Communications Act 1988 (c. 27) // http://www.hsmo.gov.uk/acts/acts1988/Ukpga 19880027 en 1.htm
[69] Telephone tapping // http://www.yourrights.org.uk/your-rights/chapters/the-right-to-privacy/telephone-tapping-and-interception-of-communications/index.shtml
[70] Criminal Justine and Public Order Act // http://www.hmso.gov.uk/acts/acts1994/Ukpga_19940033_en_1.htm

asmuo patalpina duomenis siųsti ar krauti į kompiuterio kietąjį diską ir suteikia slaptažodį kitam asmeniui tam, kad šis galėtų prieiti prie nurodytų dokumentų. Tokiu būdu, skelbimu tapo suprantamas ir neviešas medžiagos patalpinimas, kai medžiaga prieinama tik tam tikram ratui asmenų, kurie gauna priėjimo slaptažodžius ar panašiai.

1996 metais Didžiojoje Britanijoje priimtas Seksualinių nusikaltimų įstatymas (The Sexual Offence Act)[71]. Jame pažeidimu laikomas kito asmens kurstymas padaryti seksualinius veiksmus prieš nepilnamečius, taip pat ir esančius užsienyje. Įstatyme kurstymas suprantamas kaip tam tikrų veiksmų atlikimas nepriklausomai nuo priemonių, kuriomis jis atliekamas (telefonu, faksu, internetu ar pan.). Be to, kurstymas laikomas vykstančiu Didžiojoje Britanijoje, jei šioje valstybėje yra komunikacijos gavėjas. Pagal šį įstatymą Internetu perduodamos žinutės siuntėjas arba interneto svetainės kūrėjas taip pat gali būti pripažinti kurstytojais.

Apibendrinant būtina pažymėti, kad Didžiojoje Britanijoje baudžiamoji atsakomybė nustatyta už daugelį neteisėtų veikų elektroninių ryšių sektoriuje.

Vokietija

Vokietijoje galioja 1975 metų sausio 1 d. priimta naujojo Baudžiamojo kodekso redakcija. Nuo to laiko vyko diskusijos, kuriomis buvo siekiama nustatyti baudžiamosios atsakomybės pagrindus už nusikaltimus, padaromus naudojant kompiuterius. 1986 metais, vadovaujantis Europos Tarybos rekomendacija dėl minimalaus ir neprivalomo nusikalstamų veikų sąrašo, į Baudžiamąjį kodeksą buvo įtraukta keletas nusikaltimų sudėčių, priimti atskiri įstatymai.[72] Dabartiniu metu Vokietijos baudžiamajame kodekse baudžiamoji atsakomybė už *neteisėtą signalų perdavimą* elektroninių ryšių sektoriuje nustatyta:

1. už privatumo pažeidimus:

- susirašinėjimo slaptumo pažeidimą (202 str). Jame nustatyta atsakomybė:

1) už neteisėtą svetimų laiškų arba kito uždaro dokumento atidarymą arba

2) už tokių dokumentų turinio atskleidimą techninėmis priemonėmis:

- neteisėtą duomenų peržiūrą (202 a str.);

- privačių paslapčių pažeidimą (203 str.);

- svetimų paslapčių panaudojimą (204 str.);

- telefoninių pokalbių slaptumo pažeidimas (206 str.). Pastarajame nustatyta atsakomybė už susirašinėjimo ir telefoninių pokalbių slaptumo pažeidimus, kai juos atlieka šias paslaugas teikiančių įmonių darbuotojai. Pažymėtina, kad atsakomybė yra numatyta tiek tiesiogiai atliekant minėtus pažeidimus, tiek ir už leidimą ar padėjimą tai atlikti ir kt.

[71] Sexual Offence Act // http://www.hmso.gov.uk/acts/acts1997/1997039.htm
[72] Criminal law // http://www.jura.uni-muenster.de/netlaw/default.cfm?RNr=0,30,133,18,19,132,16,41,79,43*opened=43*Lang=en*133

2. už kompiuterinius nusikaltimus : kompiuterinį sukčiavimą (263 str.), kai asmuo įtakoja informacijos apdorojimo procesus, manipuliuodamas programine įranga, naudodamas nepilnus, neteisingus duomenis ar kai jie naudojami neteisėtai; už naudojamų duomenų modifikavimą (269 str.); suklastotų duomenų, gautų informacijos apdorojimo procese, panaudojimą (270 str.); neteisėtą duomenų sunaikinimą (274 str.); duomenų modifikavimą (303 a str.) ir kompiuterinį sabotažą (303 b str.) ir kt.

Be Baudžiamojo kodekso Vokietijoje už neteisėtą įsikišimą į signalų perdavimą - neteisėtą telekomunikacijų perėmimą ar jos turinio perdavimą tretiesiems asmenims arba paties telekomunikacijų fakto atskleidimą baudžiamoji atsakomybė yra nustatyta Vokietijos 1996 metų Telekomunikacijų įstatymo 12 dalies 1 skyriuje (95 paragrafas). Bausmė už šį nusikaltimą – piniginė bauda arba laisvės atėmimas iki dviejų metų. Pažymėtina, kad minėtame įstatyme tokia pati bausmė nustatyta ir už neteisėtą siuntimo įrenginių laikymą, gamybą, importą ir pan.

Už veikas elektroninių ryšių sektoriuje, susijusias su *neteisėtų signalų perdavimu* (siuntimu), baudžiamoji atsakomybė nustatyta visų pirma Vokietijos BK. Už pornografinių laiškų platinimą, prievartos, seksualiniu naudojimusi vaikais ir gyvuliais medžiagos platinimą baudžiamoji atsakomybė nustatyta Vokietijos Baudžiamojo kodekso 184 str. 3 dalyje. Platinimo sąvoka apima platinimą, viešą paskelbimą, demonstravimą ar prieigos suteikimą, gaminimą, gavimą, siuntimą, laikymą, siūlymą, pranešimą ir ketinimą tai daryti.

Baudžiamoji atsakomybė už autorių teisių pažeidimą yra nustatyta Vokietijos įstatymo „Apie autorių teises“ 108a straipsnyje[73] - „Pakartotinas neteisėtos kompiuterinės informacijos naudojimas siekiant pelno“. Baudžiamoji atsakomybė šiame straipsnyje nustatyta, kai kompiuterinė informacija neteisėtai naudojama pakartotinai ir kai tuo siekiama padidinti pelną. Patraukimas baudžiamojon atsakomybėn yra galimas tik tuo atveju, kai yra gautas nukentėjusiosios šalies pareiškimas arba kai pažeidžiamas „visuomeninis interesas“.

Svarbiausias norminis teisės aktas, kuriuo Vokietijoje reglamentuojamas interneto turinio naudojimas, įsigaliojo 1997 metų rugpjūčio mėnesį. Tai Federacinės vyriausybės įstatymas dėl informacinių ir komunikacinių paslaugų (Informations und Kommunikationsdienste Gesetz).[74] Šiuo teisės aktu buvo pakeisti 6 įstatymai : Baudžiamasis kodeksas, Administracinių teisės pažeidimų kodeksas, Įstatymas dėl nepilnamečiams žalingų publikacijų platinimo bei kiti teisė aktai), išplečiant jų taikymo sritį informacijos tvarkymui naujomis informacinėmis technologijomis, bei priimti 3 nauji teisės aktai, tarp kurių svarbiausiais –Telepaslaugų įstatymas.[75] Naujai priimtu Telepaslaugų įstatymu (Teledienstegesetz) uždraustas neteisėto

[73] Gewerbsmäßige unerlaubte Verwertung // http://www.urheberrecht.org/law/normen/urhg/1990-03-07/text/bgbl_I_422_04_02_p97-111a.php3
[74] Informations und Kommunikationsdienste Gesetz // http://www.iid.de/rahmen/iukdgbt.pdf
[75] Telekommunikationsgesetz (TKG) // http://www.netlaw.de/gesetz/tdg.htm

turinio informacijos naudojimas bei reglamentuojama interneto paslaugų teikėjo atsakomybė už informacijos, kurią jis padaro prieinamą naudojimui, turinį.

Kaip matyti, baudžiamoji atsakomybė už nusikaltimus elektroninių ryšių sektoriuje skirtingose šalyse iš esmės skiriasi. Valstybių teisės aktai turi tam tikrą „nacionalinę specifiką“, bet galima išskirti ir tam tikrų bendrų bruožų. Kaip nurodoma teisinėje literatūroje, vieni iš pavojingiausių nusikaltimų elektroninių ryšių sektoriuje – kompiuteriniai nusikaltimai yra skirtingai kriminalizuoti pasaulio šalių baudžiamuosiuose įstatymuose. Pažymima, kad šiuo metu per 100 valstybių, tame tarpe 60% Interpolo narių, nėra priėmusios įstatymų kovojant su kompiuteriniais nusikaltimais. Panašius duomenis 2001 metais pateikė ir firma McConnell International“, atlikusi tyrimą „Kompiuteriniai nusikaltimai ir bausmės“[76]. Be to, daugelyje šalių už baudžiamojo įstatymo ribų lieka tokios pavojingos veikos elektroninių ryšių sektoriuje:

1) trukdymas gauti kompiuterinę informaciją, įskaitant ir tuos atvejus, kai blokuojamas kompiuterinės sistemos darbas;
2) neteisėtas kompiuterinės informacijos platinimas;
3) neteisėta prieiga prie informacinės sistemos;
4) trukdymas platinti teisėtai sukurtą informaciją, pavyzdžiui, atjungiant www puslapius nuo interneto tinklo ar juos sugadinant;
5) neteisėtas patekimas į laidinio, mobiliojo, radijo ar palydovinio ryšio linijas.

3.3 Nusikaltimų elektroninių ryšių sektoriuje reglamentavimas Lietuvoje

[76] Cyber crime ... and punishment? // http://www.mcconnellinternational.com/services/cybercrime.htm

Lietuvoje informacinių technologijų teisinis reglamentavimas prasidėjo 1991 metais. 1996 metais buvo priimta daug informatikos sritį reglamentuojančių įstatymų, o 2003 metų gegužės 1 d. Lietuvoje įsigaliojo naujasis Baudžiamajame kodeksas[77]. Jame nustatyta baudžiamoji atsakomybė už daugelį neteisėtų veikų elektroninių ryšių sektoriuje. Baudžiamoji atsakomybė už *neteisėtą signalų perdavimą* elektroninių ryšių sektoriuje, visų pirma nustatyta LR BK XXX skyriuje „Nusikaltimai informatikai“:

1) *kompiuterinės informacijos sunaikinimas ar pakeitimas* (196 str.). Straipsnyje nustatyta baudžiamoji atsakomybė už kompiuterinės informacijos sunaikinimą, sugadinimą ar pakeitimą, jei dėl to buvo padaryta didelė žala;

2) *kompiuterinės programos sunaikinimas ar pakeitimas* (197 str.). Straipsnyje nustatyta baudžiamoji atsakomybė už kompiuterinės programos sunaikinimą, sugadinimą ar pakeitimą, taip pat už programos į kompiuterį ar kompiuterinį tinklą įdiegimą, jei dėl to buvo pakeistas kompiuterinio tinklo, duomenų banko ar informacinės sistemos darbas ir jei dėl to buvo padaryta didelė žala;

3) *kompiuterinės informacijos pasisavinimą ir skleidimą* (198 str.). Straipsnio 1-oje dalyje nustatyta baudžiamoji atsakomybė už įstatymo saugomos informacijos apie juridinį ar fizinį asmenį pasisavinimą, 2-oje – už pasisavintos įstatymo saugomos informacijos apie fizinį ar juridinį asmenį viešą paskelbimą, paskleidimą, platinimą ar kitokį informacijos panaudojimą, paskleidimą;

4) *neteisėtą prisijungimą prie kompiuterio ar kompiuterinio tinklo* (198^1 str.). Straipsnyje nustatyta baudžiamoji atsakomybė už neteisėtą prisijungimą prie kompiuterio ar kompiuterinio tinklo pažeidžiant kompiuterio ar kompiuterinio tinklo apsaugos priemones;

5*) neteisėtą disponavimą įrenginiais, kompiuterinėmis programomis, slaptažodžiais, prisijungimo kodais ir kitokiais duomenimis, skirtais nusikaltimams daryti* (198^2 str.). Straipsnio 1 ir 2 dalyje nustatyta baudžiamoji atsakomybė už įrenginių, skirtų daryti Baudžiamojo kodekso 166,196,197,198 ir 198^1 straipsniuose nustatytus nusikaltimus, neteisėtą gaminimą, gabenimą, pardavimą ar kitokį platinimą ir kt.

Pažymėtina, kad minėti straipsniai apima beveik visas neteisėtas veikas, susijusias su kompiuterių panaudojimu. Tačiau kai kurie straipsniai taisytini. Visų pirma kiek netiksliai Baudžiamojo kodekso 198 straipsnio 1 dalies dispozicijoje naudojama sąvoka „pasisavino“. Klasikinės vagystės metu „turto pasisavinimas – tai neteisėtas paimto daikto užvaldymas, turint tikslą valdyti tą daiktą kaip nuosavą“[78] ,t.y. kaltininkas išima turtą iš jo buvimo vietos ir perkelia

[77] Lietuvos Respublikos baudžiamasis kodeksas: patvirtintas 2000 m. rugsėjo 26 d. įstatymu Nr.VIII-1968, įsigaliojo 2003 m. gegužės 1 dieną: oficialus tekstas (parengtas ir išleistas vykdant Lietuvos Respublikos teisingumo ministro 2004 m. vasario 27 d. įsakymą Nr.1R-54)/Lietuvos Respublikos teisingumo ministerija.-4-asis papildytas leid. – Vilnius: VĮ Teisinės informacijos centras, 2004.p.300.

[78] Baudžiamoji teisė. Specialioji dalis. I knyga. – V.: Eugrimas, 2001.p.346.

į kitą vietą, nustatydamas užvaldytam turtui neteisėtą viešpatavimą. Kaip jau buvo minėta, skaitmeninė informacija yra specifinė, nes ji gali būti ne tik pasisavinama, bet ir kopijuojama. Pastaruoju atveju ji lieka pas seną savininką.

Toliau 198 straipsnio 2 dalies dispozicija, kurioje nustatyta atsakomybė už neteisėtai gautos informacijos viešą paskelbimą, paskleidimą ir kt. Šiandieninė interneto panaudojimo specifika leidžia į interneto puslapius įdėti įstatymų saugomą neteisėtai įgytą kompiuterinę informaciją apie juridinį ar fizinį asmenį, kuri nebus viešai prieinama, t.y. prie jos galės prieiti tik tam tikra uždara asmenų grupė. Todėl, autoriaus manymu, viešo prieinamumo požymis turi būti panaikintas.

Be minėtų straipsnių, už *neteisėtą signalų perdavimą* elektroninių ryšių sektoriuje, baudžiamoji atsakomybė nustatyta ir kituose Baudžiamojo kodekso straipsniuose:

1. *Neteisėtas susirašinėjimo, kitokių pranešimų, siuntimų ar pokalbių telefonu slaptumo pažeidimas* (166 str.). Straipsnyje nustatyta baudžiamoji atsakomybė už neteisėtą pažeidimą asmens susirašinėjimo ar kitokių paštu ar techninėmis priemonėmis siunčiamų parnešimų, siuntų slaptumą arba klausymąsi pokalbių telefonu, arba naudojimą kitų jų perėmimo priemonių. Minėto straipsnio 1 dalies konstrukcija tobulintina, nes:

1) tiek straipsnio pavadinimas, tiek ir pati konstrukcija yra sudėtinga, nes išvardinta nemažai pranešimų siuntimo formų, nors sąrašas ir nėra baigtinis;

2) vienoda baudžiamoji atsakomybė taikoma tiek įmonės teikiančios komunikacijų paslaugas darbuotojui, tiek ir bet kuriam kitam asmeniui;

3) „Pranešimo“ sąvoka neapima iliustracijų. Iliustracija [lot. Illustratio – vaizdus aiškinimas, vaizdavimas]: 1. fotografija, piešinys, brėžinys, paaiškinantis arba papildantis tekstą; 2. knygų grafikos kūrinys, aiškinantis, papildantis arba puošiantis knygos, žurnalo, laikraščio tekstą; 3.* pavyzdys, ką nors vaizdžiai paaiškinantis[79].

Taip pat būtina pažymėti, kad nei šiame straipsnyje, nei kituose BK straipsniuose nenustatyta baudžiamoji atsakomybė asmeniui, kuris pats ketina arba padeda kitam žmogui atlikti arba sudaro sąlygas neteisėtam susirašinėjimo, kitokių pranešimų, siuntų ir pokalbių telefonu slaptumo pažeidimui. Autoriaus nuomone, straipsnis taisytinas, vadovaujantis Kanados, JAV, Vokietijos ir kitų šalių pavyzdžiu.

Autorius siūlo tokią straipsnio konstrukciją:

166 straipsnis. Neteisėtas privačių komunikacijų slaptumo pažeidimas.

1. Tas, kas tiesiogiai ar naudodamasis laidinėmis, radijo, optinėmis ar kitomis elektromagnetinėmis priemonėmis bando pažeisti, pažeidžia arba sudaro sąlygas kitam asmeniui

[79] Kvietkauskas V. Tarptautinių žodžių žodynas.-Vilnius: VER, 1985.p.208.

pažeisti kito asmens privačių komunikacijų slaptumą, baudžiamas viešaisiais darbais arba bauda, arba laisvės apribojimu, arba areštu, arba laisvės atėmimu iki dvejų metų.

2. Tas, kas padarė šio straipsnio 1 dalyje numatytą veiką būdamas įmonės teikiančias komunikacijų paslaugas darbuotoju, baudžiamas viešaisiais darbais arba bauda, arba laisvės apribojimu, arba areštu, arba laisvės atėmimu iki trejų metų ir teisės dirbti minėtą darbą 5 metus atėmimu.

3. Už šiame straipsnyje numatytą veiką atsako ir juridinis asmuo.

Autoriaus nuomone, Lietuvos Respublikos BK tikslinga nustatyti baudžiamąją atsakomybę ir už veikas, kurios teisinėje literatūroje įvardijamos kaip kiber persekiojimai. Tai neteisėtos veikos, kai elektroniniais ryšiais, pavyzdžiui, elektroniniu paštu siuntinėjami nepadorūs, įžeidžiantys, grasinantys ar nuolat pasikartojantys nepageidaujami pranešimai. Atsakomybė už šias neteisėtas veikas turėtų būti nustatyta Lietuvos Respublikos BK XXIV skyriuje „Nusikaltimai asmens privataus gyvenimo neliečiamumui“.

2. *Neteisėtas naudojimasis energija ir ryšių paslaugomis* (179 str.).

Jame nustatyta baudžiamoji atsakomybė už veiką, kai neteisėtai prisijungus prie energijos tiekimo arba ryšių tinklo ar saugyklos, iškraipant skaitiklių rodmenis arba kitais neteisėtais būdais naudojamasi elektros ar šilumos energija, dujomis, vandeniu, telekomunikacijomis ar kitais ekonominę vertę turinčiais dalykais ir dėl to kitam asmeniui padaroma turtinės žalos. Atsakomybė už neteisėtą veiką elektroninių ryšių sektoriuje čia galima, kai neteisėtai prisijungus prie ryšių tinklo naudojamasi telekomunikacijomis.

Autoriaus nuomone, kiek netiksliai Baudžiamojo kodekso 179 straipsnio 1 dalies dispozicijoje naudojamas terminas “telekomunikacijos”. Minėtas terminas turėtų būti keičiamas “elektroninių ryšių” terminu, kuris apima ne tik telekomunikacijas, bet ir televizijos bei radijo transliavimą (įskaitant retransliavimą). Tai patvirtinta ir 2004-05-01 Lietuvoje įsigaliojusio Elektroninių ryšių įstatymo sąvokų analizė.

Pažymėtina, kad galiojančiame BK nėra nustatyta atsakomybė už įrenginio, skirto neteisėtai naudoti elektroninių ryšių įrenginius ar paslaugas, gaminimą, pardavimą arba kitokį platinimą. Autoriaus manymu, tokio įrenginio gaminimas, pardavimas ar kitoks platinimas yra nemažiau pavojingas nei slaptažodžių, prisijungimo kodų gaminimas, pardavimas ar kitoks platinimas. Atsižvelgiant į tai, BK 179 straipsnis galėtų būti papildytas dalimi, nustatančia baudžiamąją atsakomybę už įrenginio, skirto neteisėtai naudoti elektroninius ryšius, gaminimą, pardavimą ar kitokį platinimą.

Už *neteisėtų signalų perdavimą* elektroninių ryšių sektoriuje baudžiamoji atsakomybė visų pirma nustatyta LR BK XXIX skyriuje “Nusikaltimai intelektinei ir pramoninei nuosavybei”. *Literatūros, mokslo, meno ar kitokio kūrinio neteisėtas atgaminimas, neteisėtų*

kopijų platinimas, gabenimas ar laikymas (192 str.). Straipsnyje nustatyta baudžiamoji atsakomybė nusikaltimų elektroninių ryšių sektoriuje atžvilgiu taikoma, kai importuojamas, eksportuojamas, platinamas neteisėtas, t.y. bet kuriuo būdu neteisėtai įgytas literatūros, mokslo, meno ar kitoks kūrinys ar jo dalis, jeigu kopijų bendra vertė pagal teisėtų kopijų mažmenines kainas didesnė nei 100 MGL ir jeigu neteisėtos veikos atliekamos naudojantis elektroniniais ryšiais, pavyzdžiui, platinant internete.

191, 193, 194 ir 195 straipsniuose taip pat nustatyta atsakomybė ir už kitus intelektinės nuosavybės teisių pažeidimus, kurie atliekami naudojantis elektroniniais ryšiais.

Kituose straipsniuose baudžiamoji atsakomybė nustatyta už:

1. *Disponavimą pornografinio turinio dalykais* (309 str.).

Straipsnyje nustatyta baudžiamoji atsakomybė nusikaltimų elektroninių ryšių sektoriuje atžvilgiu taikoma už pornografinio turinio dalykų demonstravimą ar platinimą ir pornografinio turinio dalykų, kuriuose vaizduojamas vaikas arba asmuo pateikiamas kaip vaikas, platinimą, demonstravimą, reklamavimą.

2. Su viešai neskelbtinos informacijos platinimu susijusias veikas:
   1) *viešus raginimus smurtu pažeisti Lietuvos Respublikos suverenitetą* (122 str.);
   2) *valstybės paslapties atskleidimą* (125 str.);
   3) *valstybės paslapties praradimą* (126 str.);
   4) *įžeidimą* (127 str.);
   5) *neteisėtą informacijos apie asmens privatų gyvenimą atskleidimą ir panaudojimą* (168 str.);
   6) *neapykantos, prieš bet kokios tautos, rasės, etninę, religinę ar kitokią žmonių grupę kurstymą* (17 str.) ir kt.

Atsakomybė už šių veikų atlikimą, priklausomai nuo nusikaltimo ar nusižengimo pobūdžio, svyruoja nuo baudos iki laisvės atėmimo. Nusikaltimas laikytinas nusikaltimu elektroninių ryšių sektoriuje, kai atliekamas naudojantis elektroniniais ryšiais, pavyzdžiui, kompiuteriu sukuriamas ir per internetą išplatinamas pranešimas, raginantis smurtu pažeisti Lietuvos Respublikos suverenitetą.

3. *Melagingą pranešimą apie visuomenei gresiantį pavojų ar ištikusią nelaimę* (285 str.). Straipsnyje nustatyta baudžiamoji atsakomybė už melagingą pranešimą ar paskleidimą žinios apie visuomenei gresiantį pavojų arba didelę nelaimę, jeigu dėl to kilo žmonių sumaištis arba buvo padaryta didelės turtinės žalos (1 dalis), arba jeigu dėl to buvo iškviestos specialiosios tarnybos (2 dalis). Pažymėtina, kad melagingu pranešimu laikytinas bet kokiu būdu (telefonu, faksu, laišku, elektroniniu paštu ir t.t.) netikros informacijos perdavimas. Pranešimo turinys –

informacija apie galingą sprogimą, pavojingų medžiagų patekimą į aplinką, apie padėtą sprogmenį tam tikrame pastate, ant geležinkelio bėgių, laive ar orlaivyje ir kt.

Autoriaus nuomone, Lietuvos BK tikslinga nustatyti atsakomybę ir už naujas neteisėtas veikas elektroninių ryšių sektoriuje – elektroninio pašto "bombinimas" arba 'spam" žinučių siuntimas. "Bombing", angliškai reiškia bombardavimą, o "spamming"" – tai naujas žodis anglų kalboje, reiškiantis nepageidaujamos informacijos siuntimą. "Bombing" esmė tokia: konkrečiu elektroninio pašto adresu išsiunčiamas labai didelis laiškų kiekis arba labai didelių laiškų kiekis. Vartotojas gauna per 100000 laiškų ir nespėja ne tik jų peržiūrėti, bet ir trinti. "Spamming" panašus į "Bombing", nes šiuo atveju irgi siunčiama informacija, bet ne vienu adresu, o labai daugeliu adresų reklamos tikslu.[80] Tai labai panašu į lankstinukų siuntimą į paprastą pašto dėžutę, skirtumas tik tas, kad popierius kainuoja daugiau, o čia laiškus siuntinėja serveriai. Tokie kriminalistiniai nusikaltimai daro žalos tiek eiliniam vartotojui, tiek ir serveriams, kurie apkraunami nereikalinga informacija. Šių nusikaltimų kriminalizavimui galima pasinaudoti kitų užsienio šalių patirtimi.

Lietuvos teisės aktuose tikslinga apibrėžti tokias sąvokas kaip "kompiuteris", "kompiuterinė informacija", "kompiuterinis tinklas" ir t.t. Nors minėtosios sąvokos iš pažiūros atrodytų aiškios, tačiau tolesnė interneto informacinių technologijų plėtra gali sukelti problemų šias sąvokas interpretuojant baudžiamosios teisės požiūriu. Tai skatina padaryti ir tai, kad pasaulyje iki šiol nėra vieningos nuomonės dėl kai kurių iš šių sąvokų. Šios problemos sprendimas įmanomas dviem būdais:

1) vadovaujantis Kanados patirtimi, kur pačiame BK yra išspręsta sąvokų (be minėtų - dar visų kitų, pvz., pornografinė medžiaga apie vaikus) traktavimo problema. Savo ruožtu Lietuvos Respublikos BK XXX skyrių tikslinga papildyti straipsniu "Sąvokų aiškinimas". Tokia konstrukcija galiojančiame BK priimtina, pvz., XIVI skyrius "Nusikaltimai ir baudžiamieji nusižengimai krašto apsaugos tarnybai".

2) vadovaujantis Rusijos patirtimi, kur priimtas atskiras įstatymas "Dėl informacijos, informatizacijos apsaugos"(www.hro.org/docs/rlex/int/), pateikiantis daugelio sąvokų, susijusių su internetu ir kitomis informacinėmis technologijomis, apibrėžimus.

IŠVADOS

[80] Interneto kriminalistika // http://www-test.e-net.lt

Reikėtų pastebėti, jog išskirti ir smulkiai išnagrinėti visus nusikaltimus elektroninių ryšių sektoriuje šios studijos apimties tikrai nepakanka.

Atsižvelgiant į studijoje užsibrėžtą tikslą ir apibendrinant galima daryti šias išvadas:

1.Lietuvos Respublikos elektroninių ryšių įstatyme suformuluota „elektroninių ryšių“ sąvoka laikytina tinkamiausia, t.y. „elektroniniai ryšiai“ – signalų perdavimas laidinėmis, radijo, optinėmis ar kitomis elektromagnetinėmis priemonėmis

2.Elektroninė erdvė – vieta, erdvė, aplinka, kurioje galimi bet kokie elektroniniai ryšiai.

3.Nusikaltimu elektroninių ryšių sektoriuje reikėtų laikyti neteisėtą veiką, kuria pažeidžiama (perimama, pakeičiama, siunčiama, įvedama, ištrinama, naudojama, kopijuojama, platinama ir kt.) teisėta signalų perdavimo laidinėmis, radijo, optinėmis ar kitomis elektromagnetinėmis priemonėmis tvarka.

4.Nusikaltimai elektroninių ryšių sektoriuje gali būti atliekami dviejų rūšių neteisėtomis veikomis, t.y. laidinėmis, radijo, optinėmis ar kitomis elektromagnetinėmis priemonėmis signalai perduodami neteisėtai arba perduodami neteisėti signalai.

4.Išskirtiniais nusikaltimų elektroninių ryšių sektoriuje požymiais reikėtų laikyti jų didelį pavojingumą ir latentiškumą; aplinką, kurioje atliekami šie nusikaltimai; anonimiškumą tiek nusikaltėlio, tiek ir aukos; buvimą tiesioginio kontakto realiame laike tarp aukos ir nusikaltėlio; bet kurios sistemos, prijungtos prie globalaus ryšio tinklo pasiekiamumą; specifinę terminiją; veiką, atliekamą tik aktyviais veiksmais ir nusikalstamas pasekmes.

5.Pagrindiniu nusikaltimo elektroninių ryšių sektoriuje kėsinimosi objektu reikėtų laikyti įstatymų saugomą informaciją, neleistinai apdorojamą, naudojamą ir platinamą elektroninių ryšių sektoriuje.

6.Pagrindinis nusikaltimo elektroninių ryšių sektoriuje dalykas – informacija – žinios apie objektyvųjį pasaulį ir jame vykstančius procesus, kurių visapusiškumas, konfidencialumas ir prieinamumas užtikrinamas dėka kompiuterinės, telekomunikacinės ir kitokios elektroninės ar elektromagnetinės technikos, ir kurios turi kainą ir savininką.

7.Šiuo metu Lietuvoje baudžiamosios atsakomybės pagrindai nustatyti praktiškai už visas neteisėtas veikas elektroninių ryšių sektoriuje. Tačiau kai kurių neteisėtų veikų elektroninių ryšių sektoriuje negalima kvalifikuoti pagal dabar galiojančio Lietuvos Respublikos BK normas. Todėl, atsižvelgiant į autoriaus siūlomas rekomendacijas, būtina:

7.1.pataisyti Lietuvos Respublikos BK 179 straipsnio 1 dalies ir 198 straipsnio 1 ir 2 dalies dispozicijas;

7.2.reformuoti Lietuvos Respublikos BK 166 straipsnį: pakeisti straipsnio pavadinimą ir 1 dalies dispoziciją bei papildyti straipsnį dar viena dalimi.

7.3.papildyti Lietuvos Respublikos BK straipsniais, nustatančiais atsakomybę už įrenginio, skirto neteisėtai naudoti elektroninių ryšių įrenginius ar paslaugas gaminimą, pardavimą arba kitokį platinimą; kiber persekiojimą; neteisėtą elektroninio pašto „bombinimą“ arba „spam“ žinučių siuntimą.

SANTRAUKA

Šioje studijoje supažindinama su Lietuvoje iki šiol nauja nusikalstamumo rūšimi – nusikaltimais elektroninių ryšių sektoriuje, jų keliama grėsme tiek fiziniams, tiek ir juridiniams asmenims. Formuluojama nusikaltimo elektroninių ryšių sektoriuje sąvoka, pateikiama trumpa šių nusikaltimų klasifikacija, išskiriami tik šiems nusikaltimams būdingi, išskirtiniai požymiai, aptariami šiame sektoriuje atliekamų nusikaltimų būdai. Nagrinėjami nusikaltimų elektroninių ryšių sektoriuje precedentai. Apžvelgiami į kai kurie teisiniai nusikaltimų elektroninių ryšių sektoriuje aspektai, analizuojamas teisinis atsakomybės reglamentavimas tarptautiniu (regioniniu) mastu ir kai kuriose užsienio valstybėse. Analizuojami Lietuvos Respublikos Baudžiamojo kodekso trūkumai ir pateikiami pasiūlymai jo pataisymui ir papildymui .

SUMMARY

At this job the author acquaints with a new kind of criminality - crimes in sector of electronic communications, with threat which they cause physical and legal persons. The concept of a crime of sector of electronic communications is formulated, are resulted short classification of these a crime. Kinds and specific attributes of these a crime are certain, ways made a crime in this sector are discussed. Precedents in sector of electronic communications are considered. Some legal aspects a crime in sector of electronic communications are submitted, regulation of the legal responsibility internationally and in some foreign countries is analyzed. It is analyzed lacks of the Criminal code of the Lithuanian Republic and amendment for his updating and additions are offered.

LITERATŪROS SĄRAŠAS

1.Lietuvos Respublikos pagrindiniai įstatymai. – Vilnius: Saulužė, 2000.P.720.

2.Lietuvos Respublikos baudžiamasis kodeksas: patvirtintas 2000 m. rugsėjo 26 d. įstatymu Nr.VIII-1968, įsigaliojo 2003 m. gegužės 1 dieną: oficialus tekstas (parengtas ir išleistas vykdant Lietuvos Respublikos teisingumo ministro 2004 m. vasario 27 d. įsakymą Nr.1R-54)/Lietuvos Respublikos teisingumo ministerija.-4-asis papildytas leid. – Vilnius: VĮ Teisinės informacijos centras, 2004.P.300.

3.Lietuvos Respublikos Konstitucinio teismo nutarimas „Dėl telekomunikacijų įstatymo“ // Valstybės žinios. 1999, Nr.85-2548.

4.Lietuvos Respublikos visuomenės informavimo įstatymas // Valstybės žinios. 1996, Nr.71-1706; 2000, Nr.75-2272.

5.Lietuvos Respublikos telekomunikacijų įstatymas // Valstybės žinios. 1998, Nr.56-1548; 2002, Nr.75-3215.

6.Lietuvos Respublikos elektroninių ryšių įstatymas // Valstybės žinios. 2004, Nr.69-2382.

7.Abramavičius A., Bieliūnas ., Drakšienė A. ir kt. Baudžiamoji teisė: specialioji dalis. – Vilnius: Eugrimas, 2001.P.451.

8.Petrauskas R., Štitilis D. Kompiuteriniai nusikaltimai ir jų prevencija. – Vilnius: LTU, 2000.P.61.

9.Meškauskaitė L. Naujųjų informacinių technologijų teisinis reguliavimas. – Vilnius: Jurisprudencija, 2002. T.32(34).P.106.

10.Kvietkauskas V. Tarptautinių žodžių žodynas.-Vilnius: VER, 1985. P.265.

11.Kibernetinė erdvė // http://aldona.mii.lt/pms/terminai/term/z2odynas.html; prisijungimo laikas: 2004-11-09.

12.Informacinės technologijos ir nusikaltimai // http://www.infovi.vu.lt/ivs.biblioteka/temos/nusikaltimai.htm; prisijungimo laikas: 2004-10-17.

13.http://www.delfi.lt/news/economy/ITbussines/article.php?id=5150802; prisijungimo laikas: 2004-10-12.

14.Interneto kriminalistika // http://www-test.e-net.lt; prisijungimo laikas: 2004-10-12.

15.Computer-related crime: Anglysis Of Legal Policy, Paris: OECD, 1986, P.86.

16.1999 Communications Review for electronic communications infrastructure and associated servines // http://europa.eu.int/ISPO/infosoc/telecompolicy/review99/review99.htm; prisijungimo laikas: 2004-05-10.

17.Directive (2002/21/EC) on a Common Regulatory Framework // http://europa.eu.int/information_society/topics/telecoms/regulatory/new_rf/index_en.htm#reg; prisijungimo laikas: 2004-05-10.
18.The Privacy and Electronics Communications (EC Directive) Regulations 2003 // http://www.hmso.gov.uk/si/si2003/n12#n12; prisijungimo laikas: 2004-05-08.
19.Communications Act 2003 // http://www.hmso.gov.uk/acts/acts2003/30021--c.htm; prisijungimo laikas: 2004-05-10.
20.Electronics Communications Act 2000 // http://www.hsmo.gov.uk/acts/acts2000/20000007.htm; prisijungimo laikas: 2004-05-11.
21.CODE DES POSTES ET TELECOMMUNICATIONS // http://lexinter.net/servpub/code des postes et telecommunications.htm; prisijungimo laikas: 2004-05-12.
22.2003 Projet de loi sur les communications electroniques // http://dess droit-internet.univ paris1.fr/biblioteque/IMG/doc/2003-04 Avant projet loi Ctn lq.doc.; prisijungimo laikas: 2004-05-12.
23.Interception and disclosure of wire, oral, or electronic communications prohibited // http://www4.law.cornell.edu/uscode/18/2511.html; prisijungimo laikas: 2004-05-12.
24.Electronic communications policy // http://www.commnet.edu/it/policy/electronic-communications.html; prisijungimo laikas: 2004-05-12.
25.Electronic Communications Policy – University of California // http://www.ucop.edu/ucophome/policies/ec/html/welcome.htm; prisijungimo laikas: 2004-05-12.
26.What is Cyberspace? // http://www.nutball.com/classes/mrshowell/dewitt/Whatis.html; prisijungimo laikas: 2004-11-09.
27.Cybercrime // htp://faculty.ncwc.edu/toconnor/315/315lect12.htm; prisijungimo laikas: 2004-11-09.
28.Cyberspace // http://www.thefreedictionary.com/cyberspace; prisijungimo laikas: 2004-11-09.
29.Proposed Cyberspace Privacy Act // http://www1.law.ucla.edu/~kang/Scholarship/Cyberspace/CyberspacePrivacyAct/cyberspaceprivacyact.htm; prisijungimo laikas: 2004-11-09.
30.Convention on Cybercrime // http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm; prisijungimo laikas: 2004-03-05.
31.Crime in the Cyberspace // http://www.abc.net.au/rn/science/ockham/stories/s45008.htm; prisijungimo laikas: 2004-11-10.
32.Computer Crimes & Cyberspace Cases // http://www.massachusetts-lawyers.com/pages/criminal/computercrime.html; prisijungimo laikas 2004-11-11.

33.Computer Crime - Can it affect you?? // http://www3.sk.sympatico.ca/rcmpccs/cpu-crim.html; prisijungimo laikas 2004-11-15.
34.Willet G. Global Communications: a modern myth? // htp://www.unisa.ac.za/dept/press/comca/212/willet.html; prisijungimo laikas 2004-11-10.
35.Danko Vukovic „Computer Crime“ // http://www.elitesecurity.org/tema/477/.; prisijungimo laikas 2004-07-03.
36.Statement for the Record of Louis J. Freeh, Director Federal Bureau of Investigation On Cybercrime Before the Senate Committee on Judiciary Subcommittee for the Technology, Terrorism, and Government Informatikon Washington, D.C.,March 28, 2000 // http://4uth.gov.ua/usa/english/tech/crimesip/freeh328.htm; prisijungimo laikas 2004-07-03.
37.Recommendations no. R (89)9 on Computer-related crime // http://cm.coe.int/ta/rec/1989/89r9.htm; prisijungimo laikas 2004-05-11.
38.Action Plan on promoting safer use of the Internet // http://europa.eu.int/ISPO/iap/decision/en.html; prisijungimo laikas 2004-05-11.
39.COUNCIL FRAMEWORK DECISION on attack against informatikon systems // http://europa.eu.int/eur-lex/en/com/pdf/2002/com2002_0173en01.pdf; prisijungimo laikas 2004-05-11.
40.International review of criminal policy „United Nations Manual on the prevention and control of computer-related crime“ // http: // www.uncjin.org/Documents/EighthCongress.html; prisijungimo laikas 2004-05-11.
41.Fraud and related activity in connection with computers // http://www.usdoj.gov/criminal/cybercrime/fedcode.htm; prisijungimo laikas 2004-05-11.
42.Interception and disclosure of wire, oral, or electronic communications prohibited // http://www4.law.cornell.edu/uscode/18/2511.html; prisijungimo laikas 2004-05-11.
43.Certain activities relating to material involving the sexual exploitation of minors // http://www4.law.cornell.edu/uscode/18/2252.html; prisijungimo laikas 2004-05-14.
44.Communications Decency Act of 1996 // http://www.fcc.gov/Reports/tcom1996.txt; prisijungimo laikas 2004-05-14.
45.18-6713. THEFT OF TELECOMMUNICATION SERVINES // http://www3.state.id.us/cgi-bin/newidst?sctid=180670013.K; prisijungimo laikas 2004-05-14.
46.Mississippi Code of 1972 // http://www.mscode.com/free/statutes/97/025/0054.htm; prisijungimo laikas 2004-05-11.
47.Cyber crime ... and punishment? // http://www.mcconnellinternational.com/services/cybercrime.htm; prisijungimo laikas 2004-05-11.

48.Canadian Criminal Code // http://www.digitaldefence.ca/Kanada CriminalCode.htm; prisijungimo laikas 2004-05-11.
49.Canadian Radio-television and Telecommunications Commission // http://www.crtc.gc.ca/eng/statutes.htm; prisijungimo laikas 2004-05-11.
50.Computer Misuse Act 1990 In United Kingdom // http://www.hmso.gov.uk/acts/acts1990/Ukpga 19900018 en 1.htm; prisijungimo laikas 2004-05-14.
51.Theft Act 1968 // http://www.vanuatu.usp.ac.fj/Paclawmat/UK legislation/UK Theft.html; prisijungimo laikas 2004-05-14.
52.Theft Act 1978 http://www.sixthform.info/law/06 miscellaneous originals/statutes/theft act 1978.htm; prisijungimo laikas 2004-05-14.
53.Telecommunications Act 1984 // http://www.communicationsbill.gov.uk/legislation/Telecommunications Act 1984.doc; prisijungimo laikas 2004-05-14.
54.Police (health and safety) Act 1997 // http://www.hmso.gov.uk/acts/acts1997/1997042.htm; prisijungimo laikas 2004-05-11.
55.Malicious Communications Act 1988 (c. 27) // http://www.hsmo.gov.uk/acts/acts1988/Ukpga 19880027 en 1.htm; prisijungimo laikas 2004-05-11.
56. Telephone tapping // http://www.yourrights.org.uk/your-rights/chapters/the-right-to-privacy/telephone-tapping-and-interception-of-communications/index.shtml; prisijungimo laikas 2004-05-11.
57.Criminal Justine and Public Order Act // http://www.hmso.gov.uk/acts/acts1994/Ukpga_19940033_en_1.htm; prisijungimo laikas 2004-05-11.
58.Sexual Offence Act // http://www.hmso.gov.uk/acts/acts1997/1997039.htm; prisijungimo laikas 2004-05-11.
59Criminal law // http://www.jura.uni-muenster.de/netlaw/default.cfm?RNr=0,30,133,18,19,132,16,41,79,43*opened=43*Lang=en*13; prisijungimo laikas 2004-05-11.
60.Gewerbsmäßige unerlaubte Verwertung // http://www.urheberrecht.org/law/normen/urhg/1990-03-07/text/bgbl_I_422_04_02_p97-111a.php3; prisijungimo laikas 2004-05-08.
61.Informations und Kommunikationsdienste Gesetz // http://www.iid.de/rahmen/iukdgbt.pdf; prisijungimo laikas 2004-05-08.

62.Telekommunikationsgesetz (TKG) // http://www.netlaw.de/gesetz/tdg.htm; prisijungimo laikas 2004-05-11.
63.Батурин Ю. М. Проблемы компьютерного права - М.: Юридическая литература, 1991.с.271.
64.Новый Федеральный закон „О связях“ // http://www.medialaw.ru/laws/russian laws/telecom/; prisijungimo laikas: 2004-05-11.
65.Проблемы латентности комьютерной преступности // http://www.crime-research.ru; prisijungimo laikas: 2004-05-11.
66.ФБР расследует беспрецедентный взлом систем кредитных карт. // http://palm.newsru.com/world/19may2003/rus hackers.html; prisijungimo laikas: 2004-10-14.
67.Правовой анализ отдельных действий, наносящих потерпевшим ущерб в сфере высоких технологий // http://sm.aport.ru/scripts/template.dll?r...; prisijungimo laikas: 2004-10-14.
68.Киберпреступность в зарубежных странах, концепция ее детерминации и предупреждения // http://www.crime-research.ru/articles/Sabadash0904/; prisijungimo laikas: 2004-10-14.
69.Компьютерное преступление в мире без границ http://www.crime-research.org/library/peter.htm; prisijungimo laikas: 2004-10-14.