MYKOLO ROMERIO UNIVERSITETAS

Mindaugas Kiškis, Rimantas Petrauskas,
Irmantas Rotomskis, Darius Štitilis

TEISĖS INFORMATIKA IR INFORMATIKOS TEISĖ

Vadovėlis

2006
Vilnius

UDK 34:004(075.8)
Te23

2005 m. gruodžio 23 d. Nr. A-290
Aukštųjų mokyklų bendrųjų vadovėlių leidybos komisijos rekomenduota

Vadovėlis išleistas parėmus Lietuvos Respublikos švietimo ir mokslo ministerijai

Vadovėlį recenzavo Kauno technologijos universiteto Informatikos fakulteto Sisteminės analizės katedros docentas dr. *Eugenijus Mačikėnas* ir Vilniaus universiteto Teisės fakulteto Valstybės ir teisės teorijos ir istorijos katedros docentas dr. *Jaunius Gumbis*

Mykolo Romerio universiteto Ekonomikos ir finansų valdymo fakulteto Informatikos ir statistikos katedros 2006 m. rugsėjo 13 d. posėdyje (protokolo Nr. 1 INFSK-9) vadovėlis rekomenduotas spausdinti

Mykolo Romerio universiteto vadovėlių, monografijų, mokslinių, mokomųjų, metodinių bei kitų leidinių aprobavimo spaudai komisija 2006 m. liepos 4 d. posėdyje (protokolas Nr. 2L-8) vadovėlį patvirtino spausdinti

ISBN 9955-19-048-5

TURINYS

ĮVADAS

Sunku įsivaizduoti šiuolaikinę visuomenę, neturinčią modernių informacijos apdorojimo, kaupimo, perdavimo priemonių. Naujos informacinės komunikacinės technologijos užtikrina vis pigesnį ir paprastesnį informacijos priėmimo, apdorojimo, saugojimo ir perdavimo procesą ir sparčiai plinta visose visuomenės veiklos srityse. Elektroninės informacijos pavertimas masine ekonomine ir socialine vertybe – tai naujos žinių ekonomikos, kuriančios naujas ūkio šakas, keičiančios esamas ir turinčios esminį poveikį piliečių gyvenimui, pagrindas.

1992 m. Europos Komisija priėmė rekomendaciją „Informacinės technologijos ir teisininkų mokymas, kvalifikacijos kėlimas bei teisiniai tyrimai“. Šiose rekomendacijose pabrėžiama, kad teisininkams būtina suprasti informacinių technologijų svarbą bei ypatumus ir mokėti naudoti šias technologijas savo darbe. Interneto, elektroninės komercijos, elektroninių dokumentų teisiniai reglamentavimo principai, intelektinės nuosavybės ir asmens duomenų apsaugos elektroninėje erdvėje, elektroninių nusikaltimų problemos yra svarbios ne tik teisininkams, bet ir informacinių technologijų kūrėjams bei vartotojams, valstybės tarnautojams ir kitiems gyventojams. Todėl Europoje pradėtas vartoti angliškas terminas *legal informatics* apėmė ir informatikos naudojimą teisėje, ir informacinių technologijų (informatikos) teisės pagrindus. Nuo aštuntojo XX a. dešimtmečio elektroninės teisinės informacijos ir informacinių technologijų reglamentavimo problematiką imta skirti kaip savarankišką teisės sritį. P. Seipelis vienas iš pirmųjų Europos teisininkų pasiūlė šią sritį pavadinti „kompiuterijos teise“ (angl. *computing law*). Vėliau mokslininkai susitarė dėl teisės mokslo bei praktikos turinio ir pagrindinių jos institutų, bet nesusitarė dėl bendro pavadinimo. Iki šiol plačiai naudojami terminai – teisės informatika (angl. *legal informatics*), teisė ir informatika (angl. *law and informatics, law and computers*), kompiuterių teisė (angl. *computer law*), informacinių technologijų teisė (angl. *information technology law*), elektroninės erdvės teisė (ang. *cyberlaw*), informatikos teisė ir kt. Autorių nuomone, atsižvelgiant į esamą patirtį Lietuvoje vartotini du terminai:

– *teisės informatika* nagrinėjant teisės ir informacinių technologijų bendrąsias sąveikas, teisinę informaciją, elektroninės erdvės reguliavimo modelius, teisinių ir technologinių mechanizmų derinimą;
– *informatikos teisė* arba *informacinių technologijų teisė* – nagrinėjant tik socialinių santykių, susijusių su informacinėmis technologijomis (elektronine erdve), teisinio reglamentavimo specifiką.

Lietuvos švietimo ir mokslo ministro 1998 m. sausio 9 d. įsakyme Nr. 30 „Dėl mokslo sričių, krypčių ir šakų klasifikacijos“ nurodoma teisės šaka S 123 „Informatikos teisė“, todėl šis terminas vartojamas ir šiame vadovėlyje.

Nors yra bendro pavadinimo vartosenos problema, minėtos teisės ir informacinių technologijų (elektroninės erdvės) sąveika akivaizdžiai pabrėžia teisės informatikos svarbą teisės sistemai ir teisininkų profesijai žinių visuomenėje.

Ši teisinė sprecifika taip pat pagrindžia būtinybę studijuoti teisės informatiką ir informatikos teisę kaip specifinių teisės institutų ir reiškinių kompleksą. Šiame vadovėlyje nagrinėjamos pagrindinės bendrosios informacinių technologijų bei teisės sąveikos problemos ir pateikiami informatikos teisės pagrindai. Jame nenagrinėjamos pačios informacinės technologijos – jas nagrinėja tam skirta literatūra.

Vadovėlis skirtas visų lygių teisės studijų programų studentams, bet gali būti skaitomas informatikos, informacinių technologijų, verslo vadybos, viešojo administravimo ir kitų specialybių studentų bei specialistų.

Vadovėlio medžiaga suskirstyta į tris grupes. Pagrindinė medžiaga – svarbiausios skyriaus žinios ir faktai. Papildoma medžiaga reikalinga norintiems giliau susipažinti su informatikos teisės ir teisės informatikos sritimi. Įvadinė medžiaga reikalinga tiems, kuriems stinga pradinių šios krypties žinių. Pavyzdžiui, norint kalbėti apie intelektinę nuosavybę elektroninėje erdvėje, reikia suprasti pagrindines intelektinės nuosavybės sąvokas.

Pirmame skyriuje aptarta informacinių technologijų bei teisės sąveika ir socialinė teisinė reikšmė, nagrinėjamos kai kurios technologijų taikymo teisėje galimybės ir pavyzdžiai, teisinės informacijos teorijos klausimai, teisinės informacijos šaltiniai, informacinių technologijų teisinio reglamentavimo principai ir svarbios teisėje informacinių technologijų kategorijos.

Antrame skyriuje nagrinėjami interneto teisinio reguliavimo ypatumai: turinio reguliavimo principai, interneto tarpininkų vaidmuo ir atsakomybė, interneto domenų vardai ir kiti interneto teisinio reglamentavimo klausimai.

Trečiame skyriuje aptariamos intelektinės nuosavybės elektroninėje erdvėje teisinės apsaugos problemos, taip pat atskirai nagrinėjama kompiuterių programų ir duomenų bazių teisinė apsauga.

Ketvirtas skyrius skirtas privatumo ir asmens duomenų elektroninėje erdvėje teisinei apsaugai. Jame aptariama asmens duomenų teisinė apsauga, viešosios informacijos teisinis režimas (valstybės registrai, teisė į informaciją) ir privataus gyvenimo elektroniniuose ryšiuose apsauga.

Penktame skyriuje nagrinėjami elektroninės komercijos teisiniai aspektai: elektroninės komercijos teisinio reguliavimo modelis, elektroninis dokumentas ir elektroninis parašas, elektroniniai sandoriai bei elektroninės komercijos apmokestinimo problemos.

Šeštas skyrius skirtas elektroninės demokratijos reiškiniui, teisinei aplinkai ir elektroniniams rinkimams.

Paskutiniame, septintame, skyriuje nagrinėjami nusikaltimai elektroninėje erdvėje: jų apibrėžimas, ypatumai, sudėtys, teisiniai aspektai ir elektroninių nusikaltimų tyrimo problemos.

Autoriai dėkingi kolegai Martynui Mockui už pateiktą vertingą medžiagą šeštam skyriui.

1. TEISĖ IR INFORMACINĖS TECHNOLOGIJOS

1.1. Elektroninė erdvė, jos savybės ir įtaka teisiniams reiškiniams

Elektroninės informacijos erdvė – pasaulinė viešai ir visuotinai prieinama kompiuterių tinklų sistema.

Prieiga prie informacijos ir jos mainai yra svarbiausios elektroninės erdvės funkcijos. Technologinis progresas lemia, kad elektroninė erdvė tampa vis sudėtingesnė, tačiau visuomenei, verslui ir individualiems vartotojams vis lengviau prieinama, vis paprasčiau naudojama ir veiksmingesnė informacijos apykaitos priemonė. Dėl šių priežasčių socialinių santykių apimtis elektroninėje erdvėje ypač sparčiai didėja, o kai kuriose srityse (pvz., elektroniniuose atsiskaitymuose) jau beveik pasiekė tapačios veiklos mastus fizinėje erdvėje. Elektroninė erdvė gali būti naudojama:

– asmeniškai, pvz., kai vartotojai tarpusavyje pasikeičia elektroninio pašto pranešimais, skaito tinklalapiuose pateiktą informaciją;
– komunikuojant grupėje, pvz., kai vartotojai aktyviai diskutuoja ir keičiasi informacija įvairiuose forumuose, tinklalapių komentarų skiltyse, naujienų grupėse, dienoraščiuose ir pan.

Galiausiai elektroninė erdvė gali būti naudojama ir tiesiogiai interaktyviai komunikuojant virtualiose darbo grupėse, elektroninėse pokalbių svetainėse ir pan. Elektroninė erdvė tampa įprastu rinkodaros instrumentu, viešosios valdžios institucijų ir interesų grupių bendravimo su piliečiais ir visuomene priemone. Elektroninėje erdvėje išryškėjo konvergencijos požymiai – elektroniniai ryšiai pakeičia tokius įprastus dalykus kaip telefoną, televiziją, banko biurą, laikraščius, taip pat vartotojiškų sandorių pobūdį.

Būtina atkreipti dėmesį, kad elektroninė erdvė iš esmės neturi nei fizinių, nei teisinių sienų, nėra jokios „centrinės valdžios“, kuri valdytų informacijos kaitą internete. Todėl informacija, patalpinta elektroninėje erdvėje, iškart tampa visuotinai prieinama visame pa-

saulyje, be to, ji prieinama visiems vartotojams vienu metu (lygiagrečiai). Prieigos prie informacijos ir informacijos platinimo sąnaudos elektroninėje erdvėje yra nedidelės, ypač palyginus su kitomis informacijos platinimo formomis (pvz., tradicinės žiniasklaidos priemonėmis: televizija ar spauda). Iš esmės elektroninė erdvė atvėrė daug galimybių valdžios institucijoms, verslui ir visuomenei pateikti ir gauti svarbią informaciją, teikti elektronines paslaugas, siūlyti savo prekes ir paslaugas bei jas įsigyti. Paminėtina, kad elektroninė erdvė ne tik atveria naujas rinkas tradiciniams produktams ir paslaugoms, bet leidžia kurti visiškai naujus elektroninius produktus ir paslaugas, kurie pristatomi ir dažniausiai vartojami elektroninėje erdvėje (pvz., elektroniniu būdu parsisiunčiami muzikos įrašai, elektroninės knygos ir žurnalai, kompiuterių programos, prieiga prie elektroninių duomenų bazių ir pan.). Dar viena svarbi elektroninės erdvės savybė yra vadinamasis „globalaus kaimo“ efektas, t. y. visa informacija elektroninėje erdvėje bus iškart ir tuo pačiu metu prieinama viso pasaulio vartotojams, todėl pateiktą informaciją reikia įvertinti ir atsižvelgti į įvairias etines, religines ir politines normas ir požiūrius. „Globalaus kaimo“ efektas lemia ir tai, kad elektroninėje erdvėje gali būti laisvai platinama informacija, prekės ir paslaugos, kurių platinimas kai kuriose šalyse ribojamas ar net apskritai griežtai draudžiamas, pavyzdžiui, ksenofobinio pobūdžio (antisemitinė, rasistinė ir pan.) informacija, azartinių lošimų, alkoholio ar narkotinių medžiagų, vaistų reklama ir kita. Dėl techninių elektroninės erdvės savybių tokia informacija, prekės ir paslaugos yra laisvai prieinamos vartotojams visame pasaulyje ir netgi griežtomis fizinės kontrolės priemonėmis praktiškai neįmanoma visiškai apsisaugoti nuo jų platinimo. Netgi nedemokratinėse valstybėse, tokiose kaip: Iranas, Kinija, Baltarusija, iš esmės neįmanoma visiška elektroninėje erdvėje platinamos informacijos kontrolė.

Akivaizdu, kad minėtos elektroninės erdvės savybės atveria iš esmės naujos kokybės elektroninės demokratijos ir socialinės bei ekonominės plėtros galimybes. Elektroninės erdvės dėka galimas unikalus piliečių dalyvavimas priimant visuomenei svarbius administracinius bei teisinius sprendimus ir teisės aktus, itin daugėja galimybių naudotis viešosiomis paslaugomis net atokiausiuose šalies kampeliuose. Kartu didėja ir viešųjų paslaugų pasiūla bei kokybės kontrolė, atveriama rinka elektroniniams vartotojiškiems produktams ir paslaugoms, kuriami socialiniai tinklai ir diegiamos naujos socialinio bendravimo formos.

Naujos informacinės komunikacinės technologijos, sparti elektroninės erdvės – kompiuterių tinklų ir interneto – plėtra lėmė didelius teisės pokyčius. Praeito šimtmečio pabaigoje teisininkai vis plačiau pradėjo naudoti naujausias informacines technologijas. Kita vertus, pasaulinė elektroninė komunikavimo erdvė sukėlė daug teisinių problemų, kurioms išspręsti nepakako esamų teisės normų, atsirado nauji teisės institutai, naujos teisės mokslo ir teisės šakos – teisės informatika ir informatikos (informacinių technologijų) teisė. Informacinių technologijų plėtra atvėrė ir naujas erdves suvokiant, aiškinant ir taikant pačią teisę. Teisės normų gausa ir sudėtingumas paskatino pasitelkti technologines priemones teisiniuose procesuose (teisės aktų paieška, sistema, aiškinimas ir t. t.), o tai lėmė technologijų bei technologinio reguliavimo ir tradicinių teisinių normų konkurenciją. Elektroninėje erdvėje teisė tampa veiksminga tik tuo atveju, jei ją įgyvendinti pasitelkiamos techninės priemonės (pvz., informacijos privatumas užtikrinimas šifruojant), iš kitos pusės ir techninės priemonės gali pažeisti teisę (pvz., įgalinti naudotis svetima privačia informacija ar apriboti teisių išimtis) arba pačios gali būti pažeidžiamos (pvz., panaudojus neteisėtus dekoderius koduotų TV programų peržiūrai). Šiuo metu atsiranda ir naujos kartos technologijos – teisinių sprendimų paramos sistemos, teisinių dokumentų analizės ir automatinio apdorojimo sistemos, dar glaudžiau susiejančios technologijas ir teisės normas. Visa tai lemia teisės suvokimo ir tapatumo elektroninėje erdvėje klausimus.

Elektroninės erdvės globalus pobūdis lemia tai, kad nacionalinės teisinės iniciatyvos reglamentuojant elektroninę erdvę ir su ja susijusius socialinius teisinius reiškinius (elektroninę komerciją, nusikaltimus internete ir t. t.) gali nebūti veiksmingos dėl valstybių fizinių sienų, valstybės įstaigų ir pareigūnų kompetencijos ir techninių galimybių ribų. Ilgainiui būtina tarptautiniu mastu spręsti teisines problemas elektroninėje erdvėje. Europos Sąjungoje jau tvirtai apsispręsta dėl tarptautinio reglamentavimo.

Kita vis labiau ryškėjanti tendencija yra specialių internetą reguliuojančių normų vengimas. Informacinės technologijos ir socialiniai teisiniai reiškiniai elektroninėje erdvėje visų pirma turi būti reglamentuojami remiantis tokiais pačiais teisės principais kaip ir tradiciniai analogai (pvz., interneto žiniasklaida turi veikti pagal tas pačias taisykles kaip tradicinė žiniasklaida, vagystė internete turi būti kvalifi-

kuojama kaip vagystė ir t. t.). Specialus papildomas reglamentavimas turėtų būti taikomas tais atvejais, kai pasireiškia specifiniai tik elektroninei erdvei ar informacinėms technologijoms būdingi pavojai, priešingu atveju nebus išvengta diskriminavimo ir nevienodų verslo bei konkurencijos sąlygų.

1.2. Informacinių technologijų teisinio reglamentavimo principai

Informacinių technologijų ir socialinių teisinių reiškinių elektroninėje erdvėje reguliavimas turi būti griežtai pagrįstas šiais principais:

- elektroninės informacijos formos nediskriminavimo;
- technologinio neutralumo;
- funkcinio lygiavertiškumo;
- savireguliacijos skatinimo.

Elektroninės formos nediskriminavimo principas reiškia, kad informacijos teisinė galia negali būti paneigta ar apribota vien tik tuo pagrindu, kad ši informacija yra sukurta, išsiųsta, gauta ar išsaugota elektroninėmis priemonėmis. Pagal šį principą elektroninei žinutei iš esmės turi būti suteikta tokia pati teisinė galia kaip ir rašytiniam pranešimui, o teismai turėtų priimti ir vertinti elektronines žinutes kaip įrodymus.

Technologinio neutralumo principas reiškia, kad teisės normos turi būti nustatomos, aiškinamos ir taikomos atsižvelgiant į jų tikslus ir stengiantis, kad nebūtų skatinamas arba diskriminuojamas kai kurių technologijų naudojimas, taip pat kad teisės normos būtų taikomos kiek įmanoma neatsižvelgus į technologijas, naudojamas informacinės visuomenės paslaugoms teikti. Šis principas yra būtinas, kadangi vienos technologijos reglamentavimas netruks pasenti, be to, pirmenybės vienai technologijai teikimas iškreipia bendrą technologijų raidą ir konkurenciją technologijų rinkoje.

Funkcinio lygiavertiškumo principas iš esmės reiškia jau minėtą specialaus reglamentavimo išvengimą, t. y. teisės normos turi būti kuo vienodžiau taikomos informacinėms technologijoms, jų pagrindu funkcionuojančioms prekėms ir paslaugoms, atliekančioms tradicinėms (neelektroninėms) formoms būdingas funkcijas.

Tinkamomis įstatyminėmis sąlygomis savireguliacija gali funkcionuoti kaip ypač veiksmingas elektroninės erdvės ir informacinių technologijų reguliavimo mechanizmas, veiksmingesnis už valstybinio reguliavimo priemones. Dėl šios priežasties valstybinis reguliavimas neturi užkirsti kelio savireguliacijai, turi ją visapusiškai skatinti ir galiausiai palikti galimybių pačių rinkos dalyvių ir vartotojų teisėdarai, kadangi būtent rinkos dalyviai ir vartotojai gali geriausiai įvertinti savo poreikius ir proporcingai pasidalinti rizikas.

Atskirai paminėtina ir tai, kad naujos elektroninės erdvės technologijos taip pat lemia naujus informacijos kontrolės ir socialinių santykių reglamentavimo mechanizmus. Tokios technologijos yra elektroninio turinio techninės apsaugos priemonės, informacijos valdymo priemonės, įvairūs informacijos šifravimo, filtravimo ir stebėjimo mechanizmai bei programinė įranga, kurie šiuo metu plačiai naudojami užtikrinant elektroninės nuosavybės, informacijos saugą ir privatumą, atskiriant žalingą ir neteisėtą interneto turinį, nustatant ir tiriant nusikaltimus.

Nauji moksliniai tyrimai informacinių technologijų ir teisės srityje, pavyzdžiui, L. Lessigo teorija, įžvelgia tam tikrą informacinių technologijų ir teisės konvergenciją teigiant, kad žinių visuomenėje informacinės technologijos ir teisė negali egzistuoti vienas be kito. Informacinėms technologijoms būtina teisinė apsauga, taip pat socialinį interesą užtikrinančios reglamentavimo išimtys, o teisė vis labiau remiasi technologiniais teisės normų įgyvendinimo mechanizmais.

1.3. Teisės informatikos sąvoka ir turinys

Teisės informatiką galima apibrėžti kaip mokslą, nagrinėjantį informacinių technologijų, teisės sistemos ir teisinių reiškinių sąveikas. Praktiniu požiūriu teisės informatika apima informacinių technologijų teisinio reglamentavimo modelius ir institutus, teisinės informacijos teoriją, teisinės informacijos tvarkymo, t. y. kaupimo, sisteminimo, saugojimo klausimus, teisinės informacijos paieškos sistemas (tarp jų ir automatizuotas). Teisės informatiką galima suprasti ir kaip teisės mokslo šaką, kurios objektas – teisės informacinis modelis, jo sistemos, reiškiniai ir procesai – teisinio reguliavimo (teisėdaros) ir teisės įgyvendinimo mechanizmo (teisės aiškinimo, teisės realizavimo), taip pat teisinės kultūros ir sąmonės informaciniai tyrimai.

Teisė, kaip vienas iš svarbiausių žmonių elgesio reguliatorių, nulemia ir teisinės informacijos ypatumus, išskiriančius šią informaciją į atskirą socialinės informacijos rūšį, taip pat ir teisės informatikos tikslus bei principus.

Svarbiausias teisės informatikos uždavinys yra teisės informacinės problemos sprendimas optimizuojant informacinių technologijų ir informacijos teisinio reglamentavimo institutus ir teisės informacinius įrankius. Kiti svarbūs teisės informatikos tikslai yra:

1) teisėkūros formos ir turinio tobulinimas, normatyvinių teisinių aktų kodifikavimas ir sisteminimas;
2) piliečių, valstybinės valdžios ir valdymo įstaigų bei teisės taikymo institucijų aprūpinimas teisine informacija;
3) informacijos apie teisinę praktiką, visuomenės nuomonę dėl galiojančių teisės normų ir jų taikymą rinkimas, jų analizė ir gautų duomenų pateikimas valdžios ir valdymo įstaigoms, teismams, mokslo darbuotojams;
4) visuomenės informavimas teisiniais klausimais.

Įgyvendinant aukščiau minėtus tikslus atsižvelgiama į šiuos teisės informatikos ir teisinės informacijos pagrindinius principus:

1) teisinės informacijos viešumą: tik tas normatyvinis aktas gali būti teisės šaltinis, kuris viešai yra paskelbtas (šis principas įtvirtintas Lietuvos Respublikos Konstitucijoje);
2) teisinės informacijos patikimumą: informacijos patikimumas priklauso nuo informacijos šaltinio ir jos transformavimo patikimumo. Šaltinio patikimumas išreiškiamas tam tikrais rekvizitais, kurie turi būti išsaugoti perrašant dokumentą iš vienos laikmenos (pvz., popieriaus) į kitą (pvz., kompaktinę plokštelę). Transformavimo patikimumas priklauso nuo informacijos kanalo kokybės;
3) teisinės informacijos galiojimą: teisinės informacijos naudotojui turi būti teikiama informacija apie galiojančią teisę, t. y. teisinių aktų tekstuose turi būti visi jų pakeitimai ir papildymai, todėl teisinės informacijos apdorojimo priemonės turi būti tokios, kurios leidžia kuo greičiau padaryti tokius pakeitimus ir papildymus;
4) informavimo spartą: įvairių valdymo sprendimų, teisės taikymo aktų veiksmingo priėmimo ir poveikio būtina sąlyga yra greitas reikalingos informacijos suradimas. Todėl teisinės in-

formacijos bazė (bankas) turi būti prieinamas abonentui bet kuriuo jo darbo metu;
5) informavimo išsamumas ir tikslumas: teisinės informacijos gali būti per daug, bet jos negali būti per mažai, todėl turėtų būti siekiama gauti kuo išsamesnės informacijos kartu užtikrinant kuo mažesnį netikslios informacijos kiekį.

Be to, svarbu atsižvelgti į tokius bendruosius principus kaip:
1) teisinių informacinių sistemų darną su kitomis informacinėmis sistemomis (teisinės informatikos sistemos turi būti „atviros“ įvairioms kitoms informacinėms sistemoms, funkcionuojančioms Lietuvoje ir už jos ribų);
2) technologinį neutralumą, t. y. nei vienai iš esamų technologijų nesuteikiama teisinė pirmenybė;
3) naujausių techninių priemonių naudojimą (aprūpinant įvairias įstaigas techninėmis priemonėmis pirmenybė turi būti teikiama naujausioms techninėms priemonėms ir technologijoms).

1.4. Teisinė informacija ir jos tvarkymas

Teisinė informacija, kaip ir kita informacija, yra viena iš svarbiausių žinių visuomenės įrankių ir resursų. Siekiant apibrėžti teisinės informacijos sampratą, būtina aptarti bendruosius informacijos požymius ir koncepcijas.

Filosofiniu požiūriu galimos trys pagrindinės informacijos koncepcijos:
1) semiotiniu požiūriu informacija sietina su ženklų sistemomis, jų struktūromis;
2) funkciniu požiūriu informacija tapatintina su valdymo funkcijos dalimi, tam tikromis taisyklėmis, nurodymais, instrukcijomis ir komandomis;
3) atributiniu požiūriu informacija laikytina materijos atributu, kuris siejamas su entropijos samprata, atspindinčia požiūrį į gamtos ir visuomenės dėsnius.

Žinios yra tik vienas – gnoseologinis – informacijos aspektas, kurį teisiniu požiūriu lengviausia pastebėti, kadangi jis dažnai būna susijęs su teisės pažeidimais ir jų atskleidimu. Teisiniu požiūriu yra svarbus ir kitas – ontologinis – informacijos aspektas, kuris mažiau pastebimas ir dažnai pamirštamas. Ontologinė informacija atspindi informacijos su-

vokimą, taip pat teisės kaip informacijos suvokimą ir įsisąmoninimą. Ontologinis teisinės informacijos aspektas atspindi teisės sistemos esmę ir todėl yra ypač svarbi teisės filosofijos dalis.

Pagrindinės teisinės informacijos rūšys skiriamos minėtu filosofiniu pagrindu:

1) ontologinė teisinė informacija – pozityvioji teisinė informacija – teisės normos;
2) gnoseologinė teisinė informacija – informacija apie teisės suvokimą (teisės aiškinimą), žinios apie teisės normas, teisinius reiškinius (teisės taikymą, jos efektyvumą ir pan.).

Savo ruožtu svarbiausios teisinės gnoseologinės informacijos rūšys atspindi teisinių reiškinių esmę, jų pagrindines savybes, tai yra:

1) informacija apie galiojančią teisę – tai žinios apie teisės normas; norint pabrėžti šią informaciją, galima ją vadinti teisės informacija;
2) informacija apie teisės vykdymą – tai įvairios kriminologinės ir kitokios teismų, arbitražų, notarinių kontorų bei kitų teisinių institucijų žinios, duomenys apie teisės normų taikymą;
3) teisinė mokslinė informacija – tai žinios teisiniuose moksliniuose žurnaluose, knygose ir kitur.

Kaip minėta, ontologiniu požiūriu pati teisė yra informacija, o gnoseologiniu požiūriu teisės informacija yra žinios apie teisę ir su ja susijusius socialinius reiškinius. Teisinė informacija yra viena iš pagrindinių teisės informatikos ir teisės sistemos kategorijų.

Teisinė informacija gali būti skirstoma įvairiais pagrindais, iš kurių svarbiausi yra:

- pagal teisės šakas: 1) informacija apie baudžiamąją teisę, 2) informacija apie civilinę teisę, 3) informacija apie procesinę teisę ir t. t.
- pagal šaltinius: 1) informacija apie įstatymus, 2) informacija apie poįstatyminius aktus, 3) informacija apie teisės taikymo aktus (teismų ir administracinius sprendimus), 4) informacija apie jurisprudenciją (mokslo darbus) ir pan.;
- pagal informacijos laikmenas: 1) neautomatinės teisinės informa-

cijos rinkmenos, 2) automatinės teisinės informacijos rinkmenos;
- pagal priklausomybę: 1) visuotinės teisinės informacijos paieškos sistemos; 2) žinybinės teisinės informacijos paieškos sistemos (pvz., teismų sprendimų duomenų bazės); 3) komercinės teisės aktų paieškos sistemos (pvz., LITLEX ir kt.) ir t. t.

Šiuolaikinių teisės sistemų požymis yra teisės informacinės krizės didėjimas, t. y. nuolat didėjanti formaliosios teisės apimtis ir jos sudėtingumas, nuolat spartėjantys teisiniai informaciniai procesai ir teisinės informacijos mainai. Paminėtina, kad nuolat plečiama ir tobulinama tarptautinė ir regioninė teisėkūra dar labiau gilina nacionalinės teisės informacinę krizę. Deja, didesnis teisinis reguliavimas ir teisinės informacijos gausa ne tik neišsprendžia visų visuomenės socialinių problemų, bet neretai sukuria naujų (pvz., problemas dėl teisėkūros spragų ir klaidų) arba apsunkina esamos teisės taikymą ir suvokimą (pvz., prieštaringi teisės aktai ar nekompetentingas teisės aiškinimas). Daug kur vyrauja požiūris, kad kai kurios socialinės problemos atsirado dėl nepakankamo teisinio reglamentavimo, todėl buvo didinama reglamentavimo apimtis, bet nedaug dėmesio skiriama reglamentavimo kokybei. Kaip rodo sėkmingos praktikos pavyzdžiai užsienio valstybėse, kokybiškas, nors kartais ir labai minimalus (principinis) reglamentavimas (pvz., paliekantis galimybę veikti savireguliaciniams mechanizmams) yra socialiai veiksmingiausias.

Teisinės informacijos pagrindinės savybės susijusios su pačios informacijos savybėmis, tai:

1) informacijos fiksuojamumas laikmenose;

2) informacijos perduodamumas;

3) informacijos nekonkurencingumas, pasireiškiantis tuo, kad informacija, perduota į kitą sistemą, gali pasilikti ir pirmoje sistemoje.

Pirma bendroji informacijos savybė reiškia, kad šiuolaikinė teisinė informacija nuolat egzistuoti gali tik fiziniuose spaudiniuose ir laikmenose, t. y. teisės šaltiniuose. Antra bendroji informacijos savybė reiškia, kad teisinė informacija gali išlikti tik ją perduodant, o jai įsisavinti reikalinga energija, lėšos ir laikas. Trečia pagrindinė informacijos savybė yra ypač svarbi sprendžiant teisinės informacijos laikymo, apsaugos bei platinimo klausimus.

1.5. Pagrindinės informacinių technologijų kategorijos, svarbios teisėje

1.5.1. Kompiuterių sistema

Dažniausiai (socialinėje sferoje – beveik visada) kompiuterį kaip intelektinio darbo įrankį naudoja žmogus. Todėl informacinių technologijų kompiuterių sistema dažniausiai sudaryta iš:

- kompiuterinės aparatūros;
- programinės įrangos;
- duomenų (informacijos);
- procedūrų;
- žmogaus, dirbančio su kompiuterių sistema.

Kadangi kompiuteris skirtas palengvinti žmogaus darbą su informacija, todėl naudojamos patogios užduočių sudarymo procedūros ir interaktyvi sąsaja „žmogus-kompiuteris“, kada tarp žmogaus ir kompiuterio nuolat vyksta aktyvus dialogas.

Be to, žmogaus intelektualaus darbo patirtis gali būti kaupiama kompiuterio programinėje įrangoje. Tobulėjant kompiuteriams ir didėjant jų galimybėms, vis daugiau žmonijos patirties kaupiama programinėje kompiuterio įrangoje, žmogaus darbas su kompiuterinėmis sistemomis darosi vis veiksmingesnis. Todėl kompiuterinėse sistemose **kompiuterį galima vadinti intelektualiu informacijos apdorojimo įrankiu.**

Norėdamas kuo veiksmingiau naudoti šiuolaikinių kompiuterių galimybes kiekvienas tarnautojas ir specialistas turi būti ne tik informacinių paslaugų vartotojas, bet ir organizatorius. Žinios apie informacines technologijas tampa būtinos organizuojant kiekvienos institucijos informacinę veiklą tvarkant informacinį ūkį ir dokumentus, ieškant duomenų, analizuojant, priimant sprendimus ir kitus informacijos tvarkymo darbus.

Šiuolaikinių kompiuterių tobulėjimo sparta viršija lūkesčius. Tai didina informacijos apdorojimo galimybes ir greitį, bet kartu skatina kompiuterių naudotojus nuolat tobulėti. Štai keletas duomenų, rodančių kompiuterinės technikos pažangą per pastarąjį dešimtmetį. Prieš 15 metų tarnautojo darbo vietoje esančiame kompiuteryje buvo

0.5–1 megabaito atmintinė, dabar atmintinė viršija gigabaitą. Kietame magnetiniame kompiuterio diske tilpo keliasdešimt megabaitų informacijos, dabar – keliasdešimt ar keli šimtai gigabaitų. Kompiuterio mikroprocesorius („smegenys“) dirbo 8–12 megahercų dažniu, dabar – dažnai viršija 3 gigahercus. Todėl Jungtinių Amerikos Valstijų studentams pateikiamas toks 1998 m. surinktų duomenų pagrindu sudarytas palyginimas, rodantis kompiuterinės technikos tobulėjimo spartą. Jei aviacija vystytųsi tokiais tempais kaip informatika, tai po 25 metų kiekvienas norintis už 400 dolerių galėtų įsigyti lėktuvą, kuris per 6 val. apskristų aplink pasaulį sunaudojęs 19 litrų kuro. Dabartiniai duomenys dar labiau stebina.

Aišku, kad tokia sparti technologinė pažanga labai didina informacijos apdorojimo galimybes ir greitį, tačiau kelia ir didesnius reikalavimus vartotojų kvalifikacijai ir verčia kompiuterių naudotojus nuolat tobulėti.

Reikia atkreipti dėmesį į dar kelias svarbias informacinių technologijų savybes.

Pirmoji savybė – galimybė saugoti didžiulius kiekius informacijos labai mažame tūryje. Teisininko darbo vietoje esančio kompiuterio nedidelės knygos tūrį užimančiame magnetiniame kietajame diske galima sutalpinti šimtų tūkstančių knygų biblioteką arba milijoną dokumentų. Antroji savybė: nors dokumentų kompiuteryje yra labai daug, rasti reikiamą galima labai greitai – per sekundės dalį.

1.5.2. Kompiuterių tinklai

Dauguma šiuolaikinių kompiuterių sujungti informaciniais tinklais, kurie galėtų būti apibrėžti kaip dviejų kompiuterių tarpusavio jungtis ir galimybė persiųsti informaciją. Pasauliniu mastu tai – visos kompiuterių sistemos, sujungtos į bendrą tinklą. Tačiau ne visi kompiuteriniai tinklai yra vienodi. Galima būtų suskirstyti juos į dvi pagrindines rūšis:

1. pasaulinis (globalinis) tinklas – internetas (*WAN-Wide Area Networks*);
2. vietiniai (lokaliniai) tinklai – įstaigų, ministerijų, žinybų, universitetų ir kitų įstaigų vidiniai tinklai (*LAN-Local Area Networks*).

Šiuolaikiniuose komunikaciniuose tinkluose naudojami telefoninio, radijo, kabelinio, optinio ir palydovinio ryšio kanalai. Šiais ryšio kanalais visi tinklo kompiuteriai yra sujungti su tinklo tarnybine stotimi (serveriu). Didesniuose tinkluose gali būti ir daugiau negu viena tarnybinė stotis.

Specialios tinklo programinės įrangos pagalba vykdomas informacinių resursų administravimas tinkle ir užtikrinama prieiga prie jų.

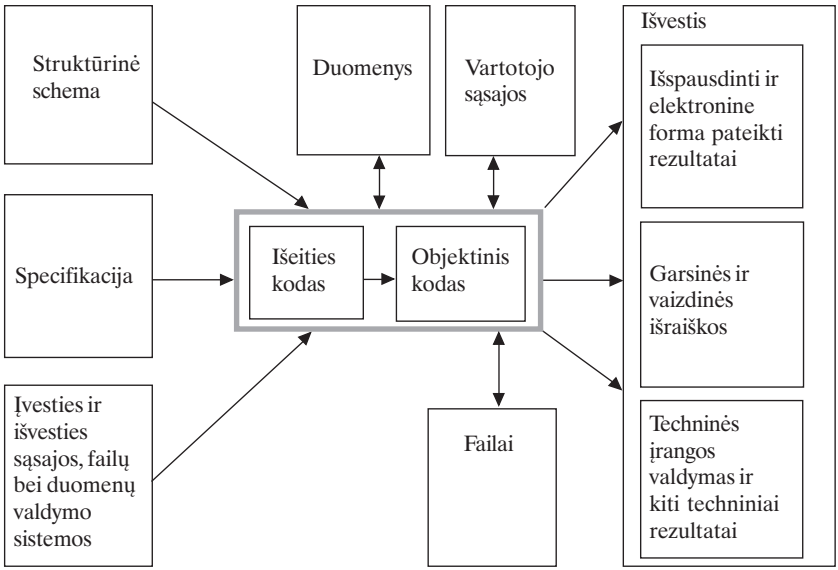
1.5.3. Kompiuterių programos

Esminis kompiuterių sistemų ir kompiuterių tinklų komponentas, įgalinantis juos veikti, yra kompiuterių programos.

Kompiuterių programos (angl. *software*) techniniu požiūriu suprantamos kaip programavimo kalbomis užrašyti matematiniai (loginiai) algoritmai. Dažniausiai kompiuterių programos yra kompiuterio darbui naudojamos operacinės sistemos, taikomoji programinė įranga bei įvairių elektroninių duomenų: skaičių, tekstų, piešinių, garsų ir kitų, masyvai. Visa ši informacija kompiuterio viduje yra skaitmenizuota ir išreikšta dvejetaine skaičiavimo sistema (nuliukais ir vienetukais). Programinė įranga suteikia kompiuteriui dirbtinio intelekto elementų, ir jis tampa intelektualiu informacijos dorokliu.

Kompiuterių programos plačiai suprantamos kaip visuma elementų ir efektų, susijusių su kompiuterių programos kūrimu ir veikimu, išskyrus techninę įrangą. Šiandien kompiuterių programa galima laikyti visumą kompiuterių programos elementų ir jų tarpusavio sąveikas, tarp jų – pirminį ir objektinį programos kodą, programos specifikacijas ir veikimo schemą, elektroniniu būdu išsaugotą informaciją (failus), duomenis, kompiuterių programa valdomo kompiuterio veikimo rezultatus: atspausdintą medžiagą, garso ir vaizdo išraiškas, grafinę vartotojo sąsają, failų ir grafinių vaizdų struktūras, interneto sąsajas ir kt. (žr. 1 schemą). Šiuolaikinė kompiuterių programos samprata taip pat apima duomenų struktūras, taip pat įvesties ir išvesties elementus – sąsajas kaip savarankiškas kompiuterių programos sudedamąsias dalis.

Svarbu suvokti dvejopą kompiuterių programų pobūdį. Kompiuterių programas apibūdina ir jų tekstinė išraiška (pirminis kodas, objektinis kodas), ir kompiuterių programa valdomo kompiuterio veikimo rezultatai (vartotojo ir kitos sąsajos, failų ir grafinių vaizdų išdėstymas, vaizdinės ir garsinės programos pateikimas). Tekstinė kompiute-



1 schema. **Kompiuterių programos elementai**

rių programos išraiška tiesiogiai lemia kompiuterių programos veikimo rezultatus ir atvirkščiai, tačiau kompiuterių programos tekstinė išraiška ir veikimo rezultatai tuo pačiu metu yra nepriklausomi, kadangi įmanoma pasiekti tokius pačius veikimo rezultatus pasitelkus kitokios tekstinės išraiškos kompiuterių programą, o skirtingos išraiškos kompiuterių programos gali atlikti tuos pačius uždavinius (pasiekti tuos pačius rezultatus). Kūrybinis procesas apima abu kompiuterių programos aspektus.

Atsižvelgiant į kompiuterių programų dvilypumą, galima jas apibūdinti kaip techninius mechanizmus, išreikštus tekstinėmis priemonėmis. Tokiais „tekstiniais mechanizmais“ galima pasiekti konkrečių naudingų rezultatų, kuriuos sudaro visuma veiksmų, kuriuos gali atlikti kompiuteris, vykdydamas kompiuterių programos instrukcijas. „Tekstiniuose mechanizmuose“, kaip ir bet kokiuose techniniuose mechanizmuose, gali būti naudojami inžineriniai sprendimai ir naujovės. Kompiuterių programas, kaip ir techninius mechanizmus, sudaro visuma tarpusavyje suderintų ir sąveikaujančių elementų (žr. 1 schemą), kurių kiekvieno „gedimas“ dažniausiai lemia viso mechanizmo „gedimą“. Be to, rezultatai, pasiekti kompiuterių programomis, taip pat gali būti pasiekti ir grynai techninėmis priemonėmis.

1.5.4. Kompiuterinės duomenų bazės

Didelius duomenų ir informacijos kiekius tvarkyti ir sisteminti naudojami specialūs duomenų formatai ir programų paketai, vadinami duomenų bazių valdymo sistemomis. Jos leidžia kurti įvairių duomenų rinkinius, duomenis peržiūrėti, keisti, kurti ataskaitas. Duomenų bazę techniniu požiūriu sudaro duomenų bazės turinys (patys duomenys) ir duomenų bazės sąsaja (duomenis valdančios programos). *Windows* aplinkoje tam dažniausiai naudojama *MS Access* programa.

Dabar duomenų bazės yra svarbiausia informacijos tvarkymo forma ir priemonė, viena iš dažniausių šiuolaikinių informacinių technologijų pritaikymo kasdieninėje aplinkoje pavyzdžių. Šiuolaikinės verslo įmonės, valstybinės institucijos bei kitos organizacijos susiduria su nuolatos didėjančiais informacijos srautais ir būtinybe juos valdyti, todėl duomenų bazės tampa pagrindiniu informacijos valdymo ir kontrolės įrankiu, būtinu informacijos valdymo elementu.

Duomenų bazės yra būtinos atliekant ir daugumą verslo valdymo funkcijų, tokių kaip apskaita ir sąskaityba, atsargų planavimas, ryšių su klientais palaikymas, pardavimų vadyba, personalo vadyba ir t. t. Šiuo metu įsitvirtino ir tokios verslo rūšys, kurios tiesiogiai priklauso nuo duomenų bazių, pavyzdžiui, įmonių katalogai, kredito biurai, įdarbinimo agentūros, bankai ir draudimo bendrovės.

Duomenų bazę galima apibrėžti tiesiog kaip informacijos rinkinį ar kompiliaciją, išdėstytą (organizuotą) sisteminiu ar metodologiniu būdu. Duomenų bazė jungia pavienius duomenis į kokybiškai naują informacijos visumą. Pažymėtina, kad duomenų bazę turi sudaryti informacijos daugetas, t. y. turi būti tam tikras minimalus sistemiškai sutvarkytas informacijos kiekis. Duomenų baze laikytinas ir automatiškai surinktas ir tvarkomas, ir neautomatiškai surinktas (net ir ranka užrašytas) informacijos rinkinys, išreikštas bet kokia forma.

Duomenų bazės santykis su kompiuterių programomis gali būti dvejopas. Jei duomenų bazių tvarkymui panaudota kompiuterių programa įdiegta į duomenų bazę taip, kad ja perteikiama duomenų bazės struktūra, tokia programa prilyginama duomenų bazei (savo ruožtu duomenų struktūros yra laikomos kompiuterių programų elementu). Jei kompiuterių programa yra tik duomenų bazės kūrimo ir (ar) tvarkymo (prieigos, keitimo, išsaugojimo) priemonė, tokia programa nelaikoma duomenų bazės dalimi.

1.5.5. Internetas – nauja socialinių ir teisinių santykių erdvė

Nors yra labai daug literatūros apie internetą, atkreipkime dėmesį į šias teisininkui svarbias interneto savybes:

1) didžiulį sukauptos ir lengvai prieinamos informacijos kiekį;
2) pasaulinę elektroninę komunikavimo erdvę;
3) paprastą informacijos paiešką;
4) komunikavimo spartą;
5) pasikeitimo informacija pigumą.

Internete informacija kaupiama milijonuose tinklo mazgų – tarnybinėse stotyse. Šios tarnybinės stotys prijungtos prie greitaeigių ryšių kanalų (palydovinių, optinių, kabelinių ir kt.). Prie kiekvienos tarnybinės stoties paprastesnėmis ryšio (telefoninio, kabelinio ir pan.) linijomis prijungiama nuo keliasdešimties iki kelių tūkstančių interneto vartotojų kompiuterių. Kiekvienoje tarnybinėje stotyje informacija kaupiama nepriklausomai nuo kitų. Šis procesas nėra kažkaip tvarkomas ar derinamas, informacijos mainai vyksta laisvai, todėl internete galima rasti daug pasikartojančios ar menkavertės, kartais net pavojingos visuomenei informacijos. Pastaruoju metu ieškoma būdų, kaip kovoti su nelegalios ir žalingos informacijos platinimu internete, bet tai yra nelengva, nes komunikavimui naudojama bendra elektroninė erdvė.

Pagrindinius interneto informacijos srautus perneša vadinamasis kamienas (*backbone*), sudarytas iš didžiausių potinklių, kurie priklauso pagrindinėms interneto paslaugų teikėjoms – kompanijoms GTE, MCI, „Sprint“, UUNet, AOL. Šie tarpusavyje sujungti tinklai sudaro itin spartaus ryšio linijas, kurios nutiestos visoje Šiaurės Amerikoje, driekiasi į Europą, Japoniją, žemyninę Aziją bei kitas pasaulio dalis. Tačiau ne visuose pasaulio taškuose tinklas vienodai gerai išplėtotas. Pavyzdžiui, Jungtinėse Valstijose yra tiek daug susikirtimo taškų, kad nutrūkus ryšiui ar sulėtėjus duomenų perdavimui vienoje linijoje srautas iškart persiunčiamas kita. Kitur nutrūkus ryšio linijai gali nebūti atsarginių kelių, ir ryšys gali itin sulėtėti ar visai nutrūkti. Tokių atvejų pasitaiko ir Lietuvoje.

Bendra elektroninė komunikavimo erdvė šiuolaikiniais ryšio kanalais aprėpia visą pasaulį ir neturi jokių geografinių sienų. Kartu ji

lengvai prieinama per bet kurį prie interneto prijungtą kompiuterį. Tai reiškia, kad kiekvienas, dirbdamas su prijungtu prie interneto kompiuteriu, patenka į bendrą elektroninę komunikavimo erdvę ir gali beveik neribojamas keistis informacija su bet kuo. Todėl internete vis daugėja nusikaltimų, o kai kurios šalys (pvz., Kinija) ar atskiros įmonės bando kontroliuoti perduodamos internetu informacijos turinį.

Nors internete sukauptas nepaprastai didelis informacijos kiekis, **informacijos paieška** atliekama labai paprastai dėl šių itin pažangių interneto sprendimų:

1) naudojamas bendras informacijos mainų protokolas;
2) sukurta efektyvi ir lengvai suprantama programinė informacijos paieškos įranga;
3) informacija saugoma hipertekstine forma;
4) naudojama unikali adresavimo sistema;
5) sukurtos specialios sistemos ir mechanizmai veiksmingai informacijos paieškai įvertinant informacijos svarbumą (reitingą).

Internetu naudojamasi įvairiomis paslaugomis, iš kurių pagrindinės ir labiausiai paplitusios yra:

1) elektroninis paštas. Ši paslauga iš pradžių buvo pritaikyta teksto persiuntimui, tačiau atsirado naujų galimybių elektroniniu paštu persiųsti garso ir vaizdo failus. Elektroninėje komercijoje tai yra populiari paslauga, naudojama sudarant elektroninius sandorius.
2) WWW (*World Wide Web*) paslauga – populiariausia interneto paslauga. Tai – viena iš svarbiausių interneto paslaugų elektroninėje prekyboje, turi ne tik katalogams būdingą funkciją, t. y. demonstruoja parduodamas prekes, bet ir leidžia subjektui tiesiogiai sąveikauti su pateikta informacija bei ją parsisiųsti;
3) *Usenet* naujienų grupės. Ši informacijos persiuntimo paslauga paremta panašiu metodu, kaip ir elektroninis paštas, tačiau naudoja kitas technologijas. Tai – pasaulinis diskusijų forumas, sudarytas iš daugelio tūkstančių naujienų grupių, kuriose diskutuojama tam tikra apibrėžta tema. Paslauga nėra labai paplitusi tarp elektroninės komercijos dalyvių;
4) internetiniai pokalbiai. Ši paslauga dažnai vadinama IRC. Internetiniai pokalbiai, kitaip negu *Usenet* naujienų grupės, leidžia vartotojams bendrauti esamuoju laiku;

5) FTP paslauga pasižymi dideliu duomenų perdavimo greičiu. Tai – elektroninei komercijai itin naudinga paslauga, įgalinanti persiųsti vartotojui reikiamą duomenų paketą;
6) „BLOGas“ (anglų k. trumpinys iš *weB LOG* arba *weB LOGging*) – internetinis dienoraštis arba automatiškai formuojami naujienų puslapiai. Prie „BLOGų“ priskiriamos specializuotos interneto svetainės arba bendrųjų svetainių sritys, kuriose talpinamos dažnai rašomos publikacijos, išdėstytos chronologine tvarka, jose autoriai dėsto savo mintis, įvykius, pastebėjimus ir idėjas pasirinkta tema. Tai palyginti naujas internetinės subkultūros reiškinys, tenkinantis socialinius (psichologinius) bei informacinius bendravimo poreikius. „BLOGas“ yra dienoraščio ir interneto žinyno hibridas.

Informacijos mainams internete naudojamas paprastasis ir bendrasis **unifikuotas TCP/IP protokolas**. Jis diegiamas automatiškai, todėl keičiantis informacija nereikia rūpintis, ar kitas kompiuteris ją supras.

Šis protokolas – tai tokia duomenų kodavimo sistema, kai visa tinklu siunčiama informacija iš pradžių kam nors adresuojama, po to siunčiama tiksliai tuo adresu. TCP/IP sudaryta iš dviejų protokolų: tai – TCP (*Transmission Control Protocol*) ir IP (*Internet Protocol*) samplaika. Visi duomenys perduodami paketais, todėl labai nedidelis informacijos praradimo pavojus. Visų pirma TCP protokolas suskaido siunčiamą informaciją porcijomis (paketais), sudeda juos į elektroninius vokus, ant jų užrašo gavėjo bei siuntėjo adresus. Tada IP protokolas suranda tinkamiausią kelią paketus siųsti internetu. Numatomas kelias, per kokius interneto mazginius punktus (maršrutizatorius) bus siunčiamas duomenų paketas. Kiekvienas maršrutizatorius perskaito gavėjo adresą ir siunčia paketą kitam maršrutizatoriui. Taigi kiekvienas interneto elektroninis laiškas gali būti padalytas į kelis duomenų paketus, kurie gali keliauti pas adresatą skirtingais keliais. Tačiau TCP protokolas vėliau surenka visus paketus ir vėl atstato pradinę informaciją.

Informacijos paieškai internete sukurta speciali lengvai suprantama ir labai veiksminga programinė įranga – interneto naršyklės *Internet Explorer* ir *Firefox*. Šie pavadinimai kilę nuo galimybės „atlikti informacijos paiešką ir navigaciją informacijos okeane“. Informaciją iš

interneto galima lengvai nukopijuoti į kompiuterio atmintinę, išspausdinti ar išsaugoti.

Informacija internete saugoma ir pateikiama hipertekstine forma, naudojant WWW (*World Wide Web* – pasaulį apimantis voratinklis) technologiją. Nors dažnai terminai WWW ir *Internetas* yra sutapatinami, iš tikrųjų tai yra du skirtingi dalykai. *Internetas* – tai kompiuterių tinklas, įgalinantis informacijos mainus tarp kompiuterių, o WWW – tai didelė atskirų informacijos failų sankaupa. Kitaip sakant, interneto tinklas nepriklauso nuo WWW, tačiau be interneto tinklo negalima būtų naudotis WWW sukaupta informacija.

WWW sudaro atskiri interneto mazguose (tarnybinėse stotyse – serveriuose) esantys puslapiai. Jie yra parašyti specialia kalba – HTML (*Hypertext Markup Language*). Naršyklės pritaikytos suprasti šią kalbą ir vienodai teisingai pavaizduoti interneto puslapius. Pagrindiniai WWW pranašumai – galimybė į elektroninį puslapį įterpti nuotraukas, paveiksliukus, filmus, garsus bei specialių nuorodų pagalba sujungti vienus puslapius su kitais.

Hiperteksto ryšiai tarp atskirų interneto puslapių kompiuterio ekrane pažymimi pabraukiant ar išskiriant spalva atitinkamą teksto dalį (dažniausiai vieną ar kelis žodžius). Toje ekrano vietoje kompiuterio žymeklis taip pat keičia pavidalą. Spragtelėjus kompiuterio pelės klavišu peršokama į susietą kitą teksto vietą, po to galima vėl grįžti atgal.

WWW veikimą grindžia visuma taisyklių, nusakančių teksto, grafikos, vaizdo ir garso informacijos, garsų perdavimą. Šios taisyklės vadinamos HTTP, lietuviškai – hiperteksto perdavimo protokolu (*Hypertext Transfer Protocol*). WWW puslapius galima atsisiųsti, nes ir interneto tarnybinės stotys – serveriai, ir naršyklės supranta HTTP protokolą.

Kadangi milijonuose kompiuterių sukauptas milžiniškas informacijos kiekis, būtinos veiksmingos ir sparčios informacijos paieškos galimybės. Todėl buvo sukurtos specialios **informacijos paieškos sistemos**, turinčios didžiules galimybes. Šiuo metu naudojama keliasdešimt tokių sistemų, iš kurių žinomiausios yra *Google*, *Yahoo*, MSN, *Altavista*, *Infoseek* ir kt. Pagal raktinį žodį ar kelis žodžius per trumpą laiką peržvelgiami milijonai interneto puslapių ir pateikiamas tinklalapių reitinguotas sąrašas, kuriuose rasti ieškomi žodžiai. Pastaruoju metu

atsirado ypač veiksmingos paieškos galimybė, kai vienu metu paieška atliekama keliomis paieškos sistemomis. Informacija internete pateikta įvairiomis kalbomis, todėl paiešką galima atlikti norima kalba, tačiau daugiausia informacijos internete yra anglų kalba.

Interneto tarnybinės stotys duomenimis keičiasi greitaeigiais ryšio kanalais paketiniu režimu. Todėl **komunikavimo sparta internete** yra labai didelė ir praktiškai priklauso nuo to, kaip dažnai sudaromi ir siunčiami duomenų paketai. Tai trunka nuo kelių minučių iki kelių valandų, išskyrus atvejus, kai tarnybinėje stotyje ar ryšio kanale atsiranda gedimų. Todėl pasitaiko, kad į kitą pasaulio kraštą (pvz., Australiją) laiškas interneto elektroniniu paštu patenka per kelias sekundes, o į miestą už keliasdešimties kilometrų keliauja kelias valandas. Labiausiai komunikavimo internete spartą mažina siauri ryšio kanalai tarp tarnybinių stočių ir vartotojų. Tai ypač būdinga ekonomiškai atsilikusioms šalims, kuriose dar naudojami pasenę analoginio telefoninio ryšio kanalai.

Informacijos mainų pigumą lemia faktas, kad internetas nėra pelno siekianti organizacija. Informacija perduodama paketiniu režimu, todėl jos perdavimas yra daug daug pigesnis negu telefonu, paštu, faksu ar telegrafu. Paprastai brangiausias interneto vartotojo prisijungimo prie vietinės tarnybinės stoties telefono kanalais laikas.

1.5.6. Interneto domenų vardai

Interneto adresavimo sistema yra bendra visiems vartotojams ir leidžia iš adreso sužinoti tam tikrą informaciją apie tinklalapio savininką. Vienas iš svarbiausių reikalavimų – interneto adresas turi būti unikalus ir nesikartoti. Interneto adresavimo schema kiekvienam prie interneto prijungtam kompiuteriui suteikia unikalų iki dvylikos skaitmenų adresą (pvz. 123.456.789.123), kuris vadinamas IP adresu.

IP adresas išreiškiamas skaitmenimis, kuriuos įsiminti sunku ir nepatogu, todėl IP adresų sistema faktiškai pakeista simboline ir vartotojams patogia interneto domenų vardų sistema. DNS (angl. *Domain Name System*) serverių pagalba beveik kiekvienas IP adresas internete susietas su domeno vardu. Įvedus domeno vardą į kompiuterį, DNS serveriai jį automatiškai pakeičia į skaičiais išreikštą IP adresą. Techniniu požiūriu domeno vardas visų pirma suprantamas kaip interneto

adresas ir apibrėžiamas kaip interneto adresų srities simbolinis pavadinimas.

Domenų (apibrėžtų sričių pavadinimų) sukūrimas – tai dar viena pažangi interneto adresų indeksavimo sistema. Ji leidžia interneto mazgus (tarnybines stotis – serverius) pavadinti žmogui suprantamais pavadinimais. „Šaknies" domenas – tai atskirai įmonei, institucijai ar organizacijai paskirtas identifikavimo vienetas, kuris jungia kelis ar net keliasdešimt kompiuterių. Tačiau žinoti vien serverio pavadinimą neužtenka, reikia dar žinoti, kurioje to serverio vietoje yra reikiama informacija. Visa tai sudaro vieną informacijos šaltinio buvimo vietą – URL (*Unified Resource Locator*).

Domeno vardas yra simbolinis IP adreso atitikmuo. Domeno vardas, kaip ir IP adresas, nurodo kompiuterio vietą internete.

Domeno vardas turi būti sudarytas bent iš dviejų dalių:

- aukščiausio lygio domeno vardo (angl. *Top Level Domain* – TLD), žyminčio šalį arba regioną („.lt", „.pl", „.eu") arba serverio rūšies („*.net", „.biz", „.gov"*);
- antrojo lygio domeno vardo (angl. *Second Level Domain* – SLD), žyminčio įstaigą, įmonę (pvz., „lrs", „mruni", „delfi").

Kaip minėta, aukščiausio lygio domenų vardai gali būti:

1) rūšiniai arba generiniai (gTLDs), pavyzdžiui, bendriniai aukščiausiojo lygio domenų vardai yra „.com", „.org", „.net", „.edu", „.int", „.info", „.biz" ir kt. Registruojant tarnybinę stotį, pagal paskirtį suteikiamos adreso galūnės: „.edu" – švietimo ir mokymo įstaigos, „.gov" – vyriausybinės organizacijos, „.net "– tinklai ir t. t.

2) teritoriniai ar regioniniai (ccTLDs). Pasaulyje egzistuoja daugiau kaip 244 šalies kodo aukščiausiojo lygio domenų vardai, kurie suteikti remiantis Tarptautinės standartizacijos organizacijos (ISO) standartu Nr. 3166, pavyzdžiui, „.lt" (Lietuvos kodas), „.pl" (Lenkijos kodas), „.eu" (Europos Sąjungos kodas).

Sujungus šias dvi privalomas domeno vardo dalis, gaunamas minimalus domeno vardas, pvz., „mruni.lt", „europa.eu".

Kai kurios interneto tarnybinės stotys teikia adresus visiems norintiems, nereikalauja nurodyti asmenį. Todėl pagal interneto adresą negalima tiksliai nustatyti, kokiai šaliai ar kokiam asmeniui jis priklauso.

1.5.7. Elektroninis parašas

Elektroninis parašas – duomenys, kurie įterpiami, prijungiami ar logiškai susiejami su kitais duomenimis siekiant patvirtinti pastarųjų tikrumą ir (ar) atpažinti pasirašantį asmenį.

Šis apibrėžimas apima materialųjį ir funkcinį elektroninio parašo elementus. Materialusis elektroninio parašo elementas – elektroninis parašas yra duomenys, logiškai susieti su kitais duomenimis (informacija, kurią patvirtina elektroninis parašas). Pažymėtina, kad elektroninio parašo technologijos nėra reglamentuojamos, elektroniniu parašu gali būti pripažįstamas tiek tam tikras informacijos šifravimo metodas, tiek piršto antspaudo elektroninis vaizdas, akies rainelės ar balso nuoskaita. Elektroninio parašo direktyva Nr. 1999/93EB vengia griežtai reglamentuoti elektroninio parašo technologijas, nes technologijos laikui bėgant keisis, todėl reikia reglamentuoti tik esminius dalykus.

Funkcinis elektroninio parašo elementas direktyvoje reiškia, kad elektroninis parašas leidžia nustatyti dokumentą pasirašiusio asmens tapatybę (identifikavimo funkcija). Elektroninio parašo direktyva nustato ryšius tarp elektroninio parašo ir kitų elektroninių duomenų teigdama, jog elektroninis parašas leidžia nustatyti informacijos kilmę. Direktyvoje apibrėžiant kitą elektroninio parašo funkciją – pasirašytos informacijos aprobavimą (patvirtinimą) – elektroninis parašas klasifikuojamas dvejopai: išskiriamas paprastasis (klasikinis) elektroninis parašas ir tobulesnis elektroninis parašas.

Paprastasis elektroninis parašas apibrėžtinas kaip technologija, pagrįsta elektroninėmis priemonėmis, naudojama ar priimta vienos šalies, siekiančios save susieti su pasirašomu dokumentu ir (ar) autentifikuoti pastarąjį, tokiu būdu įgyvendinti visas ar dalį funkcijų, kurias atlieka ranka rašyti parašai (tipinis pavyzdys – internetiniai bankai, kurie paprastesnėmis technologijomis nustato vartotoją, jo elektroninį parašą ir valią).

Pagal direktyvą tobulesnis elektroninis parašas yra toks elektroninis parašas, kuris:

1) yra susietas tik su pasirašančiuoju asmeniu;
2) leidžia nustatyti asmenį, kuris pasirašė dokumentą;
3) turi būti sukurtas tokiu būdu, kad jį kontroliuotų tik pasirašantysis asmuo;
4) yra susietas su kitais duomenimis tokiu būdu, jog bet koks duomenų pakeitimas po pasirašymo turi būti aptiktas.

Tobulesnis elektroninis parašas dažnai kuriamas naudojant asimetrinio šifravimo (dviejų raktų – privataus ir viešojo) technologiją ir infrastruktūrą ir todėl kartais žymimas raidėmis PKI (*angl. Public Key Infrastructure)*. Ateityje tam gali būti pradėti naudoti biometriniai duomenys.

Tobulesnis elektroninis parašas atlieka ne tik tikrumo nustatymo, bet ir patvirtinimo funkcijas, susijusias su dokumento turinio vientisumu. Parašas turi būti glaudžiai susietas su dokumento turiniu, tačiau taip ne visada būna saugant duomenis elektroninėje laikmenoje. Popierinio dokumento teksto ar parašo klastojimas yra palyginus nesudėtingas, nors egzistuoja pakankamai tobuli kriminalistiniai metodai, leidžiantys nustatyti klastojimą. Elektroninėse laikmenose klastoti nėra lengviau, tačiau sunkiau atskirti, kada parašai yra padirbti arba dokumento tekstas suklastotas. Direktyva nereglamentuoja, kokie metodai turi būti naudojami siekiant susieti elektroninį parašą ir kitus duomenis, tiesiog konstatuoja, kad dokumento turinys neturi būti pakeistas po jo pasirašymo (vientisumo reikalavimas). Toks reikalavimas yra gana svarbus, nes pasirašęs asmuo įgyja teisių bei pareigų. Jis turi būti užtikrintas, kad tai, ką pasirašė sąmoningai, vėliau nebus pakeista ar suklastota, kad bus pateiktas jo pasirašytas, o ne koks nors kitas dokumentas.

Kaip matome iš apibrėžimo, tobulesnio elektroninio parašo funkcinis elementas yra platesnis, o reikalavimai jam yra griežtesni, tačiau ir juridinė parašo galia yra didesnė. Elektroninis parašas kartais vadinamas skaitmeniniu parašu.

1.5.8. Elektroninis dokumentas

Elektroninės komunikacijos metu atsiranda poreikis patvirtinti faktus, pavyzdžiui, piliečio valią per rinkimus, užfiksuoti šalių teises, pareigas bei atsakomybę, gauti garantijas ir panašiai. Tai reiškia, kad elektroninė informacija turi atlikti įprasto rašytinio dokumento funkcijas. *Tokia elektroninė informacija yra vadinama elektroniniu dokumentu*. Elektroninis dokumentas gali būti pateikiamas kaip įrodymas teisme pagrindžiant faktus. Siekiant patvirtinti dokumento autorių, naudojamas elektroninis parašas. Svarbus ir saugomo ar perduodamo elektroninio dokumento tikrumas, slaptumas. Tam kompiuterinėse sistemose naudojami kriptografijos pasiekimai, šifravimas.

Elektroniniai dokumentai (žinutės) gali būti pasirašomos įvairiai. Tai gali būti paties siuntėjo sukurta simbolių seka, nuskenuotas tikro parašo vaizdas. Tačiau tokie pasirašymo būdai neleidžia tikrai nustatyti asmens tapatybės. Be to, iškilus teisiniams nesklandumams, toks parašas būtų lengvai nuginčijamas, nes, pavyzdžiui, tokiu parašu pasirašytas dokumentas nebūtų prilyginamas rašytinės formos dokumentui. Elektroniniai dokumentai gali būti pasirašomi ir elektroniniu parašu.

Elektroninis dokumentas, siunčiamas kompiuterių tinklu, yra užšifruotas tokiu būdu, jog neįmanoma jo iššifruoti, o bandant pakeisti pranešimo turinį ar patį parašą pranešimo tekstas virsta nesuprantamų simbolių virtine. Pagal naudojamą asimetrinę elektroninio parašo šifravimo technologiją (išsamiau apie šią technologiją rašome toliau šiame skyriuje) kiekvienas asmuo turi du raktus: slaptąjį (privatųjį), žinomą tik jam, ir viešąjį, kurį jis perduoda kitiems komunikacijų dalyviams. Keičiantis pranešimais siunčiamas tiktai viešasis raktas.

Kaip tokio tipo dokumento parašas atlieka išvardintas funkcijas?

1. Dokumento autoriaus nustatymas. Pranešimo autorius, siųsdamas dokumentą, jį koduoja slaptuoju raktu (pasirašo dokumentą). Pranešimo adresatas gautą žinutę iššifruoja viešuoju raktu (iš kur jis gaunamas, bus kalbama vėliau). Kitas asmuo negali apsimesti pranešimo autoriumi, nes neturi slaptojo rakto, skirto pasirašyti. Be to, siuntėjas negali paneigti, kad siuntė informaciją. Problema ta, kad trečiasis asmuo gali žinutę perskaityti naudodamasis viešuoju raktu.

2. Vientisumo užtikrinimas. Dokumento vientisumą užtikrina tai, kad pakeitus bent vieną simbolį žinutėje visas dokumento tekstas virsta neįskaitomų simbolių virtine. Čia reikėtų įvertinti dar vieną aplinkybę: kitaip negu įprasti dokumentai, elektroniniai dokumentai yra lengvai kopijuojami, neįmanoma atskirti kopijos nuo originalo, elektroninio parašo paskirtis – užtikrinti visišką kopijos atitikimą originalui. Galima netgi teigti, kad kiekvienas elektroninio dokumento egzempliorius yra jo originalas.

3. Slaptumo užtikrinimas. Kaip jau buvo minėta, elektroninio dokumento kodavimas slaptuoju raktu (pasirašymas) neatlieka duomenų slaptumo užtikrinimo funkcijos. Trečiasis asmuo viešuoju raktu gali lengvai iššifruoti žinutę. Saugumui užtikrinti naudojamas kitoks informacijos siuntimo būdas vadinamas šifravimu. Siuntėjas koduoja in-

formaciją gavėjo viešuoju raktu. Iššifruoti informaciją gali tik asmuo, turintis slaptąjį raktą, t. y. adresatas. Net pats siuntėjas negali iššifruoti informacijos, nes tą galima padaryti tik slaptuoju raktu. Kad pranešimas būtų tikrai slaptas, jį iššifruoti kompiuteriu turi būti neįmanoma arba labai sudėtinga, t. y. iššifravimo sąnaudos turi viršyti galimą ekonominę naudą.

Su elektroniniu parašu pasirašytu dokumentu galima siųsti duomenis apie autoriaus viešąjį raktą, tokiu būdu kiekvienas asmuo galės įsitikinti, ar elektroninis dokumentas yra nepakeistas. Tačiau iškyla klausimas, kas paliudys, kad tas viešasis raktas (t. y. šifravimo raktų pora) tikrai yra to asmens, kurio vardu pasirašomas elektroninis dokumentas. Todėl šį darbą turi atlikti elektroninių parašų sertifikavimo centras. Elektroninių parašų sertifikavimo centras – nepriklausoma patikima trečioji šalis, kuri registruoja asmenis ir jų viešuosius šifravimo raktus, išduoda ribotą laikotarpį galiojantį liudijimą – skaitmeninį sertifikatą, elektroninių parašų sertifikavimo centro elektroniniu parašu patvirtinantį unikalios privačiojo ir viešojo rakto poros priklausomybę tam asmeniui, tvarko ir seka sertifikatų galiojimą, suteikia informaciją apie sertifikatus. Dėl kokių nors priežasčių gali prireikti panaikinti sertifikato galiojimą (pvz., jeigu asmuo prarado privataus rakto failą, pasikeitė asmens įgaliojimai – darbuotojas pakeitė darbą ir pan.). Tuo tikslu nepriklausomas patikėtinis – sertifikavimo centras – turi organizuoti savo veiklą taip, kad asmuo nedelsdamas galėtų pranešti apie sertifikato atšaukimą, laikiną jo galiojimo sustabdymą ar galiojimo pratęsimą.

Sertifikato formatas yra aprašytas tarptautiniu standartu ITU X.509, todėl jį gali perskaityti ar kurti programos, skaitančios X.509 standartą. Prie elektroninio dokumento galima dėti kelis sertifikatus, iš kurių kiekvienas patvirtina ankstesniojo tikrumą. Paskutinysis sertifikatas turi būti pasirašytas sertifikavimo centro.

1.5.9. Duomenų šifravimas

Šifravimas yra duomenų pavertimas neįskaitomais be šifravimo rakto. Šifravimo pasekmė yra duomenų slaptumo užtikrinimas, nes informacija nesuprantama bet kokiam pašaliniam asmeniui, išskyrus tuos, kurie turi šifravimo raktą. Šifravimas išsprendžia duomenų apsaugos ir privatumo problemas, užtikrina duomenų vientisumą bei patikimumą ir leidžia saugiai bendrauti atviraisiais tinklais. Yra dvi pa-

grindinės šifravimo rūšys: simetrinė ir asimetrinė.

Šifravimas saugant kompiuterinę informaciją priklauso nuo informacijos naudojimo srities ir turi įgyvendinti šias funkcijas:

1) sumažinti neleistinos prieigos prie duomenų galimybę;
2) užtikrinti slaptumą;
3) užtikrinti duomenų vientisumą ir tikrumą;
4) užtikrinti tapatumą;
5) būti veiksmingas.

Slaptumas, reiškia, kad kiekvienas vartotojas gali būti tikras, jog duomenų slaptumas bus išsaugotas. Teisę užšifruoti duomenis gali turėti keletas žmonių, tačiau peržiūrėti užkoduotą failą gali tik asmuo, turintis šifravimo raktą. Šiuo atveju kodavimas užtikrina informacijos slaptumą perduodant ją įprastais kanalais.

Duomenų tikrumas ir vientisumas. Patikrinama, ar teisėtai buvo įvesti duomenys ir ar jie nebuvo pakeisti perduodant. Dokumento gavėjas turi būti tikras, kad negaus dokumento, kuris yra neteisėtai pakeistas arba į duomenis įterpta programa, pavojinga kompiuterių sistemai ar duomenims (kompiuterinis virusas).

Dokumento autoriaus tapatybės nustatymas. Adresatas turi būti garantuotas, kad gavo informaciją iš to asmens, iš kurio tikėjosi. Siuntėjas negali paneigti siuntęs informaciją.

Veiksmingumas. Saugumo sistema neturi stipriai riboti, mažinti darbo našumo, jis turi pakisti nežymiai.

Kad pranešimas būtų tikrai saugus, *jo iššifravimas kompiuteriu turi būti neįmanomas arba labai sudėtingas, t. y. iššifravimo sąnaudos viršyti iššifravimo ekonominę naudą.*

Šifravimas nuo kitų vartotojų apsaugo failus kompiuteryje ir informaciją, perduodamą kompiuteriniais tinklais.

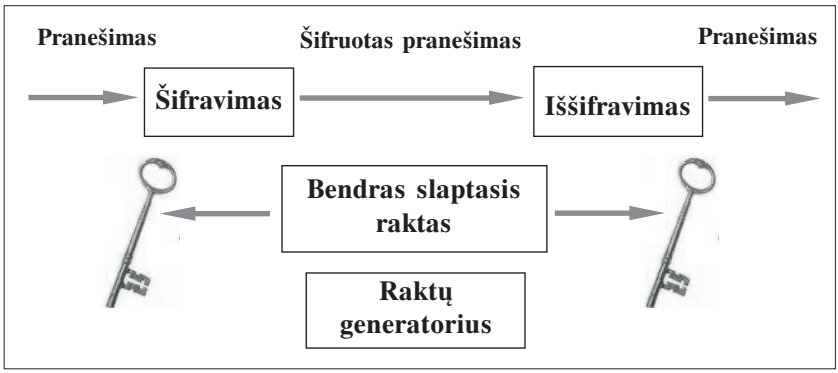
Šifravimas. Šifruojant žinutė arba failas ir raktas modifikuojami algoritmu ir gaunamas užšifruotas tekstas. Norint grąžinti pradinį tekstą reikia atlikti atvirkštinę operaciją naudojant dekodavimo raktą ir algoritmą. Šifrus gali naudoti ir vienas vartotojas, pavyzdžiui, šifruoti failus kietajame diske, kad neteisėti vartotojai negalėtų susipažinti su failų turiniu. Jeigu visi šifravimo ir dešifravimo procesai vykdomi tuo pačiu raktu, tai teisė prieiti prie to rakto reiškia teisę prieiti prie visų duomenų. Jeigu naudojami keli raktai, tai vartotojams sunku juos atsiminti, ypač kai raktus sudaro daug skaitmenų.

Šiuo metu kompiuterinėse sistemose šifravimui naudojamos simetrinės ir asimetrinės šifravimo sistemos, kurias sudaro šie pagrindi-

niai komponentai:

– duomenys, kurie turi būti užkoduoti ir iškoduoti;
– kodavimo ir iškodavimo algoritmai;
– raktai ir sertifikatai.

Simetrinės šifravimo sistemos failo, žinutės užšifravimui ir iššifravimui naudoja vieną ir tą patį slaptąjį raktą (žr. 2 pav.). Siuntėjas (koduotojas) siunčia pranešimą, kurį jis užkoduoja naudodamas jam ir gavėjui žinomą raktą ir abiem prieinamą algoritmą. Algoritmo ypatybė yra ta, kad užkoduoti ir iškoduoti informaciją galima tuo pačiu raktu (akivaizdus pavyzdys yra filmuose matyta kodų knygelė).



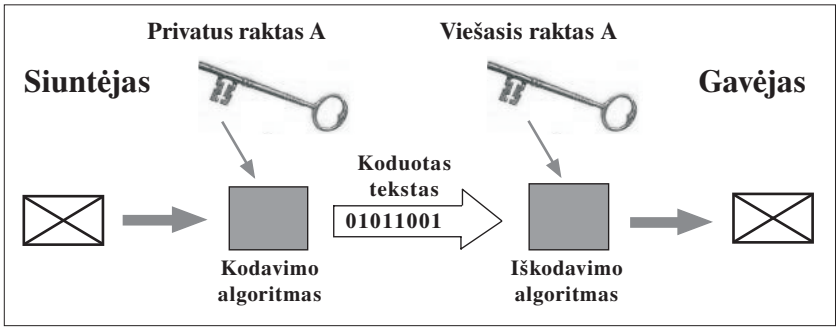
2 pav. **Simetrinio šifravimo sistema**

Kaip jau minėta, simetrinės šifravimo sistemos turi problemą: slaptas raktas turi būti žinomas ir siuntėjui, ir gavėjui, tad iškyla klausimas, kaip siuntėjui saugiai nusiųsti slaptąjį raktą gavėjui, ir kaip apsaugoti jį nuo pakeitimo. Dar viena problema yra ta, kad gavėjas negali įrodyti, jog pranešimą gavo iš tam tikro asmens, pranešimą jis galėjo užšifruoti ir pats, t. y. neatliekama tapatybės nustatymo funkcija.

Simetrinio rakto šifravimo sistemos naudojamos EDI (elektroninio duomenų perdavimo) sistemose ir net sudaro technologinį pagrindą įvairiems standartams. Simetrinis šifravimas tinka, kai reikia perduoti didelius duomenų kiekius, nes simetrinio šifravimo procesas atliekamas greitai. Tačiau jis nelabai tinka tose srityse, kuriose būtina įsitikinti duomenų siuntėjo tapatybe, (pvz., keičiantis tarnybiniais do-

kumentais elektronine forma atsiranda būtinybė užtikrinti, kad dokumento autorius yra įgaliotas asmuo, turintis teisę pasirašyti tokio pobūdžio dokumentus). Tokia sritis yra elektroninė prekyba, kur simetrinio rakto sistemos tinkamos vartoti vienas kitu iš anksto pasitikinčių partnerių. Antra vertus, jeigu firma turi keletą tūkstančių partnerių, jai prireiktų kelių tūkstančių skirtingų raktų kiekvienam klientui, be to, tokia schema reikalauja abiejų pusių išankstinio susitarimo dėl rakto (nebent jie sutinka persiųsti raktą tinklu, bet tai keltų pavojų rakto saugumui).

Asimetrinės šifravimo sistemos failo, žinutės užšifravimui ir iššifravimui naudoja du raktus: vieną privatųjį raktą naudoja žinutę užšifruoti, o kitą viešąjį raktą naudoja iššifruoti (žr. 3 pav.). Viešąjį raktą galima skelbti, o slaptasis raktas neskelbiamas. Taigi kiekvienas asmuo turi du raktus: slaptąjį, privatų, žinomą tik jam, ir viešąjį, kurį jis perduoda kitiems komunikacijų dalyviams. Keičiantis pranešimais siunčiamas tiktai viešasis raktas. Todėl nereikia jaudintis dėl slaptojo rakto saugumo, nes tekstas iššifruojamas slaptuoju raktu, kurį turi tik vienas savininkas – gavėjas. Slaptąjį rakto ir viešąjį raktus sieja tiesioginis ryšys – sudėtingas matematinis algoritmas.



3 pav. **Dviejų raktų asimetrinė šifravimo sistema**

Slaptuoju šifravimo raktu gali disponuoti tik vienas asmuo, todėl šio rakto apsauga turi būti sustiprinta asmens slaptažodžiu arba to asmens biometrinių duomenų (pirštų atspaudų, akių rainelės vaizdo) kontrole. Viešasis šifravimo raktas, kaip rodo jo pavadinimas, yra viešai skelbiamas, todėl asimetrinio šifravimo algoritmas yra vadinamas viešųjų šifravimo raktų algoritmu. Kadangi asimetriniai algoritmai yra

daug lėtesni už simetrinio šifravimo algoritmus, įgyvendinamas „skaitmeninio voko“ principas, kurio esmė yra tokia: tekstas užšifruojamas sparčiu simetriniu algoritmu naudojant neilgą, bet pakankamai saugų šifravimo raktą. Toks raktas turi būti vienkartinis (pranešimo arba seanso raktas) ir po ryšio pabaigos turi būti sunaikintas. Tik tas vienkartinis slaptasis raktas užšifruojamas gavėjo viešuoju raktu.

1.5.10. Elektroninių duomenų (informacijos) sauga

Duomenų šifravimas – viena iš priemonių, užtikrinančių **elektroninių duomenų ar informacijos (informacinių sistemų) saugą**. Šios vertybės apsaugai skiriama vis daugiau dėmesio techniniu ir teisiniu požiūriu visame pasaulyje. **Informacijos saugumas (sauga) suprantamas kaip informacijos bei sistemos infrastruktūros apsauga nuo atsitiktinio ar tyčinio, natūralaus ar dirbtinio pobūdžio poveikio, galinčio sukelti žalą informacijos ar sistemos infrastruktūros savininkams bei vartotojams.**

Praktikoje įprastai išskiriami trys pagrindiniai informacinių sistemų saugos aspektai:

- ***prieinamumas*** – galimybė tam tikrą laiką gauti reikalingą informaciją;
- ***vientisumas*** – informacijos svarbumas ir neprieštaringumas bei apsauga nuo sunaikinimo ir neteisėto pakeitimo;
- ***slaptumas*** – apsauga nuo neteisėto nuskaitymo.

Elektroninės informacijos sauga plėtojama atsižvelgiant į tam tikrus **principus, kuriais privaloma vadovautis užtikrinant elektroninės informacijos saugą**:

1. *Suvokimo principas*. Siekiant užtikrinti elektroninės informacijos saugą, reikia suvokti apsisaugojimo priemonių nuo galimos grėsmės elektroninei informacijai naudojimo būtinybę.
2. *Atsakomybės principas*. Kiekvienas elektroninės informacijos naudotojas turi suvokti savo atsakomybę ir funkcijas saugant elektroninę informaciją. Elektroninės informacijos saugą informacinėse sistemose turi užtikrinti valstybės institucijos vadovas, o ją įgyvendinti privalo saugos įgaliotiniai.
3. *Reagavimo principas*. Elektroninei informacijai kyla daug grėsmių, todėl būtina laiku aptikti ir užkirsti kelią elektroninės

informacijos saugos pažeidimams, keistis informacija apie grėsmę elektroninei informacijai ir kovos su ja priemones valstybės institucijoje ir su kitomis valstybės institucijomis.

4. *Demokratiškumo principas*. Elektroninės informacijos sauga turi būti įgyvendinama ir derėti su esminėmis demokratiškos visuomenės vertybėmis (pvz., laisve skleisti ir gauti informaciją).
5. *Rizikos įvertinimo principas*. Siekiant nustatyti esamą elektroninės informacijos saugos lygį ir parinkti būtinas elektroninės informacijos saugos priemones, būtina periodiškai įvertinti elektroninės informacijos saugos pavojus informacinėse sistemose.
6. *Elektroninės informacijos saugos kultūros ugdymo principas*. Siekiant užtikrinti elektroninės informacijos saugą, būtina ypač dėmesingai mokyti nuolatinius elektroninės informacijos naudotojus elektroninės informacijos saugos ir taip ugdyti elektroninės informacijos saugos kultūrą valstybės institucijose.
7. *Elektroninės informacijos saugos priemonių projektavimo ir diegimo principas*. Elektroninės informacijos sauga turi būti kuriama kartu su informacine sistema. Elektroninės informacijos sauga turi būti pamatinis visų informacinės sistemos paslaugų elementas, kuriam būtina užtikrinti nuolatinį lėšų, neviršijančių pačios elektroninės informacijos vertės, skyrimą.

Elektroninės informacijos saugos aplinkos klausimus galima būtų suskirstyti į keturias pagrindines grupes:

1) ***normatyvinę*** – įstatymai, poįstatyminiai aktai, standartai ir t. t.

2) ***administracinę*** – organizacijos vadovybės vykdomi bendro pobūdžio veiksmai;

3) ***procedūrinę*** – konkretūs su konkrečiais asmenimis susiję saugumo veiksmai;

4) ***programinį techninį*** – vykdomi konkretūs techninio pobūdžio veiksmai.

Dabar teisės normose dar nepakankamai aiškiai atspindimi specifiniai terminai, sampratos, pasigendama šios srities reglamentavimo pamatinėmis teisės normomis. Todėl veiksminga informacinėse sistemose tvarkomos informacijos sauga turėtų būti vienas iš svarbiausių valstybės informacinės politikos prioritetų.

Tarptautiniu mastu reglamentuoti informacinių sistemų ir jose tvarkomos informacijos saugos klausimus viena iš pirmųjų pradėjo Eu-

ropos bendradarbiavimo ir plėtros organizacija (toliau – ir OECD). OECD priimtos direktyvos vertintinos kaip specifinę reikšmę turintys teisės aktai, kurie nurodo valstybėms narėms pagrindines veiklos kryptis informacijos saugos reglamentavimo srityje.

1.6. Teisės aktų kompiuterinės bazės

Kompiuterines teisės aktų bazes (kompiuterines teisines bazes, teisinės informacijos paieškų sistemas ir kt.) šiuo metu dažnai naudoja teisininkai, verslininkai, politikai, studentai. Dažniausiai tai yra didžiulės įvairių įstatymų bei teisės aktų, komentarų, teismų sprendimų ir kitos teisinės informacijos sankaupos įvairiose kompiuterinėse sistemose, leidžiančios lengvai ir greitai rasti norimą teisinį dokumentą.

Pasaulyje yra daugybė tokių teisinių bazių: LexisNexis, Eur-Lex, CEDEX, LITLEX, Lietuvos Seimo teisinė bazė ir kt. Visas jas galima skirstyti į dvi grupes:

1) nemokamas, skirtas visuomenei;
2) mokamas, skirtas profesionalams.

Nemokamai naudotis galima, pavyzdžiui, daugiakalbiu Europos teisės portalu Eur-Lex (http://europa.eu.int/eur-lex/lt/index.html), taip pat ir lietuvių kalba. Lietuvoje dažnai naudojama nemokama **Seimo teisinė bazė** (http://www.lrs.lt), kurioje galima atlikti galiojančių Lietuvos Respublikos ar Europos Sąjungos teisės aktų paiešką. Šioje bazėje taip pat galima susipažinti su Seimo rengiamais teisės aktų projektais arba pareikšti savo nuomonę bei pastabas apie juos. Bazėje taip pat pateikta informacija apie kai kurias kitas teisės aktų duomenų bazes, tačiau gana menkos paieškos galimybės, nesaugomos skirtingos teisės aktų redakcijos.

Svarbiausia mokama Lietuvos kompiuterinė teisės aktų ir dokumentų bazė yra nuo 1994 m. veikiantis **LITLEXas** (http://www.litlex.lt, http://www.infolex.lt), kurią sukūrė ir platina Teisinės informacijos centras. Tai – išsami Lietuvos Respublikos teisės aktų ir kitų dokumentų duomenų bazė. Bazėje pateikti aktų originalai ir redakcijos: tekstai su pakeitimais ir papildymais, loginiai ryšiai. Teisės aktų galima ieškoti pagal žodžius tekste ar akto pavadinime, akto priėmimo datą, priėmusią instituciją, numerį, antraštę, rubrikas. Ją naudoja profesionalai (teisininkai, vadovai, finansininkai, vadybininkai), kuriems būtini tikslūs, patogiai ir greitai gaunami, periodiškai atnaujinami teisės aktų duomenys.

LITLEXą sudaro teisės aktai (Seimo, Vyriausybės, Prezidento, Konstitucinio Teismo, ministerijų, kitų institucijų); teisės aktų tekstai su pakeitimais; rubrikatoriai-klasifikatoriai (sąvadai). Nuolat pildomi:

- muitinės segtuvas (prekių klasifikavimas, deklaravimas, nomenklatūra, muitų tarifai);
- aplinkos segtuvas (aplinkos apsauga, ūkinė veikla, gamtos ištekliai, statyba);
- darbo segtuvas (ginčai, atsakomybė, įdarbinimas ir kt.);
- statybos segtuvas (žemės valdymas, naudojimas, statinių įteisinimas),
- Lietuvos teismų praktikos segtuvas (baudžiamoji, administracinė, civilinė teisė ir procesas, nutartys, apibendrinimai, apžvalgos, konsultacijos).

LITLEXe taip pat nurodyti kiekvieno teisės akto loginiai ryšiai su teismų praktika, įstatymais, Vyriausybės dokumentais ir kitais aktais (nuorodos į dokumentus, susijusius pagal taikymo pobūdį). Teisės aktų tekstai pateikiami tokiomis formomis:

- aktualios redakcijos (galiojantys aktų tekstai su visais pakeitimais);
- tarpinės redakcijos (dokumentų kitimo istorija);
- originalios redakcijos (pirminiai dokumentų tekstai).

Teisės aktų loginiai tarpusavio ryšiai nurodomi taip:

- akto keisti aktai;
- aktą keitę aktai;
- aktai, kuriuose minimas aktas.

Egzistuoja dvi LITLEXo versijos: **IntERnetas ir IntRAnetas.**

IntRAneto versijoje nereikia interneto ryšio, paieška vykdoma kompiuteryje arba organizacijos kompiuterių tinkle. Ši versija pasižymi ypatingai sparčia paieška, nes nenaudojamas internetas. Informacija atnaujinama elektroniniu paštu ir per FTP du kartus per savaitę.

IntERneto versijoje paieška vykdoma internete adresu www.litlex.lt/litlex prisijungus vartotojo vardu ir asmeniniu slaptažodžiu. LITLEXo IntERneto sistemoje teisės aktai papildomi ir atnaujinami kiekvieną dieną.

Literatūroje minimas dar vienas teisinių bazių pavadinimas – **teisinių žinių bazės** (angl. *Legal Knowledge Bases).* Jose, be konkrečių teisinių duomenų (priimtų įstatymų, kitų teisinių aktų, teismo spren-

dimų), pateikiamos ir taisyklės sprendimui gauti, ekspertų nuomonės ir kitos žinios.

1.7. Lietuvos teismų informacinė sistema LITEKO

Lietuvos teismų informacinė sistema LITEKO yra teismų veiklai reikalingų dokumentų bei duomenų kaupimo, tvarkymo, paieškos, teismų sprendimų ir statistinių rodiklių kaupimo, apdorojimo ir teikimo sistema, kuri veikia naudojant kompiuterius, standartines ir taikomąsias programas, duomenų bazes, duomenų perdavimo tinklus. Ji pradėta kurti 2003 m. kaip integruotas teisingumo priežiūros institucijų vidaus darbo instrumentas. Šis projektas vykdomas pagal PHARE programą kartu su Lietuvos Respublikos teisingumo ministerija.

LITEKO paskirtis – sudaryti sąlygas teismams automatizuotu būdu rinkti, kaupti, sisteminti ir teikti duomenis, susijusius su teismų gautais ir jų veiklai reikalingais dokumentais ir duomenimis, teismų sprendimais, teismų veiklos statistika, taip pat keistis duomenimis su valstybės registrais ir informacinėmis sistemomis, vykdyti kitas teisės aktuose ir šiuose nuostatuose nustatytas funkcijas.

LITEKO objektai – teismo proceso dalyvių duomenys, procesiniai dokumentai, informacija apie bylos nagrinėjimo eigą (elektroninės bylų kortelės), informacija apie bylos nagrinėjimo rezultatus, sistemos vartotojų duomenys.

LITEKO pagrindinės funkcijos – teismų gautų procesinių dokumentų registravimas ir apskaita; bylų nagrinėjimo eigos registravimas; teismo procesui reikalingų dokumentų ir duomenų paieška, rinkimas, sisteminimas; procesinių dokumentų rengimas ir teikimas byloje dalyvaujantiems asmenims; teismų sprendimų kaupimas; teismų veiklos statistinių rodiklių kaupimas, apdorojimas ir teikimas; LITEKO objektų saugojimas, sisteminimas ir teikimas (skelbimas) šių nuostatų numatyta tvarka.

LITEKO valdytojas ir centrinės duomenų bazės tvarkytojas yra Nacionalinė teismų administracija. Lietuvos Respublikos teismai yra LITEKO vietinių duomenų bazių tvarkytojai. LITEKO valdytojas yra ir LITEKO saugomų asmens duomenų valdytojas, LITEKO tvarkytojai yra LITEKO saugomų asmens duomenų tvarkytojai.

LITEKO informacinę struktūrą sudaro:

- centrinė duomenų bazė;

• teismų vietinės duomenų bazės.

Centrinėje duomenų bazėje kaupiama visuose Respublikos teismuose užregistruota informacija, ji taip pat naudojama LITEKO klasifikatoriams ir sąrašams rengti, teismams keistis informacija, statistikai skaičiuoti, teismų sprendimams viešai skelbti, ryšiams su valstybės registrais ar kitais duomenų teikėjais organizuoti, sistemos naudotojams administruoti. Keisti LITEKO centrinėje duomenų bazėje sukauptus teismų duomenis gali tik duomenis sudaręs teismas, pakeitimą atlikdamas vietinėje duomenų bazėje.

Centrinėje duomenų bazėje tvarkomi duomenys:

- centrinis bylų sąvadas: kaupiami į centrinę duomenų bazę teismų perduoti vietinėse duomenų bazėse tvarkomi duomenys;
- teisėjų sąrašas: teisėjo pavardė, vardas, gimimo data, teismas, pareigos, teisėjui suteiktas unikalus kodas;
- LITEKO centrinės duomenų bazės tvarkytojų ir naudotojų duomenys: vardas, pavardė, organizacija, kontaktinė informacija, suteiktos teisės ir prisijungimo vardai, slaptažodžiai.

Teismų vietinėse duomenų bazėse tvarkomi konkretaus teismo veiklai reikalingi duomenys bei dokumentai. Teismai LITEKO duomenis į vietines duomenų bazes įrašo nedelsdami – ne vėliau kaip per tris dienas po jų atsiradimo (pateikimo). Įvedant ir taisant informaciją vietinėse duomenų bazėse fiksuojamas vartotojo, kuris tai atliko, kodas ir įvedimo (taisymo) data. Vietinėse duomenų bazėse tvarkomi šie duomenys:

- apie teismui pateiktus procesinius dokumentus: dokumento rūšis, pateikimo data, suteiktas registracijos numeris, dokumento esmė, pagrindai, dokumento pateikėjas, pastabos, pateiktas ar turimas dokumentas elektronine forma;
- apie teismo užvestą bylą (elektroninė bylos kortelė): užvedimo data, numeris, bylą nagrinėjanti instancija, bylos gavimo aplinkybės, bylos iškėlimo pagrindas, bylos kategorijos, bylą nagrinėti paskirtas teisėjas (-ai), bylos sudėtingumo duomenys, pastabos;
- apie teismo procesą: procesinis įvykis (darbas su dokumentu, posėdis ir kt.), procesinio įvykio rezultatas (bylos išnagrinėjimas, atidėjimas, išsiuntimas į kitą teismą, proceso atnaujinimas ir kt.), data, laikas, trukmė, bylos išnagrinėjimo rezultatas, posėdžio vieta, teisėjų kolegijos (jei buvo sudaryta) nariai, teismo procesiniai dokumentai;

- apie byloje dalyvaujančius asmenis;
- apie teismo procesinį dokumentą: procesinio dokumento rūšis (nutartis, protokolas, sprendimas, nutarimas, nuosprendis ir kt.), dokumentui teisme suteiktas numeris, dokumentas elektronine forma, dokumento įregistravimo data;
- apie sistemos vartotojus: vardas, pavardė, gimimo data, pareigos, kontaktinė informacija (telefonai, elektroninis paštas), darbuotojui suteiktos teisės naudotis sistema ir prisijungimo vardai, slaptažodžiai.

LITEKO duomenys neatlygintinai teikiami institucijoms, turinčioms įstatymų ar kitų teisės aktų nustatytą teisę gauti duomenis neatlygintinai tiesioginėms funkcijoms vykdyti.

Kitiems fiziniams ar juridiniams asmenims, turintiems įstatymų ar kitų teisės aktų nustatytą teisę gauti LITEKO duomenis, LITEKO duomenys teikiami teisės aktų nustatytomis sąlygomis ir tvarka.

2. INTERNETO TEISĖ

2.1. Pagrindinė medžiaga. Interneto teisės samprata ir pagrindiniai klausimai

Interneto teise siauruoju požiūriu vadinami **interneto jurisdikcijos klausimai**, plačiai šis terminas vartojamas bendrai apibrėžiant teisės institutus, susijusius su svarbiausiais teisės taikymo internete klausimais, kurie nepriskiriami prie kitų teisės institutų ar šakų, tarp jų – **prie interneto domeno vardų, interneto jurisdikcijos, interneto turinio reglamentavimo, interneto tarpininkų veiklos (atsakomybės) reglamentavimo ir interneto administravimo teisinių klausimų**.

Interneto domeno vardai – interneto adresų srities simboliniai pavadinimai, nustatantys interneto turinio teikėją, jo prekes, paslaugas ar informaciją.

Interneto turinys yra visa informacija, prekės ir paslaugos, pateiktos internete, taip pat ir žalingo (ribojamo) turinio (pvz., smurtinio, erotinio ar pornografinio pobūdžio informacija, prekės ir paslaugos) bei neteisėto (draudžiamo, nepageidaujamo) turinio (pvz., vaikų pornografija, neteisėtos intelektinės nuosavybės kopijos ir pan.).

Interneto jurisdikcija sudaryta iš dviejų pagrindinių institutų – internete taikomos teisės ir valstybinių institucijų galios reguliuoti (spręsti ginčus, priimti privalomus sprendimus, taikyti sankcijas) visuomeninius santykius internete.

Interneto tarpininkais galima laikyti subjektus, užtikrinančius interneto infrastruktūros funkcionavimą, teikiančius interneto prieigos, prieglobos, turinio talpinimo ir perdavimo paslaugas. Faktiškai interneto tarpininkai yra interneto prieigos paslaugų teikėjai, interneto portalai, kuriuose vartotojai gali pateikti savo informaciją (pvz., failus, komentarus ir pan.). Universitetas taip pat yra interneto tarpininkas, nes suteikia interneto prieigos, elektroninio pašto, tinklalapių talpinimo paslaugas darbuotojams ir studentams. Asmuo, kuris talpina savo informaciją arba jo atrinktą ir jam žinomą kitų asmenų

informaciją, nelaikomas interneto tarpininku.

Interneto tarpininkas neturi pareigos kontroliuoti ir tikrinti informacijos, kurią interneto tarpininko paslaugų gavėjai (vartotojai) siunčia, gauna, talpina, saugo naudodamiesi interneto tarpininko infrastruktūra.

Interneto administravimas yra interneto domenų registravimas ir su tuo susijusios funkcijos, taip pat kiti centralizuotai ir vienašališkai sprendžiami interneto funkcionavimo klausimai.

2.2. Interneto domenų vardų teisiniai aspektai

2.2.1. Domeno vardo teisinė samprata

Techninis domeno vardo apibrėžimas – interneto adresų srities simbolinis pavadinimas – priimtas Europos Sąjungos elektroninės komercijos direktyvoje ir 2002 m. birželio 22 d. Europos Parlamento ir Tarybos reglamente Nr. 733/2002 dėl .eu aukščiausio lygio domeno įdiegimo. Šis apibrėžimas priimtinas objektyviuoju požiūriu, tačiau jis neparodo jokių subjektyvių teisių, kurios gali būti susijusios su domeno vardu. Teisiniu požiūriu domenų vardai panašūs į intelektinės nuosavybės objektus, prievolines arba net daiktines teises. Teisinė domenų vardų samprata atspindi domenų vardų socialinę vertę ir funkciją, nes šiuo metu domenų vardai atlieka ne tik fizinio adreso, bet ir identifikatoriaus funkciją.

2.2.2. Domeno vardo reikšmė

Domeno vardas yra panašus ir atlieka panašią funkciją kaip prekės ženklas – t. y. domeno vardas, kaip ir prekės ženklas, yra tam tikras žymuo, naudojamas siekiant atskirti vieno asmens prekes, paslaugas arba informaciją elektroninėje erdvėje nuo kito asmens prekių, paslaugų, informacijos. Taip domeno vardas elektroninėje erdvėje iš esmės dubliuoja prekės ženklą. Paminėtina, kad domenų vardai vis labiau populiarėja ir registruojami kaip prekių ženklai. Kai kurie garsūs prekės ženklai (pvz. *Google* ar *Skype*) visų pirma buvo įregistruoti kaip domeno vardai ir tik jiems išpopuliarėjus – kaip prekės ir paslaugų ženklai.

Kaip ir prekės ženklas, domeno vardas dar atlieka ir kitas funkcijas, pavyzdžiui:

- prekės, paslaugos, informacijos kilmės (šaltinio) nustatymo;
- kokybės užtikrinimo.

Kaip minėta, domenų vardai gali aiškiai rodyti interneto tinklalapio kilmės vietą (šiuo požiūriu jie yra panašūs ir į geografines nuorodas) ar net konkretų asmenį (įmonę), kuriam priklauso interneto tinklalapis, tačiau nebūtinai, nes valstybių aukščiausio lygio domenus gali registruoti ir užsienio subjektai, pavyzdžiui, televizijos kompanijos įvairiose valstybėse registruoja aukščiausio lygio domenus „.tv“, kurie priklauso Ramiojo vandenyno salų valstybei Tuvalu. Visais atvejais domenų vardai atskiria skirtingų asmenų elektroninėje erdvėje pateiktą informaciją. Be to, domeno vardas gali tapti ir kokybės simboliu (pvz., *ebay.com* yra užsitarnavęs patikimiausio ir patogiausio interneto aukcionų operatoriaus reputaciją; *google.com* visuotinai laikomas kokybiškiausiu ir išsamiausiu interneto paieškos mechanizmu). Kaip jau minėta, domeno vardas dažnai tampa visos įmonės rinkodaros strategijos ašimi ir prekės ženklu.

2.2.3. Domeno vardo teisinis statusas

Kaip jau minėta, domeno vardas gali būti laikomas intelektinės nuosavybės teisių objektu, t. y. gali būti suteiktos subjektyviosios teisės, leidžiančios domeno vardą naudoti, valdyti ir juo disponuoti.

Domeno vardo, kaip intelektinės nuosavybės, teisės statusą apibrėžia domeno vardo registracijos sąlygos ir sutartys, sudaromos registruojant domeno vardus. Subjektyviąsias teises į domeno vardą riboja ir techninės galimybės veikti savarankiškai, kadangi be domenų administratoriaus (registratoriaus), t. y. tarpininko, dalyvavimo domeno vardas negali funkcionuoti. Kaip ir daugelio intelektinės nuosavybės teisių objektų, domenų vardai yra originalūs, t. y. iš esmės įmanomas tik vienas tam tikro vardo domenas.

Domenų vardais, kaip ir bet kokia kitokia nuosavybe, galima disponuoti. Domenų vardai dažnai vertinami didelėmis sumomis, yra perparduodami, nuomojami ar net įkeičiami. Kai kuriose valstybėse (pvz., JAV, Vokietijoje) domenų vardai įvardijami kaip turtinių teisių objektas. Ši nuostata atėjo iš JAV teismų praktikos, kurioje aiškiai pripažinta domenų vardų turtinė vertė, teisės jais disponuoti, taip pat tam tikros pirmenybės teisės registruoti domenų vardus. Domeno vardas kaip nuosavybės objektas įvardijamas ir ICANN (svarbiausios tarptautinės institucijos, reguliuojančios interneto funkcionavimą) bendro-

siose domenų vardų ginčų sprendimo taisyklėse. Iš kitos pusės skirtingose valstybėse nusistovėjo nevienoda praktika pripažįstant domenų vardus turtine teise ar net ypatingu intelektinės nuosavybės objektu. Pastaruoju atveju nėra aišku, ar domeno vardas turėtų būti laikomas autorių teisių, ar pramoninės nuosavybės teisių, ar apskritai specialiųjų *sui generis* teisių objektu. Nors koreliacija tarp domeno vardo ir intelektinės nuosavybės objektų yra, akivaizdu, kad domenų vardai nėra tiesiogiai susiję su kūryba ar inovacijomis ir nedaro įtakos šiems socialiniams procesams. Domenų vardai nelaikytini intelektine nuosavybe, kadangi netenkina jokių originalumo ar naujumo reikalavimų ir daugeliu atvejų yra antriniai, yra asmens vardo ar pavadinimo, veiklos rūšies pakartojimas. Dėl šių priežasčių domeno vardas gali būti laikomi tik *kvaziintelektine* nuosavybe (tokia, kaip, pvz., geografinės nuorodos).

Atskirai pažymėtina tai, kad domenų vardų registracija yra paremta sutartiniais santykiais tarp pareiškėjo ir registratoriaus. Sutartis dėl domeno registravimo yra specifinė paslaugų sutartis, o tarp pareiškėjo ir registratoriaus susiklosto prievoliniai santykiai. Prievolinis domeno vardo supratimas įtvirtintas Australijos ir Belgijos teisės aktuose, kuriuose tuo pačiu pabrėžiama, kad domeno vardas nėra nuosavybė ir niekam nepriklauso, į jį suteikiama tik sąlyginė licencija. Domeno vardo kaip prievolinės teisės samprata pagrįsta tuo, kad domeno vardai visose pasaulio valstybėse yra išduodami už tam tikrą registracijos mokestį, be to, taikomi metiniai išlaikymo mokesčiai, domeno vardo registratorius turi sutartyse nustatytas teises apriboti domeno naudojimą ar net panaikinti jo registraciją. Tačiau pasakytina, kad konkretų domeno vardą (t. y. prievolės turinį) laisvai pasirenka pats pareiškėjas, kuris siekia pristatyti save internete, o tai nėra būdinga prievolinėms teisėms.

Apibendrinus aukščiau aptartus domeno vardo aspektus, akivaizdu, kad tai yra kompleksinis teisinis institutas, turintis panašumų į intelektinės nuosavybės, turtines ir prievolines teises. Domeno vardo negalima painioti su interneto adresu, kadangi domeno vardas atlieka ne tik adreso internete funkciją, bet ir kitas funkcijas, būdingas socialiniams žymenims, o ne adresams. Atsižvelgiant į įsigalėjusią daugelio užsienio valstybių praktiką, domeno vardas priskirtinas prie specifinių turtinių teisių, kurių apimtis ir apribojimai yra nustatomi pareiškėjo ir domeno vardo registratoriaus sutartimi. Domenų vardai *per se* nelaikytini intelektinės nuosavybės teisių objektu, tačiau inte-

lektinės nuosavybės objektas gali būti originalūs žymenys, kurių pagrindu formuojami domenų vardai.

2.2.4. Domenų vardai Lietuvoje

Interneto domenas „.lt“ įkurtas 1992 m. Iki 2003 m. Lietuvoje domenų zoną „.lt“ administravo Lietuvos mokslo ir studijų kompiuterių tinklas LITNET, šiuo metu šias funkcijas vykdo Kauno technikos universiteto (toliau – ir KTU) Informacinių technologijų plėtros institutas. 2006 m. birželio pradžioje buvo įkurta per 25 500 „.lt“ domenų vardų.

Lietuvoje domenų vardai „.lt“ suteikiami pasirašius sutartį su KTU Informacinių technologijų plėtros institutu. Domenų vardai suteikiami sumokėjus nustatytą registravimo mokestį ir vadovaujantis pirmumo principu. Nors KTU Informacinių technologijų plėtros institutas nereikalauja, kad užsakovas formaliai patvirtintų savo teisę naudotis konkrečiu pavadinimu, tačiau siekiama, kad domenų vardais „.lt“ zonoje nebūtų registruojami Lietuvoje ar užsienyje žinomi prekių ženklai nesant šių ženklų savininkų sutikimo. Visais atvejais KTU Informacinių technologijų plėtros institutas atsiriboja nuo bet kokios atsakomybės prieš trečiuosius asmenis ir visą šią atsakomybę sutartimi perkelia užsakovui.

KTU Informacinių technologijų plėtros instituto ir užsakovo sutartis sudaroma pagal patvirtintą tipinę formą. KTU Informacinių technologijų plėtros instituto tipinėje sutartyje pabrėžiama, kad domeno vardas – adresų srities simbolinis pavadinimas – sudaromas vartotojų patogumui; adresų srityje esantys duomenys atitinka tarnybinių stočių IP skaitmeninius adresus arba aprašo žemesnio lygio adresų sritis; adresų sričių simboliniai pavadinimai nusako vartotojo vietą interneto tinkle, todėl nėra nuosavybės objektai (išskyrus atvejus, kai nustatyta tvarka yra įregistruoti kaip pramoninė nuosavybė); adresų sričių simboliniai pavadinimai yra unikalūs, t. y. negali kartotis. Taigi Lietuvoje iš esmės akcentuojamas prievolinis teisių į domeno vardą pobūdis nepripažįstant jo intelektinės nuosavybės teisių specialia forma.

KTU Informacinių technologijų plėtros instituto tipinėje sutartyje taip pat pabrėžiama, kad domeno vardas – adresų srities simbolinis pavadinimas – yra viešo pobūdžio, todėl sudaromas taip, kad nepažeistų moralės normų ir neklaidintų vartotojų dėl adresų srities turinio ar priklausomybės; užsakovas, registruodamas domeno vardą, neturi pažeisti trečiųjų asmenų teisių.

Domeno vardus „.lt“ zonoje gali registruoti ir Lietuvos, ir užsienio asmenys. Fiziniai asmenys turi teisę kaip domeno vardą registruoti savo pavardę. Nedraudžiama sudaryti domenų vardus naudojant bendrinius žodžius. Apskritai ribojamas (bet nedraudžiamas) tik dviejų raidžių (ar skaičių) registravimas kaip domeno vardo, taip pat informacijos (žymenų), kurios vartojimas ribojamas ar draudžiamas Lietuvos įstatymuose, registravimas (pvz., necenzūrinių žodžių). Didžiausias adresų srities simbolinis pavadinimas yra iš 63 simbolių. Ši taisyklė iš esmės nulemta techninių interneto duomenų perdavimo protokolo reikalavimų. Nuo 2004 m. kovo 30 d. KTU Informacinių technologijų plėtros institutas leidžia „.lt“ zonoje registruoti ir domeno vardą su specifinėmis lietuviškos abėcėlės raidėmis.

KTU Informacinių technologijų plėtros institutas iš esmės neprisiima jokios atsakomybės, susijusios su domenų vardų registravimu. KTU Informacinių technologijų plėtros instituto tipinėje sutartyje aiškiai nurodoma, kad užsakovas asmeniškai atsako už trečiųjų asmenų pramoninės nuosavybės teisių (firmų vardai, prekių (paslaugų) ženklai ir pan.) ir autorių teisių (neteisėtas kūrinio naudojimas ir pan.) pažeidimus sudarant ar naudojant adresų srities simbolinį pavadinimą. KTU Informacinių technologijų plėtros institutas, gavęs informacijos apie tai, kad užsakovas pažeidė trečiųjų asmenų teises, gali vienašališkai ne ginčo tvarka sustabdyti adresų srities naudojimą iki bus išspręstas ginčas tarp užsakovo ir pretenzijas pareiškusių trečiųjų asmenų. Be to, KTU Informacinių technologijų plėtros institutas nėra ginčo šalis sprendžiant klausimą dėl adresų sričių simbolinio pavadinimo naudojimo teisėtumo. Užsakovas privalo užtikrinti, kad domeno vardas nebūtų naudojamas kaip neteisėtos veiklos įrankis. KTU Informacinių technologijų plėtros institutas, įtardamas neteisėtą veiklą, gali vienašališkai įspėti užsakovą apie galimas pasekmes, sustabdyti domeno vardo naudojimą arba nutraukti sutartį. KTU Informacinių technologijų plėtros institutas iš esmės neturi nuoseklios teisių į domeno vardą gynimo praktikos ir apskritai vengia veltis į ginčus dėl domenų vardų. Dėl šių priežasčių teisės į domenų vardus Lietuvoje gali būti efektyviai ginamos tik tada, jei jie yra tinkamai įregistruoti kaip prekių ženklai, įmonių vardai yra originalūs autoriniai kūriniai. Bendrinio pobūdžio domeno vardai iš esmės „užimami tų asmenų, kurie juos įregistravo pirmieji. Ši praktika Europos valstybėse (ypač Vokietijoje) pamažu pripažįstama nesąžininga, tačiau bent kol kas

veiksmingos alternatyvos domenų vardų suteikimui pagal paraiškų datos pirmumą nėra.

2.2.5. Ginčai dėl domenų vardų

1999 m. spalio 29 d. ICANN asociacija, bendradarbiaudama su Pasaulio intelektinės nuosavybės organizacija (toliau vadinama ir PINO), parengė ir priėmė Bendrąsias domenų vardų ginčų sprendimo taisykles. Šiuo metu tai yra pagrindinis tarptautinio lygio dokumentas, reglamentuojantis kai kuriuos domenų vardų teisinius klausimus ir taikomas sprendžiant ginčus dėl domenų vardų. ICANN pati tiesiogiai neįgyvendina Bendrųjų domenų vardų ginčų sprendimo taisyklių, t. y. nenagrinėja ginčų, tačiau akredituoja domenų vardų ginčų sprendimo paslaugų teikėjus, kuriais šiuo metu yra kelios regioninės organizacijos bei PINO Arbitražo ir tarpininkavimo centras.

Formaliai Bendrosios domenų vardų ginčų sprendimo taisyklės taikomos tik tarptautiniams aukščiausio lygio domenų vardams („.com“, „.net“, „.org“, etc. ir kai kuriems šalių kodo aukščiausio lygio domenų vardams, pvz., „.tv“, „.fm”). Bendrosios domenų vardų ginčų sprendimo taisyklės iš esmės yra procedūrinis ir neprivalomo pobūdžio dokumentas. Procedūra panaši į arbitražinę, tačiau artimiausia tarpininkavimo procedūroms. Priimtas sprendimas yra neprivalomas, sprendimu nepatenkinta šalis ginčą gali perduoti spręsti kompetentingoms teisminėms institucijoms. Bendrosios domenų vardų ginčų sprendimo taisyklės kildinamos iš domeno vardų registracijos sutarčių nuostatų, kurios vienašališkai įtrauktos į sutartį ir paskelbtos registro tvarkytojo, kuris neturi kitaip elgtis dėl ICANN akreditavimo politikos.

Pagal Bendrąsias domenų vardų ginčų sprendimo taisykles pareiškėjas gali prašyti arba tik domeno vardo perleidimo (perregistravimo), arba registracijos panaikinimo. Jokių kitų reikalavimų tenkinimas (pvz., nuostolių atlyginimas) ar priemonių taikymas (pvz., turto areštai) pagal Bendrąsias domenų vardų ginčų sprendimo taisykles nenumatytas.

Bendrosios domenų vardų ginčų sprendimo taisyklės iš pareiškėjo reikalauja įrodyti tris būtinas aplinkybes siekiant pagrįsti reikalavimą, t. y. kad:

- atsakovo domeno vardas yra tapatus arba klaidinančiai panašus į pareiškėjo žymenį, į kurį pareiškėjas turi oficialias teises;

- atsakovas neturi pagrįstų teisių arba teisėtų interesų domeno vardo atžvilgiu;
- atsakovo domeno vardas buvo užregistruotas ir naudojamas nesąžiningai pareiškėjo atžvilgiu.

Lietuvoje Bendrosios domenų vardų ginčų sprendimo taisyklės iš esmės nėra taikomos. Pagal KTU Informacinių technologijų plėtros instituto tipinę sutartį ginčai dėl „.lt“ zonos domeno vardo gali būti sprendžiami teismuose.

2.3. Interneto turinio reguliavimas

Nors internete gausu naudingos informacijos, tačiau susiduriama ir su nepageidaujama informacija – informacija, darančia žalingą poveikį pažeidžiamoms socialinėms grupėms, visai visuomenei, taip pat informacija, kurios viešą skelbimą įstatymai riboja ar netgi draudžia. Nevaržomas tokios informacijos platinimas kelia pavojų demokratinėms teisėms ir laisvėms ar net tiesioginę grėsmę visuomenei. Šios priežastys lemia interneto turinio reglamentavimo priemonių pasirinkimą.

Tačiau bet kokia interneto turinio kontrolė kelia akivaizdžias asociacijas su cenzūra, gali riboti žodžio ir išraiškos laisvę, teisę į informaciją ir yra ypač pamėgta nedemokratiškose valstybėse, pavyzdžiui, Irane, Saudo Arabijoje, Kinijoje ar Baltarusijoje. Interneto turinio kontrolė gali būti naudojama ir bandant daryti įtaką visuomenės nuomonei ar palaikyti tam tikrą politinę jėgą ir pan.

Paminėtina ir tai, kad interneto turinio reglamentavimas galiausiai atsiremia į reguliuotino turinio apibrėžimo problemą. Reguliuotinas turinys skirtingose valstybėse ir kultūrose vertinamas labai nevienodai, pasireiškia „globalaus kaimo“ efektas. Šią situaciją puikiai iliustruoja 2000 m. spręsta teisminė byla Prancūzijoje – *Yahoo! Inc. v. La Ligue Contre le Racisme et l'Antisemitisme*. Šioje byloje Prancūzijos teismo sprendimas siekė apriboti JAV kompanijos *Yahoo!* teisę skelbti informaciją savo internetiniuose puslapiuose apie galimybes įsigyti fašistinės atributikos, kadangi tokia atributika ir su ja susijusi informacija yra neteisėti pagal Prancūzijos teisę ir, nors jie skelbiami *Yahoo!* vartotojų JAV ir kitose valstybėse, informaciją apie prekes gali matyti Prancūzijos gyventojai. Prancūzijos teismas argumentavo taip: jeigu žmogus gali matyti internetinį puslapį Prancūzijoje, tinklalapio operatorius turėtų atsakyti pagal Prancūzijos teisę, todėl įpareigojo *Ya-*

hoo! pašalinti informaciją, dėl kurios kilo ginčas, arba užblokuoti prieigą prie jos. Deja, toks Prancūzijos teismo sprendimas techniškai buvo ir yra neįgyvendintas. Atsižvelgdamas į tai JAV teismas (į kurį kreipėsi *Yahoo!,* siekdama išvengti Prancūzijos teismo sprendimo vykdymo) konstatavo, kad toks Prancūzijos teismo sprendimas nėra nei pripažintinas, nei įgyvendintinas JAV, nes jis prieštarauja JAV Konstitucijos pirmajai pataisai (žodžio ir išraiškos laisvė). Abu teismai iš esmės teisingai nustatė jurisdikcijos klausimą ir taikė savo nacionalinius įstatymus, nors tuo pačiu kilo didžiulė neišsprendžiama kolizija. Aptartą *Yahoo! Inc. v. La Ligue Contre le Racisme et l'Antisemitisme* konfliktą iš esmės lėmė nevienodas to paties interneto turinio vertinimas.

2.3.1. Interneto turinio tarptautinis reglamentavimas

Dėl interneto turinio reglamentavimo problemų šis klausimas iš esmės nereglamentuotas tarptautiniu mastu. Priimta tik regioninio ir rekomendacinio pobūdžio teisės aktų, kuriais siekiama nustatyti interneto turinio reglamentavimo gaires. Europos Sąjungoje priimta tik keli su interneto turinio reglamentavimu susiję rekomendaciniai teisės aktai:

- 1996 m. Europos Komisijos komunikatas apie neteisėtą ir žalingą turinį internete;
- 1996 m. spalio 23 d. Žalioji knyga apie nepilnamečių ir žmogiškojo orumo apsaugą teikiant garso, vaizdo ir informacijos paslaugas;
- Europos Parlamento ir Tarybos 1999 m. sausio 25 d. sprendimas Nr. 276/1999/EB, patvirtinantis ilgalaikį Bendrijos veiksmų planą, kaip skatinti saugiau naudotis internetu kovojant su neteisėtu ir žalingu tarptautinių tinklų turiniu;
- Europos Parlamento ir Tarybos 2000 m. birželio 8 d. direktyva Nr. 2000/31/EB dėl kai kurių informacinės visuomenės paslaugų, ypač elektroninės komercijos, teisinių aspektų vidaus rinkoje (Elektroninės komercijos direktyva).

Daugiausia dėmesio sprendžiant interneto turinio reguliavimo problemą Europos Sąjungoje yra skiriama savireguliacijai, pabrėžiama, kad interneto turinio reglamentavimas turi būti veiksmingas, objektyviai pagrįstas ir proporcingas, tinkamai suderinti teisiniai ir techniniai instrumentai.

Vienas iš esminių interneto turinio reglamentavimo principų yra informacinės visuomenės paslaugų teikėjų atsakomybės už interneto turinį apribojimas. Šis principas aiškiai įtvirtintas Europos Sąjungos direktyvoje Nr. 2000/31/EB dėl elektroninės komercijos ir išsamiau nagrinėjamas atskirame skyriuje.

Europos Taryba yra regioninė institucija, priėmusi rekomendacinio pobūdžio teisės aktų interneto turinio reglamentavimo srityje, tarp jų:

- 1997 m. spalio 30 d. rekomendaciją Nr. (97) 20 „Dėl nepakančių pasisakymų“;
- 1997 m. spalio 30 d. rekomendaciją Nr. (97) 21 „Dėl smurto rodymo elektroninėje žiniasklaidoje“;
- 2001 m. rugsėjo 5 d. rekomendaciją Nr. (2001) 8 „Dėl savireguliacijos ir vartotojų apsaugos nuo neteisėto ir žalingo turinio informacijos naujose komunikacijose ir teikiant informacines paslaugas“;
- 2003 m. gegužės 28 d. deklaraciją „Dėl teisės komunikuoti internetu“;
- 2001 m. lapkričio 23 d. konvenciją dėl nusikaltimų elektroninėje erdvėje;
- 2002 m. lapkričio 7 d. konvencijos dėl nusikaltimų elektroninėje erdvėje papildomą protokolą.

2003 m. gegužės 28 d. deklaracijoje „Dėl teisės komunikuoti internetu“ taip pat skatinama savireguliacija siekiant išvengti neteisėto ar žalingo turinio informacijos internete, tačiau pabrėžiama būtinybė vengti tokių interneto turinio reguliavimo metodų, kurie riboja visuomenės galimybes gauti vieną ar kitą informaciją ir varžo bendravimą internetu (išskyrus turinio kontrolės priemonių diegimą bibliotekose, mokyklose, švietimo bei mokslo institucijose, siekiant apsaugoti nepilnamečius nuo neigiamos žalingos informacijos poveikio).

2001 m. lapkričio 23 d. Europos Tarybos konvencija dėl nusikaltimų elektroninėje erdvėje specialiai reglamentuoja veikas, susijusias su draudžiamu interneto turiniu, konkrečiai – vaikų pornografija. Sąvoka vaikų pornografija reiškia pornografinę medžiagą, vizualiai vaizduojančią aiškiai seksualų nepilnamečio elgesį; aiškiai seksualų asmens, atrodančio kaip nepilnametis, elgesį; tikroviškus vaizdus, rodančius aiškiai seksualų nepilnamečio elgesį. Konvencijoje rekomenduojama tiesiogiai uždrausti tokio interneto turinio medžiagos gaminimą, talpinimą ir platinimą internetu bei kitus veiksmus, aptartus žemiau.

Siekiant reglamentuoti (kriminalizuoti) interneto turinį, susijusį su rasinės ir tautinės neapykantos kurstymu, 2002 m. lapkričio 7 d. buvo priimtas Europos Tarybos konvencijos dėl elektroninių nusikaltimų papildomas protokolas. Protokole rasinę ir tautinę neapykantą kurstanti informacija apibrėžiama kaip bet koks rašytinis, vizualinis ar kitoks pateikimas minčių ir teorijų, propaguojančių diskriminaciją ar smurtą prieš individą ar jų grupes, išsiskiriančias dėl savo rasės, tikėjimo, politinių pažiūrų ir pan.

Reguliuotinu interneto turiniu laikytina ir nepageidaujama reklaminė informacija (angl. *spam*), kuri išsamiau aptarta žemiau.

2.3.2. Bendrieji interneto turinio reguliavimo principai

Neteisėtu interneto turiniu paprastai laikoma įstatymais draudžiama informacija, susijusi su nepilnamečių pornografija, nusikaltimais (tarp jų – su terorizmu, sabotažu, žudymu, šmeižtu, sukčiavimu bei kitais), informacija apie privatų asmens gyvenimą, rasistinio, ekstremistinio, fašistinio ir panašaus turinio informacija.

Žalinga ir nepageidaujama yra laikoma tokio turinio informacija, kuri gali turėti neigiamą poveikį nepilnamečiams ar kitoms jautrioms socialinėms grupėms, pavyzdžiui, pornografija, erotinio ar smurtinio pobūdžio informacija, informacija apie alkoholį, tabaką ar kitas ribojamas medžiagas.

Apibendrinant interneto turinio teisinį reguliavimą išskirtinos šios teisinio reguliavimo tendencijos:

- iki interneto atsiradimo galiojusių teisės aktų, reglamentuojančių informacijos naudojimą, pritaikymas publikuojant ir tvarkant informaciją internete;
- interneto paslaugų teikėjų atsakomybės reglamentavimas;
- savireguliavimo priemonių skatinimas;
- specifinių teisių ir pareigų interneto paslaugų teikėjams nustatymas specialiaisiais teisės norminiais aktais siekiant užtikrinti veiksmingą nusikaltimų tyrimą, kovą su tarptautiniu terorizmu, nacionalinio bei visuomenės saugumo bei kitų interesų apsaugą.

2.3.3. Interneto turinio reguliavimas Lietuvoje

Šiuo metu žalingo turinio ir neskelbtinos informacijos viešą skelbimą Lietuvoje reglamentuoja:

- 2000 m. rugpjūčio 29 d. Lietuvos Respublikos visuomenės in-

formavimo įstatymas Nr. VIII-1905;
- 1996 m. kovo 14 d. Lietuvos Respublikos vaiko teisių apsaugos įstatymas Nr. I-1234;
- 2002 m. rugsėjo 10 d. Lietuvos Respublikos nepilnamečių apsaugos nuo neigiamo viešosios informacijos poveikio įstatymas Nr. IX-1067;
- 2004 m. balandžio 15 d. Lietuvos Respublikos elektroninių ryšių įstatymas Nr. IX-2135;
- 1999 m. lapkričio 25 d. Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymas Nr. VIII-1443;
- 2003 m. kovo 5 d. Lietuvos Respublikos Vyriausybės nutarimas Nr. 250 „Dėl viešo naudojimo kompiuterių tinkluose neskelbtinos informacijos kontrolės ir ribojamos viešosios informacijos platinimo tvarkos patvirtinimo“;
- 2006 m. gegužės 25 d. Lietuvos Respublikos informacinės visuomenės paslaugų įstatymas Nr. X-614.

Vienas iš svarbiausių Lietuvos Respublikos teisės aktų, reglamentuojančių neskelbtinos ir žalingo turinio informacijos naudojimą, yra Lietuvos Respublikos visuomenės informavimo įstatymas, kurio 19 straipsnyje nurodyta, kad draudžiama skelbti informaciją, kuria:

1) raginama prievarta keisti Lietuvos Respublikos konstitucinę santvarką;
2) skatinama kėsintis į Lietuvos Respublikos suverenumą, jos teritorijos vientisumą, politinę nepriklausomybę;
3) kurstomas karas ar neapykanta, tyčiojimasis, niekinimas, kurstoma diskriminuoti, smurtauti, fiziškai susidoroti su žmonių grupe ar jai priklausančiu asmeniu dėl lyties, seksualinės orientacijos, rasės, tautybės, kalbos, kilmės, socialinės padėties, tikėjimo, įsitikinimų ar pažiūrų;
4) platinama, propaguojama ar reklamuojama pornografija, taip pat propaguojamos ir (ar) reklamuojamos seksualinės paslaugos, lytiniai iškrypimai;
5) propaguojami ir (ar) reklamuojami žalingi įpročiai, narkotinės ar psichotropinės medžiagos;
6) platinama dezinformacija ir informacija, šmeižianti, įžeidžianti žmogų, žeminanti jo garbę ir orumą;
7) pažeidžiama nekaltumo prezumpcija bei kliudoma teisminės valdžios nešališkumui.

Viešoji informacija, susijusi su erotiniu, smurtiniu turiniu, alkoholio ar tabako reklama ir vartojimu, bei kita nepilnamečių fizinei, protinei ir dorovinei raidai kenkianti informacija priskiriama prie ribojamos viešosios informacijos.

Erotinio pobūdžio informacija įstatyme įvardijama kaip informacija, kuria skatinamas lytinis geismas, rodomas tikras ar suvaidintas lytinis aktas ar kitoks seksualinis pasitenkinimas arba sekso reikmenys. Pornografinio pobūdžio informacija yra laikoma informacija, kai atvirai ir detaliai rodomas tikras ar suvaidintas lytinis aktas, lytiniai organai, tuštinimasis, masturbacija arba lytiniai iškrypimai (pedofilija, sadizmas, mazochizmas, zoofilija, nekrofilija ir kt.), ir tai yra pagrindinis tokios informacijos tikslas. Smurtinio pobūdžio informacija yra informacija, kai detaliai rodomas žmonių, gyvūnų žudymas, žalojimas, kankinimas ar kitoks prieš žmogų, bet kokią kitą gyvą būtybę nukreiptas elgesys, sukeliantis skausmą, diskomfortą arba darantis kitokią žalą (fizinę, psichologinę, materialinę), taip pat vandalizmas ir (ar) teigiamai vertinama, skatinama prievarta, žiaurumas ar mėgavimasis tuo.

Lietuvos Respublikos visuomenės informavimo įstatyme internetinėmis visuomenės informavimo priemonėmis (informacinės visuomenės informavimo priemonėmis) laikomos visos informavimo priemonės, įprastai už atlyginimą teikiančios informaciją elektroniniu būdu ir per atstumą individualiu vartotojo prašymu. Lietuvos Respublikos Vyriausybės 2003 m. kovo 5 d. nutarimu Nr. 250 patvirtintoje Viešo naudojimo kompiuterių tinkluose neskelbtinos informacijos kontrolės ir ribojamos viešosios informacijos platinimo tvarkos 4 punkte elektroninės visuomenės informavimo priemonės suprantamos kaip visuomenės informavimo priemonių (spaudos leidinių, televizijos, radijo) interneto tinklalapiai, kuriuose elektronine forma perteikiama viešoji informacija. Tačiau elektroninėmis visuomenės informavimo priemonėmis nelaikomi valstybės institucijų ir įstaigų, valstybės pareigūnų ir valstybės tarnautojų (darbuotojų) interneto tinklalapiai, skirti platinti oficialius dokumentus ir informaciją apie valstybės institucijos darbą, taip pat asmenų privatūs interneto tinklalapiai, kuriuose pateikta informacija apie interneto tinklalapių įkūrėjus, jų duomenys, kūriniai, informacija apie jų gaminamą ir parduodamą produkciją, teikiamas paslaugas ir panašiai. Tokiu būdu didelė dalis interneto tinklalapių, kuriuose gali būti pateikta neskelbtinos ar ribotinos informacijos, lieka neprižiūrima.

Viešo naudojimo kompiuterių tinkluose neskelbtinos informacijos kontrolės ir ribotinos viešosios informacijos platinimo tvarkos 5 punktas draudžia viešo naudojimo kompiuterių tinkluose skelbti ir platinti neskelbtiną ar žalingo turinio informaciją, nustatytą Lietuvos Respublikos įstatymuose.

Be to, pagal šią tvarką draudžiama neskelbtiną ar ribojamą viešąją informaciją laikyti laisvai prieinamą Lietuvos Respublikos teritorijoje esančiose tarnybinėse stotyse, skleisti elektroninėse konferencijose, siųsti elektroniniu paštu neapibrėžtam gavėjų skaičiui arba kitaip platinti viešojo naudojimo kompiuterių tinkluose, kai ribojama viešoji informacija gali tapti laisvai prieinama nepilnamečiams. Pateikiant ribojamą viešąją informaciją interneto tinklalapiuose turi būti pridėtas įspėjamasis užrašas lietuvių ir anglų kalbomis apie tai, kad pateikta informacija skiriama tik pilnamečiams.

Viešo naudojimo kompiuterių tinkluose neskelbtinos informacijos kontrolės ir ribojamos viešosios informacijos platinimo tvarka įpareigoja informacijos prieglobos paslaugų teikėjus (angl. *hosting*) teisės aktų nustatyta tvarka neatlygintinai teikti operatyvinės veiklos subjektams informaciją, fiksuojamą savo ūkinei veiklai užtikrinti, įskaitant paslaugų, susijusių su informacijos priegloba tarnybinėje stotyje, sisteminių įrašų bylas, taip pat asmenų, kuriems informacijos prieglobos paslaugų teikėjas teikia nuolatines paslaugas, duomenis.

Pagrindinis Lietuvos Respublikos vaiko teisių apsaugos įstatymo ir Lietuvos Respublikos nepilnamečių apsaugos nuo neigiamo viešosios informacijos poveikio įstatymo principas – apsauga nuo neigiamos socialinės aplinkos įtakos. Lietuvos Respublikos nepilnamečių apsaugos nuo neigiamo viešosios informacijos poveikio įstatymo 4 straipsnyje nurodoma informacija, kuri turi būti draudžiama arba ribojama: viešoji informacija, susijusi su fizinio ar psichinio smurto vaizdavimu, informacija, kurioje rodomas mirusio arba žiauriai sužaloto žmogaus kūnas, išskyrus atvejus, kai toks rodymas reikalingas tapatybei nustatyti; taip pat informacija, kurioje palankiai vertinama priklausomybė nuo narkotinių, psichotropinių medžiagų, tabako ar alkoholio, skatinamas jų vartojimas, gamyba, platinimas ar įsigijimas, kurioje teigiamai vertinama nusikalstama veika ar idealizuojami nusikaltėliai, kurioje kurstoma diskriminacija dėl tautybės, rasės, lyties, kilmės, neįgalumo, lytinės orientacijos, religijos ar kitokios priklausomybės, kurioje dažnai vartojami nešvankūs posakiai, žodžiai ar gestai. Be anksčiau minėtos informacijos, ribojama erotinio pobūdžio, su-

kelianti baimę ar siaubą, skatinanti savęs žalojimą ar savižudybę informacija.

Pagal Lietuvos Respublikos nepilnamečių apsaugos nuo neigiamo viešosios informacijos poveikio įstatymo 5 straipsnį neigiamą poveikį nepilnamečio raidai darančia ir draudžiama informacija taip pat laikoma viešoji informacija, kurioje:

1) siejant su nusikalstama veika ar kitais teisės pažeidimais skelbiami nuo teisėsaugos institucijų ar teismo besislapstančio įtariamojo padarius nusikaltimą, kaltinamojo, teisiamojo, nuteistojo ar nuo nusikalstamos veikos arba kitų teisės pažeidimų nukentėjusio nepilnamečio asmens duomenys, pagal kuriuos galima nustatyti jo asmens tapatybę;
2) skelbiami save sužalojusio ar mėginusio tai padaryti, nusižudžiusio ar mėginusio nusižudyti nepilnamečio asmens duomenys, pagal kuriuos galima nustatyti jo asmens tapatybę;
3) pateikiant duomenis apie nepilnametį žeminamas jo orumas ir (ar) pažeidžiami jo interesai;
4) piktnaudžiaujant nepilnamečių pasitikėjimu ir nepatyrimu neigiamų socialinių reiškinių kontekste pateikiamos nepilnamečių nuomonės ir vertinimai, taip pat jų nuotraukos ar filmuota medžiaga apie juos; išskyrus atvejus, kai jos turinį sudaro tik informacija apie įvykius, politinius, socialinius, religinius įsitikinimus ar pasaulėžiūrą, ši informacija yra reikšminga moksliniu ar meniniu požiūriu arba reikalinga tyrimams ar mokymui, yra viešasis interesas ją skelbti, jos apimtis ir poveikis yra mažareikšmiai.

Lietuvos Respublikos nepilnamečių apsaugos nuo neigiamo viešosios informacijos poveikio įstatyme nurodyta neskelbtina ir ribotai skelbtina informacija iš esmės atitinka Lietuvos Respublikos visuomenės informavimo įstatyme pateiktą neskelbtinos informacijos apibrėžimą. Tačiau nei Lietuvos Respublikos nepilnamečių apsaugos nuo neigiamo viešosios informacijos poveikio įstatyme, nei Lietuvos Respublikos visuomenės informavimo įstatyme pateikti neskelbtinos informacijos apibrėžimai išsamiai nenurodo, kokio turinio informacijos skelbimas turėtų būti ribojamas ar draudžiamas. Nepakankamai apibrėžta erotinio pobūdžio, sukelianti baimę ar siaubą, taip pat skatinanti alkoholio ar tabako gaminių vartojimą ir kita informacija.

Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymas reguliuoja valstybės paslapčių (politinių, ekonominių, karinių, teisėtvarkos, mokslo ir technikos duomenų, kurių praradimas arba neteisėtas atskleidimas gali pažeisti Lietuvos Respublikos suverenitetą, gynybinę ar ekonominę galią, pakenkti Lietuvos Respublikos konstitucinei santvarkai, politiniams interesams, sukelti pavojų žmogaus gyvybei bei sveikatai, jo konstitucinėms teisėms) ir tarnybos paslapčių (politinių, ekonominių, karinių, teisėtvarkos, mokslo ir technikos duomenų, kurių platinimas ribojamas dėl valstybės bei jos institucijų interesų, taip pat siekiant apsaugoti žmogaus konstitucines teises) apsaugą. Pagal šio įstatymo 7 straipsnį paslapčių subjektai (valstybės, savivaldos institucijos bei jų steigiamos įmonės ir įstaigos, kurių veikla yra susijusi su įslaptintos informacijos naudojimu ar jos apsauga ir kurioms šio įstatymo nustatyta tvarka suteikiama teisė įslaptinti bei išslaptinti informaciją), atlikdami jiems pavestas funkcijas, turi teisę sudaryti sandorius su įmonėmis, įstaigomis bei organizacijomis, kurios nėra paslapčių subjektai, dėl tam tikrų darbų ar gaminių, kuriuose yra įslaptintos informacijos, atlikimo ar sukūrimo. Tokiu būdu paslapčių subjektai yra atsakingi už neskelbtinos informacijos platinimo kontrolę, įskaitant ir tokios informacijos platinimą informacinėmis technologijomis. Tokiais atvejais perdavę įslaptintą informaciją jie privalo kontroliuoti perduotos informacijos apsaugą ir užtikrinti, kad visi asmenys, susiję su neskelbtinos informacijos apsauga, turėtų atitinkamus leidimus dirbti ar susipažinti su šia informacija.

Lietuvoje už minėtuose įstatymuose numatytos tvarkos pažeidimą (įskaitant ir šios tvarkos pažeidimą interneto aplinkoje) atsakomybę nustato Lietuvos Respublikos administracinių teisės pažeidimų, baudžiamasis, civilinis kodeksai.

Lietuvos Respublikos administracinių teisės pažeidimų kodekso 214 straipsnyje numatyta atsakomybė už viešai neskelbtinos informacijos platinimą. Administracine tvarka baudžiama už Lietuvos Respublikos Vyriausybės 1996 m. rugsėjo 25 d. nutarimu Nr. 1111 patvirtintos Erotinio ir smurtinio pobūdžio spaudos leidinių, kino filmų ir videofilmų, radijo ir televizijos programų platinimo tvarkos pažeidimą, tačiau nieko nekalbama apie atsakomybę už tokio paties turinio informacijos platinimą internete. Vadovaujantis funkcinio lygiavertiškumo principu į šios normos sritį realiai patenka tik internete platinami erotinio ir smurtinio pobūdžio kino filmai ir vaizdajuostės.

Administracinių teisės pažeidimų kodekso 214(4) straipsnis numato atsakomybę už informacijos apie tabako gaminius ir alkoholinius gėrimus teikimo tvarkos pažeidimą, 214(6) straipsnis – už Respublikos Prezidento įžeidimą arba šmeižimą masinės informacijos priemonėse, 214(8) straipsnis – už įstatymų uždraustos reklamos ir informacijos, uždraustos ar neteisėtos veiklos reklamos ir informacijos apie šią veiklą arba prekių ar paslaugų, kurių gamyba ir pardavimas yra įstatymų uždrausti, reklamos skleidimą visuomenės informavimo priemonėse.

Lietuvos Respublikos baudžiamajame kodekse numatyta baudžiamoji atsakomybė už tokias su viešai neskelbtinos informacijos platinimu susijusias veikas:

1) viešus raginimus smurtu pažeisti Lietuvos Respublikos suverenitetą;
2) Valstybės paslapties atskleidimą;
3) Valstybės paslapties praradimą;
5) mažamečio asmens tvirkinimo veiksmus;
6) tikrovės neatitinkančios informacijos apie kitą žmogų, galinčios paniekinti ar pažeminti tą asmenį arba pakirsti pasitikėjimą juo, skleidimą;
7) įžeidimą;
8) neteisėtą informacijos apie asmens privatų gyvenimą atskleidimą ar naudojimą;
9) kurstymą prieš bet kokios tautos, rasės, etninę, religinę ar kitokią žmonių grupę;
10) skatinimą vartoti narkotines ar psichotropines medžiagas;
11) pornografinio turinio produkcijos gaminimą, platinimą, viešą demonstravimą. Atsakomybė už šių veikų atlikimą priklauso nuo nusikaltimo ar nusižengimo pobūdžio ir svyruoja nuo baudos iki laisvės atėmimo.

2.3.4. Interneto turinio reguliavimo perspektyvos

Išnagrinėjus esamas teisines interneto turinio reguliavimo priemones akivaizdu, kad praktinis informacijos turinio reguliavimo priemonių taikymas yra ypač sudėtingas dėl reguliuotino turinio neapibrėžtumo ir subjektyvių kriterijų, kuriais remiantis išskiriamas žalingas ir nepageidaujamas interneto turinys. Aptartas *Yahoo! Inc. v. La Ligue Contre le Racisme et l'Antisemitisme* atvejis parodo šių kriterijų

nevienareikšmį vertinimą. Paminėtina ir tai, kad priverstinis ir visa apimantis interneto turinio reguliavimas nei teisiškai, nei techniškai nėra įmanomas, bet to, yra sunkiai suderinamas su pamatinėmis demokratinėmis vertybėmis. Daugelyje valstybių interneto turinio reguliavimas iš esmės yra savanoriškas, pagrįstas savitvarka ir įgyvendinamas techninėmis priemonėmis – specialiais interneto turinio filtrais. Deja, tokios techninės priemonės – filtruojanti programinė įranga – nėra tobulos, jas reikia specialiai pritaikyti pagal jų naudojimo kontekstą ir tikslus, jos atmeta dalį pageidaujamo interneto turinio (pvz., erotinio turinio filtrai blokuoja turinį, skirtą AIDS prevencijai), taip pat neatpažįsta dalies nepageidaujamo turinio.

Apskritai interneto turinio reguliavimas yra naujas reiškinys, ne visuomet nuoseklus. Lietuvoje šiuo metu neveikia ir menkai pripažįstama savireguliacija kaip alternatyva vyriausybiniam reguliavimui. Iš kitos pusės, dauguma Lietuvos interneto paslaugų teikėjų taiko individualius interneto turinio reguliavimo mechanizmus, veiksmingai reaguoja į pranešimus apie neteisėtą ir žalingą interneto turinį.

Bendra yra tai, kad internetui bandoma pritaikyti tradicinėms visuomenės informavimo priemonėms taikomas normas, bet tai ne visuomet įmanoma. Taip pat reikia pripažinti, kad veiksmingos ir visa apimančios interneto turinio reguliavimo teisinės ar techninės priemonės šiuo metu dar nesukurtos.

2.4. Interneto jurisdikcija

Jurisdikcija nusprendžia, kurios valstybės teisė bus taikoma ir kurios valstybės teismai spręs ginčą. Atsižvelgus į pasaulinį elektroninės erdvės pobūdį valstybių teisės taikymas internete yra viena iš esminių ir iki šiol neišspręstų teisės problemų. Internete jurisdikciją sunkina tai, kad labai dažnai elektroninė informacija, prekės ir paslaugos, jų teikėjas ir vartotojas yra skirtingose valstybėse ir vadovaujasi skirtingomis taisyklėmis. Neretai pasitaiko, kai internete platinama informacija, prekės ir paslaugos, kurios tam tikroje valstybėje yra draudžiamos ar ribojamos. Šioje situacijoje būtina įvertinti nacionalinės teisės taikymo internete galimybes, taip pat specifines interneto jurisdikcijos perspektyvas.

Tradiciškai jurisdikcija suprantama kaip veikianti valstybės teritorijoje, todėl apibrėžti tinkamą ginčo nagrinėjimo vietą bei taikytiną teisę pasauliniame teritorinių ribų neturinčiame internete galbūt net

neįmanoma. Pagal nacionalinę teisę jurisdikcijos klausimai sprendžiami remiantis šalių įstatymais, dvišalėmis ar daugiašalėmis tarptautinėmis sutartimis.

Tarptautinė teisė pripažįsta du pagrindinius jurisdikcijos principus:

- pilietybės;
- teritorijos.

Galimi ir kiti teisminio priklausymo variantai, pavyzdžiui, universaliosios jurisdikcijos principas, pagal kurį ginčas gali būti nagrinėjamas bet kurioje pasaulio valstybėje. Deja, elektroninė erdvė neturi „centrinės valdžios“, nėra visuotinių tarptautinių sutarčių dėl jos statuso (kaip dėl kitų bendrų erdvių – kosmoso ar Antarktidos teritorijos – statuso).

Tradicinės jurisdikcijos požiūriu bet kurį teisinį santykį galima lokalizuoti, t. y. vadovaujantis iš anksto apibrėžtais kriterijais susieti jį su konkrečios valstybės teisės sistema. Toks susiejimas atliekamas per iškilusio ginčo objektą, subjektą, veiką, papildomus kriterijus. Vadovaujantis funkcinio lygiavertiškumo principais, taip pat jurisdikcija turėtų būti taikoma ir elektroniniams, ir įprastiems teisiniams santykiams, jei jų esmė yra tokia pati. Funkcinio lygiavertiškumo principas taikomas reglamentuojant didelę dalį tradicinių teisinių santykių, kai jie atliekami elektroninėje erdvėje, pavyzdžiui, baudžiamojoje teisėje iš esmės priimtas principas, kad asmuo, padaręs teisės pažeidimą elektroninėje erdvėje, gali būti teisiamas tos valstybės, kurioje būdamas įvykdė tą nusikaltimą, teisme ir pagal tos valstybės įstatymus. Kitaip tariant, tai – nusikaltimo vietos, akto atlikimo vietos principas (lot. *lex loci actus*). Deja, jį taikyti elektroninėje erdvėje nėra paprasta dėl nusikaltimo vietos fakto nustatymo problemų bei galimybių dirbtinai išvengti atsakomybės specialiai atliekant veiksmus parankioje jurisdikcijoje (tai – įprasta praktika norint paslėpti nusikaltimo pėdsakus).

Kitas bendras principas įprastas nacionalinėse teisės sistemose – atsakovo ar vienos iš sutarties šalių gyvenamoji vieta (buveinė). Pagal tradicinį šio principo taikymą civiliniame procese ginčas bus sprendžiamas toje valstybėje ar net vietovėje, kurioje gyvena atsakovas. Deja, elektroninėje erdvėje galimi dideli atstumai tarp ieškovo ir atsakovo, todėl šį principą taikyti būtų tiesiog neracionalu ar neįmanoma.

Pastebima tendencija, kad tarptautinė teisė pereina nuo griežto, formalaus reglamentavimo prie lanksčių kolizinių normų, vis labiau toleruojamas glaudžiausio ryšio (*lex convienens*, angl. *proper law*), ša-

lių valios autonomijos (*lex voluntatis*) taisyklių taikymas. Pagal pirmąjį, glaudžiausio ryšio, principą kilęs ginčas turėtų būti sprendžiamas toje valstybėje, kuri glaudžiausiai susijusi su teisiniu santykiu. Pagal antrąjį principą ginčas bus sprendžiamas šalių susitarimu pasirinktoje valstybėje. Šie principai yra bene vieninteliai lengvai pritaikomi elektroninėje erdvėje, tačiau jie nėra tinkami sprendžiant viešosios teisės jurisdikcijos klausimus. Priklausomai nuo teisinio santykio rūšies ir konkrečių aplinkybių elektroninėje erdvėje galėtų būti taikomos ir kitos tradicinės jurisdikcijos taisyklės, tarp jų – žalos padarymo vietos teisė, daikto buvimo vietos teisė ir kt.

Minėti tarptautinės teisės jurisdikcijos principų pavyzdžiai rodo ir galimybes juos taikyti elektroninėje erdvėje, ir su tuo susijusias problemas. Visais atvejais būtina suvokti, kad internete galimos situacijos, kai tradicinių nacionalinių jurisdikcijos principų taikymas veda į aklavietę dėl esamų kultūrinių skirtumų ir elektroninės erdvės globalumo, t. y. pasireiškia „globalaus kaimo“ efektas. Šią situaciją puikiai iliustruoja 2000 m. spręsta teisminė byla Prancūzijoje – *Yahoo! Inc. v. La Ligue Contre le Racisme et l'Antisemitisme*.

Dėl aukščiau minėtų situacijų teisės moksle jau senokai diskutuojama apie specialiosios interneto jurisdikcijos perspektyvas tapatinant jas su jurisdikcijos taisyklėmis, taikomomis dėl naudojimosi tarptautiniais vandenimis, kosmosu ar Antarktidos teritorija. Nustačius specialiąją interneto jurisdikciją, valstybės neturės spręsti, ar jų įstatymai yra taikomi nagrinėjant konkretų ginčą, bus užtikrintas didesnis saugumas, griežčiau apibrėžta atsakomybė. Deja, praktiškai tai yra beveik neįgyvendinama dėl tų pačių kultūrinių skirtumų tarp valstybių ir negalėjimo šias taisykles įgyvendinti visame pasaulyje. Iš kitos pusės speciali interneto jurisdikcija pripažinta ir iš dalies įsitvirtino tose srityse, kuriose valstybių nacionalinė jurisdikcija (ir nacionalinis reglamentavimas) tik pakartojo interneto bendruomenės nustatytas taisykles ir taikė bendruosius teisės principus, pavyzdžiui, sprendžiant ginčus dėl interneto domenų vardų.

Kur kas priimtinesnis interneto jurisdikcijos modelis yra tradicinių jurisdikcijos principų papildymas (bet ne pakeitimas) specialiaisiais interneto jurisdikcijos principais. Europos Sąjungos direktyva Nr. 2000/31/EB dėl elektroninės komercijos yra vienas iš pirminių specialiųjų interneto jurisdikcijos principų šaltinių. Pagrindinis jurisdikcijos principas, suformuluotas šioje direktyvoje, yra informacinės visuomenės paslaugų kilmės principas, teigiantis, kad paslaugų teikėjui (asmeniui, teikiančiam paslaugas elektroninėje erdvėje) paprastai taiko-

mi tos valstybės, kurioje jis faktiškai veikia (yra įsisteigęs), bet ne tos valstybės, kurioje fiziškai yra interneto serveris ar tinklalapis, kurių pagalba vykdoma veikla, įstatymai. Šis principas nėra absoliutus.

Direktyva numato kilmės principo išimtis, pvz., jurisdikcijos kilmės principas gali būti netaikomas:

- dėl viešosios tvarkos, viešojo saugumo, visuomenės sveikatos ir vartotojų apsaugos interesų;
- jei paslaugos yra žalingos arba kelia žalą vienam ar daugiau išvardintų objektų;
- kai valstybių narių taisyklės yra būtinos ir proporcingos minėtų objektų atžvilgiu.

2.4.1. Interneto jurisdikcijos reglamentavimas Lietuvoje

Kadangi Lietuva yra Europos Sąjungos narė, Lietuvoje interneto jurisdikcijos klausimai iš esmės sprendžiami remiantis minėtoje Europos Sąjungos direktyvoje Nr. 2000/31/EB dėl elektroninės komercijos įtvirtintu kilmės principu, taip pat nacionaline teise, dvišalėmis bei daugiašalėmis tarptautinėmis sutartimis. Atskirai reikėtų paminėti Lietuvos Respublikos civiliniame kodekse įtvirtintas tarptautinės privatinės teisės nuostatas, nurodančias konkretiems teisiniams santykiams taikytiną teisę. Nors daugelyje šių taisyklių nepaminėti elektroninės erdvės teisiniai santykiai, tačiau jos turėtų būti taikomos ir teisiniams santykiams elektroninėje erdvėje. Bendrųjų jurisdikcijos principų tęstinumas taikomas ir pagal Lietuvos baudžiamuosius bei administracinius įstatymus.

Lietuvoje taip pat ratifikuota 2001 m. lapkričio 23 d. Europos Tarybos konvencija dėl elektroninių nusikaltimų, kurioje nustatytos specialiosios jurisdikcijos taisyklės nusikaltimams elektroninėje erdvėje, – iš esmės įtvirtinamas pažeidimo vietos padarymo principas, o ypatingai sunkiems nusikaltimams – ir universalios jurisdikcijos taisyklę, pagal kurią kiekviena valstybė turi teisę taikyti atsakomybę.

2.5. Interneto tarpininkų veiklos reglamentavimas

Interneto tarpininkais galima laikyti visus subjektus, užtikrinančius interneto techninės infrastruktūros funkcionavimą, tarp jų – subjektus, teikiančius interneto prieigos, prieglobos, turinio talpinimo ir perdavimo paslaugas. Faktiškai interneto tarpininkai yra interneto prieigos paslaugų teikėjai, įvairūs interneto portalai, kuriuose vartotojai

gali pateikti savo informaciją (pvz., failus, komentarus ir pan.). Universitetas taip pat yra interneto tarpininkas, kadangi teikia interneto prieigos, elektroninio pašto, tinklalapių talpinimo paslaugas darbuotojams ir studentams.

Be interneto tarpininkų interneto funkcionavimas nebūtų įmanomas, kadangi interneto vartotojai gali prisijungti prie interneto, siųsti ir talpinti informaciją tik per interneto tarpininkus, tiesioginis vartotojo prisijungimas iš esmės yra negalimas. Bet ir pats interneto vartotojas, kuris sudaro galimybes savo administruojamame tinklalapyje kitiems asmenims talpinti ar saugoti informaciją (pvz., komentarus), tampa interneto tarpininku. Asmuo – interneto vartotojas, kuris talpina savo informaciją arba paties parinktą kitų asmenų informaciją, t. y. pats talpina, siunčia, saugo informaciją arba ją kontroliuoja, nelaikomas interneto tarpininku, nes minėti veiksmai tarpininkavimui nebūdingi.

Interneto tarpininkas neprivalo kontroliuoti ir tikrinti informacijos, kurią interneto tarpininko paslaugų gavėjai (vartotojai) siunčia, gauna, talpina, saugo naudodamiesi interneto tarpininko infrastruktūra, todėl interneto tarpininko ir jo teikiamų paslaugų vartotojų santykiai iš esmės yra anonimiški. Jei interneto tarpininkas žino ir kontroliuoja jo infrastruktūroje esantį interneto turinį, jis laikomas atsakingu už tokį turinį. Tik kilus konfliktinei situacijai interneto tarpininkas privalo imtis interneto turinio reguliavimo veiksmų. Interneto tarpininkas laikomas infrastruktūros teikėju taip pat, kaip telekomunikacijų operatorius ir iš esmės neatsako už vartotojų neteisėtą naudojimąsi šia infrastruktūra.

Pagal direktyvoje Nr. 2000/31/EB dėl elektroninės komercijos įtvirtintus principus interneto tarpininkai yra atsakingi už visą medžiagą, kuri yra patalpinta jų internetiniuose serveriuose ar tinklalapiuose, tik tuo atveju, jeigu paslaugų teikėjai apie šią informaciją žino ir šią informaciją kontroliuoja.

Išimtys nustatytos tik interneto tarpininkams (kaip informacinės visuomenės paslaugų teikėjams), kurie teikia informacijos perdavimo ar talpinimo paslaugas – t. y. iš esmės tarpininkauja vartotojams ir interneto turinio teikėjams. Tačiau tokiems interneto tarpininkams taip pat gali tekti prisiimti atsakomybę, jei jie žinojo apie pažeidimą, tačiau nesiėmė jokių veiksmų tam pažeidimui pašalinti ar kitaip prisidėjo prie pažeidimo. Šie principai pirmąkart suformuluoti Jungtinių Amerikos Valstijų teisėje, vėliau priimti ir kitose valstybėse, tarp jų – Europos Sąjungos valstybėse. Šiuo metu šie principai Lietuvoje išsa-

miai reglamentuoti Lietuvos Respublikos informacinės visuomenės paslaugų įstatyme.

Informacinės visuomenės paslaugų įstatyme ir Europos Sąjungos elektroninės komercijos direktyvoje vartojama informacinės visuomenės paslaugų teikėjo sąvoka nėra tapati interneto tarpininko sąvokai. Pavyzdžiui, elektroninėje komercijoje informacinės visuomenės paslaugų teikėju gali būti laikomas bankas, per kurį vykdomi elektroniniai atsiskaitymai, transportavimo įmonė, pristatanti prekę, ir pan. Informacinės visuomenės paslaugų teikėjo sąvoka yra daug platesnė, apimanti įvairias paslaugas, teikiamas per atstumą elektroninėje erdvėje, tačiau pagrindiniai reglamentavimo principai, susiję su atsakomybe už interneto vartotojų (informacinės visuomenės paslaugos gavėjų) siunčiamą ar saugomą interneto turinį, yra taikomi interneto tarpininkams.

Interneto tarpininkai neprivalo tikrinti ir kontroliuoti jų tinklais perduodamą ir jų serveriuose talpinamą turinį ir už jį neatsako, jei informacinės visuomenės paslaugų (t. y. prieigos ar talpinimo paslaugų) teikėjas:

- neinicijuoja informacijos perdavimo;
- neparenka informacijos gavėjo;
- neparenka ir nekeičia informacijos;
- neturi faktinių žinių apie neteisėtą informaciją;
- sužinojęs apie neteisėtą informaciją, ją pašalina arba užblokuoja priėjimą prie jos.

Šie atsakomybės ribojimo principai taikomi ir tuo atveju, kai perduotos informacijos saugojimas yra automatinis, tarpinis ir trumpalaikis, t. y. skirtas tik tam, kad informacija būtų apskritai perduota elektroninių ryšių tinklu, jeigu informacija nėra saugoma ilgiau, negu pagrįstai būtina, kad ji būtų perduota. Tarpininkas, perduodantis informaciją elektroninių ryšių tinklu, neatsako už automatinį, tarpinį ir laikiną tos informacijos saugojimą, skirtą tik tam, kad vėlesnis tos informacijos perdavimas kitiems jos prašantiems paslaugos gavėjams būtų veiksmingas, jeigu paslaugos teikėjas atitinka minėtas sąlygas, be to, laikosi savo verslo srityje įprastų informacijos atnaujinimo taisyklių, nekliudo teisėtai naudotis technologija, kuri šioje verslo srityje yra pripažįstama ir naudojama siekiant gauti duomenų apie informacijos naudojimą. Neteisėtu būdu įgytos, sukurtos, pakeistos ar naudojamos informacijos panaikinimo tvarka, taip pat kriterijai, kada paslaugos teikėjas laikomas sužinojęs apie neteisėtą paslaugos gavėjo veiklą arba

apie tai, kad paslaugos gavėjo pateikta informacija įgyta, sukurta, pakeista ar naudojama neteisėtu būdu, šiuo metu nėra reglamentuoti.

Informacinės visuomenės paslaugų teikėjai (ir interneto tarpininkai) turi reaguoti į suinteresuotų asmenų pretenzijas dėl neteisėtos informacijos saugojimo (ar) perdavimo, taip pat privalo nedelsdami informuoti valstybės institucijas apie įtariamą neteisėtą paslaugos gavėjo (vartotojo) veiklą arba tai, kad paslaugos gavėjo pateikta informacija gali būti įgyta, sukurta ar pakeista neteisėtu būdu. Pagal valstybės institucijų reikalavimą informacinės visuomenės paslaugų teikėjai (ir interneto tarpininkai) privalo atskleisti informaciją, leidžiančią nustatyti paslaugų gavėjus, su kuriais atitinkami paslaugų teikėjai yra susitarę dėl informacijos saugojimo.

Kai informacinės visuomenės paslaugų teikėjas (ir interneto tarpininkas) pateikia vartotojui skirtą informaciją naudodamasis nuorodomis į kitos elektroninės komercijos įmonės internetinio puslapio turinį, pavyzdžiui, pateikia nuorodą į gamintojo puslapyje esantį produkto aprašymą, jis įprastai tampa atsakingas ir už šios medžiagos turinį. Jei informacinės visuomenės paslaugų teikėjas (ir interneto tarpininkas) pastebi, kad tie internetiniai puslapiai, į kuriuos pateikta nuorodų jo internetiniame puslapyje, pažeidžia įstatymus, jis turi nedelsdamas pašalinti šias nuorodas. Jei internetiniame puslapyje yra nuorodų į kitus puslapius, vartotojui turi būti visiškai aišku, kada yra išeinama iš pirminio puslapio. Tokios pačios taisyklės taikomos ir tuo atveju, kai interneto puslapiuose naudojami daugialypiai rėmeliai ar kitos priemonės, leidžiančios virtualiai pasiekti kituose puslapiuose esančią informaciją.

KONTROLINĖS UŽDUOTYS

1. Apibūdinkite interneto domeno vardo santykį su kitokiais naudojamais informacijos ar prekių žymenimis.
2. Paaiškinkite skirtumą tarp žalingo ir nepageidaujamo interneto turinio, nurodykite tokio atskyrimo problemas.
3. Apibūdinkite pagrindinę interneto jurisdikcijos taisyklę.
4. Paaiškinkite, kokias funkcijas atlieka interneto tarpininkai ir kodėl būtinas jų atsakomybės apribojimas.

Literatūra

1. Doukidis G., Mylonopoulos N. A., Pouloudi N. Social and Economic Transformation in the Digital Era. – London: Idea Group Publishing, 2004.
2. Lemley M. A., Menell P. S., Merges R. P., Samuelson P. Software and Internet Law (2nd. ed.). – New York: Aspen Law & Business, 2003.
3. Lloyd I. Information Technology Law (4th ed.). – LexisNexis, 2000.
4. Lessig L. Code and Other Laws of the Cyberspace. – New York: Basic Books, 1999.
5. Lessig L. The Law of the Horse: What Cyberlaw Might Teach, 113 Harvard Law Review, 501-33 (1999) // http://www.lessig.org/content/articles/works/finalhls.pdf.
6. Berman B. Cyberlaw: Problems of Policy and Jurisprudence in the Information Age. – New York: West Group, 2003.
7. Computer Law / Ed. by Chris Reed (3rd ed.). – Blackstone Press Limited, 1996.
8. Bowrey K. Law and Internet Culture. – Cambridge University Press, 2005.
9. Delta G. B. Law of the Internet. – Aspen Law & Business, 2005.
10. Sparrow A. P. The Law of Internet & Mobile Communications: the EU and US Contrasted. – Tfm Publishing, 2004.
11. Farber R., Cockfield M. A. Cyberspace Law: Cases and Materials. – New York: Aspen Publishes, 2002.
12. Lipton J. A Framework for Information Law and Policy. In Oregon Law Review. 2004. Voll. 82. No 3.

3. INTELEKTINĖS NUOSAVYBĖS TEISINĖ APSAUGA ELEKTRONINĖJE ERDVĖJE

3.1. Įvadinė medžiaga. Intelektinės nuosavybės pagrindinės kategorijos

Tradiciškai išskiriamos kelios **intelektinės nuosavybės sampratos**, kuriose intelektinė nuosavybė traktuojama kaip:

- intelektinės veiklos rezultatas;
- objektyvia forma išreikšta nauja ir naudinga informacija;
- nematerialiai vertybė;
- išimtinės asmens teisės į jo intelektinės veiklos rezultatą;
- kultūros ir technologinio progreso būtinas elementas;
- kūrėjo santykis su kūryba ir požiūris į kūrybos rezultatą.

Intelektinę nuosavybę, kaip ir materialią nuosavybę, galima suprasti objektyviuoju ir subjektyviuoju požiūriu.

Objektyviuoju požiūriu intelektinė nuosavybė yra žmogaus intelektinio darbo rezultatas, t. y. žmogaus sukurta informacija, turinti estetinę, intelektinę, techninę ar kitokią funkciją.

Subjektyviuoju požiūriu intelektinė nuosavybė yra kompleksas išimtinių subjektyvinių teisių, leidžiančių kontroliuoti informacijos (intelektinės nuosavybės objektyviuoju požiūriu) vartojimą. Teisėje įprasta intelektinę nuosavybę apibrėžti remiantis įvairiomis subjektyvinėmis teisėmis, įtvirtintomis įstatymuose, pavyzdžiui, patentais, autorinėmis teisėmis, gretutinėmis teisėmis, prekės ženklais, dizainu ir t. t. Dauguma nacionalinių, regioninių ir tarptautinių teisės aktų reglamentuoja būtent intelektinės nuosavybės subjektyvines teises.

Teises, kurios laikomos intelektinės nuosavybės teisėmis, išvardija 1967 m. Pasaulinės intelektinės nuosavybės organizacijos (WIPO) steigiamosios konvencijos 2 straipsnio nuostatos, kuriose teigiama, kad **intelektinė nuosavybė apima teises, susijusias su**:

- literatūros, meno ir mokslo kūriniais;
- artistų vaidybine veikla, fonogramų įrašais, radijo ir televizijos laidomis;

- išradimais visose žmogaus veiklos srityse;
- moksliniais atradimais;
- pramoniniais pavyzdžiais (pramoniniu dizainu);
- prekių ir paslaugų ženklais, firmų vardais ir kitais komerciniais žymenimis;
- apsauga nuo nesąžiningos konkurencijos;
- kitas panašaus pobūdžio teises, kylančias iš intelektinės veiklos pramonės, mokslo, literatūros ar meno srityse.

Atsižvelgiant į naujausias intelektinės nuosavybės tendencijas **prie intelektinės nuosavybės teisių taip pat galima priskirti teises, susijusias su**:

- slapta informacija;
- naudingais modeliais (mažaisiais arba inovaciniais patentais);
- kompiuterių programomis;
- duomenų bazėmis;
- puslaidininkių gaminių topografijomis;
- mikroorganizmais;
- techninėmis apsaugos priemonėmis.

Aukščiau paminėti intelektinės nuosavybės objektai taip pat skirstomi į dvi dideles dalis:

- literatūros, meno ir mokslo kūrinius – autorių teisių ir gretutinių teisių objektus (dažnai vadinamus intelektine nuosavybe siauruoju požiūriu);
- pramoninę nuosavybę – patentus, prekių ženklus, pramoninį dizainą ir kita.

Šių teisių palyginimas pateikiamas lentelėje.

Skirtingos intelektinės nuosavybės teisės nekonkuruoja tarpusavyje, t. y. gali galioti ir būti taikomos vienu metu. Tai dažnai taikoma naujoms intelektinės nuosavybės elektroninėms formoms, pavyzdžiui, kompiuterių programos ir duomenų bazės vienu metu gali būti saugomos autorių teisėmis, teisėmis į informacijos slaptumą, patentais (jei tenkinami jiems keliami reikalavimai) ir *sui generis* teisėmis. Atskiri jų elementai taip pat gali būti registruoti kaip prekių ženklai ar pramoninis dizainas.

1 lentelė. **Pagrindinės intelektinės nuosavybės formos**

Autorių teisės ir gretutinės teisės	Pramoninė nuosavybė
Saugomi bet kokie kūriniai ir gretutinių teisių objektai	Saugomi tik objektai, atitinkantys griežtus reikalavimus
Suteikiamos automatiškai ir nemokamai, be specialių autoriaus ar teisių įgijėjo pastangų	Suteikiamos tik atlikus specialias registravimo ir ekspertizės procedūras, kurios gali užtrukti net keletą metų, teisių registravimas ir palaikymas yra mokamas ir gana brangus
Automatiškai galioja tarptautiniu mastu (tarptautinių susitarimų pagrindu)	Iš esmės nacionalinės teisės, tarptautiniu mastu galioja tik atlikus nacionalines procedūras
Gausu nekomercinio ir panašaus pobūdžio išimčių ir apribojimų	Išimčių ir apribojimų beveik nėra
Leidžiamas savarankiškas analogiško (panašaus) objekto sukūrimas	Bet koks analogiško (panašaus) objekto sukūrimas ar naudojimas laikomas teisių pažeidimu

3.2. Pagrindinė medžiaga. Intelektinė nuosavybė elektroninėje erdvėje

Atsiradus kompiuteriams, elektroninei erdvei ir kompiuterių tinklams, atsirado visiškai naujos intelektinės nuosavybės formos ir nauji iššūkiai intelektinės nuosavybės teisėms, todėl susiformavo savarankiškas intelektinės nuosavybės elektroninėje erdvėje institutas.

Visų pirma į elektroninę erdvę buvo perkelti tradiciniai intelektinės nuosavybės objektai, pavyzdžiui, tekstiniai kūriniai, fotografijos, audiovizualiniai objektai ir pan. Tokiu būdu **pagrindinis intelektinės nuosavybės elektroninėje erdvėje objektas yra tradiciniai kūriniai elektronine forma**, pavyzdžiui, elektroniniai tekstai, elektroniniai muzikos įrašai, elektroniniai paveikslėliai ir pan.

Dažniausiai sutinkamos **specifinės naujos intelektinės nuosavybės elektroninėje erdvėje formos yra kompiuterių programos ir duomenų bazės**. Pati elektroninė erdvė iš esmės yra kompiuterių ir kompiuterių programų veikimo (sąveikos) rezultatas.

Kompiuterių programa yra laikomas specialių instrukcijų (kodo) rinkinys, kurio dėka kompiuteris veikia tam tikru būdu arba pasiekiamas tam tikras veiklos rezultatas.

Duomenų baze yra laikomas susistemintas informacijos (duomenų) rinkinys, kuriuo galima individualiai naudotis elektroniniu ar kitu būdu.

Savarankiškomis intelektinės nuosavybės elektroninėje erdvėje formomis atskirais atvejais galima laikyti ir **interneto domeno vardus – simbolinius interneto adresų pavadinimus**, ir **interneto turinį – daugialypės terpės objektus**.

Elektroninėje erdvėje reikalingas ir specialus intelektinės nuosavybės teisių išplėtimas, kadangi autoriams, išradėjams ir kitiems intelektinės nuosavybės teisių turėtojams būtina kontroliuoti intelektinės nuosavybės naudojimą ir tradicinėje, ir elektroninėje erdvėje. Be to, būtinos ir specialios intelektinės nuosavybės teisių išimtys, susijusios su elektroninės erdvės techninėmis savybėmis.

Specialiosios intelektinės nuosavybės teisės elektroninėje erdvėje yra teisės (teisės leisti ar drausti) į:

- intelektinės nuosavybės **atgaminimą (kopijavimą) elektroninėje erdvėje**, apimantį specialias *kvazi* atgaminimo formas, pavyzdžiui, interneto nuorodas, langų elementus (*frames*), integruotą daugialypį turinį;
- intelektinės nuosavybės **platinimą elektroninėje erdvėje**, įskaitant platinimą telefono linijomis, interneto serveriuose, tinklalapiuose, P2P tinklais ir pan.;
- intelektinės nuosavybės **padarymą viešai prieinamą kompiuterių tinklais (talpinimą internete)**.

Kitos specialios teisės yra susijusios su atskirais intelektinės nuosavybės elektroninėje erdvėje objektais, pavyzdžiui, kompiuterių programomis ar duomenų bazėmis.

Specialios **intelektinės nuosavybės teisių išimtys elektroninėje erdvėje** yra susijusios su būtinybe užtikrinti elektroninės erdvės, interneto ar kompiuterių funkcionavimą, suderinamumą ir galimybėmis juos panaudoti pagal paskirtį. Tokios išimtys yra:

- **laikinas intelektinės nuosavybės atgaminimas elektroninėje erdvėje**, kuris būtinas, pavyzdžiui, kompiuterių programos paleidimui (laikina kopija operatyvinėje atmintyje – RAM), informacijos perdavimui internete (laikinos kopijos tarpiniuose serveriuose) ir pan.;

- **intelektinės nuosavybės atgaminimas ir naudojimas derinimo, klaidų taisymo ir pasiekiamumo tikslais**, pavyzdžiui, teisė dekompiliuoti kompiuterių programą (atkurti pirminį programos kodą) suderinamumo tikslais, teisė pasidaryti atsarginę ar asmeninę kopiją, teisė taisyti programos klaidas ir kt.

Kiti svarbūs intelektinės nuosavybės elektroninėje erdvėje klausimai, kurie taip pat atskiria ją nuo tradicinės intelektinės nuosavybės problemų, yra:

- intelektinės nuosavybės pažeidimai elektroninėje erdvėje;
- techninių apsaugos priemonių naudojimas intelektinės nuosavybės apsaugai;
- kolektyvinio teisių administravimo taikymas intelektinei nuosavybei elektroninėje erdvėje;
- intelektinės nuosavybės teisių suderinimas su naujomis kūrybos ir inovacijų formomis elektroninėje erdvėje – *Atvirojo kodo*, *Kūrybinės bendrumos* ir kitais judėjimais.

Techninės apsaugos priemonės yra įvairiausi mechanizmai ir priemonės, kuriuos intelektinės nuosavybės teisių turėtojai gali naudoti siekdami uždrausti tam tikrus veiksmus (pvz., kopijavimą) su intelektinės nuosavybės objektu. Techninės apsaugos priemonės gali būti specialūs techniniai raktai, papildomi elektroniniai signalai, elektroniniai „vandens ženklai“, speciali programinė įranga, net sąmoningai paliekamos klaidos informacijoje.

Kolektyvinis administravimas yra organizuotas: intelektinės nuosavybės teisių turėtojų asociacijos įgyvendina intelektinės nuosavybės teises, surenka ir paskirsto atlyginimą už pasinaudojimą teisėmis. Kolektyvinis intelektinės nuosavybės teisių administravimas elektroninėje erdvėje kelia problemų dėl didelių teisių savininkų galimybių individualiai administruoti savo teises, techninių apsaugos priemonių taikymo, taip pat dėl kolektyvinio administravimo neveiksmingumo.

Atvirojo kodo (angl. *Open Source*) judėjimas yra kompiuterių programų, kurių kodas pateikiamas viešai nagrinėti ir tobulinti, autorių virtualaus bendravimo ir kompiuterių programų kodo apsikeitimo forma. **Kūrybinės bendrumos (angl. *Creative Commons)* judėjimas** yra atvirojo kodo principais pagrįsta bet kokios informacijos (kūrinių, naujovių) apsikeitimo ir tobulinimo forma. Ir Atvirojo kodo, ir Kūrybinės bendrumos judėjimai pasikliauja intelektinės nuosavybės naudojimo sutartimis (licencijomis), kuriose nustatomos pagrindinės teisinės taisyklės dėl intelektinės nuosavybės.

3.3. Pagrindinė medžiaga. Intelektinės nuosavybės pažeidimai elektroninėje erdvėje

Intelektinės nuosavybės pažeidimu laikomas intelektinės nuosavybės produktų atgaminimas, platinimas, naudojimas, laikymas ir gabenimas be teisių turėtojo sutikimo ar sutarties su teisių turėtoju (arba jo atstovu). Pažeidimu laikytinas ir bet koks intelektinės nuosavybės įstatymų pažeidimas, įskaitant neturtinių teisių pažeidimus. Pažeidimai gali būti padaromi ir komerciniais, ir ne komerciniais tikslais. **Komerciniai tikslai** – kai siekiama betarpiško pasipelnymo, kai intelektinės nuosavybės teisių objektas naudojamas kitai veiklai, susijusiai su komercija.

Intelektinės nuosavybės pažeidimai elektroninėje erdvėje yra specifiniai intelektinės nuosavybės teisių pažeidimai:

- tradiciniai intelektinės nuosavybės pažeidimai, kurių padarymo vieta ar įrankis yra elektroninė erdvė arba elektroninės erdvės technologijos;
- specifiniai intelektinės nuosavybės pažeidimai, padaromi tik elektroninėje erdvėje:
  - nuorodų į neteisėtas intelektinės nuosavybės kopijas talpinimas ir platinimas;
  - intelektinės nuosavybės neteisėtų kopijų talpinimas ir platinimas kompiuterių tinklais (įskaitant beserverinius P2P tinklus);
  - techninių apsaugos priemonių ir teisių valdymo informacijos pažeidimai;
  - intelektinės nuosavybės pažeidimų elektroninėje erdvėje įrankių platinimas ir neleistini veiksmai su jais.

3.3.1. Intelektinės nuosavybės elektroninėje erdvėje istorinė raida

Intelektinės nuosavybės raida elektroninėje erdvėje neatsiejama nuo esminių technologinių pasiekimų. XIX–XX a. vyko ypač sparti intelektinės nuosavybės objektų plėtra, atsirado ir masiškai paplito fotografija, kinas, garso įrašai, radijo, televizijos, palydovinės ir kabelinės transliacijos, galiausiai – kompiuteriai ir kompiuterių tinklai. Kiekviena iš šių naujų technologinių sričių sukūrė naujus intelektinės nuosavybės objektus, atsirado subjektyvinės teisės į šiuos objektus ir teisinės problemos.

XX a. 8 dešimtmetyje prasidėjusi informacinė revoliucija pavertė informaciją ir intelektinę nuosavybę masine preke, kuri gali būti ypač lengvai atgaminta, taip pat internetu perduota į bet kurį pasaulio kampelį itin mažomis sąnaudomis. Internete ypač svarbus tapo interneto tarpininkų, kurie perduoda elektroninę informaciją (tame tarpe – ir intelektinės nuosavybės turinį), vaidmuo platinant ir saugant intelektinę nuosavybę. Intelektinės nuosavybės pažeidimai internete dėl jų paprastumo pasiekė neregėtą mastą, tačiau akivaizdus ir intelektinės nuosavybės teisių turėtojų noras padidinus savo intelektinės nuosavybės teises informacinių technologijų pagalba pasipelnyti vartotojų sąskaita (reikalaujant nepagrįstos kainos už intelektinės nuosavybės teises, reikalaujant atlyginimo už tradiciškai neatlygintiną – asmeninį ir nekomercinį – pasinaudojimą intelektine nuosavybe, taip pat siekiant neterminuotų intelektinės nuosavybės teisių).

Žinių visuomenėje intelektinė nuosavybė ypač reikšminga, kadangi intelektinės nuosavybės teisės iš esmės yra teisės, leidžiančios kontroliuoti informacijos vartojimą. Informacija yra pagrindinė žinių visuomenės vertybė ir žinių ekonomikos resursas. Apskritai žinių visuomenėje vis labiau ryškėja kolizija tarp teisės į informaciją, kaip pagrindinės žmogaus teisės, ir intelektinės nuosavybės, kaip teisės kontroliuoti informaciją.

Žinių visuomenės technologijos išryškino ir kitas didėjančias intelektinės nuosavybės problemas: pasenusią ir neveiksmingą kolektyvinio administravimo sistemą, neteisingą atlyginimą tikriesiems intelektinės nuosavybės kūrėjams.

XX a. paskutiniojo dešimtmečio pabaigoje elektroninėje erdvėje taip pat atsirado ir įsitvirtino alternatyvūs intelektinės nuosavybės judėjimai, tokie kaip Atvirojo kodo kompiuterių programų (angl. *Open source*) ir Kūrybinės bendrumos (angl. *Creative Commons*) judėjimai, pabrėžiantys intelektinės nuosavybės svarbą socialiniam informacijos prieinamumui, socialiniam planavimui, kultūros ir technologijų plėtrai.

Atvirojo kodo judėjimas yra kompiuterių programų, kurių kodas pateikiamas viešai analizuoti ir tobulinti, autorių virtuali bendruomenė. Kiekvienas asmuo gali laisvai naudotis atvirojo kodo kompiuterių programomis, jas perdirbti, tobulinti su sąlyga, kad jo panaudotas ar perdirbtas kompiuterių programos kodas liks atviras – t. y. laisvai prieinamas ir viešas. Atvirojo kodo judėjimas neturi būti tapatinamas su nemokamomis kompiuterių programomis, kadangi atvirojo kodo pro-

gramos nebūtinai turi būti platinamos ir prieinamos nemokamai, svarbu, kad programos kodas būtų laisvai prieinamas ir viešas, t. y. būtų galimybė šį kodą ar jo elementus naudoti kuriant naujas kompiuterių programas. Praktiškai Atvirojo kodo judėjimo tęstinumas užtikrinamas specialiomis atvirojo kodo licencijomis (susitarimais dėl atvirojo kodo kompiuterių programų teisinio statuso ir panaudojimo sąlygų). Atvirojo kodo judėjimas neprieštarauja ir jokiu būdu neneigia intelektinės nuosavybės teisių reikalingumo, priešingai, jis iš esmės priklauso nuo intelektinės nuosavybės teisių, kurios naudojamos ginant atvirojo kodo (ir jo pagrindu sukurto naujo kodo) viešumą ir prieinamumą.

Kūrybinės bendrumos (angl. *Creative Commons)* judėjimas yra atvirojo kodo principais pagrįsta bet kokios informacijos (kūrinių, inovacijų) vartojimo ir tobulinimo forma, aiškiai apibrėžtų licencijų ribose leidžianti viešai platinti ir naudoti intelektinės nuosavybės teisėmis saugomą turinį. Priklausomai nuo autoriaus ar teisių turėtojo pasirinktų licencijos sąlygų kiti asmenys gali naudotis Kūrybinių bendrumų informacija nemokamai ar už atlyginimą, gali jį perdirbti, panaudoti nekomerciniams projektams ir pan. Kūrybinės bendrumos itin supaprastina intelektinės nuosavybės naudojimą, kadangi naudotojams nebereikia individualiai derinti licencijos sąlygų, bendrauti su autoriumi (teisių turėtoju ir pan.).

Intelektinės nuosavybės pažeidimų elektroninėje erdvėje skiriamasis bruožas yra tas, kad jie padaryti elektroninėje erdvėje arba naudojant elektronines technologijas. Apskritai įprasta intelektinės nuosavybės pažeidimus tapatinti su intelektinės nuosavybės produktų atgaminimu, platinimu, naudojimu, laikymu ir gabenimu siekiant komercinių tikslų, t. y. tokiais veiksmais, kurie daro ypač didelę žalą intelektinės nuosavybės teisių turėtojams, valstybei ir visuomenei, nors pažeidimais pripažintini ir tie atvejai, kai minėtos veikos atliekamos nesiekiant komercinių tikslų. Komercinių tikslų siekiančiais laikomi tie atvejai, kai siekiama tiesiogiai pasipelnyti, taip pat kai intelektinės nuosavybės teisių objektas naudojamas kitai veiklai, susijusiai su komercija (pvz., įmonės dokumentams rengti), nors pats intelektinės nuosavybės teisių objekto naudojimas nėra komercinis, t. y. tuo neuždirbamos tiesioginės pajamos arba nesutaupomos lėšos. Pažeidimu laikytinas ir bet koks intelektinės nuosavybės įstatymų pažeidimas ar intelektinės nuosavybės licencinės sutarties pažeidimas, tarp jų – intelek-

tinės nuosavybės teisių objekto naudojimas be teisių turėtojo sutikimo (sutarties).

Pažeidimus komerciniais tikslais įprasta vadinti intelektinės nuosavybės „piratavimu“. Ši sąvoka apibūdinti intelektinės nuosavybės pažeidimus elektroninėje erdvėje ypač tinka todėl, kad intelektinės nuosavybės „piratai“ grobia ir išnaudoja svetimą intelektinę nuosavybę savo tikslams, beveik neįdėdami jokių pastangų šioms vertybėms sukurti. Intelektinės nuosavybės sukūrimo sąnaudos dažniausiai labai didelės, o intelektinės nuosavybės produktų neteisėto atgaminimo bei platinimo sąnaudos nepalyginimai mažesnės, ypač internete.

Neteisėta („piratine“) intelektine produkcija laikomos visos neteisėtai įgytos (nesant įsigijimo dokumentų ir (ar) licencijos), atgamintos (neturint autoriaus, teisių turėtojo ar juos atstovaujančios organizacijos sutikimo) intelektinės produkcijos (autorinių kūrinių, audiovizualinės produkcijos, fonogramų, kompiuterių programų, atlikimų, transliacijų ir kt.) fiksacijos, kopijos, papildomos teisėtai turimų egzempliorių kopijos, padarytos neturint tam teisės ar pažeidžiant įstatymuose nustatytas išimtis, papildomos kopijos, padarytos viršijant licencijose numatytą leidžiamą kopijų skaičių ar jų paskirtį, taip pat laikmenos, kuriose užfiksuotos ar išsaugotos tokios kopijos ir bet kokie kiti objektai, kurie pažeidžia intelektinės nuosavybės teises.

Intelektinės nuosavybės pažeidimai elektroninėje erdvėje visų pirma turi būti vertinami taip pat, kaip ir tradiciniai intelektinės nuosavybės pažeidimai, tačiau dėl jų specifikos ir daromos žalos kai kuriais atvejais traktuotini kaip pavojingesnės veikos. Intelektinės nuosavybės pažeidimai įtraukti į daugelio išsivysčiusių valstybių baudžiamuosius ir administracinius kodeksus, taip pat ir Europos Sąjungos bei Jungtinių Tautų Organizacijos rekomendacijas dėl neteisėtų ir nusikalstamų veikų kvalifikavimo. Intelektinės nuosavybės pažeidimai visose valstybėse, taip pat ir Lietuvoje, laikomi civilinių teisių pažeidimais. Lietuvos Respublika pasirašė ir ratifikavo pagrindines tarptautines konvencijas, reglamentuojančias intelektinės nuosavybės teisių pažeidimus, bei Europos Sąjungos direktyvas intelektinės nuosavybės klausimais. Naujausia Europos Sąjungos direktyva Nr. 2004/48/EB dėl intelektinės nuosavybės teisių gynimo šiuo metu baigiama įgyvendinti Lietuvos intelektinės nuosavybės teises reglamentuojančiuose įstatymuose.

Vienas iš išsamiausiai intelektinės nuosavybės pažeidimus regla-

mentuojančių teisės aktų Lietuvoje yra Autorių teisių ir gretutinių teisių įstatymas, kuris konkrečiai reglamentuoja autorių teisių ir gretutinių teisių pažeidimus bei gynimą.

Vadovaujantis Autorių teisių ir gretutinių teisių įstatymo 64 straipsnio nuostatomis, autorių teisių pažeidimais yra laikomi šie veiksmai:

1) kūrinio ar gretutinių teisių objekto panaudojimas (įskaitant išleidimą, atgaminimą, viešą atlikimą, transliavimą bei retransliavimą ar viešą paskelbimą), importavimas ir platinimas be autoriaus ar gretutinių teisių subjekto licencijos (nesudarius sutarties arba pažeidžiant jos sąlygas);
2) kūrinių ir gretutinių teisių objektų neteisėtų kopijų importavimas, eksportavimas, platinimas, gabenimas ar laikymas komerciniais tikslais;
3) įstatyme ar autorinėse sutartyse nustatyto autorinio atlyginimo nesumokėjimas;
4) bet kokių techninių apsaugos priemonių, kurias autorių teisių ar gretutinių teisių subjektai naudoja šiame įstatyme numatytoms savo teisėms įgyvendinti arba apsaugoti, pašalinimas, taip pat paslaugų tai padaryti siūlymas bei atitinkamų prietaisų, leidžiančių pašalinti tokias technines apsaugos priemones, gaminimas, importavimas, gabenimas, laikymas turint tikslą platinti ir platinimas;
6) informacijos apie autorių teisių ar gretutinių teisių valdymą panaikinimas arba pakeitimas be autorių ar gretutinių teisių subjektų leidimo, taip pat kūrinių, atlikimų įrašų, fonogramų ar jų kopijų platinimas, importavimas, transliavimas, viešas paskelbimas ar padarymas viešai prieinamais be leidimo panaikinus arba pakeitus informaciją apie teisių valdymą; autoriaus ar atlikėjo asmeninių neturtinių teisių pažeidimas;
7) kitų įstatymo nuostatų pažeidimas.

Šios nuostatos Autorių teisių ir gretutinių teisių įstatyme įtvirtintos vadovaujantis Europos Sąjungos direktyvomis, TRIPS ir PINO interneto sutarčių nuostatomis.

Atkreiptinas dėmesys, kad įstatyme pateiktas pažeidimų sąrašas nėra baigtinis.

Panašų autorių teisių ir gretutinių teisių pažeidimų sąrašą pateikia ir galiojantys administraciniai ir baudžiamieji įstatymai. Tačiau administraciniai ir baudžiamieji įstatymai specialiai nereglamentuoja ir nekriminalizuoja intelektinės nuosavybės pažeidimų elektroninėje erd-

vėje, o specifinių intelektinės nuosavybės teisių pažeidimų, padaromų tik elektroninėje erdvėje, tokių kaip nuorodų į neteisėtai platinamas intelektinės nuosavybės kopijas teikimas interneto svetainėse, taip pat operacijos P2P tinkluose bei šių tinklų operatorių veiksmai su neteisėtu intelektinės nuosavybės turiniu, šiuo metu specialiai nenumato ir nereglamentuoja.

Kitų intelektinės nuosavybės teisių pažeidimai yra paprastesni ir rečiau padaromi elektroninėje erdvėje, todėl atskirai nenagrinėtini.

Dėl intelektinės nuosavybės tarptautinio pobūdžio intelektinės nuosavybės pažeidimai yra tarptautinis reiškinys. Dėl menkų intelektinės nuosavybės pažeidimų padarymo sąnaudų, pavyzdžiui, masinių intelektinės nuosavybės produktų (fonogramų ar kompiuterių programų) atgaminimo ir tiražavimo sąnaudų, net ir nedidelė valstybė (pvz., Taivanas) gali nelegalia produkcija aprūpinti ne tik savo vidaus rinką, bet internetu – visą pasaulį. Be to, pažeidėjų pelnas tiesiogiai proporcingas pagamintos ir realizuotos „piratinės“ produkcijos kiekiui. Vidaus rinkos ribotumas, taip pat masto ekonomikos tikslai bei siekis mažinti savikainą skatina „piratus“ aktyviai veržtis į užsienio rinkas ir išnaudoti pasaulinės elektroninės erdvės teikiamas galimybes. Pažymėtina, kad internete nėra kliūčių neteisėtą piratinę produkciją platinti tiek vidaus rinkose, tiek ir visame pasaulyje.

Paplitus skaitmeniniams įvairių kūrinių fiksavimo formatams, kompiuteriniais tinklais gali būti neteisėtai platinamos ne tik kompiuterių programos, bet ir garso bei vaizdo produkcija, fonogramos, literatūros ir meno kūriniai, taip pat kita informacija. Intelektinės nuosavybės neteisėtos skaitmeninės kopijos gali būti lengvai atgaminamos, platinamos ir perduodamos kompiuterių tinklais pasauliniu mastu be jokių fizinių informacijos laikmenų. Piratai taip pat sėkmingai išnaudoja naujausius teisėtus verslo modelius ir technologinius pasiekimus – elektroninius interneto aukcionus, kompiuterinių failų beserverinių mainų sistemas (P2P tinklus, tokius kaip *Napster*, *Kazaa*, *Morpheus*, *Grokster*, *eDonkey*, *Bittorent*), esamojo laiko interneto komunikacijų sistemas (ICQ, IRC), socialinių ryšių tinklalapius, „BLOGus“ ir naujienų grupes.

Nors labiausiai paplitusios intelektinės produkcijos laikmenos vis dar – garsajuostės ir vaizdajuostės, kuriose fonogramos ir garso bei vaizdo informacija saugoma analogine forma, kaip įrašas magnetinėje juostoje, tačiau pastaruoju metu ypač sparčiai plinta skaitmeninės intelektinės produkcijos laikmenos arba elektroniniai šios produkcijos failai internete. Intelektinės nuosavybės elektroninė forma iš es-

mės nesusidėvi naudojant, taip pat leidžia vartotojui tuoj pat pasiekti bet kurią įrašytos informacijos dalį. Pati naujausia skaitmeninio informacijos pateikimo tendencija yra vadinamasis srautinis elektroninio turinio pateikimas (angl. *streaming*), t. y. tik laikinos tarpinės intelektinės nuosavybės objektų trumpų dalių ar epizodų fiksacijos, vienu metu nepateikiančios vartotojui viso intelektinės nuosavybės objekto.

Per pastaruosius keletą metų masiškai paplito įrašomosios kompaktinės plokštelės ir kitos įrašomosios laikmenos (pvz., daugkartinio naudojimo *flash* atmintinės, nešiojami kietieji diskai ir pan.), taip pat žymiai sumažėjo kokybiško įrašymo įrangos kainos. Šių technologijų paplitimas ir prieinamumas nulėmė sparčią interneto ir įvairiausių inovacijų plėtrą, tačiau taip pat padaugėjo ir intelektinės nuosavybės teisių pažeidimų, ypač – neprofesionalių pažeidimų, kuomet fonogramų, kompiuterių programų ar audivizualinių kūrinių neteisėtos kopijos atgaminamos ir platinamos namų (buitinėmis) sąlygomis. Minėtos pažeidimo priemonės yra iš esmės universalios, todėl pritaikomos pažeisti įvairias intelektinės nuosavybės formas: fonogramas ir audioviazualinius kūrinius, kompiuterių programas ar kitus intelektinės nuosavybės objektus. Intelektinės nuosavybės neprofesionalių ir elektroninių pažeidimų paplitimui didelės įtakos turėjo asmeninių kompiuterių ir plačiajuostės (angl. *broadband*) interneto prieigos paplitimas namuose ir įstaigose. Plačiai paplitusios techninės ir programinės įrangos, universalių interneto priemonių pagalba šiandien kiekvienas asmeninio kompiuterio naudotojas gali atgaminti bet kokią skaitmeninę informaciją beveik neribotais kiekiais.

Kaip jau minėta, saugomos skaitmeniniu formatu informacijos bei intelektinės nuosavybės objektų (tarp jų fonogramų, audioviazualinių kūrinių) kopijos yra absoliučiai tapačios originalui – neteisėtos kopijos kokybė nėra blogesnė negu teisėtų kopijų. Neteisėtos skaitmeninės kopijos neturi kokybės trūkumų, kurie būdingi analoginėms kopijoms. Dėl šios priežasties skaitmeninis pažeidimas laikomas itin pavojingu. Dar visai neseniai skaitmeninių kopijų kūrimas ir fiksavimas naujose laikmenose buvo sudėtinga ir brangi technologinė procedūra, reikalaujanti nemažų investicijų, o dabar skaitmeninių kompaktinių plokštelių kopijavimas arba tiesiog neteisėtos produkcijos failų parsisiuntimas prieinamas beveik kiekvienam kompiuterių vartotojui ir beveik nieko nekainuoja. Naudojant naujus skaitmeninius formatus ir informacijos glaudinimo standartus (MP3, DivX, MP4) fonogramas ar audiovizualinę informaciją galima išsaugoti nedidelės

apimties failuose, be to, eksponentiškai didėjant elektroninių informacijos laikmenų talpai ir mažėjant kainai failų dydis (megabaitų skaičius) tampa vis mažiau svarbiu fiziniu apribojimu. Elektroniniai failai P2P tinklais gali būti lengvai perduodami ir platinami internete pasauliniu mastu, tam nereikia papildomų materialių laikmenų, nes apsiribojama laikinomis srautinėmis fiksacijomis.

MP3, DivX, MP4 ir kiti informacijos glaudinimo standartai yra informacinių technologijų progreso išdava. Naudojant MP3 ar DivX kodavimo algoritmus, skaitmeninė informacija papildomai suspaudžiama, todėl gali būti užfiksuota efektyviau – suglaudinto skaitmeninio failo apimtis gali būti sumažinta nuo kelių iki kelių dešimčių kartų, tuo pat metu beveik neprarandamas informacijos turinys ir kokybė. Šių glaudinimo algoritmų pagalba net į įprastines laikmenas (pvz., įrašomas kompaktines plokšteles CD-R) galima įrašyti žymiau daugiau informacijos: ilgesnės trukmės fonogramas ar net kelis garso bei vaizdo kūrinius. MP3, DivX, MP4 algoritmai sukurti naudoti teisėtai, tačiau intelektinės nuosavybės pažeidėjai pasinaudojo šiais technologiniais pasiekimais. MP3, DivX, MP4 formatais išsaugotos neteisėtos intelektinės nuosavybės kopijos yra sparčiai platinamos, kadangi mažiau apkrauna lokaliuosius kompiuterių tinklus bei internetą.

Pažymėtina, kad MP3, DivX, MP4 algoritmai įdiegė ir visiškai naujus teisėtus intelektinės nuosavybės platinimo ir panaudojimo būdus – iš esmės įmanomas tapo ir buvo sėkmingas intelektinės nuosavybės (elektroninių įrašų, knygų, filmų) teisėtas platinimas internete, atsirado ir suklestėjo specializuotų skaitmeninių grotuvų rinka. Tik minėtų technologijų dėka galima įsigyti intelektinės produkcijos, pritaikytos individualiems vartotojų poreikiams ir apskritai neprieinamos kitais būdais, pavyzdžiui, galima gauti konkrečios dainos elektroninį įrašą, nereikia pirkti viso albumo. Paminėtina, kad tokios individualios prekės ir paslaugos yra ypač patrauklios ir reikalingos vartotojams – 2006 m. vasarį populiariausias legalių skaitmeninių muzikos įrašų pardavimo portalas internete (www.itunes.com) minėjo 1 milijardo parduotų muzikos įrašų sukaktį, nors pats portalas gyvuoja tik keletą metų (žr. www.apple.com/itunes/1billion/).

Šios technologijos kelia ir kitų kontroversijų, pavyzdžiui, susijusių su vartotojų teisėmis atgaminti legaliai turimą intelektinę nuosavybę ir naudoti asmeniniuose kompaktiniuose skaitmeniniuose grotuvuose. Beje, būtent kompaktinių skaitmeninių grotuvų masinis paplitimas ir akivaizdūs jų techniniai pranašumai prieš kitus analoginius atkūrimo įrenginius lemia ypač spartų MP3, DivX, MP4 standartų inte-

lektinės produkcijos (tiek legalios, tiek nelegalios) masinį paplitimą ir teisėtos tokios produkcijos rinkos perspektyvas artimiausioje ateityje.

Pastaruoju metu plintant interneto ir duomenų perdavimo technologijoms, ypač tarp pavienių vartotojų P2P (angl. *peer to peer*), labai padidėjo vartotojų galimybės gauti informaciją apie kitų vartotojų turimas neteisėtas intelektinės nuosavybės objektų kopijas, jomis apsikeisti, parsisiųsti neteisėtos intelektinės produkcijos failus. Praktinis šios problemos pavyzdys yra jau minėtas *Napster* interneto portalas ir vėlesni jo klonai (pvz., *eDonkey* ar *Bittorent*). Šiuo metu egzistuojantys fonogramų, audiovizualinės produkcijos ir kompiuterių programų mainų tinklai yra decentralizuoti, todėl sukontroliuoti jų pagalba vykdomus neteisėtų intelektinės nuosavybės kopijų mainus ir platinimą esamomis techninėmis priemonėmis neįmanoma. Vienintelė priemonė suvaldyti jų veiklą yra tokių tinklų programinės įrangos ir veiklos pripažinimas intelektinės nuosavybės pažeidimų elektroninėje erdvėje įrankiais. Būtent tokią nuostatą suformulavo Jungtinių Amerikos Valstijų teismai, dar 1999 m. sprendimu pripažindami *Napster* tinklą iš esmės prisidėjusį prie intelektinės nuosavybės teisių pažeidimų, kuriuos jo vartotojai atliko pasinaudoję tinklu. Ši nuostata palaikyta ir 2005 m. *Grokster* byloje.

Būtina akcentuoti, kad intelektinės nuosavybės pažeidimai internete ir juos palengvinančios technologijos neturi būti suabsoliutinami. Nemažai pažeidimų padaroma dėl pačių intelektinės nuosavybės teisių turėtojų konservatyvios ar net neteisėtos politikos, piktnaudžiavimo turimomis intelektinės nuosavybės teisėmis. Be to, technologijų, naudojamų darant intelektinės nuosavybės pažeidimus, teisėtas naudojimas nepalyginamai reikšmingesnis, o ypač reikšmingas užtikrinant informacijos ir socialinių paslaugų prieinamumą visai visuomenei ir ilgalaikę visuomenės socialinę bei ekonominę plėtrą.

3.4. Papildoma medžiaga. Kompiuterių programų teisinės apsaugos ypatumai

3.4.1. Kompiuterių programos teisinė samprata

Teisiniuose dokumentuose sąvoka „kompiuterių programa“ dažniausiai apibrėžiama kaip visuma instrukcijų, pateikiamų žodžiais, kodais, schemomis ar kitu pavidalu, kurios įgalina kompiuterį atlikti tam tikrą užduotį ar pasiekti tam tikrą rezultatą, kai tos instrukcijos pateikiamos tokiomis priemonėmis, kurias kompiuteris gali perskaityti; ši

sąvoka apima ir parengiamąją projektinę tokių instrukcijų medžiagą su sąlyga, kad iš jos galima būtų sukurti minėtą instrukcijų visumą.

Teisininkui labai svarbu suvokti dvejopą kompiuterių programų prigimtį ir jas sudarančius elementus, kadangi šiems elementams galiausiai ir taikoma teisinė apsauga. Teisiniu požiūriu svarbūs ir saugotini kompiuterių programos elementai yra ir jų tekstinė išraiška (pirminis kodas, objektinis kodas), ir kompiuterių programa valdomo kompiuterio veikimo rezultatai (vartotojo ir kitos sąsajos, failų ir grafinių vaizdų išdėstymas, garsinės ir vaizdinės programos pristatymas). Tekstinė kompiuterių programos išraiška tiesiogiai lemia kompiuterių programos veikimo rezultatus ir atvirkščiai, tačiau kompiuterių programos tekstinė išraiška ir veikimo rezultatai tuo pat metu ir nepriklauso vienas nuo kito, kadangi įmanoma pasiekti tokius pačius veikimo rezultatus pasitelkus kitokios tekstinės išraiškos kompiuterių programą, o skirtingos išraiškos kompiuterių programos gali atlikti tuos pačius uždavinius (pasiekti tuos pačius rezultatus). Kūrybinis procesas apima abu šiuos kompiuterių programos aspektus.

3.4.2. Kompiuterių programų teisinės apsaugos istorinė raida

Kompiuterių programų teisine apsauga mokslo ir įstatymų leidybos lygiu pradėta aktyviai domėtis XX a. šeštajame dešimtmetyje. 1971 m. kompiuterių programų teisinės apsaugos klausimams spęsti prie Pasaulinės intelektinės nuosavybės organizacijos (PINO) sudaryta speciali darbo grupė, kurios pasiūlymai buvo gana kontroversiški ir praktiškai neįgyvendinti. 1978 m. PINO patvirtino kompiuterių programų teisinės apsaugos pavyzdinių principų projektą, kuris numatė galimybę kompiuterių programoms taikyti ypatingą *sui generis* teisinę apsaugą, pagrįstą autorių teisių režimo modifikacija. Šis projektas nebuvo priimtas, o PINO apskritai atsisakė siekio priimti kokias nors rekomendacijas dėl kompiuterių programų teisinės apsaugos. Tuo pat metu, kaip ir PINO, kompiuterių programų teisinės apsaugos klausimais aktyviai domėjosi Tarptautinė pramoninės nuosavybės apsaugos asociacija (AIPPI). 1975 m. AIPPI rekomendavo kompiuterių programų teisinei apsaugai taikyti autorių teises.

Pirmuosius bandymus nustatyti teisinę apsaugą kompiuterių programoms galima apibendrinti kaip bandymus apsispręsti, ar kompiuterių programoms turi būti taikomos jau esamos tradicinės intelekti-

nės nuosavybės teisės normos, ar turi būti ieškoma naujų *sui generis* teisinių instrumentų. Tradicinės intelektinės nuosavybės normų šalininkai kaip modelį kompiuterių programų teisinei apsaugai siūlė esamus intelektinės nuosavybės teisės institutus – autorių teises, patentų teisę, taip pat komercinių paslapčių teisę. Šios intelektinės nuosavybės formos pradėtos realiai taikyti kompiuterių programoms nuo 1980 m. Jungtinių Amerikos Valstijų autorių teisių akto pakeitimų.

3.4.3. Kompiuterių programų apsauga autorių teisėmis

Intelektinės nuosavybės teisės ir, konkrečiai, autorių teisių pasirinkimą kompiuterių programų apsaugai lėmė kelios priežastys. Visų pirma kompiuterių programos yra nematerialus turtas, todėl intelektinės nuosavybės teisė, kurios objektas yra nematerialūs žmogaus intelektinės veiklos rezultatai, labiausiai atitinka kompiuterių programų kaip apsaugos objekto ypatumus. Antra, ankstyvosios kompiuterių programos, ypač išreikštos popieriuje, buvo gana panašios į kalbines ar gramatines struktūras, todėl suprantama, kodėl konkrečia teisinės apsaugos forma pasirinktos autorių teisės. Trečia, tradicinė autorių teisė nereikalauja iš autorių ar autorių teisių turėtojų atlikti kokias nors procedūras tam, kad jų kūriniai būtų saugomi autorių teisėmis, – pats kūrinio sukūrimas yra teisinis faktas, lemiantis autorių teisių taikymą, todėl tokia teisinė apsauga yra paprasta ir pigi. Be to, būtina turėti omenyje, kad intelektinės nuosavybės teisės, ypač autorių teisės, turi gana senas tradicijas, yra suvienodinti tarptautiniu mastu, įtvirtinti praktikoje ir pažįstami teisės institutai, tai ypač svarbu taikant teisę. Šie antriniai faktoriai taip pat prisidėjo pasirenkant autorių teises kaip pagrindinę kompiuterių programų teisinės apsaugos formą.

Pradedant 1980 m. Jungtinių Amerikos Valstijų autorių teisių akto pakeitimais, kompiuterių programų bei duomenų bazių teisinei apsaugai buvo pradėtos taikyti autorių teisės normos, t. y. kompiuterių programos buvo pradėtos laikyti autorių teisių objektais nustatant, kad kompiuterių programos saugomos taip pat kaip literatūros kūriniai. Tapačios nuostatos 1984 m. įtrauktos į Australijos, 1985 m. į Japonijos, Prancūzijos ir Jungtinės Karalystės autorių teisių įstatymus, taip pat įsigalėjo šių šalių teismų praktikoje. Pirmosios pastangos nustatyti autorinę teisinę apsaugą kompiuterių programoms – tik nežymūs pakeitimai esamuose autorių teises reglamentuojančiuose norminiuose

aktuose: kompiuterių programos buvo įvardintos kaip autorių teisių objektas, tuo pačiu įtvirtinta taisyklė, kad kompiuterių programoms taikomos taisyklės ir principai tapatūs literatūros kūrinių teisinei apsaugai, kurios pagrindinės nuostatos suformuluotos 1886 m. rugsėjo 9 d. Berno konvencijoje dėl literatūros ir meno kūrinių apsaugos.

Netrukus po šių pirminių pakeitimų autorių teisė, taikoma kompiuterių programoms, išsiplėtė iki savarankiško intelektinės nuosavybės instituto, kurį su tradicine autorių teise sieja tik bendri pagrindiniai principai, t. y. pradėjo formuotis savarankiški kompiuterių programų teisinės apsaugos institutai.

1991 m. gegužės 14 d. Europos Sąjungos Ministrų Taryba priėmė direktyvą dėl kompiuterių programų teisinės apsaugos Nr. 91/250/EEB, kurią iki šiol galima laikyti vienu iš išsamiausių bandymų reglamentuoti kompiuterių programų autorinę teisinę apsaugą. Svarbu pažymėti, kad direktyvos Nr. 91/250/EEB preambulėje nurodyta, kad kompiuterių programų apsauga pagal autorinę teisę jokiu būdu neapriboja kitų galimų kompiuterių programų apsaugos formų. Direktyvos Nr. 91/250/EEB nuostatas šiuo metu papildo keletas kitų direktyvų, susijusių su autorių teisėmis, tame tarpe – direktyva Nr. 92/100/EEB dėl intelektinės nuosavybės nuomos ir panaudos teisių, direktyva Nr. 93/83/EEB dėl autorių teises ir gretutines teises reglamentuojančių taisyklių suvienodinimo palydovinių bei kabelinių transliacijų srityje, direktyva Nr. 93/98/EEB dėl autorių teisių apsaugos terminų suvienodinimo, direktyva Nr. 2001/29/EB dėl kai kurių autorių teisių ir gretutinių teisių aspektų informacinėje visuomenėje. Visos šios direktyvos įgyvendintos Lietuvos Respublikos autorių teisių ir gretutinių teisių įstatyme ir kituose įstatymuose.

Kompiuterių programų autorinę teisinę apsaugą tarptautiniu mastu galutinai įtvirtino Sutartis dėl intelektinės nuosavybės teisių prekyboje aspektų (TRIPS), taip pat 1996 m. gruodžio 20 d. PINO autorių teisių sutartis. Pastaroji sutartis įtvirtino keletą naujų autorių teisių principų – autoriaus ar teisių turėtojo teisių galiojimą elektroninėje erdvėje, teisinę apsaugą techninės apsaugos priemonėms, taip pat galimybę išplėsti teisinės apsaugos išimtis. Šie principai išplėtoti Europos Sąjungos direktyvoje Nr. 2001/29/EC dėl kai kurių autorių teisių ir gretutinių teisių aspektų informacinėje visuomenėje.

3.4.4. Pagrindiniai kompiuterių programų autorinės teisinės apsaugos principai

Autorių teisės taikomos kompiuterių programoms vadovaujantis trimis teisinės apsaugos principais:

1) programa saugoma pagal autorinę teisę taip pat kaip literatūros kūrinys;
2) programa saugoma nepriklausomai nuo jos išraiškos formos;
3) programa saugoma tik tuo atveju, jei ji yra originali.

Kompiuterių programos turi būti saugomos autorių teisės normomis kaip literatūros kūriniai pagal Berno konvenciją dėl literatūros ir meno kūrinių apsaugos. Nuoroda į Berno konvenciją suprantama kaip nuoroda į autorių teisių principų, nustatytų Berno konvencijoje, galiojimą kompiuterių programoms, tačiau ji nereiškia, kad kompiuterių programa visiškai sutapatinama su literatūros kūriniu. Kompiuterių programos teisinė apsauga apima ir programos paruošiamąją medžiagą ir sąsajas, kas iš esmės apima aukščiau aptartus techninius kompiuterių programos elementus, kurių visuma sudaro kompiuterių programą. Paminėtina, kad kai kurios šiuolaikinės programos, pavyzdžiui, tvarkyklės, pagal savo funkcijas gali būti prilygintos sąsajoms, todėl jų teisinė apsauga yra ypač svarbi.

Pagal bendrą autorių teisių principą autorių teisės į kompiuterių programą atsiranda nuo jo sukūrimo momento, t. y. nuo kompiuterių programos išeities kodo užbaigimo momento. Sukurta programa turi būti užfiksuota bet kokioje materialioje laikmenoje, kad ją galėtų suvokti kiti asmenys. Kompiuterių programos kūrimo paruošiamosios medžiagos teisinė apsauga turėtų būti nustatyta nuo to momento, kai paruošiamoji medžiaga pasiekia tokį kokybinį lygį, jog ją naudojant vėlesniame etape galima sukurti baigtinę kompiuterių programą; teisinė apsauga, taikytina paruošiamajai medžiagai, prilyginama teisinei apsaugai, kuri bus taikoma baigtinei kompiuterių programai. Teisinė apsauga taikytina kompiuterių programoms, išreikštoms bet kokia forma. Kadangi būna autorystės nustatymo sunkumų, autorių teisių turėtojams rekomenduotina pasirūpinti autorystės užfiksavimo mechanizmu, pavyzdžiui, įtraukti į kompiuterių programą individualizuotas programos kodo eilutes, įterpti komentarus, sąmoningas klaidas ir pan. Kompiuterių programų registravimas dažnai yra sudėtingas ir menkavertis jų autorystės ir sukūrimo laiko įrodymas.

Idėjos ir išraiškos dichotomijos doktrina yra ypač svarbi kompiu-

terių programoms. Ši doktrina daugeliu atvejų lemia kompiuterių programų tekstinių ir netekstinių išraiškos elementų teisinės apsaugos ribas. Idėjos ir išraiškos dichotomijos doktrinos taikymas kompiuterių programoms sudėtingas tuomet, kai programuotojas turi labai ribotas išraiškos priemones, kad kompiuterių programoje įgyvendintų tas pačias idėjas ir principus.

Pagal pamatinį autorių teisių principą kompiuterių programa turi būti saugoma, jei ji yra originali, t. y. ji yra paties autoriaus intelektinės veiklos rezultatas. Jokie kiti kriterijai negali būti taikomi siekiant nustatyti, ar programa yra saugotina. Siekiant patikrinti programos originalumą negali būti taikomi kiekybiniai ar estetiniai kriterijai. Berno konvencija ar kiti tarptautiniai dokumentai nepateikia jokių kriterijų, kas laikytina „kūriniu“ kiekybės ir kokybės požiūriu, taip pat nėra jokių „originalumo“ kriterijų. Deja, tai, kas sudaro kūrinį, o kompiuterių programų atveju – kelių eilučių kodas yra laikytinas programa, turi būti vertinama individualiai, nėra aiškių objektyvių kriterijų. Sprendžiant tokias situacijas reikėtų įvertinti, ar konkretus kodas yra naujas, ar šis kodas yra pakeičiamas (t. y. ar galimos kitos išraiškos), ar nustatytas atgaminimo faktas ir kokiais tikslais jis buvo atliktas, o sprendžiant klausimą, ar konkretus kodas gali būti pripažįstamas savarankiška kompiuterių programa, būtina įvertinti, ar šis kodas gali atlikti tam tikrą savarankišką funkciją bei pasiekti konkretų rezultatą.

Kompiuterių programų teisinei apsaugai taikomos ir yra ypač svarbios autorinės teisės objekto ribojimo doktrinos, idėjos ir išraiškos dichotomijos doktrina, taip pat *scenes-a-faire* doktrina.

Apibendrinant galima teigti, kad kompiuterių programų autorinė apsauga yra tapati literatūros kūrinių autorinei apsaugai. Svarbiausia kompiuterių programų autorinės apsaugos problema (ir ribotumas) yra kompiuterių programų netekstinių elementų apsauga. Pagal tradicinius autorių teisių principus autorių teisė efektyviai saugo tik nuo kompiuterių programų tiesioginio atgaminimo, o autorių teisės suteikiama apsauga nuo netiesioginio atgaminimo, kai naudojami ribotos išraiškos, tačiau nauji ir efektyvūs techniniai sprendimai, yra nepakankama. Ši aplinkybė tapo viena iš svarbiausių prielaidų patentinei kompiuterių programų apsaugai.

Neturtinių autorių teisių, ypač teisės į kūrinio pavadinimą ir autoriaus vardo nurodymą, teisės į kūrinio neliečiamumą ar teisės sunaikinti kūrinį, taikymas kompiuterių programoms ir kitiems utilitarinio

pobūdžio kūriniams gali būti nesuderinamas su turtinėmis teisėmis į kompiuterių programą. Neturtinių autoriaus teisių nesuderinamumas su kompiuterių programomis buvo pabrėžtas dar XX a. devintajame dešimtmetyje. Dėl utilitarinio ir techninio kompiuterių programų pobūdžio ir jurisprudencijos daugelyje valstybių neturtinės autorių teisės, taikomos kompiuterių programoms, yra arba apribotos, arba leidžiamas neturtinių teisių į kompiuterių programas atsisakymas ar perleidimas.

Išimtinės turtinės autorių teisės į kompiuterių programą yra tapačios turtinėms teisėms į bet kokius kitokius kūrinius. Kompiuterių programoms iš esmės svarbesnės yra turtinių teisių išimtys. Kompiuterių programų, kaip teisinės apsaugos objekto, technologiniai ypatumai lemia skirtingas autoriaus (teisių turėtojo) teisių į kompiuterių programas išimtis. Išimčių turinys yra gana vienodas tarptautiniu mastu, o bendrasis jų principas yra būtinumas sąžiningai naudoti kompiuterių programas pagal jų tiesioginę paskirtį. Ypač specifinė išimtis iš autoriaus (teisių turėtojo) teisių yra programos naudotojo teisė dekompiliuoti programą ar jos dalį siekiant suderinti su kitomis. Programos įprastas naudojimas – įkrovimas į kompiuterio techninę įrangą ir paleidimas, taip pat techninis aptarnavimas yra veiksmai, kurie techniškai reikalauja programos atgaminimo, todėl formaliai jiems reikalingas autorių teisių subjekto sutikimas, tačiau šiais atvejais turi būti laikoma, kad toks sutikimas yra gautas, jei įgyta teisė naudotis pačia programa ar jos kopija. Atskirai svarbu atkreipti dėmesį į informacinės visuomenės paslaugų teikėjų atsakomybės problemas. Teikiant interneto prieigos ar informacijos perdavimo bei talpinimo paslaugas techniškai būtina laikinai atgaminti siunčiamą informaciją (tarp jų – kompiuterių programas) panašiai kaip ir įprastai naudojant kompiuterių programas, todėl būtina speciali išimtis laikinam techniniam atgaminimui. Be to, turi būti apribota paslaugų teikėjų atsakomybė tuo atveju, kai šių paslaugų vartotojai teikėjo kompiuterių tinklais perduoda arba paslaugų teikėjo serveryje talpina neteisėtas kompiuterių programų kopijas, kur jomis gali naudotis kiti asmenys.

Kompiuterių programų autorių teisių turėtojai paprastai reglamentuoja kompiuterių programų naudotojų teises licencinėmis sutartimis, kuriomis šios teisės į kompiuterių programą gali būti perduodamos visiškai arba iš dalies. Plačiai paplito ir teisiškai pripažįstamos vadinamosios atplėšiamos kompiuterių programų pakuotės *(shrink-wrap)* bei elektroninės licencinės sutartys.

Kompiuterių programų atgaminimas, pritaikymas ir keitimas gali būti atliekami teisių turėtojui nesutikus, jei tokie veiksmai yra būtini teisėtam įgijėjui kompiuterių programas naudojant pagal paskirtį (įkraunant, paleidžiant ir pan.), taip pat taisant klaidas. Tai galioja teisėtam programos įgijėjui, t. y. tik asmeniui, kuris teisėtai turi programos kopiją, taip pat turi teisę naudotis ta programa. Pažymėtina, kad programos paskirtis gali būti apibrėžta licencinėje sutartyje, kurioje gali būti numatytos programos naudojimo sąlygos (vartotojų skaičius, įranga, vieta ir pan.), taip pat funkcijos, kurias turi atlikti programa (pvz., teksto procesorius, interneto naršyklė ir pan.). Licencinėse sutartyse neretai leidžiama programą naudoti tik konkrečiame kompiuteryje, iš anksto nustatomas tam tikras programos paleidimų skaičius arba programą leidžiama naudoti tik tam tikrą laiką po jos įgijimo (pastarosios nuostatos ypač dažnai pasitaiko kompiuterių programų demonstracinių versijų (*shareware*) ar preliminariųjų kompiuterių programų versijų (vadinamųjų *beta* versijų) licencinėse sutartyse). Jei sutartyje nieko nenurodyta, programos paskirtį lemia faktinės aplinkybės, pavyzdžiui, programos gebėjimas atlikti tam tikras užduotis, galimybė perkelti programą iš vienos sistemos į kitą jos nepakeitus, techniniai apribojimai, kurie gali būti nustatyti vartotojų skaičiui ir pan. Klaidų taisymas taip pat gali būti papildomai reglamentuotas licencinėje sutartyje. Licencinės sutarties nuostatas, reglamentuojančias programos klaidų taisymą, būtina suderinti su nuostatomis, leidžiančiomis vartotojui atskleisti ir taisyti programos kodą, kadangi techniškai gali būti labai sunku ar net neįmanoma ištaisyti programos klaidas nepakeitus programos kodo. Kadangi kompiuterių programų autorių teisių turėtojai stengiasi neatskleisti programos kodo, dažnai licencinėse sutartyse tiesiog draudžiama pačiam vartotojui taisyti klaidas siūlant tam tikras klaidų taisymo ir vartotojo aptarnavimo paslaugas. Dėl minėtų priežasčių apskritai galima pastebėti vis didesnę licencinių sutarčių svarbą kompiuterių programų apsaugai.

Teisėtam kompiuterių programos naudotojui turi būti leidžiama sukurti atsarginę programos kopiją. Atsarginės kopijos sukūrimas negali būti draudžiamas sutartimis, jeigu asmuo turi teisę naudoti programą ir tai yra reikalinga naudojant programą. Tais atvejais, kai atsarginę programos kopiją pateikia pats programos platintojas, naujos atsarginės kopijos sukūrimas negali būti leistinas. Jei pasibaigia teisė naudoti programą, jokia kopija, įskaitant ir atsarginę, negali būti kuriama. Netekus teisės naudoti programą, visos atsarginės kopijos

turi būti sunaikintos. Tai svarbu ir įvairių riboto naudojimo programų atveju, pavyzdžiui, bandomoji programos kopija turėtų būti sunaikinta (ištrinta) pasibaigus bandymo laikotarpiui.

Kaip jau minėta, kompiuterių programų autorinė apsauga yra paprasčiausias ir pigiausias kompiuterių programų teisinės apsaugos būdas, kuris nereikalauja iš kompiuterių programų gamintojų jokių papildomų pastangų ar investicijų. Kūrinio – kompiuterių programos arba net jos dalių arba funkcinių schemų – sukūrimo faktas yra vienintelė ir pakankama sąlyga taikant autorinę teisinę apsaugą. Šios autorinės teisinės apsaugos ypatybės lemia, jog autorinė teisinė apsauga išlieka pakankamai svarbi kompiuterių programų teisinės apsaugos forma. Autorinės teisinės apsaugos taip pat pakanka saugant kompiuterių programas nuo tiesioginio neteisėto atgaminimo ir platinimo – „piratavimo“. Tačiau autorių teisės negali apsaugoti inovatyvių ribotos išraiškos sprendimų, panaudotų kompiuterių programose, be to, tradiciškai autorių teisės numato išimtis, kurios apriboja investicijų grąžą.

3.4.5. Kompiuterių programų patentinės apsaugos principai

Noras apsaugoti kompiuterių programų elementus, nesaugomus autorių teisės, taip pat siekis išvengti tradicinių autorių teisių išimčių lėmė alternatyvių kompiuterių programų teisinės apsaugos formų paiešką. Kaip alternatyva autorių teisėms pradėta taikyti patentinė apsauga. Patentinę apsaugą iš pradžių pradėta taikyti techniniams mechanizmams, prie kurių buvo priskirtas kompiuterių programa valdomas kompiuteris, vėliau – atskiriems kompiuterių programų techniniams elementams, o šiuo metu ir kompiuterių programoms *per se*, net matematiniams algoritmams ir matematiniams bei verslo metodams, išreikštiems kompiuterių programų pagalba. Tradicinė patentų teisė skirta apsaugoti techninius išradimus – inovatyvių idėjų techninį pritaikymą, sukuriantį tam tikrą techninį rezultatą, todėl kompiuterių programos, veiklos būdai ir metodai tradiciškai priskiriami prie nepatentuotinų objektų. Vien dėl šios priežasties kyla pagrįstų abejonių, ar techniniams išradimams skirta sistema tinka saugant išradimus elektroninėje erdvėje. Kompiuterių programų patentinė apsauga iki šiol yra kontroversiška problema, iš esmės skiriasi nacionalinių patentų biurų nuostatos šiuo klausimu. Kitaip nei autorių teisės, patentai yra registruojamos, brangios ir nacionaliniu mastu ribotos teisės.

Jungtinių Amerikos Valstijų kompiuterių programoms ypač dažnai taikoma patentinė apsauga. Šiuo metu Jungtinėse Amerikos Valstijose iš esmės leidžiamas kompiuterių programų patentavimas *per se*, jei patento objektas atitinka tradicinius reikalavimus patentui: naujumą, išradimo lygį ir yra naudingas (techninio pritaikomumo kriterijus faktiškai pakeistas į naudingumo kriterijų). Europoje kompiuterių programų patentinė apsauga paplitusi mažiau negu Jungtinėse Amerikos Valstijose, tačiau prieinama netiesiogiai. Tokią situaciją iš dalies lemia Europos Sąjungos patentinės politikos nenuoseklumas. Kompiuterių programų patentavimui Europoje ypač reikšminga 1973 m. Europos patentų konvencija, kurios 52 straipsnio 2 dalis įtvirtina principą, kad kompiuterių programos *per se* negali būti patentinės apsaugos (patento) objektas. Naudodamas *per se* išlygą Europos patentų biuras kompiuterių programų patentavimo draudimą interpretavo labai liberaliai.

Itin kontroversiškai nagrinėjamas kompiuterių programų patentinės apsaugos srities klausimas, ar galima įgyti patentą matematiniams algoritmams, kurie sudaro bet kokios kompiuterių programos pagrindą.

Naujausia praktika pripažįsta: jeigu paprastas kompiuteris, vykdydamas specialią kompiuterių programą, pasiekia naujų objektyvių rezultatų, šis kompiuterio ir kompiuterių programos kompleksas gali būti laikomas specialiu, kokybiškai nauju mechanizmu, kuris gali būti patentuojamas, jei tenkinami įprasti patentabilumo kriterijai. Svarbu, kad patentinė paraiška būtų suformuluota apimant procesą, kuris įgyvendinamas kompiuterių programą įkrovus į kompiuterį ir vykdant tam tikras funkcijas, arba kad paraiška būtų suformuluota apimant gaminį, kuris pagamintas kompiuterių programą susiejus su tam tikra materialia struktūra, pavyzdžiui, magnetine laikmena ar kompiuterio atmintimi. Kad atitiktų patentabilumo kriterijus, patentavimui pateiktas procesas turi arba sukelti tam tikras fizines transformacijas ne kompiuteryje, arba turi būti apribotas konkrečiu naudojimo būdu ir technologijos sritimi. Šiuo metu kompiuterių programos patentuotinumui pakanka vienintelio kriterijaus – „naudingo, konkretaus ir materialaus rezultato“.

Nors aukščiau išdėstyta kompiuterių programų patentavimo tvarka iš esmės yra pagrįsta, praktinė problema, su kuria susiduriama patentuojant kompiuterių programas, yra tradicinių patentuotinumo kriterijų, ypač naujumo ir išradimo lygio reikalavimų vertinimo, sudė-

tingumas kompiuterių programų atveju. Vien dėl šios priežasties yra išduota daugybė patentų, kurie akivaizdžiai neatitinka tradicinių patentuotinumo kriterijų, tačiau jų nuginčijimas yra painus (dėl didelių sąnaudų ir tradicinių patentų teisėtumo prezumpcijų). Be to, kompiuterių programų patentai aktyviai pradėti naudoti ne inovacijų apsaugos, o konkurencijos ribojimo tikslais. Kompiuterių programų (matematinių algoritmų ir verslo metodų) patentavimo kritikai nurodo, kad tokie patentai prieštarauja patentų teisės socialiniams tikslams ir vietoj to, kad skatintų inovacijas, ekonominį vystymąsi ir konkurenciją, juos nepagrįstai suvaržo, skatina rinkos monopolizaciją, užkerta kelią naujų rinkos dalyvių, ypač nedidelių ir vidutinių įmonių, atsiradimui ir atvirojo kodo kompiuterių programų plėtrai.

Nors vertinimai kontroversiški, vis dėlto galima daryti išvadą, kad kompiuterių patentavimas pernelyg išplito, negalima jo atsisakyti. Iš kitos pusės yra akivaizdus poreikis užtikrinti nuoseklų tradicinių patentuotinumo kriterijų taikymą ir veiksmingas priemones prieš piktnaudžiavimą patentų sistema.

Panašias taisykles ilgainiui suformulavo ir Europos patentų biuras, interpretuodamas Europos patentų konvencijos Nr. 52(3) straipsnyje numatytą *per se* išlygą. Europos patentų biuro praktika šiandien beveik atmetė Europos patentų konvencijos 52(2)(c) straipsnio draudimą patentuoti kompiuterių programas. Draudimo, įtvirtinto Europos patentų konvencijos 52(2)(c) straipsnyje, priežastys glūdi europietiškoje patentų teisės tradicijoje, kuri numato patentinę apsaugą tik techninio pobūdžio išradimams. Tradiciškai kompiuterių programos laikytos panašiomis į literatūros kūrinius, todėl pagal šį tradicinį vertinimą net ir be esamos tiesioginės išimties jų neturėtų apimti patentabilaus išradimo samprata. Iš kitos pusės toks aiškinimas lemia, kad išradimai, susiję su kompiuterių programomis arba kuriuose kompiuterių programos sudaro tik dalį, gali būti patentuojami, jeigu jie atitinka bendruosius patentuotinumo kriterijus. Naujausia praktika EPO *de facto* panaikino 1973 m. Europos patentų konvencijoje numatytą kompiuterių programų *per se* patentuotinumo išimtį.

Jungtinių Amerikos Valstijų patentų ir prekių ženklų biuro nuostata (naudingumo teorija) ir Europos patentų biuro nuostata (techninio efekto teorija) dėl kompiuterių programų patentinės apsaugos yra panašios. Nors Europos Sąjungos Parlamentas 2005 m. nepritarė pateiktam direktyvos dėl kompiuterinių išradimų patentinės apsaugos projektui, bet tai neapribojo kompiuterių programų patentinės

apsaugos galimybių. Šis nepritarimas veikiau turėtų būti suprastas kaip signalas atidžiau vertinti kompiuterių programų patentų kokybę.

Šiuo metu kompiuterių programų patento objektu gali būti kompiuterių programa *per se*, jeigu tokia kompiuterių programa atitinka įprastus naujumo, išradimo lygio kriterijus ir specialų naudingumo ar techninio įnašo kriterijų, kuris pasireiškia tuo, kad kompiuterių programą vykdanti įprasta techninė įranga gali sukelti tam tikrus padarinius ar pakitimus techninėje srityje.

Patentinė apsauga negali ir neturi pakeisti kompiuterių programų autorinės teisinės apsaugos. Ji gali būti taikoma papildomai, kai kompiuterių programoje yra įgyvendintas išradimas. Patentinės apsaugos svarbiausias pranašumas yra tvirta ir besąlygiška teisinė apsauga, beveik neturinti išimčių, kaip autorių teisės (įskaitant idėjos ir išraiškos sutapimo, *scenes-a-faire* doktrinas). Bet koks patentuoto kompiuterių programos elemento naudojimas bus laikomas patento pažeidimu. Iš kitos pusės neverta pamiršti esminių patentų trūkumų: patento gavimo procedūra, skirtingai nuo autorinės teisės realizavimo mechanizmo, yra formalizuota, ilgai trunka, yra brangi, be to, apribota valstybės sienų. Kad patentas galiotų, per patento galiojimo laikotarpį reikia mokėti patento palaikymo mokesčius, kurie didėja progresyvine tvarka kartu su patento galiojimo terminais. Dauguma šiuolaikinių kompiuterių programų inovacijų yra inkrementinio pobūdžio, todėl gali neatitikti išradimo lygio kriterijų, be to, inkrementinio pobūdžio inovacijos yra pagrįstos tokių pačių ankstesnių inovacijų naudojimu. Inkrementinių inovacijų patentavimas nepaprastai apsunkintų patentų sistemą, be to, būtų beveik neįmanomas jų licencijavimas (dėl daugybės licencijų būtinybės). Tokioje sparčiai besivystančioje srityje kaip kompiuterių programų kūrimas nepriimtina ir tai, kad nuo patentinės paraiškos pateikimo momento iki patento išdavimo dažniausiai praeina gana daug laiko, tuo tarpu pats patento galiojimo laikas (20 metų) yra akivaizdžiai per ilgas kompiuterių programoms, kurios pasensta per metus. Patentinės paraiškos daugelyje jurisdikcijų skelbiamos viešai (taip atskleidžiant informaciją konkurentams). Dėl patentinės apsaugos brangumo ir sudėtingumo individualūs programuotojai ir nedidelės įmonės beveik prarado galimybes savarankiškai įgyti patentus, o kompiuterių programų natūrali monopolizacija lėmė šiuolaikinės kompiuterių programų industrijos koncentraciją, kuri savo ruožtu sudarė ypač palankias sąlygas konkurencijos ir vartotojų teisių pažeidimams.

3.4.6. Kitos kompiuterių programų teisinės apsaugos formos

Kaip minėta, dėl autorių teisių ribotumo ir patentinės apsaugos kontroversiškumo dar XX a. aštuntame dešimtmetyje buvo siūlyta kompiuterių programoms taikyti ypatingą – *sui generis* – teisinę apsaugą. Tačiau išsivysčiusioms pasaulio valstybėms pagrindine kompiuterių programų teisinės apsaugos forma pasirinkus autorių teisę, *sui generis* teisinės apsaugos pasiūlymai laikinai buvo užmiršti.

Šiuo metu kompiuterių programoms pritaikytos modifikuotos autorių teisių ir patentų teisės normos, kurios ilgainiui įgijo esminių skirtumų nuo tradicinių kūrinių apsaugai taikomų taisyklių, leidžia kalbėti apie *de facto* kompiuterių programų *sui generis* teisinę apsaugą. Pagrindą šiai išvadai suteikia ir praktinis *sui generis* teisinės apsaugos pritaikymas kitiems žinių ekonomikos produktams – puslaidininkių gaminių topografijoms ir, ypač, duomenų bazėms. *Sui generis* teisinė apsauga, pagrįsta autorių teisės apsaugos objekto išplėtimu, įtvirtinta Europos Sąjungos direktyvoje dėl duomenų bazių teisinės apsaugos Nr. 96/9/EB.

Prie *sui generis* teisinės apsaugos galima priskirti ir siūlymus taikyti kompiuterių programoms labai ribotą teisinę apsaugą arba jos apskritai atsisakyti. Šie pasiūlymai pastaruoju metu įgavo išraišką Atvirojo kodo ir Kūrybinės bendrumos judėjimuose. Atvirojo kodo kompiuterių programos reikalauja tik tiek teisinės apsaugos, kad užtikrintų šių programų kodo nuolatinį atvirumą, t. y. kodo viešumą ir nevaržomą galimybę naudoti diegiant tolimesnes inovacijas. Paminėtina, kad atvirumas nesiejamas su neatlygintinumu. Kitokia kompiuterių programų teisinė apsauga, ypač patentai kompiuterių programų algoritmams, kelia tiesioginę grėsmę atvirojo kodo programinei įrangai, kadangi riboja galimybes šias inovacijas naudoti naujoms inovacijoms. Šis argumentas buvo viena iš svarbiausių priežasčių, dėl kurių Europos Sąjungos Parlamentas nepritarė direktyvos dėl išradimų, susijusių su kompiuteriais, projektui. Atvirojo kodo kompiuterių programų apsaugai šiuo metu itin svarbios licencinės sutartys, o ne intelektinės nuosavybės įstatymai. Nenuoseklus ir išimtinai nacionalinis licencinių sutarčių reglamentavimas (ir su tuo susijusios jų įgyvendinimo problemos) yra viena iš atvirojo kodo kompiuterių programų raidos kliūčių.

Kaip subsidiari kompiuterių programų teisinė apsauga, įvairiose

valstybėse taip pat taikoma komercinių paslapčių apsauga, prekių ir paslaugų ženklai. Šie intelektinės nuosavybės institutai padeda apsaugoti atskirus kompiuterių programų elementus, pavyzdžiui, originalias grafines, vaizdo ir garso išraiškas, taip pat saugo kompiuterių programas, kliudydami gaminti neteisėtas kompiuterių programų kopijas, o jas pagaminus užtraukia papildomą teisinę atsakomybę.

Kompiuterių programų apsaugai taip pat pasitelkiamos techninės apsaugos priemonės, kurioms nustatyta speciali teisinė apsauga, draudžianti techninių apsaugos priemonių pažeidimus. Techninių apsaugos priemonių teisinė apsauga visų pirma įtvirtinta 1996 m. PINO autorių teisių sutartyje, taip pat Europos Sąjungos direktyvoje Nr. 2001/29/EB dėl kai kurių autorių teisių ir gretutinių teisių aspektų informacinėje visuomenėje. Tačiau techninės apsaugos priemonės gali užkirsti kelią ne tik neteisėtai naudoti kompiuterių programas, bet ir teisėtiems veiksmams, pavyzdžiui, kompiuterių programos atgaminimui ar dekompiliavimui siekiant užtikrinti šios kompiuterių programos dermę su naujai kuriama kompiuterių programa. Deja, esamas techninių apsaugos priemonių reguliavimas iš esmės nenumato veiksmingų mechanizmų, užtikrinančių sąžiningo naudotojo teises.

Kompiuterių programos ypatingos tuo, kad tai yra savo forma ir turiniu itin sparčiai tobulėjantis intelektinės nuosavybės objektas. Kaip minėta aukščiau, autorių teisė ir patentai sunkiai dera su šia kompiuterių programų savybe: kompiuterių programų naudojimo laikas yra labai trumpas (dažniausiai trumpesnis negu 5 metai), tuo tarpu patentų ir, ypač, autorių teisių galiojimo terminai daug ilgesni, be to, kompiuterių programos neturi jokios išliekamosios ar kultūrinės vertės. Vien dėl šių priežasčių galima pritarti nuomonėms, jog esamos kompiuterių programų teisinės apsaugos formos yra nepakankamos ir negali patenkinti informacinės visuomenės poreikių, todėl būtina tolesnė kompiuterių programų teisinės apsaugos reforma.

3.4.7. Kompiuterių programų teisinės apsaugos ypatumai Lietuvoje

Lietuvoje kompiuterių programų teisinė apsauga užtikrinama daugiausia autorių teisėmis, taip pat įmanoma ir kompiuterių programų patentinė apsauga. Autorių teisių ir gretutinių teisių įstatymo 2 straipsnio nuostatos pateikia įstatyme vartojamus terminus, sąvokas, taip pat ir kompiuterių programos sąvoką. Kompiuterių programa apibrė-

žiama kaip visuma instrukcijų, pateikiamų žodžiais, kodais, schemomis ar kitu pavidalu, kurios įgalina kompiuterį atlikti tam tikrą užduotį ar pasiekti tam tikrą rezultatą, kai tos instrukcijos pateikiamos tokiomis priemonėmis, kurias kompiuteris gali perskaityti; ši sąvoka apima ir parengiamąją projektinę tokių instrukcijų medžiagą, jeigu iš jos galima sukurti minėtą instrukcijų visumą. Sąvoka atskiria kompiuterių programą ir kompiuterių programą lydinčią medžiagą (aprašymus, vartotojų instrukcijas ir panašią, į programą integruotus garso ir vaizdo kūrinius – originalias garso ir vaizdo išraiškas). Kompiuterių programos aprašymai, vartotojo instrukcijos, originalios garso ir vaizdo išraiškos yra kitokios prigimties negu kompiuterių programa, todėl pateiktus kartu su kompiuterių programa arba integruotai su kompiuterių programa neišnyksta kaip savarankiški kūriniai ir turėtų būti saugomi kaip savarankiški įprasti autoriniai kūriniai ar gretutinių teisių objektai. Tais atvejais, kai kompiuterių programos vaizdinis ir garsinis apipavidalinimas sudaro kompiuterių programos sąsajos (dažniausiai – vartotojo sąsajos) sudedamąją dalį, jis laikytinas kompiuterių programos sudedamąja dalimi.

Iš esmės Autorių teisių ir gretutinių teisių įstatyme kompiuterių programoms taikomos bendrosios autorių teisių normos, išskyrus keletą specifinių normų. Kompiuterių programoms ir duomenų bazėms taikomos normos dėl autorių teisių objekto reikalavimų, autorių teisių nesaugomų objektų, subjektų, teisių galiojimo termino, neturtinių autorių teisių, pagrindinių autorių turtinių teisių ir jų išimčių.

Specifinės yra Autorių teisių ir gretutinių teisių įstatymo nuostatos dėl kompiuterių programų, sukurtų darbuotojui atliekant tarnybines pareigas, autorinių teisių. Pagal įstatymo 10 straipsnio 2 dalies nuostatas turtinės teisės į kompiuterių programą, sukurtą darbuotojui einant savo tarnybines pareigas ar vykdant tarnybinę užduotį, priklauso darbdaviui visą jų galiojimo laiką, išskyrus tuos atvejus, kai šalių sutartyje nustatyta kitaip. Ši prezumpcija yra kitokia negu prezumpcija, taikoma įprastiems literatūros ir meno kūriniams, į kuriuos darbdavys įgyja turtines teises tik 5 metams (įstatymo 9 str. 2 d.). Šis skirtumas pabrėžia kompiuterių programos, kaip utilitarinio (taikomojo) kūrinio, prigimtį.

Deja, Autorių teisių ir gretutinių teisių įstatyme neatsižvelgta į prieštaravimą tarp įstatyme įtvirtintų autoriaus asmeninių neturtinių teisių ir turtinių teisių, kadangi įstatyme numatytos turtinės autorių teisės į kompiuterių programas, pavyzdžiui, teisė adaptuoti ar dekom-

piliuoti kompiuterių programą (įstatymo 30 ir 31 str.), prieštarauja autoriaus teisei į kūrinio neliečiamybę, t. y. teisei uždrausti bet kokius kūrinio pakeitimus.

Išimtinės teisės į kompiuterių programas ir šių teisių apribojimai (naudotojų teisės) Lietuvoje reglamentuojami iš esmės taip pat, kaip ir Europos Sąjungos teisės aktuose.

Nors įstatymo 20 straipsnis leidžia kūrinį atgaminti asmeniniais tikslais, ši išimtis netaikoma kompiuterių programoms ir kai kuriems kitiems kūriniams.

Patentų išdavimą Lietuvos Respublikoje reglamentuoja 1994 m. sausio 18 d. Lietuvos Respublikos patentų įstatymas Nr. I-372. Šio įstatymo 2 straipsnio 2 dalies 3 punktas tiesiogiai numato, kad išradimais nelaikomos „kompiuterių programos“. Šios nuostatos perimtos iš 1973 m. Europos patentų konvencijos (Miuncheno konvencijos), kurios narė Lietuva yra nuo 2004 m. spalio 5 d. Lietuvos Respublikos patentų įstatymo 2 straipsnio 2 dalyje beveik tiksliai pakartotos Europos patentų konvencijos 52(2) straipsnio nuostatos, tačiau labai svarbu atkreipti dėmesį, kad kompiuterių programų patentavimo išimtis Lietuvos Respublikos patentų įstatyme suformuluota žymiai plačiau negu 1972 m. Europos patentų konvencijoje, kadangi Lietuvos įstatymas nenumato jokių išlygų, kad minėtas apribojimas taikomas tik kompiuterių programoms *per se*.

Kitaip nei Europos patentų biuras, neoficialus Lietuvos valstybinis patentų biuras, taikydamas minėtas nuostatas, nenumato jokių kompiuterių programų patentavimo galimybių Lietuvoje. Kompiuterių programų patentavimo galimybė Lietuvoje niekada nebuvo išbandyta praktikoje, kadangi Lietuvoje nebuvo pateikta jokių patentinių paraiškų, kurios apimtų kompiuterių programas.

Kompiuterių programų patentavimo negalimumą Lietuvoje lemia kelios priežastys: visų pirma svarbu pažymėti, kad Lietuvos jurisdikcija ir ekonominė rinka multinacionalinių patentų savininkams yra per maža, todėl išlaidos, susijusios su Lietuvos patento gavimu ir išlaikymu, gali tiesiog neatsipirkti; antra, nacionalinė kompiuterių programų industrija yra jauna, nauji produktai dažnai nėra tokie novatoriški, kad atitiktų griežtus patentuotinumo kriterijus; trečia, galimi nacionaliniai išradėjai ir patentuotojai dažnai neturi pakankamai žinių apie galimybes apginti savo intelektualinę nuosavybę patentų teisės priemonėmis; ketvirta, esamas teisinis režimas neskatina multinacionalinių patentų savininkų pateikti patentines paraiškas Lietuvoje, kadangi tas pats rezultatas (teisinė apsauga Lietuvos teritorijoje) gali

būti pasiektas ir žymiai veiksmingesnių Europos patentų dėka, išplečiant jų galiojimą Lietuvoje. Kadangi jau nuo 1995 m. Europos patentų biuro išduoti patentai (Europos patentai) gali galioti Lietuvoje atlikus nesudėtingą nacionalinę procedūrą, kuri neapima patento teisėtumo ar patento objekto patentuotinumo tikrinimo. Atsižvelgiant į tai ir remiantis liberalia Europos patentų biuro praktika galima teigti, kad tikslinga kompiuterių programų išradimams teikti pareiškas pagal Europos patentų konvenciją, vėliau išplečiant Europos patentų galiojimą Lietuvos jurisdikcijoje, o ne pirma siekti nacionalinio patento.

3.5. Papildoma medžiaga. Duomenų bazių teisinė apsauga

Savarankišku intelektinės nuosavybės apsaugos objektu pripažįstamos ne tik kompiuterių programos, bet ir duomenų bazės.

Duomenų bazių teisinė apsauga faktiškai įtvirtinta 1886 m. Berno konvencijoje dėl literatūros ir meno kūrinių apsaugos. Berno konvencijos 2 straipsnio 5 dalis nustatė, kad teisinė apsauga taikoma literatūros ir meno kūrinių rinkiniams, pavyzdžiui, enciklopedijoms ir antologijoms, kurie dėl turinio parinkimo ir išdėstymo yra intelektualinės kūrybos rezultatas, nepažeidžiant autorinės teisės į kiekvieną kūrinį. Literatūros ir meno kūrinių arba tiesiog informacijos rinkiniai faktiškai yra neautomatinės duomenų bazės, pavyzdžiui, Lietuvos Aukščiausiojo Teismo praktikoje duomenų baze vienareikšmiškai pripažinti spausdintiniai žodynai. Duomenų bazėmis laikytinos chrestomatijos, poezijos rinkiniai, bibliotekų katalogai, taip pat bet kokie kiti informacijos rinkiniai, pavyzdžiui, telefonų direktorija, įmonių katalogas. Duomenų bazės yra būtinos atlikti ir daugumą verslo valdymo funkcijų tokių kaip: apskaita ir sąskaityba, atsargų planavimas, ryšių su klientais palaikymas, pardavimų vadyba, personalo vadyba ir t. t.

Lietuvos autorių teisių ir gretutinių teisių įstatymo 2 straipsnyje duomenų bazė apibrėžiama kaip susistemintas ar metodiškai sutvarkytas kūrinių, duomenų arba kitokios medžiagos rinkinys, kuriuo galima individualiai naudotis elektroniniu ar kitu būdu, išskyrus kompiuterių programas, naudojamas kurti ar valdyti tokių duomenų bazes. Autorių teisių ir gretutinių teisių įstatymo 4 straipsnio 3 dalies 2 punkte kūrinių rinkiniai ar duomenų rinkiniai, duomenų bazės (išreikštos techninėmis priemonėmis skaityti pritaikyta ar kita forma), kurie dėl turinio parinkimo ar išdėstymo yra autoriaus intelektinės kūrybos rezultatas, yra įvardinti autorių teisių objektais. Autorių teisės kūrinių rin-

kiniams ir duomenų bazėms taikomos nepažeidžiant autorių teisių į kūrinį ar kūrinius, kurių pagrindu buvo sudarytas rinkinys, bet netaikomos duomenims ar medžiagai, nesantiems autorių teisių objektais, iš kurių sudaryta duomenų bazė.

Atsižvelgiant į Europos Sąjungos direktyvos Nr. 96/9/EB dėl teisinės duomenų bazių apsaugos nuostatas ir užsienio praktiką, duomenų bazę galima apibrėžti tiesiog kaip informacijos rinkinį ar kompiliaciją, išdėstytą arba organizuotą sisteminiu ar metodologiniu būdu. Duomenų bazė jungia pavienę, individualią informaciją į kokybiškai naują informacijos visumą. Pažymėtina, kad duomenų bazę turi sudaryti informacijos daugetas, t. y. turi būti tam tikras minimalus sistemiškai organizuotas informacijos kiekis. Duomenų baze laikytinas ir automatiškai tvarkomas, ir neautomatizuotas (net ir ranka užrašytas) informacijos rinkinys, jei jis išreikštas bet kokia forma.

Pagrindiniai duomenų bazės elementai yra duomenų bazės turinys (informacija – duomenys, kūriniai ir pan.) ir jų tvarkymo priemonės (sąsajos). Automatinių duomenų bazių tvarkymo priemonės (sąsajos) dažniausiai yra specializuotos kompiuterių programos. Duomenų bazės santykis su kompiuterių programomis gali būti dvejopas. Jei duomenų bazių tvarkymui panaudota kompiuterių programa integruota į duomenų bazę taip, kad ja perteikiama duomenų bazės struktūra, tokia programa faktiškai prilyginama duomenų bazei (savo ruožtu duomenų struktūros yra laikomos kompiuterių programų elementu). Tuo atveju, jei kompiuterių programa yra tik duomenų bazės kūrimo ir (ar) tvarkymo (prieigos, keitimo, išsaugojimo) įrankis, tokia programa nelaikoma duomenų bazės dalimi. Atkreiptinas dėmesys, kad ir duomenų bazės turinys, ir duomenų bazės tvarkymo priemonės atskirai gali būti skirtingų intelektinės nuosavybės teisių objektas bei priklausyti skirtingiems intelektinės nuosavybės teisių turėtojams, tačiau teisėtai naudojant šiuos elementus gali būti kuriamas kokybiškai naujas intelektinės nuosavybės objektas – duomenų bazė.

3.5.1. Duomenų bazių teisinės apsaugos formos ir jų principai

Duomenų bazių teisinė apsauga visų pirma užtikrinama autorių teisėmis – kaip minėta, Lietuvos autorių teisių ir gretutinių teisių įstatymo 4 straipsnio 3 dalies 2 punktas laiko duomenų bazes autorių teisių objektu. Duomenų bazės yra saugomos kaip originalūs kūrinių

rinkiniai remiantis bendraisiais autorių teisių principais: laikantis bendrųjų originalumo, teisių išnaudojimo, riboto teisių galiojimo laike ir teritorijoje bei turtinių teisių išimčių taisyklių. Kaip ir bet kokia kita informacija, duomenų bazės taip pat gali būti saugomos kaip komercinės paslaptys. Jų apsaugai šiuo metu pasitelkta daug techninės apsaugos priemonių. Specifinės duomenų bazės gali būti papildomai saugomos ir taikant asmens privatumo, valstybės paslapties ir kitas apsaugos taisykles. Nuo 1996 m. Europos Sąjungoje duomenų bazėms gali būti taikoma ir ypatinga *sui generis* teisinė apsauga, numatyta Europos Sąjungos direktyvoje Nr. 96/9/EB.

Visoms minėtoms duomenų bazių teisinės apsaugos formoms (autorių teisėms, *sui generis* teisėms, komercinių paslapčių apsaugai) nereikia registracijos ar kitų formalių procedūrų, jos atsiranda sukūrus duomenų bazes ir taikomos lygiagrečiai. Tarptautiniu mastu *sui generis* teisės įprastai galioja vadovaujantis vienodumo bei abipusiškumo principais.

Duomenų bazių *sui generis* teisinė apsauga iš esmės skiriasi nuo autorių teisių, nors ir reglamentuojama autorių teisių įstatymuose (pvz., Lietuvos autorių teisių ir gretutinių teisių įstatymo IV skyriaus 61–64 straipsniuose). Nustatant specialią duomenų bazių *sui generis* teisinę apsaugą, Europos Sąjungoje siekta apsaugoti investicijas į duomenų bazių gamybą, ypač tais atvejais, kai galutinės duomenų bazės negali saugoti tradicinė autorių teisė (pvz., dėl neoriginalumo, idėjos ir išraiškos sutapimo, išraiškos ribotumo ir pan.). Duomenų bazių išraiška tradicinių autorių teisių požiūriu iš esmės yra duomenų bazės struktūra, kurią gali lemti objektyvūs ir racionalūs kriterijai (o ne kūrybos laisvė). Dėl šios priežasties, kaip ir kompiuterių programų atveju, autorių teisių taikymas duomenų bazėms gali būti labai ribotas (žr. aukščiau). Duomenų bazių teisinei apsaugai taikant tradicines autorių teises, saugoma tik originali duomenų bazės struktūra (t. y. duomenų bazės gamintojui suteikiamos autorių teisės į duomenų bazės struktūrą), bet ne duomenų bazės turinys (išskyrus atvejį, kai duomenų bazės gamintojas yra ir turinio, kurį sudaro savarankiški autorių teisių objektai, teisių turėtojas). Šiuo atveju duomenų bazės turinys, t. y. individualios informacijos, sudarančios duomenų bazę, vienetai gali būti autorių teisių objektai kaip savarankiški kūriniai, tačiau gali būti ir apskritai nesaugomi autorių teisės, jei jie nėra autorių teisių objektai. Tokio paties turinio (informacijos) alternatyvus originalus parinkimas ir išdėstymas gali būti laikomas nauja duomenų baze, nepažeidžiančia

pirmosios duomenų bazės kūrėjo autorių teisių (pvz., dvi tos pačios poezijos rinktinės, išdėstytos tematiškai ir chronologiškai, iš esmės yra dvi skirtingos duomenų bazės). Tradicinė autorių teisė taip pat nesaugo neoriginalių informacijos rinkinių (nulemtų funkcinių kriterijų, pvz., telefonų sąrašo, išdėstyto abėcėline tvarka) nepriklausomai nuo investicijų.

Be to, taikant tradicines autorių teises, neišvengiamai taikomos ir turtinių teisių išimtys, kurios apriboja duomenų bazių gamintojų galimybes greitai susigrąžinti investicijas į duomenų bazių kūrimą. Tradicinės autorių teisės požiūriu, duomenų bazės gali būti naudojamos švietimo ir mokslinio tyrimo tikslais, daromos jų asmeninės kopijos ir kita. Teisėtas duomenų bazės ar jos kopijos naudotojas turi teisę atlikti bet kokius veiksmus be autoriaus arba kito autorių teisių subjekto leidimo įskaitant duomenų bazės atgaminimą, adaptavimą ir perdavimą, reikalingus siekiant sužinoti duomenų bazės turinį ir juo tinkamai naudotis. Apskritai pažymėtina, kad tradicinių turtinių autorių teisių išimčių apimtis, taikoma duomenų rinkiniams ir duomenų bazėms, yra gana neaiški.

Šie argumentai, taip pat ir spekuliatyvios nuostatos (duomenų bazių verslo skatinimas) lėmė Europos Sąjungos sprendimą nustatyti duomenų bazių *sui generis* teisinę apsaugą.

3.5.2. Duomenų bazių *sui generis* teisinės apsaugos ypatumai

Duomenų bazių *sui generis* teisinė apsauga paremta vadinamąja „esminių investicijų“ doktrina. Ši doktrina teigia, kad duomenų bazės gamintojas, įrodęs, kad parinkdamas, sudarydamas, tikrindamas bei pateikdamas duomenų bazės turinį padarė esminių kokybinių ir (ar) kiekybinių investicijų, turi teisę uždrausti duomenų bazės turinio (viso ar pagrindinės dalies) perkėlimą į kitą laikmeną, viešą platinimą ar perdavimą. Investicijos į duomenų bazės turinį gali būti tiek intelektinės, tiek finansinės, tiek organizacinės, o jų esmingumą lemia kokybiniai ir kiekybiniai kriterijai. Ši doktrina dėl visiško neapibrėžtumo, nekonkretumo ir objektyvių kriterijų nebuvimo gali būti vertinama tik kritiškai. Nors nuo Europos Sąjungos direktyvos Nr. 96/9/EB priėmimo praėjo dešimtmetis, nė vienoje Europos Sąjungos valstybėje įstatymų leidėjai, teismai ar jurisprudencija nesugebėjo suformuluoti aiškių „esminių investicijų“ kriterijų. Pažymėtina, kad rinkos sąlygomis funkcionuojančioje visuomenėje bet koks informacijos tvar-

kymas reikalauja didelių intelektinių, finansinių ir organizacinių sąnaudų. Viena iš pagrindinių to priežasčių – eksponentiškai didėjantis informacijos kiekis ir dažnėjantis naudojimasis duomenų bazėmis kasdieniuose socialiniuose procesuose. Kyla klausimas: ar toks įprastinių duomenų kasdieninis tvarkymas, kuris tam tikrais atvejais gali būti netgi pareiga, o daugeliu atvejų – socialinė būtinybė, taip pat šių duomenų integravimas į masinius produktus arba paslaugas yra pakankama „esminė investicija“?

Sui generis teisės galioja 15 metų nuo duomenų bazės sudarymo datos (skaičiuojant nuo sausio 1 dienos po tų metų, kuriais duomenų bazė buvo sudaryta arba pirmą kartą tapo viešai prieinama), tačiau šis terminas gali būti neribotai pratęstas kiekvieną kartą duomenų bazės turinį papildant ar atnaujinant, t. y. darant papildomas „esmines investicijas“. Tokia *de facto* neterminuota duomenų bazių apsauga yra viena iš kontroversiškiausių duomenų bazių *sui generis* teisinės apsaugos nuostatų, kritikuojama Europos Sąjungos, ypač kitų valstybių mokslininkų. Neterminuotas *sui generis* teisių galiojimas kelia rimtą grėsmę šių teisių socialinei funkcijai ir gali iš esmės suvaržyti informacijos socialinę apytaką, būtiną švietimui, naujoms inovacijoms ir kūrybai, visuomenės kultūrinei ir technologinei pažangai. Pažymėtina, kad duomenų bazės turinio pildymas ir atnaujinimas rinkos sąlygomis yra absoliuti būtinybė, kurią lemia šiuolaikinės visuomenės poreikiai, o ne duomenų bazių gamintojo laisvas pasirinkimas. Neterminuotos *sui generis* teisės sunkiai suderinamos su žmogaus teise į informaciją ir žodžio laisve. Kyla ir etinių klausimų dėl duomenų bazių, kuriose saugomi ir tvarkomi ypatingi duomenys, pvz., asmens duomenys, medicininiai duomenys ir panašūs.

3.5.3. *Sui generis* teisių į duomenų bazes apribojimai

Sui generis teisinei apsaugai nustatyti specifiniai apribojimai bei išimtys. Duomenų bazės, kuri teisėtai bet kuriuo būdu tapo viešai prieinama, gamintojas negali kliudyti teisėtiems duomenų bazės naudotojams perkelti į kitas laikmenas arba naujai panaudoti bet kokiais tikslais nedideles (vertinant kokybiniu ar kiekybiniu požiūriu) duomenų bazės turinio dalis, tačiau duomenų bazės teisėtas naudotojas neturi teisės atlikti veiksmų, kurie prieštarautų įprastam duomenų bazės naudojimui, pažeistų duomenų bazės gamintojo teisėtus interesus arba pažeistų autorių teisių ir gretutinių teisių subjektų teises į kūrinius ir gretutinių teisių objektus, kurie sudaro duomenų bazės turinį. Duo-

menų bazių gamintojui draudžiama sutartimi (licencija) suvaržyti minėtas duomenų bazės gamintojo teises. Neleidžiama daryti pakartotinių duomenų bazės ištraukų ir naudoti nedideles duomenų bazės turinio dalis, kai šie veiksmai trikdo tos duomenų bazės įprastą naudojimą arba pažeidžia teisėtus duomenų bazės gamintojo interesus. Nedidelės duomenų bazės dalys nėra aiškiai apibrėžtos. Remiantis Europos Sąjungos valstybių praktika, nedidelė dalis kiekybiniu požiūriu neturėtų viršyti 10 procentų viso duomenų bazės turinio, o kokybiniu požiūriu turi būti vertinamas duomenų bazės turinio dalies vertingumas, unikalumas ir pakeičiamumas (lyginant su likusia dalimi).

Papildomai numatytos ir duomenų bazės, kuri bet kuriuo būdu tapo viešai prieinama, teisėto naudotojo teisės be duomenų bazės gamintojo leidimo perkelti ar naujai naudoti didesnę duomenų bazės turinio dalį, kai neelektroninės duomenų bazės turinys perkeliamas į kitą laikmeną asmeniškai naudoti; duomenų bazės dalis pateikiama kaip pavyzdys mokymo ar įvairių sričių mokslinio tyrimo tikslais, jeigu yra nurodomas jos šaltinis ir naudojimą atitinka siekiamas nekomercinis tikslas; arba duomenų bazė perkeliama ir naudojama visuomenės ir valstybės saugumo interesais, viešojo administravimo ar teismo proceso tikslais. Naudotojo teisės naudoti didesnę duomenų bazės turinio dalį asmeniškai arba mokymo ar įvairių sričių mokslinio tyrimo tikslais gali būti apribotos sutartimi (licencija). Be to, būtina atkreipti dėmesį, kad visos nurodytos duomenų bazės naudotojo teisės (tiek į nedidelės, tiek į didesnės duomenų bazės turinio dalies naudojimą) gali būti suvaržytos techninėmis duomenų bazių apsaugos priemonėmis, kurios, kitaip nei sutartiniai suvaržymai, nėra draudžiamos, taip pat nenumatytas joks techninių apsaugos priemonių ir naudotojo teisių derinimo mechanizmas.

Nagrinėjant minėtus *sui generis* teisių apribojimus, pastebimas jų neadekvatumas: iš esmės absoliučios ir neterminuotos duomenų bazės gamintojo teisės ir minimalios naudotojo teisės, kurios gali būti lengvai eliminuotos techninėmis apsaugos priemonėmis ar licencijos sąlygomis. Atkreiptinas dėmesys, kad duomenų bazių turinio nedidelių dalių naudojimas ribojamas dėl duomenų bazių gamintojų interesų, o esminės dalies asmeninio naudojimo teisės apskritai taikomos tik neelektroninių duomenų bazių turiniui. Taip nepagrįstai diskriminuojamos neelektroninės duomenų bazės (nors jos gali būti ir vertingesnės kultūriniu požiūriu, ir brangesnis jų sukūrimas). Duomenų bazių turinio esminės dalies naudojimas mokymo ar įvairių sričių moks-

linio tyrimo tikslais taip pat apribotas tik pavyzdžio pateikimu.

Praktiškai didžiausias *sui generis* teisių į duomenų bazes apribojimas yra bendras šių teisių neapibrėžtumas (įstatyminis reikalavimas įrodyti „esmines investicijas“ į duomenų bazės turinį), o ne aukščiau minėtos duomenų bazių naudotojų teisės. Būtent tokią praktiką formuoja Europos Sąjungos valstybių nacionaliniai teismai, taip pat Europos Teisingumo Teismas. Dėl Europos Sąjungos direktyvoje Nr. 96/9/EB įtvirtintų duomenų bazių *sui generis* teisinės apsaugos principų neapibrėžtumo dauguma nacionalinių bylų, susijusių su šių teisių taikymu, patenka į Europos Teisingumo Teismą, kuris formuoja vadinamąją „šalutinio produkto“ (angl. *spin-off*) doktriną, kuria vadovaujantis *sui generis* teisės netaikomos, jei duomenų bazė sukuriama kaip subproduktas veiklos, kurios pagrindinis tikslas nėra duomenų bazės sukūrimas. „Šalutinio produkto“ doktrina faktiškai eliminuoja *sui generis* teisinę apsaugą duomenų bazėms, apimančioms sporto varžybų tvarkaraščius, televizijos programas ir jų sąvadus, telefono numerių duomenų bazes ir pan. Kaip jau minėta, tokios duomenų bazės nėra saugomos ir autorių teisėmis, kadangi jos netenkina originalumo kriterijaus ir nulemtos funkcinių reikalavimų. Deja, teismų praktika kol kas neapibrėžė neaiškių *sui generis* teisių klausimų: „esminių investicijų“ kriterijų, galimybės neterminuotai pratęsti *sui generis* teises ar naudotojų teisių apimtį (teises į nedidelės ar didesnės duomenų bazių turinio dalies panaudojimą), tačiau akivaizdžiai linkstama siaurinti duomenų bazių *sui generis* teisinės apsaugos apimtį.

Apskritai duomenų bazių *sui generis* teisinė apsauga net ir pačioje Europos Sąjungoje atvirai vertinama kaip abejotinas socialinis eksperimentas. Europos Sąjunga, taikydama duomenų bazių *sui generis* teisinę apsaugą, liko vieniša: kitos išsivysčiusios valstybės (Jungtinės Amerikos Valstijos, Japonija, Kanada, Australija) ir besivystančios valstybės šios iniciatyvos nepalaikė. Per dešimt metų Europos Sąjungos direktyva Nr. 96/9/EB nesukėlė duomenų bazių industrijos ar su ja susijusių verslų proveržio Europos Sąjungoje, tuo tarpu Jungtinių Amerikos Valstijų duomenų bazių industrija nepatiria jokių sunkumų ir klesti, nors duomenų bazės saugomos tik tradicinėmis autorių teisėmis, komercinėmis paslaptimis ir techninėmis apsaugos priemonėmis. Dėl šių priežasčių „įšaldytas“ ir Europos Sąjungos inicijuotas PINO duomenų bazių sutarties, kuri nustatytų tarptautinę duomenų bazių *sui generis* teisių apsaugą, pasiūlymas.

3.5.4. Duomenų bazių teisinė apsauga Lietuvoje

Kaip jau minėta, Lietuvoje šiuo metu aiškiai įtvirtinta duomenų bazių teisinė apsauga autorių teisėmis, taip pat duomenų bazių *sui generis* teisinė apsauga. Duomenų bazių *sui generis* teisinės apsaugos normos yra pažodžiui perkeltos iš Europos Sąjungos direktyvos Nr. 96/9/EB jų nė kiek neaiškinant. Autorių teisių normos, taikomos duomenų bazėms, taip pat jau pasenusios ir prieštaringos, ypač neaiškus bendrųjų turtinių autorių teisių išimčių santykis su specifiniu duomenų bazių teisiniu reglamentavimu, taip pat duomenų bazių autorių teisių išimčių santykis su duomenų bazių *sui generis* teisinės apsaugos taisyklėmis (Autorių teisių ir gretutinių teisių įstatymo 32 str. ir 61–64 str.). Lietuvoje nėra teisinių apribojimų duomenų bazių apsaugai taikyti ir komercines paslaptis (neviešoms duomenų bazėms) bei techninės apsaugos priemones, kurios ypač paplitusios praktikoje. Kaip ir kompiuterių programų atveju, didelę reikšmę duomenų bazių teisiniam režimui turi licencinės sutartys, kurios ypač varžo duomenų bazių naudotojų teises.

Deja, Lietuvoje kol kas nėra jokios teismų praktikos dėl duomenų bazių *sui generis* teisinės apsaugos apimties, galiojimo ar apribojimų, tačiau esant būtinybei turėtų būti vadovaujamasi Europos Teisingumo Teismo praktika ir Europos Sąjungos jurisprudencija, taip pat turėtų būti įvertinti duomenų bazių *sui generis* teisinės apsaugos socialinės apsaugos tikslai bei būtinybė užtikrinti teisių turėtojų, naudotojų ir visuomenės interesų pusiausvyrą.

3.6. Papildoma medžiaga. Intelektinės nuosavybės techninių apsaugos priemonių teisiniai aspektai

Siekdami užkirsti kelią intelektinės nuosavybės teisių pažeidimams elektroninėje erdvėje, intelektinės nuosavybės gamintojai ir platintojai greta įprastų teisinių priemonių (teisinės atsakomybės) pradėjo naudoti įvairias technines apsaugos priemones, teisių valdymo mechanizmus ir sutartinius apribojimus autorinių kūrinių ir gretutinių teisių objektų laikmenoms, jų atgaminimui ir net įprastam naudojimui. Tokios techninės apsaugos priemonės dažnai gali būti veiksmingesnės negu atitinkami įstatyminiai draudimai ar ribojimai. Techninėmis apsaugos priemonėmis laikoma bet kokia technologija, įtaisai ar jų sudedamosios dalys, skirti normaliai veikiant uždrausti arba riboti su autorių teisių, gretutinių teisių ar *sui generis* teisių objektais atlieka-

mus veiksmus, kurių neleidžia autorių teisių, gretutinių teisių ar *sui generis* teisių subjektai. Techninės apsaugos priemonės laikomos veiksmingomis, jei saugomo autorių teisių, gretutinių teisių ar *sui generis* teisių objekto naudojimą teisių subjektai kontroliuoja taikydami prieigos kontrolę ar apsaugą (kodavimą, elementų perstatymą arba kitokį intelektinės nuosavybės objekto transformavimą) arba kopijų kontrolės būdą, užtikrinantį siekiamą apsaugą. Techninės apsaugos priemonės neturi trukdyti elektroninei įrangai normaliai veikti ir ją technologiškai tobulinti.

Įsipareigojimai užtikrinti techninių priemonių ir informacijos apie autorių ir gretutinių teisių valdymą teisinę apsaugą įtraukti į TRIPS sutartį ir WIPO interneto sutartis, taip pat Europos Sąjungos norminius aktus.

Skaitmeninėse garso bei vaizdo informacijos laikmenose (kompaktinėse plokštelėse, DVD laikmenose) plačiausiai naudojamas techninis apribojimas yra draudimas skaitmeninę informaciją atkurti skaitmeniniu formatu. Vartotojui naudojant tokią informacijos laikmeną, informacija (fonograma, garso ir vaizdo kūrinys ir pan.) atkuriama tik analogine forma, nėra galimybės informaciją atgaminti skaitmenine forma. Tam, kad analoginė informacija būtų paversta skaitmenine (t. y. tam, kad būtų pagaminta skaitmeninė fiksacija), būtina sudėtinga konversijos procedūra, kurios metu taip pat nukenčia ir tokios informacijos tikslumas bei kokybė. Dėl šios priežasties skaitmeninės informacijos analoginis pažeidimas palyginti menkai paplitęs.

Kitos populiarios techninės priemonės yra informacijos šifravimas, įvairūs programiniai ir aparatiniai kodai. Šifravimas ypač paplitęs televizijos ir radijo veikloje, kabelinėse ir palydovinėse transliacijose. Tam, kad būtų atgaminti užšifruoti garso ir vaizdo kūriniai ir fonogramos, naudojamos televizijos, radijo, kabelinėse ar palydovinėse transliacijose, vartotojas turi įsigyti specialų dekoderį, dekodavimo korteles ir kita tuo pačiu sumokėdamas ir už šių kūrinių naudojimą. Prie šifravimo techninių priemonių priskirtina ir *Macrovision* sistema, taip pat specialios apsaugos sistemos (papildomo ryškumo signalo įrašymas), užkertančios kelią kompaktinių plokštelių ir DVD laikmenų kopijavimui (pvz., CSS kodavimas, žr. žemiau). Visos šios techninės priemonės pakankamai patikimai saugo kūrinius ir gretutinių teisių objektus nuo neteisėto atgaminimo ir naudojimo, ypač nuo privataus nekomercinio pažeidimo.

Pradėjus taikyti technines kūrinių ir gretutinių teisių objektų apsaugos priemones, atsirado ir naujos neteisėtos veiklos formos – įren-

ginių, skirtų pašalinti ar apeiti technines apsaugos priemones, gamyba ir platinimas. Tokia veikla tiesiogiai nepažeidžia autorių ar gretutinių teisių į techninėmis priemonėmis apsaugotą objektą, todėl siekiant išspręsti šį kazusą techninėms priemonėms buvo numatyta atskira teisinė apsauga. Visose išsivysčiusiose valstybėse draudžiama pašalinti bet kokias autorių ar gretutinių teisių objekto technines apsaugos priemones, taip pat gaminti ar platinti prietaisus arba kitokius įrankius, skirtus pašalinti minėtas technines priemones. Pažymėtina, kad tam tikrais atvejais techninių priemonių pašalinimas yra būtinas siekiant įgyvendinti įstatymuose numatytas išimtis iš autorių ir gretutinių teisių (pvz., užtikrinti suderinamumą arba pagaminti atsarginę kopiją), todėl techninių priemonių taikymas ir apsauga iki šiol sukelia teorinių ir praktinių problemų.

Savotiška autorinių kūrinių ir gretutinių teisių objektų apsaugos forma yra ir informacijos apie autorių ir gretutinių teisių valdymą pateikimas. Informacija apie autorių ir gretutinių teisių valdymą suprantama kaip informacija, identifikuojanti kūrinį, kūrinio autorių, kitą autorių teisių subjektą arba atlikėją, kūrinio atlikimą, fonogramą, fonogramos gamintoją, kitą gretutinių teisių subjektą, taip pat informacija apie kūrinio, atlikimo ar fonogramos naudojimo sąlygas ir tvarką. Tokia informacija paprastai pateikiama kiek galima akivaizdžiau, kad vartotojui būtų aiškus atitinkamo intelektinės nuosavybės objekto teisių turėtojas ir vartotojo teisės į tokį objektą, tokiu būdu informuojant vartotoją apie galimus intelektinės nuosavybės teisių pažeidimus. Informacijos pašalinimas ar pakeitimas gali suklaidinti vartotoją bei paskatinti neteisėtas veikas. Pats informacijos pašalinimas ar pakeitimas taip pat pažeidžia autorių arba gretutinių teisių turėtojo interesus. Dėl šių priežasčių informacijai apie autorių ir gretutinių teisių valdymą taikoma speciali teisinė apsauga.

Šiuo metu ypač sparčiai plinta DVD standarto laikmenos, kurios ateityje turėtų pakeisti kompaktines plokšteles bei kompaktines kasetes įrašant fonogramas ir garsinę bei vaizdinę informaciją. DVD standarto laikmenose fonogramos ar audivizualinė informacija užfiksuota skaitmenine forma, taip pat apsaugota nuo atgaminimo specialių šifravimo algoritmų pagalba. DVD standarto laikmenose naudojamas specialus CSS (*Contents Scrambling System*) kodavimo algoritmas, kuris turi neleisti įrašą atgaminti skaitmenine forma, tačiau leidžia įrašą atgaminti analogine (prastesnės kokybės) forma. Dar neseniai šis standartas buvo laikomas saugiu ir neįveikiamu „piratams“, tačiau 1999 m. pavasarį pasauliniame interneto tinkle pasirodė DeCSS kompiu-

terių programa, kurios pagalba skaitmeninė informacija, išsaugota DVD laikmenose, gali būti atgaminta skaitmenine forma. Minėta programa buvo sukurta teisėtiems tikslams: siekiant užtikrinti DVD standarto dermę su *Linux* ir kitomis nekomercinėmis kompiuterių operacinėmis sistemomis, tačiau ji taip pat atvėrė kelią DVD laikmenose išsaugotos informacijos pažeidimui. Jungtinėse Amerikos Valstijose ir kitose šalyse iki šiol vyksta teisminiai procesai dėl DeCSS kompiuterių programos legalumo.

Veiksmingų techninių apsaugos priemonių šalinimas ar vengimas, kai asmuo tai daro tyčia, yra laikomas techninių apsaugos priemonių pažeidimu. Intelektinės nuosavybės pažeidimu, be kita ko, laikomas paslaugų tai padaryti siūlymas bei atitinkamų prietaisų, leidžiančių pašalinti tokias technines apsaugos priemones, gaminimas, importavimas, gabenimas, laikymas turint tikslą platinti ir platinimas.

Viena iš specifinių techninės apsaugos priemonių yra informacijos apie teisių valdymą įdiegimas į intelektinės nuosavybės objektus. Šios informacijos apie autorių teisių ar gretutinių teisių valdymą panaikinimas arba pakeitimas be autorių ar gretutinių teisių subjektų leidimo, taip pat kūrinių, atlikimų įrašų, fonogramų ar jų kopijų platinimas, importavimas, transliavimas, viešas paskelbimas ar padarymas viešai prieinamais be leidimo panaikinus arba pakeitus informaciją apie teisių valdymą taip pat yra laikomas autorių teisių ir gretutinių teisių pažeidimu.

Minėtos nuostatos Autorių teisių ir gretutinių teisių įstatyme įtvirtintos įgyvendinant PINO interneto sutarčių nuostatas.

Techninių apsaugos priemonių apsauga įtvirtinta ir Lietuvos Respublikos baudžiamojo kodekso XXX skirsnio nuostatose, kurios numato baudžiamąją atsakomybę už informacijos apie autorių teisių ar gretutinių teisių valdymą sunaikinimą arba pakeitimą (193 str.); neteisėtą autorių ar gretutinių teisių techninių apsaugos priemonių pašalinimą (194 str.). Šioms veikoms keliamas komercinių tikslų reikalavimas. Subjektyviai šios veikos turi būti padarytos tiesiogine tyčia kaltininkui suvokiant nusikalstamos veikos pobūdį ir norint taip veikti. Už šias veikas taikomos sankcijos yra viešieji darbai arba bauda, arba laisvės apribojimas, arba areštas, arba laisvės atėmimas iki dvejų metų. Be to, atsakomybė gali būti taikoma ir juridiniam asmeniui.

Deja, nustatyta techninių apsaugos priemonių teisinė apsauga yra besąlygiška ir nenumato jokių išimčių, todėl neįgyvendinamos autorių teisių ir gretutinių teisių išimtys: teisė atgaminti asmeniniais tiks-

lais, švietimo ir mokslo tikslais ir kt. Daugumos valstybių, tarp jų ir Lietuvos, įstatymai nenumato jokio mechanizmo, kaip vartotojui įgyvendinti savo įstatymines teises (pvz., asmeninės kopijos teisę ar teisę pasinaudoti intelektine nuosavybe mokslo ir švietimo tikslais). Tokia situacija akivaizdžiai lemia intelektinės nuosavybės naudotojo (vartotojo) teisių ir intelektinės nuosavybės teisių pažeidimų koliziją, t. y. vartotojas, norėdamas įgyvendinti savo teises, iš esmės neturi kitos išeities, tik pažeisti technines apsaugos priemones. Kadangi už techninių apsaugos priemonių pažeidimus numatyta net ir baudžiamoji atsakomybė, būtina nedelsiant spręsti šią teisių koliziją.

3.7. Papildoma medžiaga. Intelektinės nuosavybės kolektyvinio administravimo problemos elektroninėje erdvėje

Kolektyvinis teisių administravimas yra intelektinės nuosavybės teisių turėtojų pavedimas centralizuotoms asociacijoms tvarkyti ir ginti jų intelektinės nuosavybės teises, rinkti atlyginimą už jų intelektinės nuosavybės naudojimą. Lietuvos ir užsienio autorių teises Lietuvoje kolektyviai administruoja 1991 m. įsteigta Lietuvos autorių teisių gynimo asociacijos agentūra (LATGA-A). Atlikėjų ir fonogramų gamintojų teisėms kolektyviai administruoti 1999 m. atlikėjų ir fonogramų gamintojų iniciatyva įsteigta Lietuvos gretutinių teisių asociacija (AGATA).

Kolektyvinio administravimo asociacijos dažniausiai atlieka dvi pagrindines funkcijas: rūpinasi užmokesčio už autorių teisių ar gretutinių teisių panaudojimą (visų pirma teisės atgaminti kūrinį) surinkimu, taip pat rūpinasi autorių bei gretutinių teisių apsauga. Tradiciškai įgaliojimus atstovauti autoriui ar gretutinių teisių turėtojui kolektyvinio administravimo institucija įgyja sudarydama atitinkamą (pavedimo) sutartį su autorių ar gretutinių teisių turėtoju ar jį atstovaujančia institucija, todėl kolektyvinio administravimo asociacijų teisės tiesiogiai priklauso nuo šių asociacijų narių mandato. Vietoj tokio sutartinio mandato šiuo metu plačiai taikomas įstatyminio atstovavimo principas, reiškiantis, kad kolektyvinio administravimo institucijos pagal įstatymą laikomos visų autorių teisių turėtojų atstovais ir administruoja visas atitinkamas teises.

Kai kurių autorių ir gretutinių teisių (pvz., autorių teisės leisti kūrinio kabelinę retransliaciją, transliavimą radijuje ar televizijoje) įgyvendinimas apskritai leidžiamas tik per autorių teisių kolektyvinio

administravimo asociaciją. To priežastys yra būtinybė bendrai nustatyti retransliacijos licencijos tarifus ir išvengti ypač sudėtingo atskiro licencijavimo. Šitaip kolektyvinis administravimas užtikrina ir viešąjį interesą – visuomenės galimybę per transliacijas susipažinti su visais kūriniais už protingai nustatytą kainą. Jei reikėtų individualiai derėtis su kiekvieno kūrinio teisių turėtoju, tai labai apsunkintų ir pabrangintų visuomenės galimybę gauti šią informaciją. Kitose srityse, ypač kur autorių ir gretutinių teisių turėtojai yra ekonomiškai ir organizaciniu požiūriu pajėgūs subjektai, kolektyvinio administravimo taikymas yra neveiksmingas, kadangi būtų neefektyvus ir kartotų pačių autorių ir gretutinių teisių turėtojų veiklą. Tokios sritys yra, pavyzdžiui, autorių teisės į kompiuterių programas, autorių teisės arba *sui generis* teisės į duomenų bazes, pagrindinės teisės į garso ir vaizdo (kino, video, TV laidas) produkciją ir pan. Kolektyvinis administravimas iš esmės netaikomas ir pramoninės nuosavybės srityje, tačiau joje gana aktyviai veikia teisių turėtojų interesus vienijančios ir atstovaujančios organizacijos.

Sparčiai tobulėjant technologijoms, ypač plintant techninėms apsaugos priemonėms bei autorių teisių ir gretutinių teisių valdymo technologijoms, didėja autorių ir gretutinių teisių turėtojų galimybės administruoti savo teises ir kontroliuoti saugomų kūrinių naudojimą. Šiuo metu techninių apsaugos priemonių ir autorių bei gretutinių teisių valdymo priemonių teisinė apsauga yra atskirai reglamentuojama, o šios priemonės tampa alternatyva kolektyviniam teisių administravimui. Be to, Kūrybinės bendrumos judėjimas taip pat yra orientuotas į paties autoriaus galimybes licencijuoti savo kūrinį ir individualiai nustatyti jo naudojimo tvarką.

Pramoninės nuosavybės srityje veikia teisių turėtojų interesus vienijančios organizacijos, kurios neatlieka formalių kolektyvinio administravimo funkcijų, tačiau yra joms artimos: organizuoja savo narių intelektinės nuosavybės teisių gynimą, inicijuodamos civilines ir administracines arba baudžiamąsias bylas prieš intelektinės nuosavybės teisių pažeidėjus, bendradarbiauja su teisėsaugos institucijomis intelektinės nuosavybės gynimo srityje, užsiima aktyvia lobistine veikla, atstovavimu atitinkamai industrijai ir veiklos koordinavimu nacionaliniu ar tarptautiniu mastu.

Kolektyvinis intelektinės nuosavybės teisių administravimas iš esmės tinka tvarkant teises industrinėje visuomenėje, bet ne žinių visuomenėje. Ypač kolektyvinis administravimas netinka elektroninėje erdvėje. Pagrindinės to priežastys yra kolektyvinio administravimo ir

technologinių intelektinės nuosavybės teisių administravimo mechanizmų nesuderinamumas. Svarbiausi elektroninės erdvės iššūkiai kolektyviniam administravimui šiuo metu yra nesuderinamumas su individualiu technologiniu teisių administravimu, taip pat dvigubas arba nepagrįstas tų pačių intelektinės nuosavybės naudojimo būdų apmokestinimas.

Techninių apsaugos priemonių bei autorių teisių ir gretutinių teisių valdymo technologijų naudojimas – t. y. plintantis individualus teisių administravimas – lemia dvigubą ar net apskritai nepagrįstą autorinio atlyginimo mokėjimą už intelektinės nuosavybės naudojimą. Geriausiai šią problemą iliustruoja kolektyvinio administravimo asociacijų renkamas atlyginimas už audiovizualinių kūrinių ar fonogramose įrašytų kūrinių atkūrimą asmeniniais tikslais, kuris dažnai vadinamas „tuščios laikmenos mokesčiu“. Pagal galiojančias taisykles (Autorių teisių ir gretutinių teisių įstatymo 20 str.) tuščios laikmenos mokestį siekiama rinkti:

- už visas laikmenas, tarp jų laikmenas, naudojamas su intelektine nuosavybe visiškai nesusijusiais tikslais (pvz., viešojo administravimo tikslais, duomenų saugyklose, asmeninėms foto ir audiovizualinėms fiksacijoms ir pan.);
- tais atvejais, kai kūrinio asmeninis atgaminimas yra uždraustas techninėmis priemonėmis, t. y. kūrinio teisėtai atgaminti asmeniniais tikslais iš esmės neįmanoma. Paminėtina, kad šiuo metu apie 90 proc. viešai platinamų kūrinių dėl taikomų techninių apsaugos priemonių negali būti teisėtai atgaminami asmeniniais ar kitais tikslais;
- nepriklausomai nuo to, kad panašus tuščios laikmenos mokestis jau buvo sumokėtas kitose Europos Sąjungos valstybėse, o nacionaliniams subjektams nėra realių galimybių atgauti šį mokestį;
- nepriklausomai nuo to, kad autorinis atlyginimas buvo sumokėtas įsigyjant individualias licencijas (pvz., įsigyjant kūrinį interneto muzikos įrašų parduotuvėje).

KONTROLINĖS UŽDUOTYS

1. Apibūdinkite intelektinę nuosavybę elektroninėje erdvėje.
2. Paaiškinkite pagrindinius intelektinės nuosavybės elektroninėje erdvėje skirtumus nuo tradicinių intelektinės nuosavybės formų.

3. Palyginkite ir paaiškinkite kompiuterių programų ir duomenų bazių teisinius skirtumus.
4. Palyginkite ir paaiškinkite teisinių ir techninių apsaugos priemonių taikymą intelektinei nuosavybei.
5. Įvardinkite ir paaiškinkite kolektyvinio teisių administravimo ir teisių valdymo technologijų panašumus ir skirtumus.

Literatūra

1. Cornish W. Intellectual Property: Omnipresent, Distracting, Irrelevant? – Oxford: University Press, 2004.
2. Merges R. P., Menell P. S., Lemley M. A. Intellectual Property in the New Technological Age (3rd ed.). – New York: Aspen, 2003.
3. Lessig L. Code and Other Laws of the Cyberspace. – New York: Basic Books, 1999.
4. Lessig L. The Future of Ideas: The Fate of the Commons in a Connected World. – New York: Random House Inc., 2002.
5. Lessig L. Free Culture: How Big Media Uses Technology and the Law to Lock Down Creativity. – Penguin Press, 2004.
6. Fisher W. W. Promises to Keep: Technology, Law, and the Future of Entertainment. – Stanford University Press, 2004.
7. Landes W. M., Posner R. A. The Economic Structure of Intellectual Property Law. – Harvard University Press, 2003.
8. Lemley M. A., Menell P. S., Merges R. P., Samuelson P. Software and Internet Law (2nd. ed.). – New York: Aspen Law & Business, 2003.
9. Digital Dilemma: Intellectual Property in the Information Age. Washington, DC: National Academy Press, 2000 // http://www.nap.edu/html/digital_dilemma/.
10. Barlow J. P. The Economy of Ideas. Wired, Issue 2.03, March 1994.
11. Kiškis M. Tarptautinio intelektinės nuosavybės piratavimo prevencija. – Vilnius: Lietuvos teisės universitetas, 2000.
12. Intelektinės nuosavybės piratavimo prevencija / Babachinaitė G., Gutauskas A., Jurgelaitienė G., Kiškis M., Starkus S. Nusikalstamumo ir kitų nepageidautinų socialinių procesų prevencijos problemos bei jų sprendimas Europos valstybėse. – Vilnius: Lietuvos teisės universitetas, 2003.
13. Vaidhyanathan S. Copyrights and Copywrongs: The Rise of Intellectual Property and how It Threatens Creativity. – New York: NYU Press, 2001.
14. Sannikov A. G. Technologii na rubeže vekov i intellektualnaja sobstvennost. – Moskva, 2003.

4. PRIVATUMO IR ASMENS DUOMENŲ TEISINĖ APSAUGA ELEKTRONINĖJE ERDVĖJE

4.1. Įvadinė medžiaga. Privatumo pagrindai

Pastaraisiais metais, plintant informacinėms komunikacinėms technologijoms, ypač svarbus privatumo ir asmens duomenų apsaugos elektroninėje erdvėje aspektas. Elektroniniuose ryšiuose, internete apdorojama vis daugiau duomenų, susijusių su konkrečiu asmeniu. Apie asmenį galima surinkti informaciją, kuri gali apibūdinti jo įpročius, pomėgius ir kita. Neteisėtai renkant bei netinkamai naudojant šiuos duomenis, gali kilti didelė grėsmė asmens privatumui.

1890 m. Jungtinių Amerikos Valstijų teisininkai Samuelis Warrenas ir Louisas Brandeisas parašė darbą apie asmens teisę į privatumą ir apibrėžė ją kaip „teisę būti paliktam vienam“ (angl. *right to be left alone*). Jie pirmieji išreiškė privatumą kaip didžiulę socialinę vertybę, kuri turi būti saugoma įstatymo ir teisėjų.

Vėliau privatumo koncepcija vystėsi kita linkme, šiuo metu privatumas dažnai tapatinamas su asmens duomenų apsauga. Reikėtų paminėti, kad asmens duomenų apsauga sudaro tik vieną iš keturių privatumo elementų, tačiau asmens duomenų apsauga yra labai svarbi privatumo kategorija, siejama su asmens teise kontroliuoti informacijos apie save tvarkymą.

Teisė į privataus gyvenimo neliečiamumą yra konstitucinė žmogaus teisė, įtvirtinta ir tarptautinės teisės aktuose, ir Lietuvos Respublikos Konstitucijoje. Ši teisė pagal jos įteisinimo laiką priskirtina prie vadinamųjų *trečiosios kartos* teisių, nes daugelyje šalių buvo įtvirtinta žymiai vėliau negu socialinės, ekonominės ar politinės teisės.

Paminėtini pagrindiniai tarptautiniai dokumentai, kuriuose įtvirtinta teisė į privataus gyvenimo neliečiamumą. Visuotinės žmogaus teisių deklaracijos 12 straipsnyje nurodoma: „Niekas neturi patirti savavališko kišimosi į jo asmeninį ir šeimyninį gyvenimą, jo buto neliečiamybę, susirašinėjimo slaptumą, kėsinimosi į jo garbę ir orumą. Kiekvienas žmogus turi teisę į įstatymo apsaugą nuo tokio kišimosi arba

tokių pasikėsinimų“. Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijoje[1] taip pat nustatyta: „Kiekvienas žmogus turi teisę į tai, kad būtų gerbiamas jo asmeninis ir jo šeimos gyvenimas, buto neliečiamybė ir susirašinėjimo slaptumas“.

Lietuvoje teisė į privataus gyvenimo neliečiamumą įtvirtinta Lietuvos Respublikos Konstitucijos 22 straipsnyje, kuriame nurodyta, kad „žmogaus privatus gyvenimas neliečiamas. Asmens susirašinėjimas, pokalbiai telefonu, telegrafo pranešimai ir kitoks susižinojimas neliečiami“. Lietuvos Respublikos Konstitucijos 22 straipsnio 3 dalies nuostata, kad „informacija apie privatų gyvenimą gali būti renkama tik motyvuotu teismo sprendimu ir tik pagal įstatymą“ ir 4 dalies nuostata, kad „įstatymas ir teismas saugo, kad niekas nepatirtų savavališko ar neteisėto kišimosi į jo asmeninį ar šeimyninį gyvenimą, kėsinimosi į jo garbę ir orumą“ yra svarbiausios teisės į privatų gyvenimą neliečiamybės garantijos. Šiomis garantijomis asmens privatus gyvenimas saugomas nuo valstybės, kitų institucijų, jų pareigūnų, kitų asmenų neteisėto kišimosi. Teisė į privataus gyvenimo neliečiamybę taip pat yra įtvirtinta ir Lietuvos Respublikos civiliniame kodekse bei kituose įstatymuose.

Gali kilti klausimas: kas yra privatus žmogaus gyvenimas? Lietuvos Respublikos Konstitucinio Teismo jurisprudencijoje teigiama, kad **„privatus žmogaus gyvenimas – tai individo asmeninis gyvenimas: gyvenimo būdas, šeimyninė padėtis, gyvenamoji aplinka, santykiai su kitais asmenimis, individo pažiūros, įsitikinimai, įpročiai, jo fizinė bei psichinė būklė, sveikata, garbė, orumas ir kt.“**. Paminėtina, kad Lietuvoje, kitaip nei daugelyje kitų valstybių, įvirtinta teisė ne į privatumą, o teisė į privatų gyvenimą. Teisė į privatumą ir teisė į privatų gyvenimą nėra tapačios. Tačiau preziumuotina, jog ši problema neturi didelės praktinės įtakos vertinant teisės į privatų gyvenimą apsaugą elektroniniuose ryšiuose, todėl nebus smulkiau nagrinėjama.

Tarptautinių teisės aktų analizė (žr. Visuotinės žmogaus teisių deklaracijos 12 straipsnį, Tarptautinio pilietinių ir politinių teisių pakto 17 straipsnį, Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos 8 straipsnį ir kt.) leidžia daryti išvadą, kad **asmens teisės į privatumą turinį sudaro keturi savarankiški ir kartu tarpusavyje susiję elementai**:

– *informacinis privatumas* yra susijęs su duomenų apie asmenį

[1] Lietuvoje įsigaliojo nuo 1995 metų.

tvarkymu ir vadinamas asmens duomenų apsauga: t. y. kai asmuo pats gali disponuoti savo asmens duomenimis, žinoti apie savo duomenų tvarkymą, susipažinti su savo asmens duomenimis, reikalauti ištaisyti duomenis ir pan.;
– *fizinis privatumas* (kūno neliečiamumas), t. y. žmogui nesutikus, jam negali būti atliekami jokie medicininiai ar moksliniai bandymai (pavyzdžiui, priverstinai atliekami narkotikų testai ir pan.);
– *komunikacinis privatumas*, t. y. asmens susirašinėjimo, pokalbių telefonu, telegrafo pranešimų ir kitokio susižinojimo neliečiamumas;
– *teritorinis privatumas*, t. y. asmens būsto arba teritorijos neliečiamumas.

4.2. Pagrindinė medžiaga. Asmens duomenų teisinės apsaugos elektroninėje erdvėje ypatumai

4.2.1. Asmens duomenų teisinės apsaugos elektroninėje erdvėje pagrindinės kategorijos ir principai

Asmens duomenų apsaugą galima tapatinti su vienu iš keturių privatumo elementų – informaciniu privatumu. A. Saarenpaa asmens duomenų apsauga laiko savarankišką privatumo dalį – informacinį privatumą, kuris reiškia fizinių asmenų privatumo ir jų sąmoningo apsisprendimo teisių apsaugą kontroliuojant, ribojant ir reguliuojant asmens duomenų tvarkymą asmens duomenų teisinės apsaugos norminių aktų pagalba.

Nors asmens duomenys gali būti tvarkomi tiek automatiniu, tiek neautomatiniu būdu (pvz., tvarkant asmens duomenų susistemintas rinkmenas: sąrašus, kartotekas ir pan.), rankiniu būdu asmens duomenys beveik netvarkomi dėl informacinių technologijų paplitimo, daugiausiai asmens duomenys tvarkomi automatiniu būdu[2], kuris šiame skyriuje bus tapatinamas su asmens duomenų tvarkymu elektroninėje erdvėje (arba tiesiog asmens duomenų tvarkymu).

Kalbant apie asmens duomenų apsaugą kyla vienas iš pagrindinių klausimų: kas yra asmens duomenys? Pavyzdžiui, žmogui keliaujant

[2] Duomenų tvarkymo veiksmai, visiškai ar iš dalies atliekami automatinėmis priemonėmis.

po Lietuvą telekomunikacijų operatoriai dažnai fiksuoja jo mobiliojo telefono buvimo vietą ir kartu to žmogaus judėjimo duomenis. Ar tai yra asmens duomenys? Galima pateikti asmens duomenų apibrėžimą. **Asmens duomenys – bet kuri informacija, susijusi su fiziniu asmeniu – duomenų subjektu, kurio tapatybė yra žinoma arba gali būti tiesiogiai ar netiesiogiai nustatyta pasinaudojus tokiais duomenimis kaip asmens kodas, vienas arba keli asmeniui būdingi fizinio, fiziologinio, psichologinio, ekonominio, kultūrinio ar socialinio pobūdžio požymiai**.

Pabrėžtini du kriterijai: tiesioginis ir netiesioginis asmens tapatybės nustatymas, tai leidžia apimti daug duomenų, kurie, atrodo, turi menką ryšį su konkrečiu asmeniu. Duomenys gali būti asmeniniai netgi tada, jeigu jų pagalba asmuo gali būti nustatytas tik pasitelkus kitus duomenis – pagalbinius. Kita vertus, svarbu tai, kad asmens tapatybę būtų galima nustatyti nepanaudojus pernelyg didelių laiko, darbo ir kitokių sąnaudų.

Asmens duomenys, kurie tiesiogiai ir vienareikšmiškai nurodo konkretų asmenį, yra asmens kodas, paso numeris, vairuotojo pažymėjimo numeris ir pan. Su tokiais duomenimis susieti visi kiti duomenys tampa asmens duomenimis. Asmens duomenimis taip pat gali būti ir asmeninės informacijos sankaupa, sistema, pagal kurią įmanoma nustatyti asmens tapatybę, tačiau iš kurios atskirų duomenų elementų neįmanoma nustatyti asmens.

Išskirtina ypatingų asmens duomenų kategorija. Ypatingi asmens duomenys – duomenys, susiję su fizinio asmens rasine ar etnine kilme, politiniais, religiniais, filosofiniais ar kitais įsitikinimais, naryste profesinėse sąjungose, sveikata, lytiniu gyvenimu, taip pat informacija apie asmens teistumą. Šių duomenų apsaugai taikomi griežtesni reikalavimai, negu saugant „įprastus“ asmens duomenis.

Nustatyti šie teisėto asmens duomenų tvarkymo kriterijai:

- asmens duomenų subjektas duoda sutikimą tvarkyti jo asmens duomenis;
- sudaroma arba vykdoma sutartis, kai viena iš šalių yra duomenų subjektas;
- įstatymai įpareigoja duomenų valdytoją tvarkyti asmens duomenis;
- siekiama apsaugoti asmens duomenų subjekto esminius interesus;
- įgyvendinami oficialūs įgaliojimai, suteikti valstybės bei savivaldybių institucijoms arba trečiajam asmeniui, kuriam teikiami as-

mens duomenys;
- asmens duomenis reikia tvarkyti dėl teisėto intereso, kurio siekia duomenų valdytojas arba trečiasis asmuo, kuriam teikiami asmens duomenys, ir jei duomenų subjektų interesai nėra svarbesni.

Duomenų valdytojai turi laikytis tam tikrų principų, siekiančių ne tik apginti žmogaus privatumą, bet ir įdiegti gerus verslo įpročius bei sukurti efektyvų ir patikimą duomenų valdymą. Galima išskirti šiuos **pagrindinius asmens duomenų apsaugos principus**:
- *asmens duomenų rinkimo apribojimo* (asmens duomenys turi būti gaunami teisėtai ir naudojant teisingas priemones);
- *kokybės* (asmens duomenys turi būti tikslūs, baigtini ir atnaujinti);
- *tikslo nustatymo* (tikslai, kuriems yra renkami asmens duomenys, turi būti nurodyti ne vėliau negu asmens duomenų rinkimo metu ir tolesnis jų naudojimas turi būti apribotas šių tikslų pasiekimu);
- *asmens duomenų naudojimo apribojimo* (asmens duomenys neturi būti atskleisti, padaryti prieinami ar kitaip panaudoti kitiems tikslams, negu tie, kurie atitinka tikslo nustatymo principą, išskyrus atvejus, kuomet gaunamas asmens duomenų subjekto sutikimas arba pagal įstatymą);
- *saugumo užtikrinimo* (asmens duomenys privalo būti saugomi protingomis saugumo priemonėmis prieš tokias rizikas (pavojus) kaip: netekimas, praradimas, neteisėta prieiga prie asmens duomenų, jų sunaikinimas, panaudojimas, pakeitimas ar atskleidimas);
- *atvirumo* (turi būti atvira informacija apie duomenų valdytoją, jo buveinę ir duomenų tvarkymo tikslą);
- *individualaus dalyvavimo* (asmuo turi turėti tam tikras teises);
- *atsakomybės* (asmens duomenų valdytojas privalo būti atsakingas už tai, kaip jis laikosi priemonių, įgyvendinančių aukščiau nurodytus tikslus).

Asmens duomenų tvarkymo procese išskirtini šie asmens duomenų tvarkymo dalyviai: duomenų valdytojas, duomenų tvarkytojas ir duomenų subjektas. Duomenų valdytojas – juridinis ar fizinis asmuo, kuris vienas arba drauge su kitais nustato asmens duomenų tvarkymo tikslus ir priemones. Duomenų tvarkytojas – juridinis ar fizinis (kuris nėra duomenų valdytojo darbuotojas) asmuo, duomenų valdytojo įga-

liotas tvarkyti asmens duomenis. Duomenų tvarkytojas ir (ar) jo skyrimo tvarka gali būti nustatyti įstatymuose ar kituose teisės aktuose. Duomenų valdytojo ir duomenų tvarkytojo, nesančio duomenų valdytoju, santykiai turi būti reglamentuojami rašytine sutartimi, išskyrus atvejus, kai tokius santykius nustato įstatymai ar kiti teisės aktai.

Asmens duomenų tvarkymo procese asmens duomenų subjektas turi tam tikras teises, iš kurių galima išskirti pagrindines:

1) žinoti (būti informuotas) apie savo asmens duomenų tvarkymą;

2) susipažinti su savo asmens duomenimis ir kaip jie yra tvarkomi;

3) reikalauti ištaisyti, sunaikinti savo asmens duomenis arba sustabdyti, išskyrus saugojimą, savo asmens duomenų tvarkymo veiksmus, kai duomenys tvarkomi nesilaikant šio ir kitų įstatymų nuostatų;

4) nesutikti, kad būtų tvarkomi jo asmens duomenys.

Duomenų valdytojas turi motyvuotai pagrįsti atsisakymą vykdyti duomenų subjekto prašymą įgyvendinti šiame įstatyme nustatytas duomenų subjekto teises. Duomenų valdytojas, gavęs duomenų subjekto prašymą, ne vėliau kaip per 30 kalendorinių dienų nuo duomenų subjekto kreipimosi dienos turi pateikti jam atsakymą. Jei duomenų subjekto prašymas išreikštas rašytine forma, duomenų valdytojas turi pateikti jam atsakymą raštu.

Asmens duomenų tvarkymą, išskyrus asmens duomenų tvarkymą elektroniniuose ryšiuose, reglamentuoja Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas. Šio įstatymo įgyvendinimą prižiūri Valstybinė duomenų apsaugos inspekcija. Ši institucija prižiūri ir Lietuvos Respublikos elektroninių ryšių IX skirsnio „Asmens duomenų tvarkymas ir privatumo apsauga“ įgyvendinimą.

Asmens duomenų apsaugos modeliai gali būti skirstomi:

1) reguliavimas bendraisiais įstatymais;

2) sektorinis reguliavimas, kai tam tikroms sritims taikomi specialūs teisės aktai (pvz., elektroniniai ryšiai);

3) savireguliacija;

4) apsauga techninėmis priemonėmis.

4.2.2. Asmens duomenų apsaugos elektroninėje erdvėje bendrieji reguliavimo aspektai

Asmens duomenų apsaugą reglamentuojantys tarptautiniai aktai gali būti skirstomi į privalomuosius ir rekomendacinio pobūdžio aktus. Iš rekomendacinio pobūdžio aktų paminėtinos 1980 m. EBPO

gairės dėl privatumo apsaugos ir asmens duomenų judėjimo tarp valstybių narių. Šios gairės atspindi neoficialų tarptautinį susitarimą dėl asmens duomenų apsaugos principų: asmens duomenų rinkimo apribojimo, duomenų kokybės, tikslo nustatymo, asmens duomenų naudojimo apribojimo, atvirumo, individualaus dalyvavimo, atskaitomybės. Nustatydamos pagrindinius asmens duomenų apsaugos principus gairės tampa atrama vyriausybėms bei verslui siekiant geriau apsaugoti asmens duomenis bei nustatyti atitinkamą reguliavimą. Taip pat paminėtinos 1990 m. Jungtinių Tautų kompiuterizuotų asmens duomenų bylų gairės, kurios atspindi EBPO gairėse įtvirtintus asmens duomenų apsaugos principus. Šiose gairėse valstybėms narėms, įgyvendinančioms nacionalinius teisės aktus dėl kompiuterizuotų asmens duomenų bylų, patariama atsižvelgti į gairėse numatytus principus.

Pagrindinis privalomojo pobūdžio asmens duomenų apsaugos tarptautinis aktas – 1981 m. Strasbūro konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108). Ši konvencija įsigaliojo 1985 metais. Lietuva šią konvenciją pasirašė 2000 m. vasario 11 d., o ratifikavo – 2001 m. birželio 1 d. Lietuvoje konvencija įsigaliojo nuo 2001 m. spalio 1 d.

Šia konvencija siekiama užtikrinti, kad tvarkant asmens duomenis automatizuotai visų šalių teritorijose bus gerbiamos kiekvieno asmens, nepaisant jo tautybės ir gyvenamosios vietos, teisės ir pagrindinės laisvės, o svarbiausia – jo teisė į privatų gyvenimą. Konvencijoje nustatyti asmens duomenų apsaugos principai panašūs į tuos, kurie paminėti EBPO gairėse, be to, papildomai įtrauktas principas, reikalaujantis atitinkamų apsaugos priemonių ypatingiems duomenims, t. y. tokiems duomenims, kurie atskleidžia rasinę kilmę, politinius įsitikinimus, religines nuostatas, yra susiję su sveikata ir pan.

Vienintelis bendro pobūdžio įpareigojantis teisės aktas Europos Sąjungoje – Europos Parlamento ir Tarybos direktyva Nr. 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo. Ši direktyva taikoma automatiniais būdais tvarkant visus asmens duomenis arba dalimis ir neautomatiniais būdais tvarkant asmens duomenis, kai tie duomenys sudaro arba yra skirti sudaryti rinkmenų sistemos dalį. Direktyvos tikslas yra dvejopas. Viena, direktyva siekiama saugoti fizinių asmenų pagrindines teises ir laisves, ypač jų privatumo teisę tvarkant asmens duomenis. Kita vertus, direktyva nevaržo ir nedraudžia laisvo asmens duomenų judėjimo tarp valstybių narių dėl priežasčių, susijusių su asmens duomenų apsauga.

Direktyvoje įtvirtinti tokie reglamentavimo principai:

1) *duomenų kokybė* (direktyvos 6 str.). Asmens duomenys turi būti:
– tvarkomi teisingai ir teisėtai;
– surinkti įvardintais, aiškiai apibrėžtais ir teisėtais tikslais, o po to tvarkomi su šiais tikslais suderintais būdais;
– adekvatūs, susiję ir savo apimtimi neviršijantys tikslų, kuriems jie renkami ir (arba) vėliau tvarkomi;
– tikslūs ir, jei būtina, nuolat atnaujinami; turi būti imtasi visų reikalingų priemonių, kad duomenys, kurie yra netikslūs ar neišsamūs, palyginus su tikslais, dėl kurių jie buvo surinkti ar po to tvarkomi, būtų ištrinti arba ištaisyti;
– laikomi tokio pavidalo, kad duomenų subjektų tapatybes užtruktų nustatyti ne ilgiau, nei tai yra reikalinga tais tikslais, dėl kurių duomenys buvo surinkti arba po to tvarkomi.

2) *teisėtas duomenų tvarkymas* (direktyvos 7 str.). Asmens duomenis galima tvarkyti tik tuo atveju, jeigu:
– duomenų subjektas yra nedviprasmiškai davęs sutikimą;
– tvarkyti reikia vykdant sutartį, kurią duomenų subjektas yra sudaręs kaip viena iš šalių, arba duomenų subjekto reikalavimu norint imtis priemonių prieš sudarant sutartį;
– tvarkyti reikia vykdant teisinę prievolę, kuri privaloma duomenų valdytojui;
– tvarkyti reikia norint apsaugoti gyvybinius duomenų subjekto interesus;
– tvarkyti reikia vykdant užduotį, atliekamą visuomenės labui, arba įgyvendinant oficialius įgaliojimus, suteiktus duomenų valdytojui arba trečiajai šaliai, kuriai atskleidžiami duomenys;
– tvarkyti reikia dėl teisėtų interesų, kurių siekia duomenų valdytojas arba trečioji šalis (šalys), kurioms atskleidžiami duomenys, išskyrus atvejus, kai duomenų subjekto teisės ir laisvės yra viršesnės negu šie interesai.

3) *ypatingi asmens duomenys* (direktyvos 8 str.). Nustatomas draudimas tvarkyti asmens duomenis, kurie atskleidžia rasinę ar etninę kilmę, politines, religines ar filosofines pažiūras, priklausymą profesinėms sąjungoms, taip pat tvarkyti duomenis apie asmens sveikatą ar intymų gyvenimą, išskyrus tam tikrus atvejus.

4) *duomenų subjekto teisės*. Direktyva suteikia duomenų subjektui, kurio asmens duomenys tvarkomi, tam tikras teises, pvz.:
– teisę gauti informaciją apie tvarkomus asmens duomenis;

– teisę į informacijos ištrynimą bei ištaisymą;
– teisę prieštarauti dėl asmens duomenų tvarkymo;
– teisę į kompensaciją, kai neteisėtai tvarkomi asmens duomenys.

5) *duomenų saugumas* (direktyvos 17 str.). Direktyva numato pareigą duomenų valdytojui įgyvendinti technines ir organizacines apsaugos priemones. Šios priemonės turi atitikti esamą situaciją ar riziką, kurią galėtų sukelti duomenų tvarkymas.

6) *duomenų perdavimas trečiosioms valstybėms.* Direktyva nustato bendrą principą: asmens duomenys, kurie yra tvarkomi arba juos perdavus ketinama tvarkyti, gali būti perduoti į trečiąją šalį tik tuo atveju, jeigu nepažeisdama nacionalinių nuostatų, priimtų pagal kitas šios direktyvos nuostatas, ši trečioji šalis užtikrina adekvatų apsaugos lygį.

Bendrąją duomenų apsaugos direktyvą Lietuvoje įgyvendina Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas. Pirmoji šio įstatymo redakcija buvo priimta 1996 metais. Naują įstatymo redakciją Lietuvos Respublikos Seimas priėmė 2003 metais. Įstatymo bendrasis tikslas – ginti žmogaus privataus gyvenimo neliečiamumo teisę tvarkant asmens duomenis. Įstatymas reglamentuoja santykius, kurie atsiranda tvarkant asmens duomenis automatiniu būdu, taip pat neautomatiniu būdu tvarkant asmens duomenų susistemintas rinkmenas: sąrašus, kartotekas, bylas, sąvadus ir kita.

Įgyvendindamas Bendrąją duomenų apsaugos direktyvą įstatymas tuo tikslu nustato panašius asmens duomenų teisėto tvarkymo kriterijus bei asmens duomenų tvarkymo principus.

Naujoje 2003 metų įstatymo redakcijoje patikslinta įstatymo taikymo sritis. Numatyta, kad įstatymas taikomas ne tik fiziniams ir juridiniams asmenims, bet ir duomenų valdytojo padaliniui (filialui arba atstovybei). Atsižvelgus į praktikoje kylančius neaiškumus, patikslinta duomenų tvarkytojo sąvoka. Be to, įstatymas papildytas naujomis sąvokomis, tai – duomenų tvarkymas automatiniu būdu ir vieša duomenų rinkmena. Nėra privalomas raštiškas duomenų subjekto sutikimas tvarkyti jo asmens duomenis. Teisė spręsti, ar reikalauti iš duomenų subjekto raštiško sutikimo, paliekama duomenų valdytojui, nes ginčo atveju jis turės pateikti įrodymus, kad duomenų subjektas davė aiškiai išreikštą sutikimą tvarkyti asmens duomenis. Įstatyme nustatyta, kad tvarkomi duomenys turi būti tapatūs, tinkami ir tik tokios apimties, kuri būtina jų rinkimo ir tolesnio tvarkymo tikslais. Jei duomenys yra neišsamūs arba netikslūs, palyginus su tikslais, dėl kurių buvo surinkti ar po to tvarkomi, jie turi būti ištaisyti, papildyti, sunaikinti, sustab-

dytas jų tvarkymas. Įstatyme įtvirtintas bendras principas, kad draudžiama tvarkyti ypatingus asmens duomenis, išskyrus įstatyme nustatytą baigtinį sąrašą atvejų, kada ypatingi asmens duomenys gali būti tvarkomi. Įstatyme įtvirtinta nuostata, siaurinanti asmens kodo naudojimo sritį. Asmens kodą be duomenų subjekto sutikimo galima naudoti tik tada, jei tokia teisė yra nustatyta įstatymuose, atliekant mokslinį ar statistinį tyrimą, taip pat valstybės registruose ir informacinėse sistemose. Nustatyta, kad be duomenų subjekto sutikimo asmens duomenys mokslinio tyrimo tikslais gali būti tvarkomi tik pranešus įstatymo vykdymo priežiūros institucijai, kuri, atlikusi išankstinę patikrą, nustato, ar toks tvarkymas nepažeis duomenų subjektų teisių. Šiuo įstatymu praplėstos duomenų subjekto teisės. Duomenų subjektui suteikta teisė reikalauti sustabdyti savo asmens duomenų tvarkymo veiksmus. Įstatyme taip pat nustatyta papildoma duomenų valdytojo pareiga renkant asmens duomenis tiesiogiai iš paties duomenų subjekto iš kitų šaltinių informuoti duomenų subjektą apie jo teisę susipažinti su savo asmens duomenimis, reikalauti ištaisyti neteisingus, neišsamius, netikslius savo asmens duomenis, taip pat pateikti kitą papildomą informaciją (duomenų tvarkymo teisinis pagrindas, duomenų saugojimo terminas, teisė kreiptis į įstatymo vykdymo priežiūros instituciją), kiek tokios papildomos informacijos reikia, kad būtų užtikrintas teisingas asmens duomenų tvarkymas, išskyrus atvejus, kai duomenų subjektas tokią informaciją jau turi. Įstatyme įtvirtinta norma, kad duomenų valdytojo ir duomenų tvarkytojo santykiai turi būti reglamentuojami rašytine sutartimi, išskyrus atvejus, kai tokius santykius nustato įstatymai ar kiti teisės aktai. Nustatyta, kad ne tik duomenų tvarkytojas, bet ir duomenų valdytojo bei tvarkytojo atstovai turi veikti tik pagal duomenų valdytojo nurodymus. Įstatyme įtvirtintos normos, reglamentuojančios išankstinę patikrą. Pateiktas baigtinis sąrašas atvejų, kada įstatymo vykdymo priežiūros institucija atlieka išankstinę patikrą. Įstatyme patikslintos duomenų teikimo į užsienio valstybes sąlygos, taip pat įstatymo vykdymo priežiūros institucijos – Valstybinės duomenų apsaugos inspekcijos – funkcijos, teisės.

Įstatymo priežiūrą vykdo Valstybinė duomenų apsaugos inspekcija. Asmens duomenų apsaugos srities svarbą patvirtina 2005 metais inspekcijos atliktas darbas: išnagrinėti 686 duomenų valdytojų pranešimai apie duomenų tvarkymą, išnagrinėti 102 asmenų skundai (prašymai), atliktos 63 prevencinės patikros bei parengtos 342 išvados dėl išankstinės patikros (iš viso 405), atsakyta į 84 konvencijos ETS Nr. 108 šalių klausimus, parengta 15 metodinių dokumentų, suderinti 157

teisės aktai ir duomenų valdytojų pateikti dokumentai, suteiktos 2207 konsultacijos, parengti 4 teisės aktai ir 100 visuomenės informavimo priemonių, parengtos 44 išvados dėl Europos Sąjungos institucijų rengiamų dokumentų.

Įstatymo 7 straipsnis nustato reikalavimus asmens kodo naudojimui. Pagal minimo straipsnio 2 dalį naudoti asmens kodą tvarkant asmens duomenis galima tik gavus duomenų subjekto sutikimą. 3 dalyje nustatyti atvejai, kai asmens kodą galima naudoti be duomenų subjekto sutikimo:

- jei tokia teisė numatyta įstatymuose;
- atliekant mokslinį arba statistinį tyrimą;
- valstybės registruose ir informacinėse sistemose, jeigu jie yra įteisinti teisės aktų nustatyta tvarka;
- juridiniams asmenims, kurių veikla susijusi su paskolų teikimu ir skolų išieškojimu, draudimu ar nuomos verslu, taip pat sveikatos apsaugos ir socialinio draudimo bei kitų socialinės globos institucijų ir švietimo įstaigų, mokslo ir studijų institucijų veikloje bei įstatymų nustatytais atvejais tvarkant įslaptintus duomenis.

Valstybinė duomenų apsaugos inspekcija nagrinėja pranešimus dėl neteisėto asmens kodo tvarkymo ir imasi įstatymuose numatytų priemonių.

Svarbu paminėti, kad teismų praktika draudžia asmens kodo tvarkymą tiesioginės rinkodaros tikslu. Lietuvos vyriausiasis administracinis teismas 2004 m. lapkričio 26 d. administracinėje byloje Nr. N12-1483-04 priėmė nutartį, kurioje konstatavo, kad tiesioginės rinkodaros tikslu tvarkomas fizinio asmens kodas yra perteklinis duomuo, ir jo tvarkymas minėtu tikslu pažeidžia Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo 3 straipsnio 1 dalies 4 punktą.

Įstatymas nustato specialius reikalavimus, jei asmens duomenys tvarkomi specialiais nustatytais tikslais:

- socialinio draudimo ir socialinės globos tikslais (įstatymo 9 str.);
- sveikatos apsaugos tikslais (įstatymo 10 str.);
- rinkimų, referendumo, piliečių įstatymų leidybos iniciatyvos tikslais (įstatymo 11 str.);
- mokslinio tyrimo tikslais (įstatymo 12 str.);
- statistikos tikslais (įstatymo 13 str.);
- rinkodaros tikslais (įstatymo 14 str.);
- mokumui įvertinti ir įsiskolinimui valdyti (įstatymo 16 str.).

Itin svarbi asmens duomenų apsaugos sritis, susijusi su tiesiogine rinkodara. Neteisėta rinkodara, vykdoma elektroninių ryšių tinklais, t. y. nepageidaujama komercinė informacija, kuri dažnai vadinama elektroninėmis šiukšlėmis arba *spamu*[3]. Tokiu būdu komercinė reklama gali pasiekti milijonus žmonių, o sąnaudos itin mažos. Tokia komercinė informacija gali būti užsakoma ir platinama už atlygį, daugiausia smulkių verslo subjektų, kurie siekia sau kuo pigesnės ir tuo pačiu platesnės reklamos sklaidos. Paminėtina, kad Lietuvoje ne vieną kartą nepageidaujamos komercinės informacijos (arba spamo) siuntėjai buvo patraukti atsakomybėn. 2004 m. lapkričio 22 d. Valstybinėje duomenų apsaugos inspekcija gavo R. L. skundą dėl nepageidaujamo elektroninio pašto pranešimo. Tyrimo metu nustatyta, kad serveris, iš kurio siųstas nepageidaujamas elektroninio pašto pranešimas, priklauso UAB „Biuro sprendimų tinklas“. UAB „Biuro sprendimų tinklas“, atsakydama į inspekcijos klausimą, pranešė, kad už nustatyto serverio išlaikymą minėtai bendrovei moka ir už jį atsako UAB „Interprekyba“. Inspekcijos darbuotojai minėtoje bendrovėje atliko asmens duomenų tvarkymo teisėtumo patikrą ir nustatė, kad iš UAB „Interprekyba“ pareiškėjui siųstas elektroninio pašto pranešimas tiesioginės rinkodaros tikslu be išankstinio abonento sutikimo, taip pažeista Elektroninių ryšio įstatymo 68 straipsnio 1 dalis.

Kol kas įstatymas nereglamentuoja duomenų tvarkymo naudojant vaizdo stebėjimo ir fiksavimo įrangą.

Aštuntasis įstatymo skirsnis skirtas reglamentuoti atsakomybės klausimus. Pagal įstatymo 33 straipsnį duomenų valdytojams, duomenų tvarkytojams ir kitiems asmenims, pažeidusiems įstatymą, taikoma Lietuvos Respublikos įstatymų nustatyta atsakomybė. Lietuvos Respublikos administracinių teisės pažeidimų kodekso 214–14 straipsnyje „Neteisėtas asmens duomenų tvarkymas“ nustatyta atsakomybė už pažeidimus, susijusius su neteisėtu asmens duomenų tvarkymu pažeidžiant Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymą. Už šį pažeidimą taikomos sankcijos: bauda iki 1000 Lt, pakartotinai – bauda iki 2000 Lt. Duomenų subjekto teisių, numatytų Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatyme, pažeidimas užtraukia administracinę atsakomybę pagal Lietuvos Respubli-

[3] *Spamas* – tai nepageidaujama (nesant informacijos gavėjo sutikimo ar prašymo) ir (ar) nepageidautina (prieštaraujant informacijos gavėjui) plataus masto, dažniausiai reklaminiais komerciniais tikslais (visada siekiant gauti tam tikrą naudą) elektroniniu paštu siunčiama įvairi informacija, apkraunanti informacines sistemas bei interneto vartotojų elektroninio pašto dėžutes ir atnešanti žalą fiziniams bei juridiniams asmenims.

kos administracinių teisės pažeidimų kodekso 214-16 straipsnį. Valstybinės duomenų apsaugos inspekcijos pareigūnų teisėtų nurodymų nevykdymas yra baudžiamas pagal Lietuvos Respublikos administracinių teisės pažeidimų kodekso 214-17 straipsnį. Šiame kodekse yra ir normų, numatančių administracinę atsakomybę ir *lex specialis* asmens duomenų apsaugos teisės normų pažeidimo atveju, pavyzdžiui, kodekso 214-23 straipsnis numato atsakomybę už neteisėtą asmens duomenų tvarkymą elektroninių ryšių srityje.

Įstatymą detalizuoja poįstatyminiai teisės aktai. Nemažą jų dalį sudaro Lietuvos Respublikos Vyriausybės nutarimai. Kaip pavyzdį galima paminėti Lietuvos Respublikos Vyriausybės 2002 m. vasario 20 d. nutarimą Nr. 262 „Dėl Asmens duomenų valdytojų valstybės registro reorganizavimo, šio registro nuostatų ir asmens duomenų valdytojų pranešimo apie duomenų tvarkymą automatiniu būdu tvarkos patvirtinimo“. Šiuo nutarimu nustatyta asmens duomenų valdytojų pranešimo apie duomenų tvarkymą automatiniu būdu tvarka bei patvirtinti asmens duomenų valdytojų valstybės registro nuostatai. Valstybinės duomenų apsaugos inspekcijos direktoriaus įsakymais taip pat patvirtinti:

– rekomenduojama pranešimo apie duomenų tvarkymą forma;
– reikalavimai duomenų apsaugos priemonių aprašui;
– išankstinės patikros taisyklės ir pan.

Valstybinė duomenų apsaugos inspekcija be privalomų poįstatyminių teisės aktų leidžia ir rekomendacijas, kurios nėra privalomojo pobūdžio. Visos inspekcijos rekomendacijos skelbiamos inspekcijos tinklalapyje http://www.ada.lt

4.3. Papildoma medžiaga. Privatumo ir asmens duomenų apsauga elektroniniuose ryšiuose

4.3.1. Privatumo ir asmens duomenų apsaugos elektroniniuose ryšiuose pagrindiniai ypatumai

Dėl elektroninių komunikacijų ir ryšio priemonių konvergencijos[4] pastaruoju metu vietoj telekomunikacinių naudojama elektroninių ryšių sąvoka. Elektroniniai ryšiai – signalų perdavimas laidinėmis, radijo, optinėmis ar kitomis elektromagnetinėmis priemonėmis – su-

[4] Konvergencija – žiniasklaidos, telekomunikacijų ir informacijos technologijų sektorių susiliejimas, įskaitant fiksuotųjų, judriųjų, antžeminių ir palydovinių ryšių, ryšių ir vietos nustatymo sistemų susiliejimą.

daro galimybę žmonėms bendrauti nepaisant jų fizinio buvimo vietos. Tačiau elektroniniai ryšiai suteikia ne tik neabejotinų pranašumų, bet ir kelia vis didesnę grėsmę žmogaus privačiam gyvenimui. Elektroninių ryšių paslaugų ir tinklų teikėjai, vykdydami savo veiklą, tvarko daugybę duomenų, kurių dauguma priskirtina prie asmens duomenų. Elektroniniais ryšiais taip pat perduodama elektroninių ryšių paslaugų gavėjų siunčiama informacija (turinys). Todėl toks duomenų tvarkymas ir perdavimas neabejotinai turi (gali turėti) didelį poveikį elektroninių ryšių paslaugų gavėjų privatumui.

Europos Sąjungos privatumo ir asmens duomenų apsaugos elektroniniuose ryšiuose reguliavimas pritaikytas išimtinai elektroninių ryšių sektoriui. Tam skirta 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva Nr. 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (direktyva dėl privatumo ir elektroninių ryšių). Ši direktyva priklauso naujajai elektroninių ryšių reguliavimo direktyvų sistemai ir pakeitė senosios reguliavimo sistemos 1997 m. gruodžio 15 d. Europos Parlamento ir Tarybos direktyvą Nr. 97/66/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos telekomunikacijų srityje. 2002/58/EB direktyva taip pat papildo bendrąją duomenų apsaugos direktyvą Nr. 95/46/EB, kurios bendrieji duomenų apsaugos principai taip pat svarbūs elektroninių ryšių sektoriui. Vis dėlto 2002/58/EB direktyvos normos laikytinos *lex specialis*.

Viešųjų elektroninių ryšių paslaugų abonentai gali būti fiziniai ar juridiniai asmenys, tad 2002/58/EB direktyva siekiama apsaugoti fizinių asmenų teises ir ypač jų teisę į privatumą, taip pat teisėtus juridinių asmenų interesus.

2002/58/EB direktyva Lietuvoje įgyvendinta Lietuvos Respublikos elektroninių ryšių įstatymo IX skirsnyje, ir, kaip jau minėta, už šio skirsnio priežiūrą atsakinga Valstybinė duomenų apsaugos inspekcija. Atkreiptinas dėmesys, kad juridiniams asmenims apsauga taikoma tik tiesioginės rinkodaros ir abonentų sąrašų atvejais.

Privatumo ir asmens duomenų apsaugos elektroniniuose ryšiuose reguliavimą galima suskirstyti į šias pagrindines grupes:

1) viešųjų elektroninių ryšių paslaugų ir tinklų saugumo;
2) ryšio slaptumo;
3) srauto duomenų tvarkymo;
4) detaliųjų sąskaitų;
5) abonentų sąrašų;
6) tiesioginės rinkodaros;

7) ryšio linijos nustatymo.

Šios grupės aptartinos išsamiau.

Viešųjų elektroninių ryšių paslaugų ir tinklų saugumas. Pagal Lietuvos Respublikos elektroninių ryšių įstatymo 62 straipsnį viešųjų elektroninių ryšių paslaugų teikėjai privalo įgyvendinti tinkamas technines ir organizacines priemones, kad užtikrintų savo teikiamų paslaugų saugumą, o prireikus – kartu su viešųjų ryšių tinklų teikėjais imtis tokių pat priemonių užtikrinti viešųjų ryšių tinklų saugumą. Šios priemonės turi užtikrinti iškilusią grėsmę atitinkantį saugumo lygį.

Be to, iškilus ypatingai elektroninių ryšių tinklo ar jo dalies saugumo pažeidimo grėsmei, viešųjų elektroninių ryšių paslaugų teikėjas privalo informuoti abonentus apie tokią grėsmę ir tais atvejais, kai paslaugų teikėjo taikomos priemonės nepanaikina grėsmės kilmės priežasčių, taip pat informuoti abonentus apie visas įmanomas gelbėjimo priemones ir nurodyti tikėtinas jų kainas. Saugumo pažeidimo grėsmė gali kilti atviruoju tinklu, pavyzdžiui, internetu, teikiamoms elektroninių ryšių paslaugoms, taip pat kitais atvejais. Paslaugų teikėjai, siūlantys viešai prieinamų elektroninių ryšių paslaugas internetu, turėtų informuoti naudotojus ir abonentus apie tai, kokias priemones jie galėtų taikyti savo pranešimams apsaugoti, pavyzdžiui, specialią programinę įrangą ar šifravimo technologijas. Reikalavimas pranešti abonentams apie konkretų pavojų saugumui neatleidžia paslaugų teikėjo nuo įsipareigojimo savo lėšomis imtis tinkamų ir skubių priemonių pašalinti bet kokį naują, nenumatytą saugumo pavojų ir atkurti normalų paslaugos saugumo lygį. Informacija abonentui apie saugumo pavojų turėtų būti teikiama nemokamai.

Papildomai paminėtina, kad Valstybinė duomenų apsaugos inspekcija yra priėmusi rekomendacinio pobūdžio aktą – rekomendacijas „Dėl viešųjų elektroninių ryšių tinklų ir paslaugų saugumo užtikrinimo“. Šių rekomendacijų tikslas – supažindinti paslaugų teikėjus ir tinklų teikėjus, abonentus ir paslaugų naudotojus su galimomis asmens privatumo pažeidimo grėsmėmis, pateikti metodinius nurodymus dėl naudotinų apsaugos priemonių.

Ryšio slaptumas. Lietuvos Respublikos elektroninių ryšių įstatymo 63 straipsnis įtvirtina konfidencialumo apsaugą ir draudžia ne faktiniams elektroninių ryšių paslaugų naudotojams, neturintiems atitinkamų faktinių elektroninių ryšių paslaugų naudotojų sutikimo, klausytis, įrašyti, kaupti ar kitu būdu perimti informaciją. Šios nuostatos nedraudžia techninio informacijos saugojimo, būtino informacijai perduoti (pvz., balso pašto paslauga mobiliajame telefone).

Lietuvos Respublikos elektroninių ryšių įstatymo 63 straipsnio nuostatų pažeidimas gali užtraukti baudžiamąją atsakomybę pagal Lietuvos Respublikos baudžiamojo kodekso 166 straipsnį „Neteisėtas susirašinėjimo, kitokių pranešimų, siuntų ar pokalbių telefonu slaptumo pažeidimas“.

Srauto duomenų tvarkymas. Pagal Lietuvos Respublikos elektroninių ryšių įstatymo 3 straipsnio 52 punktą srauto duomenimis laikytini „duomenys, tvarkomi siekiant perduoti informaciją elektroninių ryšių tinklu ir (arba) tokio perdavimo apskaitai“. Europos Sąjungos direktyvos Nr. 2002/58/EB preambulės 15 punkte paminėta, kad „srauto duomenys gali, inter alia, apimti duomenis, nurodančius pranešimo maršrutą, trukmę, laiką ar apimtį, naudojamą protokolą, siuntėjo ar gavėjo galinio įrenginio vietą, tinklą, kuriame pranešimas atsirado ar pasibaigė, ryšio pradžios bei pabaigos laiką“. Remiantis šiomis sąvokomis, tradicinės telefonijos atveju srauto duomenų pavyzdžiu yra informacija apie sujungimo laiką, trukmę bei skambinančiojo telefono numerį, o elektroninio pašto atveju – siuntėjo IP adresas, elektroninio pašto adresas, elektroninio pašto žinutės dydis, elektroninio pašto žinutės pavadinimas[5], elektroninio pašto žinutės priedų dydis ir tipas.

Galima daryti išvadą, kad srauto duomenys – itin specifiniai duomenys, kurie gali atskleisti daugybę asmeninio gyvenimo detalių tokių kaip: asmens įpročiai, pomėgiai, asmenų, su kuriais bendraujama, ratas ir pan. Tokie duomenys saugotini tiek, kiek jie reikalingi sąskaitoms pateikti ir sumokėti už tinklų sujungimus, ir tik ribotą laiką (pagal Lietuvos Respublikos elektroninių ryšių įstatymo 64 straipsnio 2 dalį – 6 mėnesius nuo sąskaitos išrašymo dienos[6]). Jeigu vėliau viešai prieinamų elektroninių ryšių paslaugų teikėjas pageidauja tvarkyti šiuos duomenis elektroninių ryšių paslaugų rinkodaros tikslais arba pridėtinės vertės paslaugai sukurti, tai leidžiama tik sutikus abonentui, kuris, remdamasis tikslia ir išsamia teikėjo informacija apie nu-

[5] Tačiau šiuo ir kai kuriais kitais atvejais srauto duomenys taip pat gali būti traktuojami kaip turinio duomenys, nes suteikiama informacija ir apie elektroninių komunikacijų turinį.

[6] Lietuvos Respublikos elektroninių ryšių įstatymo 77 straipsnis numato, kad „Vyriausybės įgaliotos institucijos – operatyvinės veiklos subjekto – nurodymu ūkio subjektai, teikiantys elektroninių ryšių tinklus ir (ar) paslaugas, turi tokią informaciją saugoti ilgiau, bet ne ilgiau kaip 6 mėnesius papildomai, jeigu ši informacija reikalinga operatyvinės veiklos subjektams, ikiteisminio tyrimo įstaigoms, prokurorui, teismui ar teisėjui nusikalstamoms veikoms užkardyti, tirti, nustatyti.

matomus duomenų tolimesnio tvarkymo būdus, apsisprendžia ir gali nesutikti arba panaikinti duotą sutikimą tvarkyti tokius duomenis. Suteikus ryšių rinkodaros paslaugas arba pridėtinės vertės paslaugas, sunaikinami arba padaromi anoniminiais tokioms paslaugoms reikalingi srauto duomenys. Paslaugų teikėjai privalo visada informuoti abonentus apie tai, kokių tipų duomenis tvarko, kokiais tikslais ir kokį laiką.

Įsipareigojimas sunaikinti srauto duomenis arba padaryti juos anoniminiais, kai jų jau nereikia pranešimui perduoti, neprieštarauja tokioms interneto procedūroms kaip, pavyzdžiui, IP (interneto protokolų) adresų atsarginis saugojimas sričių (domenų) vardų sistemoje ar fizinių adresų junginyje arba prisijungimo su slaptažodžiu informacijos naudojimas siekiant valdyti teisę prieiti prie tinklų ar paslaugų.

Paslaugos teikėjas gali tvarkyti su abonentais ir naudotojais susijusius srauto duomenis, kai pavieniais atvejais tai yra būtina norint aptikti pranešimų perdavimo techninius gedimus ar klaidas. Teikėjui taip pat leidžiama pateikiant sąskaitas naudotis srauto duomenimis, jeigu reikia nustatyti ir nutraukti sukčiavimą, kai nesumokama už suteiktas elektroninių ryšių paslaugas.

Detaliosios sąskaitos. Detalioji sąskaita už suteiktas elektroninių ryšių paslaugas – tai viešųjų elektroninių ryšių paslaugų teikėjų parengtas dokumentas, atitinkantis įstatymų ir kitų teisės aktų reikalavimus, kuriame chronologiškai išdėstytos visos pagal viešųjų elektroninių ryšių paslaugų teikėjo ir abonento sudarytą paslaugų teikimo sutartį suteiktos apmokestinamos elektroninių ryšių paslaugos atsiskaitomuoju laikotarpiu.

Detalioji sąskaita suteikia abonentams galimybę stebėti ir kontroliuoti savo išlaidas už suteiktas elektroninių ryšių paslaugas. Universaliųjų paslaugų ir paslaugų gavėjų teisių direktyvos Nr. 2002/22/EB 10 straipsnis kartu su I priedu numato, kad universaliųjų paslaugų teikėjai privalo teikti detaliąsias sąskaitas abonentams (esant jų prašymui).

Valstybinė duomenų apsaugos inspekcija 2005 metais patvirtino reikalavimus detaliosioms sąskaitoms, nustatančius viešųjų elektroninių ryšių paslaugų teikėjų teikiamų detaliųjų sąskaitų turinį ir jų pateikimo viešųjų elektroninių ryšių paslaugų abonentams – fiziniams asmenims – formas.

Abonentų sąrašai. Elektroninių ryšių paslaugų abonentų sąrašai yra plačiai paplitę ir vieši. Pagal Universaliųjų paslaugų ir paslaugų gavėjų teisių direktyvos Nr. 2002/22/EB 5 straipsnį universaliųjų pa-

slaugų operatoriai turi užtikrinti viešųjų abonentų sąrašų buvimą. Į šiuos abonentų sąrašus įtraukiami visi abonentai, išskyrus tuos, kurie nesutinka būti įtraukti. Fizinių asmenų teisė į privatumą ir juridinių asmenų teisėti interesai reikalauja, kad abonentas apsispręstų ne tik dėl to, ar jo asmens duomenys skelbtini sąraše, bet ir dėl to, kokie duomenys skelbtini.

Pagal Lietuvos Respublikos elektroninių ryšių įstatymo 67 straipsnį, kai viešuoju abonentų sąrašu siekiama daugiau negu tik suteikti galimybę ieškoti abonentų kontaktinių duomenų pagal jų vardus (pavardes), turi būti gautas atitinkamo abonento sutikimas.

Tiesioginė rinkodara. Direktyva Nr. 2002/58/EB skiria automatinę tiesioginę rinkodarą ir neautomatinę tiesioginę rinkodarą. Remiantis direktyvos Nr. 2002/58/EB 13 straipsniu, naudoti automatinio skambinimo sistemas (skambinimo automatus), faksimilinius aparatus (faksus) ar elektroninį paštą tiesioginės rinkodaros tikslais gali būti leidžiama tik gavus išankstinį abonentų sutikimą. Direktyvos Nr. 2002/58/EB 13 straipsnis suteikia valstybėms narėms kitų tiesioginės rinkodaros formų pasirinkimo laisvę (pvz., neautomatinės tiesioginės rinkodaros). Lietuvos įstatymų leidėjai nusprendė, kad abonentų sutikimas būtinas ir automatinėje tiesioginėje rinkodaroje, ir neautomatinėje tiesioginėje rinkodaroje. Taigi elektroniniuose ryšiuose tiesioginę rinkodarą galima naudoti tik laikantis vadinamojo *OPT-IN* principo.

Paminėtina, kad paties ūkio subjekto panašių prekių ar paslaugų rinkodaros atveju Lietuvos Respublikos elektroninių ryšių įstatymas nustato „OPT-OUT“ principą. Įstatymo 68 straipsnio 2 dalyje nurodyta, jog asmuo, kuris teikdamas paslaugas ar parduodamas prekes Asmens duomenų teisinės apsaugos įstatymo nustatyta tvarka ir sąlygomis gauna savo klientų elektroninio pašto adresus, gali naudoti šiuos duomenis savo paties panašių prekių ar paslaugų rinkodarai, jei klientams suteikia aiškią, nemokamą ir lengvai įgyvendinamą galimybę nesutikti arba atsisakyti tokio duomenų naudojimo anksčiau nurodytais tikslais, kai šie duomenys yra renkami, ir jei siunčiant kiekvieną žinutę klientas iš pradžių neprieštaravo dėl tokio duomenų naudojimo.

Pagal Lietuvos Respublikos elektroninių ryšių įstatymo 68 straipsnio 3 dalį draudžiama tiesioginės rinkodaros tikslu siųsti elektroninio pašto pranešimus slepiant siuntėjo, kurio vardu informacija siunčiama, tapatybę arba nenurodant galiojančio adreso, kuriuo gavėjas galėtų reikalauti nutraukti tokios informacijos siuntimą.

Ryšio linijos nustatymas. Kalbant apie ryšio linijos, iš kurios skambinama, nustatymą, būtina apsaugoti skambinančio asmens teisę neleisti nustatyti liniją, iš kurios skambinama, taip pat ir asmenų, kuriems skambinama, teisę atsisakyti skambučių iš nenustatytų linijų. Lietuvos Respublikos elektroninių ryšių įstatymo 70 straipsnis užtikrina šias pagrindines teises:

– teisę skambinančiajam panaikinti galimybę nustatyti ryšio liniją, iš kurios skambinama;
– teisę abonentui, kuriam skambinama, panaikinti galimybę nustatyti ryšio liniją, iš kurios skambinama;
– teisę atsisakyti skambučio iš nenustatytos linijos;
– teisę uždrausti nustatyti ryšio liniją, į kurią skambinama.

2003 metais Lietuvos Respublikos Vyriausybė nutarimu Nr. 212 nustatė ryšio linijos, iš kurios skambinama, nustatymo draudimo netaikymo tvarką. Ši tvarka apibrėžia būdus, kuriais viešųjų telekomunikacijų paslaugų teikėjai ir (ar) viešųjų telekomunikacijų tinklų operatoriai gali netaikyti ryšio linijos, iš kurios skambinama, nustatymo draudimo. Minimi atvejai susiję su erzinančiais ir piktybiniais skambučiais.

4.3.2. Privataus gyvenimo neliečiamumo ribojimas elektroniniuose ryšiuose nusikaltimų tyrimo tikslais

Elektroniniai ryšiai suteikia ne tik neabejotinų pranašumų, bet kelia vis didelę grėsmę žmogaus gyvenimo privatumui. Neabejotina, kad elektroninės komunikacijos didžiausią įtaką gali daryti asmens santykiams su kitais asmenimis elektroninių ryšių tinklų pagalba. Asmens bendravimo privatumas labiausiai pažeistas gali būti bendraujant elektroninio ryšio priemonėmis.

Paminėtina, kad didžiausią grėsmę žmogaus teisei į privataus gyvenimo neliečiamumą kelia elektroninių ryšių perėmimas. Pastaruoju metu išaiškėjo gana dideli teisėsaugos atliekamos elektroninių ryšių kontrolės mastai.

Teisės į privatų gyvenimą teisėto ribojimo galimybė. Paminėtina, kad teisė į privatų gyvenimą nėra absoliuti – ji nepriskirta toms žmogaus teisėms, kurių ribojimas nėra galimas. Įgyvendindamas savo teises ir naudodamasis savo laisvėmis žmogus privalo laikytis Lietuvos Respublikos Konstitucijos ir įstatymų, nevaržyti kitų žmonių teisių ir laisvių. Todėl toks žmogus, kuris negerbia kitų žmonių teisių ir laisvių, negali tikėtis savo teisių ir laisvių, įskaitant privataus gyvenimo nelie-

čiamumą, užtikrinimo. Lietuvos Respublikos Konstitucinis Teismas pažymėjo, kad „asmuo, darydamas nusikalstamas ar kitas priešingas teisei veikas, neturi ir negali tikėtis privatumo. Žmogaus privataus gyvenimo apsaugos ribos baigiasi tada, kai jis savo veiksmais nusikalstamai ar kitaip neteisėtai pažeidžia teisės saugomus interesus, daro žalą atskiriems asmenims, visuomenei ir valstybei“.

Lietuvos Respublikos Konstitucijos 22 straipsnis ir Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos 8 straipsnio 2 dalis numato, kad ši teisė esant tam tikroms aplinkybėms gali būti ribojama. Pavyzdžiui, minima teisė gali būti ribojama dėl valstybės intereso gauti informacijos apie asmenį, pavyzdžiui, padariusį nusikaltimą. Kaip minėta, Lietuvos Respublikos Konstitucijos 22 straipsnio 3 dalyje teigiama, kad „informacija apie privatų asmens gyvenimą gali būti renkama tik motyvuotu teismo sprendimu ir tik motyvuotu teismo sprendimu ir tik pagal įstatymą“. Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos 8 straipsnyje nustatyta, kad „valstybės institucijos neturi teisės apriboti naudojimosi šiomis teisėmis, išskyrus įstatymų nustatytus atvejus ir kai tai būtina demokratinėje visuomenėje valstybės saugumo, visuomenės apsaugos ar šalies ekonominės gerovės interesams siekiant užkirsti kelią viešosios tvarkos pažeidimams ar nusikaltimams, taip pat būtina žmonių sveikatai ar moralei arba kitų asmenų teisėms ir laisvėms apsaugoti“.

Taigi teisės į privataus gyvenimo neliečiamybę ribojimas turi būti paremtas tam tikrais principais. Čia svarbi Europos Žmogaus Teisių Teismo praktika. Bylose *Amannas prieš Šveicariją, Armstrongas prieš Jungtinę Karalystę, Khanas prieš Jungtinę Karalystę* Europos Žmogaus Teisių Teismas suformavo šias pagrindines žmogaus teisių ribojimo sąlygas:

1) teisėtumo sąlygą, nurodančią, kad ribojimai gali būti nustatomi tik viešai paskelbtu ir aiškiai suformuluotu įstatymu;

2) būtinumo sąlygą, nurodančią, kad ribojimai gali būti nustatomi tik tuomet, kai tai reikalinga demokratinėje visuomenėje.

Žmogaus teisių ribojimo klausimu pasisakė ir Lietuvos Respublikos Konstitucinis Teismas. 2002 m. rugsėjo 19 d. Lietuvos Respublikos Konstitucinio Teismo nutarime teigiama, kad pagal Konstituciją riboti konstitucines žmogaus teises ir laisves galima, jeigu laikomasi šių sąlygų:

– tai daroma pagal įstatymą;
– ribojimai yra būtini demokratinėje visuomenėje siekiant apsaugoti kitų asmenų teises bei laisves ir Konstitucijoje įtvirtintas

vertybes, taip pat konstituciškai svarbius tikslus;
– ribojimais nėra paneigiama teisių ir laisvių prigimtis bei jų esmė;
– yra laikomasi konstitucinio proporcingumo principo.

Teisės į privatų gyvenimą ribojimas elektroniniuose ryšiuose[7] taip pat turėtų būti vykdomas vadovaujantis aukščiau išvardintais principais ir sąlygomis. Elektroninių ryšių kontrolę (plačiuoju požiūriu), vykdomą operatyviniais ar kitais nusikaltimų tyrimo tikslais, galima skirstyti į dvi grupes:

1) buvusių elektroninių ryšių įvykių kontrolę – informacijos apie buvusius elektroninių ryšių įvykius (srauto duomenis) gavimą iš elektroninių ryšių paslaugų teikėjų;

2) elektroninių ryšių tinklais perduodamos informacijos kontrolę (kompetentingų teisėsaugos institucijų vykdomą elektroninių ryšių turinio ar kitos elektroninių ryšių tinklais perduodamos informacijos kontrolę).

Kiekvienos kontrolės grupės įgyvendinimui praktikoje teisės aktai nustato šiek tiek skirtingus reikalavimus. Toliau aptarsime abi elektroninių ryšių kontrolės grupes.

Buvusių elektroninių ryšių įvykių kontrolė. Kas yra laikoma elektroninių ryšių įvykiais, kurių metu sugeneruojami srauto duomenys? 2002 m. rugsėjo 19 d. Lietuvos Respublikos Konstitucinio Teismo nutarime telekomunikacijų įvykis apibūdinamas kaip „informacijos perdavimo, siuntimo, priėmimo telekomunikacijų tinklais faktas“. Pagal Lietuvos Respublikos elektroninių ryšių įstatymo 3 straipsnio 52 punktą srauto duomenimis laikytini „duomenys, tvarkomi siekiant perduoti informaciją elektroninių ryšių tinklu ir (arba) tokio perdavimo apskaitai“. Direktyvos dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje Nr. 2002/58/EB preambulėje paminėta, kad „srauto duomenys gali *inter alia* apimti duomenis, nurodančius pranešimo maršrutą, trukmę, laiką ar apimtį, naudojamą protokolą, siuntėjo ar gavėjo galinio įrenginio vietą, tinklą, kuriame pranešimas atsirado ar pasibaigė, ryšio pradžios bei pabaigos laiką“. Remiantis šiomis sąvokomis galima teigti, kad tradicinės telefonijos atveju srauto duomenimis laikytina informacija apie sujungimo laiką, trukmę, skambinančiojo telefono numerį ir panaši, o elektroninio pašto atveju srauto duomenimis gali būti laikomi šie duomenys: siuntėjo IP adresas ir elektroninio pašto adresas, elektroninio pašto žinutės dy-

[7] Šis ribojimas taip pat gali būti vadinamas elektroninių ryšių kontrole.

dis, elektroninio pašto žinutės pavadinimas[8], elektroninio pašto žinutės priedų dydis, tipas ir panašūs.

Pagal Lietuvos Respublikos elektroninių ryšių įstatymo 77 straipsnio 1 dalį „ūkio subjektai, teikiantys elektroninių ryšių tinklus ir (ar) paslaugas, privalo kompetentingoms institucijoms – operatyvinės veiklos subjektų pagrindinėms institucijoms, Vyriausybės nurodytoms ikiteisminio tyrimo įstaigoms, prokurorui, teismui ar teisėjui – pateikti turimą informaciją“. Šiai informacijai priklauso ir informacija apie elektroninių ryšių įvykius, t. y. srauto duomenys.

Jei informacija renkama operatyvinės veiklos tikslais, pagal Lietuvos Respublikos operatyvinės veiklos įstatymą yra būtina teismo nutartis. Šiame įstatyme nustatyta, kad „operatyviniam tyrimui reikalingą konkrečią informaciją apie buvusius telekomunikacijų įvykius iš telekomunikacijų operatorių ir telekomunikacijų paslaugų teikėjų operatyvinės veiklos subjektai turi teisę gauti motyvuota apylinkės teismo teisėjo nutartimi, priimta pagal operatyvinės veiklos subjektų vadovų ar jų įgaliotų vadovų pavaduotojų motyvuotus teikimus“. Pagal įstatymo 10 straipsnio 13 dalį „telekomunikacijų operatoriams ar telekomunikacijų paslaugų teikėjams turi būti pateikiamas pranešimas, kuriame nurodomi teikimo numeris, nutarties priėmimo data ir nutartį priėmęs teismas“. Pagal įstatymą už tokio pranešimo turinio atitikimą teismo nutarčiai įstatymų nustatyta tvarka atsako pranešimą teikiantis pareigūnas. Paminėtina, kad nustatant reikalavimus buvusių elektroninių ryšių kontrolei užsienio valstybių praktikoje tokia kontrolė galima tik su teismo sankcija. Tokia praktika taikoma Jungtinėse Amerikos Valstijose, Suomijoje, Švedijoje, Estijoje, Latvijoje ir kitose valstybėse.

Svarbu atkreipti dėmesį į tai, kad nuo 2003 m. gegužės 1 d. įsigaliojus naujajam Lietuvos Respublikos baudžiamojo proceso kodeksui ikiteisminio tyrimo pareigūnams nebereikia motyvuotos teismo nutarties gauti informaciją apie buvusius elektroninių ryšių įvykius, kai šios informacijos reikia ikiteisminio tyrimo stadijoje[9]. Kita vertus, Lie-

---

[8] Tačiau šiuo ir kai kuriais kitais atvejais srauto duomenys taip pat gali būti traktuojami kaip turinio duomenys, nes suteikiama informacija ir apie elektroninių komunikacijų turinį.

[9] 1961 m. Lietuvos Respublikos baudžiamojo proceso kodekse 2002 metais įvestas naujas 198-3 straipsnis reglamentavo informacijos iš telekomunikacijų operatorių ir telekomunikacijų paslaugų teikėjų gavimą. Šio straipsnio 2 dalyje buvo nurodyta, jog informacija apie buvusius telekomunikacijų įvykius gaunama teismo nutartimi.

tuvos Respublikos Konstitucijoje, taip pat minėtame Lietuvos Respublikos Konstitucinio Teismo nutarime yra motyvuotos teismo nutarties reikalavimas minėtai informacijai gauti. Todėl elektroninių ryšių paslaugų teikėjai, teikdami informaciją apie buvusius elektroninių ryšių įvykius, turėtų reikalauti teismo sprendimo, kitu atveju kiltų pavojus pažeisti asmenų, apie kuriuos teikiama informacija, privataus gyvenimo neliečiamybę.

Lietuvos Respublikos elektroninių ryšių įstatymo 77 straipsnyje teigiama, kad „Vyriausybės nurodytos ikiteisminio tyrimo įstaigos Vyriausybės nustatyta tvarka organizuoja ir sudaro galimybę gauti šią informaciją savo padaliniams ir (ar) kitoms ikiteisminio tyrimo įstaigoms“. Srauto duomenų kontrolei, kurios metu ribojama asmens teisė į privatų gyvenimą, turi būti nustatyta griežta procedūra. Tačiau minima tvarka Vyriausybės iki šiol nepatvirtinta.

Didelę reikšmę buvusių elektroninių ryšių kontrolei turės 2006 m. kovo 15 d. Europos Parlamento ir Tarybos direktyva Nr. 2006/24/EB dėl duomenų, gautų arba tvarkomų teikiant viešai prieinamas elektroninių ryšių paslaugas arba viešuosius ryšių tinklus, saugojimo ir iš dalies keičianti direktyvą Nr. 2002/58/EB, kurioje informacijos apie srauto duomenis teikimo teisėsaugos institucijoms tikslais numatyta pareiga elektroninių ryšių paslaugų teikėjams srauto duomenis privalomai kaupti ir saugoti nuo 6 mėnesių iki 2 metų nuo jų užfiksavimo. Kadangi, kaip parodė praktika, ūkinei veiklai užtikrinti informaciją apie srauto duomenis elektroninių ryšių paslaugų teikėjai kaupia ne ilgiau kaip kelis mėnesius, nustačius reikalavimą duomenis kaupti iki dvejų metų, duomenys, sudarantys privataus gyvenimo paslaptį, tam tikrą laikotarpį teisėsaugos tikslais būtų kaupiami be teismo leidimo. Kaip minėta, pagal Lietuvos Respublikos Konstitucijos 22 straipsnį informacija apie privatų gyvenimą gali būti renkama tik motyvuotu teismo sprendimu ir tik pagal įstatymą. Taip pasisakė ir Lietuvos Respublikos Konstitucinis Teismas. Todėl toks įpareigojimas be motyvuoto teismo sprendimo saugoti informaciją ilgiau negu reikia užtikrinti ūkinę veiklą taip įsiterpiant į žmogaus privatų gyvenimą gali prieštarauti Konstitucijos 22 straipsnio nuostatoms. Galimas direktyvos nuostatų, susijusių su duomenų saugojimo laikotarpiu, prieštaravimas žmogaus teises reglamentuojantiems tarptautinės teisės aktams nagrinėjamas ir mokslinėje literatūroje, tačiau diskusijos tik prasideda. Lietuvos įstatymo leidėjui reikėtų įvertinti minėtos direktyvos įtaką ir santykį su Lietuvos Respublikos Konstitucija bei pasiruošti atlikti veiksmus

(įskaitant teisės aktų pakeitimus), kuriais būtų išvengta direktyvos normų prieštaravimo Lietuvos Respublikos konstitucinėms normoms.

Elektroninių ryšių turinio ir srauto duomenų kontrolė esamuoju laiku. Kas yra elektroninių ryšių turinys ar kita elektroninių ryšių tinklais perduodama informacija? Teisės aktuose nenustatyta, kas laikoma turinio duomenimis. Tačiau teisės literatūroje nurodoma, kad turinio duomenimis (ang. *communication*) laikoma bet kokia informacija, kuria keičiasi šalys viešųjų elektroninių ryšių paslaugų teikimo atveju. Kitaip tariant, turinio duomenimis laikomas pokalbio telefonu ar susirašinėjimo elektroniniu paštu turinys. Prie kitais elektroniniais ryšiais perduodamos informacijos priskirtina informacija apie srauto duomenis ir panaši.

Manoma, kad procesiniai reikalavimai srauto ir turinio duomenų rinkimui turėtų skirtis, kadangi turinio duomenys atskleidžia komunikacijų turinį, todėl jų neteisėtas atkleidimas daro didesnę žalą negu srauto duomenų neteisėtas atkleidimas. Todėl turinio duomenų kontrolės sankcionavimas turėtų būti griežtesnis. Tačiau reikėtų paminėti, kad gana lengva atskirti tradicinių telekomunikacijų turinio duomenis nuo srauto duomenų, o kitų susižinojimo formų, pavyzdžiui, interneto, kuris priskiriamas prie elektroninių ryšių, atveju toks atskyrimas gana sunkus. Tradicinių telekomunikacijų procesų turinio ir srauto duomenų takoskyra tarp srauto duomenų (kas skambino, kur skambino, kiek truko skambutis) ir turinio duomenų (pokalbio turinio) buvo gana aiški, tačiau toks atskyrimas interneto atveju yra gana sudėtingas, jeigu iš viso įmanomas. Nėra aišku, ar turinio duomenimis laikytinas visas elektroninių paketų turinys, ar srauto duomenys yra tik elektroninių paketų antraštės, ar srauto duomenimis laikytinos *clickstreams* ang. ar http užklausos. Tokiu atveju užklausa *http:///searchengine/com/++aids++homosexuality++symptoms* būtų laikoma srauto duomeniu, kai tuo tarpu minima užklausa susijusi su susižinojimo turiniu. Taip pat galima pateikti ir kitą pavyzdį – DTMF[10] kodų rinkimą elektroninių komunikacijų metu. Pavyzdžiui, surinkus atitinkamą telefoninės bankininkystės numerį po įvykusio sujungimo atsiranda galimybė paslaugas valdyti DTMF kodų pagalba. Kadangi DTMF kodai renkami jau įvykus sujungimui, galima teigti, kad tai yra elektroninių ryšių turinys. Tačiau, kita vertus, DTMF kodais siekiama inicijuoti tam

[10] DTMF yra toninio signalo tipas, kai naudojamas dviejų tonų signalas surinkti numerį, užsakyti (valdyti) paslaugą ir pan.

tikras paslaugas (veiksmus), todėl šios komandos gali turėti ir srauto duomenų požymių. Kai kurie telekomunikacijų operatoriai Valstybinės duomenų apsaugos inspekcijos tinklapyje adresu http://www.ada.lt skelbiami deklaravę technines komandas pradėti sujungimus kaip tvarkomus asmens, t. y. srauto duomenis. Šie pavyzdžiai verčia atkreipti dėmesį į diskusijų sritį – minėtų dviejų kategorijų (turinio duomenų ir srauto duomenų) sujungimo, šias kategorijas kartu pavadinant komunikacijomis (elektroniniais ryšiais), problemą.

Paminėtina, kad kitaip negu gaunant informaciją apie buvusius elektroninių ryšių įvykius iš elektroninių ryšių paslaugų teikėjų, elektroniniais ryšiais perduodamos informacijos kontrolė esamuoju laiku atliekama pačių kontroliuojančių subjektų. Pagal Lietuvos Respublikos elektroninių ryšių įstatymo 77 straipsnį, „kai yra motyvuota teismo nutartis, ūkio subjektai, teikiantys elektroninių ryšių tinklus ir (ar) paslaugas, privalo sudaryti techninę galimybę operatyvinės veiklos subjektams įstatymų nustatyta tvarka, ikiteisminio tyrimo įstaigoms – Lietuvos Respublikos baudžiamojo proceso kodekso nustatyta tvarka, kontroliuoti elektroninių ryšių kanalais perduodamos informacijos turinį“. Atkreiptinas dėmesys, kad elektroninių ryšių paslaugų teikėjams nenustatyta pareiga užtikrinti kitos elektroniniais ryšiais perduodamos informacijos kontrolę.

Lietuvos Respublikos operatyvinės veiklos įstatyme nustatytos elektroninių ryšių tinklais perduodamos informacijos kontrolės galimybės laiko atžvilgiu. Nors įstatyme nustatyta sankcionuoto termino pratęsimo procedūra, maksimalus terminas nenustatytas. Tai reiškia, kad nustatyta tvarka pratęsiant sankcionuotą laikotarpį galima neribotą laiką kontroliuoti žmogaus privatų gyvenimą, kiek tai susiję su elektroniniais ryšiais. Kaip teigiamą pavyzdį galima paminėti Lietuvos Respublikos baudžiamojo proceso kodeksą, kuris nustato iki 9 mėnesių trukmės elektroninių ryšių tinklais perduodamos informacijos ribojimo terminą.

Elektroniniais ryšiais perduodamos informacijos kontrolė pagal Lietuvos Respublikos įstatymus gali būti vykdoma operatyvinio tyrimo ar baudžiamojo proceso metu, todėl šie procesai nagrinėtini atskirai.

Elektroniniais ryšiais perduodamos informacijos kontrolė vykdant operatyvinę veiklą. Lietuvos Respublikos operatyvinės veiklos įstatymo 10 straipsnio 10 dalyje nustatyta, kad „telekomunikacijų operatorius ar telekomunikacijų paslaugų teikėjas privalo sudaryti techninę galimybę vykdyti telekomunikacijos priemonėmis perduodamos infor-

macijos kontrolę“. Šioje dalyje, aprašant procedūrą, minimas terminas – techninių priemonių panaudojimas specialia tvarka. Pagal įstatymo 3 straipsnio 8 dalį „techninių priemonių panaudojimas specialia tvarka – motyvuota teismo nutartimi sankcionuotas techninių priemonių panaudojimas operatyvinėje veikloje kontroliuojant ar fiksuojant asmenų pokalbius, kitokį susižinojimą ar veiksmus“. Žodžiai „ar veiksmus“ iš esmės turėtų apimti techninių priemonių naudojimą renkant srauto duomenis, nes būtent srauto duomenys yra susiję su tam tikrais telekomunikacijų paslaugų vartotojų veiksmais. Remiantis šia sąvoka galima teigti, kad Lietuvos Respublikos operatyvinės veiklos įstatymas numato ir turinio, ir srauto kompiuterinių duomenų surinkimo esamuoju laiku procedūras.

Elektroniniais ryšiais perduodamos informacijos kontrolė baudžiamojo proceso metu. Elektroniniais ryšiais perduodamos informacijos kontrolę ikiteisminio tyrimo institucijos atlieka pagal Lietuvos Respublikos baudžiamojo proceso kodekso taisykles. Tokios kontrolės tvarka kodekse išsamiai nustatyta, išskyrus, pavyzdžiui, reikalavimą[11], kad telekomunikacijų operatoriai privalo sudaryti sąlygas klausytis telefoninių pokalbių ar kontroliuoti kitą telekomunikacijų tinklais perduodamą informaciją. Lietuvos Respublikos baudžiamojo kodekso 154 straipsnyje nustatyta, kad „ikiteisminio tyrimo pareigūnas gali klausytis telefoninių pokalbių, kontroliuoti kitą telekomunikacijų tinklais perduodamą informaciją ar daryti įrašus“. To paties straipsnio 4 dalyje nurodyta, jog „telekomunikacijų operatoriai privalo sudaryti sąlygas klausytis telefoninių pokalbių ar kontroliuoti kitą telekomunikacijų tinklais perduodamą informaciją ar daryti įrašus“. Toks neapibrėžtumas gali lemti situaciją, kai telekomunikacijų operatorius nežinos apie jo tinkle vykdomą konkrečių asmenų perduodamos informacijos kontrolę.

Pažymėtina, kad pagal Lietuvos Respublikos baudžiamojo proceso kodekso 154 straipsnį, kuriame numatyta, kad pagal teisėjo nutartį gali būti kontroliuojama „kita telekomunikacijų tinklais perduodama informacija“, internetu perduodamos informacijos kontrolei taip pat reikalinga teismo nutartis. Lietuvos Respublikos baudžiamojo kodekso 154 straipsnyje naudojama telekomunikacijų tinklais perduodamos informacijos sąvoka, todėl, atrodytų, problemų dėl turinio ir srauto

[11] Be to, šis reikalavimas pagal savo esmę turėtų būti išdėstytas ne Lietuvos Respublikos baudžiamojo proceso kodekse, o Lietuvos Respublikos elektroninių ryšių įstatyme.

duomenų atskyrimo neturėtų kilti, ši sąvoka, kategorija apima tiek srauto, tiek turinio duomenis, kuriuos elektroninėje erdvėje, kaip jau minėta, dažnai sunku atskirti. Tačiau kodekso 154 straipsnio 2 dalis numato tik telekomunikacijų tinklais perduodamų srauto duomenų kontrolės ir fiksavimo galimybę. Todėl gali kilti problemų dėl šios normos įgyvendinimo internetu. Tačiau, kita vertus, tai pateisinama tuo, kad turinio ir srauto duomenų kontrolės sąlygos gali skirtis.

Lietuvos Respublikos baudžiamojo proceso kodekse kitos, ne turinio, elektroniniais ryšiais perduodamos informacijos kontrolei nustatytos platesnės galimybės – šią informaciją galima kontroliuoti ir tada, „jeigu yra pagrindas manyti, kad tokiu būdu galima gauti duomenų apie nesunkius nusikaltimus, numatytus Lietuvos Respublikos baudžiamojo kodekso 166, 196, 197, 198(1) straipsniuose, 309 straipsnio 1 ir 2 dalyse“. Taigi kodeksas įgyvendina skirtingų reikalavimų nustatymo turinio ir srauto duomenų kontrolei principą, nors, kaip minėta, šį principą sunku įgyvendinti internete.

Elektroniniais ryšiais perduodamos informacijos kontrolės priežiūra. Lietuvos Respublikos Vyriausybė ilgai delsė įgalioti specialią instituciją – konkretų operatyvinės veiklos subjektą. Tik 2000 metų gruodį Vyriausybės nutarime buvo įvardinta, kad valstybės įgaliota institucija – Valstybės saugumo departamentas. Deja, iki šiol nenustatyta tvarka, pagal kurią Valstybės saugumo departamentas kiekvienam operatyvinės veiklos subjektui, o baudžiamajame procese – ir ikiteisminio tyrimo įstaigai, sudarytų technines galimybes savarankiškai kontroliuoti elektroninių ryšių tinklais perduodamos informacijos turinį. Europos Žmogaus Teisių Teismo praktika dėl Europos žmogaus teisių konvencijos teigia, kad valstybės turi užtikrinti, kad jų teisės aktai numatytų garantijas ir apsaugą nuo galimo piktnaudžiavimo kontroliuojant elektroninių ryšių turinį. Kadangi Lietuva ratifikavo minėtą konvenciją ir prisiėmė atitinkamus įsipareigojimus, taip pat privalo užtikrinti minimų garantijų užtikrinimą nacionaliniuose teisės aktuose.

Valstybės įgaliota institucija įvardijus Valstybės saugumo departamentą, tapo aišku, kad elektroninių ryšių tinklu siunčiamos techninės komandos „pradėti“ ar „nutraukti“ pasiklausymą ar kitą elektroninių ryšių tinklais perduodamos informacijos kontrolę bus saugomos šio departamento patalpose. Tai reiškia, kad ta pati institucija tam tikrais atvejais ir organizuos perduodamos informacijos kontrolės vykdymą, ir saugos šios kontrolės įrodymus. Technines komandas pradėti ar pabaigti pasiklausymą ar kitos elektroniniais ryšiais perduodamos informacijos kontrolę turi saugoti ne pati operatyvinę veiklą vyk-

danti institucija, nes tokiu atveju, kai ta pati institucija ir vykdo operatyvinę veiklą, ir kontroliuoja tokios veikos vykdymą, negalima užtikrinti tokios veiklos skaidrumo.

Kita galima elektroninių ryšių turinio ar kitos elektroniniais ryšiais perduodamos informacijos perėmimo proceso kontrolės forma – parlamentinė kontrolė. Paminėtina, kad pagal Operatyvinės veiklos įstatymą asmenų konstitucinių teisių ir laisvių apsaugą vykdant operatyvinę veiklą kontroliuoja Operatyvinės veiklos parlamentinės kontrolės komisija. Tokia komisija buvo sukurta tik 2003 m. pabaigoje, kilus prezidentūros skandalui, o komisijos nuostatai buvo patvirtinti tik 2004 metais. Komisijos nuostatuose įtvirtintos teisės sudaro tam tikras prielaidas kontroliuoti teisėsaugos institucijas, kai kuriais atvejais sunku išvengti politinių sprendimų. Manytina, kad šios komisijos kontrolę reikia derinti su specialios ir nuo politinės valdžios nepriklausomos institucijos (komisijos) vykdoma operatyvinės veiklos kontrole. Pagal šiuo metu galiojantį Lietuvos Respublikos operatyvinės veiklos įstatymą parlamentinei komisijai suteikta teisė tirti tik šiurkščius Operatyvinės veiklos įstatymo pažeidimo bei operatyvinės veiklos subjektų nustatytų veiklos ribų peržengimo atvejus. Tuo tarpu speciali institucija galėtų nagrinėti ir paprastus skundus dėl teisės į privatų gyvenimą pažeidimo (įskaitant jau įvykusios elektroninių ryšių kontrolės teisėtumo įvertinimą). Tokia institucija taip pat turėtų teikti ir periodines ataskaitas apie vykdytas „sekimo“ priemones (elektroninių ryšių kontrolės skaičius, kokiems nusikaltimams tirti buvo panaudotos elektroninio sekimo priemonės, elektroninių sekimo priemonių panaudojimo tęstinumas ir pan.)[12]. Panašios institucijos jau veikia Vokietijoje, Prancūzijoje, Jungtinėje Karalystėje ir kitose valstybėse.

4.4. Papildoma medžiaga. Privatumas elektroninėje darbo vietoje

Praktikoje vis labiau plinta darbdavio vykdoma darbuotojo elektroninės darbo vietos kontrolė. Darbdavys nori žinoti, ką darbo metu veikia darbuotojas. Tokia kontrolė pasireiškia darbo internete, elektroninio pašto, darbo su programomis, kompiuteryje saugomos elektroninės informacijos kontrole. Pastaruoju metu ypač sparčiai plinta

[12] Metinės ataskaitos, kuriose nurodyti elektroninių ryšių kontrolės mastai, trukmė ir kita informacija, jau leidžiamos tokiose valstybėse kaip: Prancūzija, Švedija, Australija, Kanada, JAV ir kt.

IP telefonija, todėl elektroninės darbo vietos kontrolė gali apimti ir darbuotojo pokalbių stebėjimą.

Darbdaviui kontroliuojant elektroninę darbuotojo darbo vietą, susiduria du priešingi interesai: darbuotojo ir darbdavio. Viena, darbuotojas kaip asmuo turi teisę į privatų gyvenimą ir tikisi, kad ši teisė nebus pažeista. Kita vertus, yra priežastys, sąlygos, aplinkybės, verčiančios darbdavius stebėti ir kontroliuoti darbuotojus darbo vietoje elektroninių priemonių pagalba. Paminėti galima darbo tvarkos ir drausmės užtikrinimo, darbuotojų darbo našumo ir efektyvumo didinimo, darbdavio finansinių resursų taupymo, darbdavio gero vardo išsaugojimo, kompiuterių sistemos apsaugos ir veiksmingumo poreikius ir kt. Visa tai sudaro teisėtą darbdavio verslo interesą.

Skirtingos elektroninės darbo vietos kontrolės koncepcijos. Verta paminėti, kad skirtingose teisės tradicijose darbdavio ir darbuotojo santykis, darbdaviui kontroliuojant elektroninę darbuotojo darbo vietą, įtvirtintas nevienodai.

Jungtinių Amerikos Valstijų Konstitucija tradiciškai ne itin saugo darbuotojų gyvenimo privatumą elektroninėje darbo vietoje. Jungtinių Amerikos Valstijų federaliniuose ir valstijų teisės aktuose darbuotojų privatumui taip pat skiriama labai mažai dėmesio. Vienas iš pagrindinių Jungtinių Amerikos Valstijų teisinės sistemos federalinių įstatymų, susijusių su darbuotojo elektroninės darbo vietos apsauga, – Elektroninių komunikacijų privatumo įstatymas. Šiame federaliniame įstatyme numatytos trys išimtys, kada darbuotojas turėtų apriboti savo privatumo siekius, o darbdaviui suteikiama teisė tikrinti elektroninę darbuotojo darbo vietą:

- teikėjo (angl. *provider*) išimtis;
- įprastinės verslo eigos (angl. *ordinary course of business*) išimtis;
- sutikimo (angl. *concent*) išimtis.

Teikėjo išimtis reiškia, kad jeigu darbdavys sudaro sąlygas darbuotojui darbinių funkcijų atlikimui naudoti darbdaviui priklausančią elektroninio pašto sistemą, pastarasis turi teisę tikrinti darbuotojo elektroninę darbo vietą.

Elektroninių komunikacijų privatumo įstatymas taip pat įgalina darbdavį kontroliuoti elektroninę darbuotojo darbo vietą remiantis įprastinės verslo eigos išimtimi, jei to reikia, pavyzdžiui, saugant įmonės teises ar turtą.

Sutikimo išimtis reiškia, kad darbuotojo sutikimas lėmė jo paties teisės į privatumą apribojimą, suteikė darbdaviui besąlygišką teisę tik-

rinti jo elektroninę darbo vietą. Sutikimas gali būti išreikštas (pasirašytas) arba numanomas. Pavyzdžiui, teigiama, kad darbuotojas davė sutikimą tikrinti elektroninį paštą, jei jis, žinodamas apie egzistuojančią elektroninio pašto tikrinimo galimybę, toliau naudojosi elektroninio pašto sistema.

Taigi elektroninių komunikacijų privatumo įstatymas suteikia darbdaviams plačias teises kontroliuoti darbuotojo elektroninę darbo vietą. Tai, kad darbdavio darbo kontrolės interesai nusveria darbuotojo privatumo interesus, rodo ir keletas Kalifornijos teismuose išnagrinėtų bylų. Viena iš tokių bylų – *Bourke v. Nissan Corp.* Teismas šioje byloje konstatavo, kad darbdavys turėjo visišką teisę tikrinti darbuotojo elektroninį paštą, kadangi darbuotojas buvo iš anksto informuotas apie tokio tikrinimo galimybę. Tai, kad darbuotojas turėjo slaptažodį prisijungti prie kompiuterio, neturėjo įtakos, kadangi darbuotojas nepagrįstai tikėjosi privatumo.

Jungtinėse Amerikos Valstijose federaliniai bei valstijų įstatymai ir teismai darbdaviui, kontroliuojančiam elektroninę darbuotojo darbo vietą, dažniausiai suteikia pirmenybę prieš darbuotojo interesus. Teismų interpretacija didžiąja dalimi remiasi tuo, jog elektroninė darbo vieta priklauso darbdaviui, todėl darbdavys pagrįstai tikisi, kad tokia darbo vieta būtų tinkamai naudojama. Dėl šios priežasties darbdavys Jungtinėse Amerikos Valstijose turi plačias teises kontroliuoti darbuotojo elektroninę darbo vietą.

Europoje darbuotojų privačiam gyvenimui elektroninėje darbo vietoje saugoti skiriama daugiau dėmesio negu Jungtinėse Amerikos Valstijose. Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos 8 straipsnis asmenims garantuoja teisę į asmeninį ir šeimos gyvenimą, buto neliečiamybę ir susirašinėjimo slaptumą[13].

Pagal Europos Sąjungos bendrosios duomenų apsaugos direktyvos Nr. 95/46/EB 29 straipsnio nuostatas sudaryta duomenų apsaugos darbo grupė, sudaryta iš įvairių valstybių duomenų apsaugos institucijų atstovų[14] (toliau – Duomenų apsaugos darbo grupė), pateikė tris principus, kurie turi būti taikomi elektroninei darbo vietai:

1) darbuotojai gali teisėtai tikėtis privatumo darbo vietoje, ir jis

[13] Lietuva Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvenciją ratifikavo 1995 metais, taigi šios konvencijos nuostatos privalomos ir Lietuvoje.

[14] Darbo grupė buvo įsteigta vadovaujantis direktyvos Nr. 95/46/EB 29 straipsniu. Tai – nepriklausomas Europos Sąjungos patariamasis organas duomenų apsaugos ir privatumo klausimais.

neišnyksta dėl to fakto, kad darbuotojai naudoja darbdavio komunikacinę įrangą ar kitas verslo priemones. Darbuotojo teisėti privatumo lūkesčiai gali būti sumažinti, jeigu darbdavys suteikia jam tinkamą informaciją, t. y. privatumas elektroninėje darbo vietoje gali būti ribojamas;

2) bendrasis korespondencijos slaptumo principas apima komunikacijas darbo vietoje: ir elektroninį paštą, ir pridėtus su juo susijusius failus. Todėl darbdavys turi žinoti, kad elektroninis paštas taip pat sudaro darbuotojo privataus gyvenimo sritį;

3) privataus gyvenimo gerbimas apima ir teisę sukurti bei puoselėti santykius su kitais žmonėmis. Faktas, kad tokie santykiai didele dalimi įgyvendinami darbo vietoje (pavyzdžiui, darbuotojas kompiuteriu siunčia elektroninę žinutę auklei klausdamas, kaip sekasi prižiūrėti vaiką), apriboja teisėtą darbdavio poreikį į sekimo priemones.

Šiuo metu pagrindinis Europos Sąjungos teisės aktas, iš dalies reglamentuojantis darbdavio ir darbuotojo santykius kontroliuojant elektroninę darbo vietą, yra Europos Parlamento ir Tarybos direktyva dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo Nr. 95/46/EB. Ši direktyva nustato bendruosius principus, kurių laikydamiesi duomenų valdytojai turi tvarkyti asmens duomenis (tarp jų ir darbdaviai, tvarkydami darbuotojų asmens duomenis), tačiau neskirta specialiai reglamentuoti elektroninės darbo vietos kontrolę.

Kai kuriose Europos Sąjungos valstybėse jau yra priimti teisės aktai, reguliuojantys elektroninės darbo vietos kontrolę. Pirmasis teisės aktas, reglamentuojantis privatumą atskiros valstybės darbo vietoje, – 2001 m. Suomijos privatumo apsaugos darbo veikloje įstatymas (nauja redakcija įsigaliojo 2004 m.). Pavyzdžiui, 6-ame šio įstatymo skyriuje reglamentuojamas darbdaviui priklausančių elektroninių pašto žinučių perėmimas. Pagrindinė nustatyta taisyklė – darbdavys tam tikrais atvejais gali kontroliuoti jam priklausantį elektroninį paštą, jeigu laikosi tam tikrų sąlygų (pvz., elektroninio pašto žinutė turi būti susijusi su darbo santykiais; elektroninio pašto žinutės gali būti skaitomos tik dalyvaujant serverio administratoriui ir kitiems asmenims).

Belgijoje pasirašyta darbuotojų privatumą ir darbdavių interesus reglamentuojanti 2002 m. Nacionalinė kolektyvinė sutartis Nr. 81, skirta apsaugoti privataus sektoriaus darbuotojų teisę į privatumą, kai renkami elektroninės komunikacijos duomenys darbuotojų kontrolės tikslais; sutartį pasirašė Belgijos darbuotojų ir darbdavių atstovai. Šioje

kolektyvinėje sutartyje apibrėžtos priežastys, pateisinančios darbuotojų kontrolę, kontrolės būdai, kuriuos gali naudoti darbdaviai, bei reikalavimai teisėtam surinktų duomenų tvarkymui. Kontrolę pateisinančiomis priežastimis laikoma: neteisėtų šmeižikiškų veiksmų, kuriais siekiama pažeminti kito asmens orumą, prevencija; darbdavio materialinių ar verslo interesų apsauga; įmonės kompiuterių sistemos efektyvaus veikimo apsauga; vidaus darbo taisyklių laikymasis. Duomenų, susijusių su darbuotojo aplankytais interneto tinklapiais ar išsiųstų elektroninių laiškų apimtimi ir kiekiu, tvarkymas bus laikomas teisėtu, kol iš tų duomenų nebus įmanoma nustatyti konkretaus darbuotojo. Tačiau Belgijoje daugeliu atvejų turi būti gautas darbuotojo sutikimas jį kontroliuoti. Gali būti numatytas reikalavimas prieš pradedant bet kokį elektroninį duomenų tvarkymą iš pradžių gauti profesinės sąjungos ar kitų kolektyvinių darbuotojų atstovų sutikimą.

Didžiojoje Britanijoje elektroninės darbo vietos kontrolės klausimai išsamiai reglamentuoti asmens duomenų apsaugos priežiūros institucijos 2003 m. išleistame Duomenų apsaugos darbo santykiuose praktiniame sąvade (angl. *Employment practices data protection code*), kurio trečioji dalis skirta kontrolei darbo vietoje. Pažymėtina, kad šis sąvadas yra rekomendacinio pobūdžio, tačiau papildo 1998 m. Jungtinės Karalystės duomenų apsaugos įstatymą, interpretuoja jo nuostatų taikymą elektroninei darbo kontrolei. Duomenų apsaugos darbo santykiuose praktinis sąvadas nedraudžia elektroninės kontrolės darbo vietoje ir įvardija ją kaip pagrįstą darbo santykių komponentą. Kol darbdaviai laikysis sąvade įtvirtintų gairių, palaikančių pusiausvyrą tarp darbuotojų privatumo ir darbdavių interesų, elektroninė kontrolė bus teisėta ir pagal Duomenų apsaugos įstatymą. Skaidrumas ir proporcingumas – du pagrindiniai principai, kurių privalo laikytis darbdaviai. Norintys vykdyti elektroninę kontrolę darbdaviai privalo informuoti darbuotojus ir kitus susijusius asmenis apie rengiamą ar vykdomą kontrolę (skaidrumas), taip pat privalo nutraukti darbo santykiams nereikalingą ir neadekvatų asmens duomenų rinkimą (proporcingumas).

Panašių teisės aktų yra ir kitose Europos Sąjungos valstybėse. Specialūs privatumą elektroninėje darbo vietoje reglamentuojantys teisės aktai galioja Portugalijoje, Austrijoje, Prancūzijoje, Italijoje.

Galima paminėti ir vieną iš didžiausią atgarsį visuomenėje sukėlusių bylų – telekomunikacijų paslaugų teikimo įmonės *Soneros* saugos skyriaus darbuotojų privatumo pažeidimo bylą. Penki kaltinamieji

– buvę *Soneros* saugos skyriaus darbuotojai – buvo nuteisti už tai, kad slapta ir neteisėtai kontroliavo *Soneros* darbuotojų pokalbius telefonu. Ši byla tapo pavyzdžiu kitiems darbdaviams, kad slaptas ir neteisėtas darbuotojų pokalbių telefonu pasiklausymas (kontrolė) yra baudžiamas kaip kriminalinis nusikaltimas.

Atskira sritis – darbuotojo pokalbių telefonu ar susirašinėjimo elektroniniu paštu kontrolė. Šios kontrolės metu darbdavys sužino darbuotojo pokalbių ir laiškų turinį.

Padėtis Lietuvoje. Lietuvos Respublikos Konstitucijos 22 straipsnyje teigiama: „Žmogaus privatus gyvenimas neliečiamas. Asmens susirašinėjimas, pokalbiai telefonu, telegrafo pranešimai ir kitoks susižinojimas neliečiami. Informacija apie privatų asmens gyvenimą gali būti renkama tik motyvuotu teismo sprendimu. Įstatymas ir teismas saugo, kad niekas nepatirtų savavališko ir neteisėto kišimosi į jo asmeninį ir šeimyninį gyvenimą, kėsinimosi į jo garbę ir orumą“. Lietuvos Respublikos Konstitucinio Teismo jurisprudencijoje teigiama, kad „privatus žmogaus gyvenimas – tai individo asmeninis gyvenimas: gyvenimo būdas, šeimyninė padėtis, gyvenamoji aplinka, santykiai su kitais asmenimis, individo pažiūros, įsitikinimai, įpročiai, jo fizinė bei psichinė būklė, sveikata, garbė, orumas ir kt.“.

Gali kilti klausimas, ar darbo vietoje darbuotojas turi tam tikrą privatumą. 2000 m. gegužės 8 d. nutarime Konstitucinis Teismas pažymėjo, kad privataus gyvenimo teisinė samprata siejama su asmens būsena, kai asmuo gali tikėtis privatumo, su jo teisėtais privataus gyvenimo lūkesčiais. Jei asmuo atlieka viešo pobūdžio veikas ir tą supranta arba turi ir gali suprasti, nors ir būdamas savo namuose ar kitose privačiose valdose, tai tokios viešo pobūdžio veikos nebus apsaugos objektas pagal Konstitucijos 22 ir Konvencijos 8 straipsnius, ir asmuo negali tikėtis privatumo. Galima pasiremti ir Lietuvos Aukščiausiojo Teismo praktika. Byloje *J. Bartasiūnienė prieš viešąją įstaigą „Humana people to people Baltic“* Lietuvos Aukščiausiasis Teismas konstatavo: „pagal CK 2.23 straipsnyje įtvirtintą teisės į privatų gyvenimą sampratą privatus yra toks žmogaus gyvenimas, kuris vyksta ne viešumoje, vieša darbo vieta nėra privati asmens sfera. Pardavėjas negali reikalauti, kad jam būtų užtikrintas privatumas jo darbo vietoje prekybos salėje, todėl pardavimo salės, kartu ir pardavėjo darbo, stebėjimas nėra slaptas asmens privataus gyvenimo stebėjimas“.

Taigi galima daryti išvadą, kad tokioje darbo vietoje, kuri nėra vieša, darbuotojas gali turėti teisę į privatų gyvenimą, ir ši teisė turi

būti gerbiama. Tačiau vis dėlto lieka neaišku, kokiais atvejais darbuotojas gali tikėtis privatumo darbo vietoje, kokiais negali.

Pagrindinis įstatymas, reglamentuojantis darbdavio ir darbuotojo santykius Lietuvoje, yra Darbo kodeksas. Deja, šis įstatymas nereguliuoja elektroninės darbo vietos apsaugos ir nesuteikia darbdaviui jokių teisių kontroliuoti darbuotojo elektroninę darbo vietą. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatyme yra numatytos sąlygos ir principai, susiję su asmens duomenų apie asmenį rinkimo teisėtumu. Remdamasis šiais principais darbdavys gali rinkti darbuotojo asmens duomenis, tačiau šis asmens duomenų rinkimas yra susijęs su informaciniu privatumu ir neapima darbuotojo komunikacinio privatumo[15].

Galima teigti, kad Lietuvoje reikia bent minimaliai reglamentuoti teisinę darbuotojo ir darbdavio santykių privatumo apsaugą. Pageidautinas reglamentavimas įstatymu, kuris padėtų išvengti dviprasmybių.

Lietuvos Respublikos Konstitucinis Teismas pasisakė, kad „pagal Konstituciją riboti konstitucines žmogaus teises ir laisves galima, jeigu yra laikomasi šių sąlygų: tai daroma įstatymu; ribojimai yra būtini demokratinėje visuomenėje siekiant apsaugoti kitų asmenų teises bei laisves ir Konstitucijoje įtvirtintas vertybes, taip pat konstituciškai svarbius tikslus; ribojimais nėra paneigiama teisių ir laisvių prigimtis bei jų esmė; yra laikomasi konstitucinio proporcingumo principo“. Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos, kuri Lietuvoje ratifikuota, 8 straipsnyje taip pat nustatyta, kad „valstybės institucijos neturi teisės apriboti naudojimosi šiomis teisėmis, išskyrus įstatymų nustatytus atvejus ir kai tai būtina demokratinėje visuomenėje valstybės saugumo, visuomenės apsaugos ar šalies ekonominės gerovės interesams siekiant užkirsti kelią viešosios tvarkos pažeidimams ar nusikaltimams, taip pat būtina žmonių sveikatai ar moralei arba kitų asmenų teisėms ir laisvėms apsaugoti“. Taigi darbdavys, neteisėtai apribojęs darbuotojo teisę į privatumą, pavyzdžiui, neteisėtai kontroliavęs darbuotojo elektroninio pašto žinutes ar pokalbius telefonu, gali būti patrauktas net baudžiamojon atsakomybėn. Todėl labai svarbu, kad šioje srityje būtų kuo daugiau aiškumo, ypač dėl elektroninių komunikacijų, kurios susijusios su komunikaciniu privatumu, kontrolės.

---

[15] Darbuotojo susirašinėjimas elektroniniu paštu priskiriamas prie komunikacinio privatumo.

Manytina, kad privatumo darbo vietoje ribos turėtų baigtis ten, kur kėsinamasi padaryti arba padaromas teisės pažeidimas ar nusikaltimas, nesilaikoma įstatymų ir darbo sutarties, kitų darbdavio ir darbuotojo susitarimų. Darbuotojui privatumas negali būti garantuojamas ir tuo atveju, kai pažeidžiamas ar kėsinamasi pažeisti teisėtą darbdavio verslo interesą. Visa tai turėtų būti įtvirtinta teisės aktuose.

Elektroninės darbo vietos kontrolei turėtų būti taikomi bendrieji asmens duomenų apsaugos principai. Reglamentuojant darbdavio ir darbuotojo santykius, kontroliuojant elektroninę darbo vietą, remiantis bendraisiais teisės principais turėtų būti siekiama darbuotojo ir darbdavio interesų pusiausvyros. Kaip rodo bendrieji teisės principai, negalima teikti pirmenybės darbuotojo asmens privatumui ir visiškai ignoruoti darbdavio interesus ir atvirkščiai, turi būti surasta šių dviejų konfliktuojančių interesų pusiausvyra, todėl negalima teigti, kad darbuotojas turi visišką teisę į privatumą arba kad darbdavys turi besąlygišką teisę tikrinti darbuotojo elektroninę darbo vietą.

Svarbiausia, kad praktikoje nebūtų vadovaujamasi vien sutikimo principu. Pernelyg dažnai gali iškilti abejonių, kad toks „sutikimas“ duotas laisva valia, kadangi darbuotojas pagrįstai bijo, kad gali atsidurti nepalankioje padėtyje, jeigu nesutiks.

Svarbiausias principas, kurio turėtų laikytis darbdaviai, – proporcingumo principas. Elektroninės darbo vietos kontrolė turi būti vykdoma tada, kai tai neišvengiamai reikalinga. Jei nustatytas tikslas gali būti pasiektas mažiau privatumą pažeidžiančiomis priemonėmis, darbdavys turi apsvarstyti šią galimybę. Pavyzdžiui, darbuotojo kompiuterio kietajame diske elektronine forma saugomos informacijos kasdieninė ir įprasta kontrolė neturėtų būti leistina, išskyrus atvejus, kai turima konkrečių įrodymų apie darbuotojo platinamą nelegalią programinę įrangą ar vykdomą kitą neteisėtą veiklą. Darbuotojo susirašinėjimas elektroninio pašto dėžutės, priklausančios darbdaviui, pagalba galėtų būti kontroliuojamas tuomet, jei darbdavys nustatė aiškias taisykles dėl elektroninio pašto naudojimo asmeniniais tikslais būdo ir laiko.

Proporcingos elektroninės darbo vietos kontrolės priemonės taip pat turėtų būti aiškiai ir nedviprasmiškai įvardytos darbo sutartyse arba lydimuosiuose vidaus norminiuose dokumentuose (pavyzdžiui, darbo tvarkos taisyklėse), su kuriais darbuotojas yra supažindinamas.

Kitas svarbus principas – būtinybės principas. Šis principas reiškia, kad darbdavys, prieš imdamasis bet kokios elektroninės darbo vie-

tos kontrolės priemonių, turi įvertinti, ar ši priemonė yra būtina konkrečiam tikslui pasiekti.

Taip pat svarbus ir skaidrumo principas. Šis principas skelbia, kad darbdavys turi aiškiai ir skaidriai pateikti informaciją apie savo veiksmus, susijusius su elektroninės darbo vietos kontrole.

Be to, darbuotojai ir patys turėtų būti aktyvesni bei ginti savo teises į privatų gyvenimą, reikalaudami iš darbdavių paaiškinimų dėl elektroninės darbo vietos kontrolės priemonių. Bet kuriuo atveju slaptas darbuotojo elektroninės darbo vietos stebėjimas laikytinas asmens teisės į privatumą ribojimu ir todėl gali būti leistinas tik konkrečiais atvejais, trumpą laiko tarpą ir turi būti vykdomas laikantis griežtų taisyklių.

Pagal aukščiau išvardintus principus darbdavys, norėdamas kontroliuoti darbuotojo elektroninį paštą, turėtų nustatyti šiuos pagrindinius dalykus:

– ar darbuotojui leidžiama asmeniniais tikslais naudoti elektroninį paštą;
– kada ir kokiais atvejais darbuotojui leidžiama naudotis asmenine elektroninio pašto dėžute;
– kokiais atvejais yra daromos elektroninio pašto žinučių atsarginės kopijos;
– informuoti, kada elektroninio pašto žinutės ištrinamos iš serverio.

Stebint interneto prieigą kiek įmanoma dažniau turi būti taikomos techninės prieigos kontrolės priemonės, pavyzdžiui, darbdaviui nepriimtinų interneto tinklapių lankymo uždraudimas. Darbdavys taip pat turi nustatyti aiškias taisykles, kada darbuotojui leidžiama asmeniniais tikslais naršyti internete. Darbuotojai taip pat turi būti informuojami apie nustatytas technines prieigos kontrolės (apribojimo) priemones.

KONTROLINĖS UŽDUOTYS

1. Nurodykite teisės į privatų gyvenimą ir asmens duomenų apsaugos santykį.
2. Įvardinkite, kuo skiriasi duomenų valdytojas nuo duomenų tvarkytojo.

3. Apibūdinkite Lietuvoje taikomą asmens duomenų apsaugos elektroninėje erdvėje modelį.
4. Įvardinkite pagrindinius asmens duomenų apsaugos elektroninėje erdvėje principus.
5. Įvardinkite ir apibūdinkite Lietuvoje nustatytą principą tiesioginės rinkodaros atveju (OPT-IN ar OPT-OUT).
6. Nurodykite pagrindines direktyvos Nr. 2002/58/EB dėl privatumo ir asmens duomenų apsaugos elektroniniuose ryšiuose reglamentuojamas sritis.
7. Nurodykite, kiek laiko elektroninių ryšių paslaugų teikėjai gali saugoti elektroninių ryšių srauto duomenis.
8. Atskleiskite teisėsaugos institucijų vykdomai elektroninių ryšių turinio kontrolei taikomus reikalavimus.
9. Nurodykite pagrindinėes darbdavio vykdomos elektroninės darbo vietos kontrolės koncepcijas.
10. Apibūdinkite principus, kuriais turėtų vadovautis Lietuvos darbdavys, siekdamas kontroliuoti elektroninę darbo vietą.

Literatūra

1. PHARE projekto LT02/IB-JH-02/03 „Asmens duomenų apsaugos administracinių ir techninių gebėjimų stiprinimas“ medžiaga // http://www.ada.lt.
2. Carey P. Data protection: a practical guide to UK and EU law. – Oxford University press, 2004.
3. Civilka M., Lamanauskas T., Nosinaitė G., Sauliūnas D., Štitilis D., Toliušis S., Ulevičius L. Informacinių technologijų teisė. – Vilnius: Teisės Institutas, 2004.
4. Data protection – European Commission // http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm.
5. Baibridge D. Data protection. – Emis Professional pub., 2005.
6. Lasprogata G., King N. J., Pillay S. Regulation of Electronic Employee Monitoring: Identyfying Fundamental Principles of Employee Privacy through Comparative Study of Data Privacy legislation in the European Unijon. United States and Canada. – 2004 Stan. Tech. L. Rev. 4 // http://stlr.stanford/STLR/Articles/04_STRL_4.
7. Jarukaitis I., Lamanauskas T., Civilka M., Rakauskaitė A. Elektroninių ryšių teisė. – Vilnius: Eugrimas, 2005.

8. Pivec E. M., Brinkerhoff S. E-mail in the workplace: limitation on privacy // Human Rights Magazine. 1999. Vol. 26. No. 1.
9. Maxwell W. Electronic Communications: the New EU Framework. Part I. Booklet 1.5. – New York: Oceana Publications, Inc., 2002.
10. Saarenpaa A. Data Protection – some comments from the Finnish point of view // Judicial Academy of Northern Finland. Publications 3/2001. – Rovaniemi, 2001.
11. The New Data Retention Directive // European Media, IP & IT Law Review. 2006. No. 1.
12. Valstybinės duomenų apsaugos inspekcijos 2005 metų veiklos ataskaita // http://www.ada.lt.
13. Žmogaus teisių įgyvendinimas Lietuvoje: 2005 m. apžvalga. Žmogaus teisių stebėjimo institutas. 2005 // http://www.hrmi.lt;
14. Štitilis. D. Privataus gyvenimo elektroniniuose ryšiuose ribojimas nusikaltimų tyrimo tikslais // Jurisprudencija. 2006. Nr. 9(87).

5. TEISINIAI ELEKTRONINĖS KOMERCIJOS ASPEKTAI

5.1. Įvadinė medžiaga. Elektroninės komercijos samprata ir ypatumai

Pasaulyje nėra nusistovėjusio visuotinai priimtino elektroninės komercijos apibrėžimo. Jo nepateikia netgi Europos Sąjungoje 2000 m. birželio 8 d. priimta Elektroninės komercijos direktyva.

Elektroninę komerciją būtų galima apibrėžti kaip prekybą prekėmis arba paslaugomis, kai sandoriai sudaromi arba vykdomi elektroninėmis priemonėmis.

Elektroninėje prekyboje gali būti teikiamos paslaugos bei prekiaujama dviejų rūšių produktais:

1. materialiais produktais (šių produktų neįmanoma persiųsti elektronine erdve. Tai tradicinės prekės, kuriomis buvo prekiaujama iki atsirandant informacinėms technologijoms ir kurios negali būti arba nėra išreikštos skaitmenine forma);

2. skaitmeniniais produktais (tai produktai, kurie informacinėmis technologijomis išreiškiami skaitmenine forma ir gali būti siunčiami elektronine erdve).

Remiantis tokia pat objekto klasifikacija, 1997 m. ES Komisijos pranešime „Europos elektroninės komercijos iniciatyva“ buvo išskirti du elektroninės komercijos tipai:

1. tiesioginis (persiuntimas skaitmeninių produktų tiesioginiu darbo režimu arba naudojant kitas elektronines priemones);
2. netiesioginis (materialūs produktai užsakomi elektroninėmis priemonėmis, tačiau pristatomi tradiciniu būdu).

Pagrindiniai elektroninės komercijos modeliai pagal subjektus, kurie dalyvauja komerciniuose sandoriuose, vykdomuose elektroninėje erdvėje, yra tarp verslo atstovų (B2B – didmeninė prekyba) ir tarp verslo atstovų bei pirkėjų (B2C – mažmeninė prekyba). Literatūroje išskiriami ir kiti elektroninės komercijos modeliai: tarp fizinių subjektų (C2C), tarp verslo subjektų ir valstybinių institucijų (B2G), tarp fizinių subjektų ir valstybinių institucijų (C2G).

Elektroninė komercija, pasitelkus pažangias informacines technologijas, suteikia naujų galimybių reklamuojant prekes, jas pristatant į kitas valstybes arba teikiant paslaugas tų valstybių piliečiams, sandorio šalims atliekant atsiskaitymus arba įgyvendinant kitas verslo stadijas. Šios technologijos taip pat turi didelę įtaką įmonių valdymui bei prekinių ir finansinių srautų kontrolei. Norint suprasti, kokios naujovės veikia tradicinę tarptautinę komerciją, reikia apibrėžti, kuo pasižymi elektroninė komercija ir kuo ji skiriasi nuo tradicinės. Ne visi elektroninės komercijos bruožai turi išskirtinę įtaką, palyginti su gerai žinomais tradiciniais tarptautinio verslo modeliais. Remiantis D. A. Hardesty, būtų galima išskirti šias pagrindines savybes, būdingas tik elektroninei komercijai:

Pasauliniu mastu vykdoma prekyba. Istoriškai geografinės valstybių sienos buvo kliūtis norint prekes parduoti kitos valstybės teritorijoje. Naujos elektroninės komercijos galimybės leidžia bendrovėms lanksčiau pradėti savo verslą ne tik nacionalinės valstybės teritorijoje, bet ir visame pasaulyje. Labiausiai tai veikia smulkų ir vidutinį verslą, kurie be didesnių lėšų gali pradėti tarptautinę prekybą. Tokia galimybė pirmiausia priklauso nuo visą pasaulį apimančio internetinio tinklo.

Informacinių technologijų požiūriu naudoti vietinius tinklus komerciniuose sandoriuose taip pat įmanoma, nors jie naudojami daug rečiau. Kuriami ir tarptautiniu mastu veikiantys uždari tinklai, tačiau jie dažniausiai naudojami konkretiems iš anksto numatytiems tikslams, neįtraukiant galimybės vykdyti komercinius sandorius.

Technologiniai pokyčiai ir lėmė pasauliniu mastu vykdomos prekybos prieinamumą smulkioms bei vidutinio dydžio bendrovėms. Naujumas pasireiškia tuo, kad elektroninėje komercijoje pardavėjai gali ne tik prekiauti visame pasaulyje, bet ir patys tuo momentu būti savo valstybėje. Elektroninė komercija suteikė galimybę pardavėjui ir pirkėjui išvengti tiesioginio susitikimo bet kurioje sandorio stadijoje.

Anonimiškumas. Daugelis pirkėjų ir pardavėjų, dalyvaujančių internetu sudarytuose sandoriuose, niekada vienas kito nemato. Ateityje vis platesnis elektroninių pinigų naudojimas dar labiau sumažins galimybę atsekti pirkėją. Naudojami informacijos persiuntimo protokolai leidžia lengvai nustatyti kompiuterių sistemos IP adresą, tačiau tai nesuteikia informacijos apie vartotoją, besinaudojantį ta kompiuterių sistema. Daugelis finansinių operacijų, atliekamų naudojantis elektroniniais pinigais, valstybinėms institucijoms gali likti nežinomos.

Skaitmeniniai produktai. Ne visi produktai gali būti išreikšti skaitmenine forma. Dažniausiai skaitmenine forma parduodama programinė įranga, muzikos įrašai, knygos, videokūriniai. Bendrovėms, pardavinėjančioms tokias prekes, visiškai nereikalingi kai kurie komercinės veiklos etapai. Pardavėjams nebereikia pirkti žaliavų, gaminti prekių. Daugelis pirkėjų gali atsisiųsti tą pačią prekę, o bendrovei nereikia rūpintis tokios prekės skaičiaus padauginimu. Programinė įranga suteikia galimybę pirkėjams parsisiųsti vienintelio pardavėjo duomenų bazėje esančio produkto kopijas negaištant tam laiko ir neatliekant papildomų komandų. Tokie informacinių technologijų pranašumai, be abejo, palengvina prekiautojų darbą, tačiau valstybinėms institucijoms darosi vis sunkiau sukontroliuoti prekių srautus. Padidėja galimybės nuslėpti parduotų prekių kiekį.

Nuotoliniu būdu valdoma bendrovė. Elektroninę komerciją vykdančios bendrovės daugelį operacijų, turinčių įtakos komercinei veiklai, gali atlikti nuotoliniu būdu. Labiausiai tai lemia programinės įrangos teikiamos galimybės. Naudodamasis programine įranga pardavėjas gali nustatyti, kokias prekes parduoti, kokias išimti iš apyvartos, nustatyti norimą kainą, pateikti reklamą, atsiskaityti su pirkėju už įsigytas prekes arba suteiktas paslaugas, taip pat persiųsti prekes į kompiuterinę pirkėjo sistemą. Tokiu atveju nuotoliniu būdu valdoma visa įmonė.

Nematerialumas. Parduodamos skaitmeninės prekės, internetinė svetainė, kurioje bendraujama su pirkėju, arba programinė įranga, naudojama komercinėms operacijoms atlikti, neturi jokios materialios išraiškos. Todėl kartais būna sunku apibrėžti, kokios valstybės jurisdikcijai priklauso vienas arba kitas objektas. Jų neapčiuopiamumas apsunkina, o kartais neleidžia nustatyti geografinės jų buvimo vietos. Net ir teismo priimti sprendimai gali nesusilaukti tinkamo įgyvendinimo be kitos valstybės pagalbos, jei nebus materialaus turto, į kurį būtų galima nukreipti sprendimo vykdymą.

Be abejo, šios penkios D. A. Hardesty išskirtos elektroninės komercijos savybės, palyginti su tradicine komercija, yra unikalios ir būdingos tik jai vienai.

5.2. Pagrindinė medžiaga. Elektroninės sutartys ir elektroninės komercijos teisinio reguliavimo modelis

5.2.1. Elektroninės komercijos teisinio reglamentavimo iniciatyvos

Europos Sąjungos elektroninės komercijos teisė sparčiai vystosi. Nors įstatymų leidybos mašina įprastai yra gana lėta, tačiau informacinių technologijų raidos tempai reikalauja ir atitinkamos teisinės bazės. Pastarajame dešimtmetyje pasirodė su elektronine komercija susijusius santykius reglamentuojančių direktyvų. Direktyvos orientuojamos dviem kryptimis: rinkos ir individo. Orientacija į individą yra labai stipri vartotojo apsaugos srityje. Šias vartotojo apsaugos nuostatas galima aptikti Vartotojų apsaugos, susijusios su nuotolinės prekybos sutartimis (toliau Nuotolinės prekybos direktyva), Elektroninės komercijos, Asmens duomenų apsaugos ir kitose direktyvose.

Interneto kompiuterių tinklui tapusį globalia komunikacine aplinka, verslo kompanijos, norėdamos išnaudoti interneto galimybes, pradėjo ieškoti naujų, šiai aplinkai tinkančių verslo formų.

Viena iš tokių verslo formų yra sutarčių sudarymas naudojant kompiuterines priemones, kompiuterių tinklą. Ši verslo kryptis turi keletą pranašumų:

1. sumažina išlaidas;
2. taupo sutarčiai sudaryti skirtą laiką;
3. pateikia produkciją naujoms rinkoms;
4. suteikia galimybę sudaryti tarptautines sutartis;
5. suteikia galimybę teikti paslaugas (sudaryti sutartis) 365 dienas per metus ir 24 valandas per parą.

Tobulėjant naujam sutarčių sudarymo būdui atsiranda poreikis jas reglamentuoti teisiškai. Įstatymo normų, reguliuojančių įprastai sudarytas sutartis, dažnai neužtenka, jos neretai trukdo verslo santykiams, plėtojamiems internetu.

Su šiomis elektroninio dokumento reglamentavimo bei elektroninės informacijos įrodomosios vertės problemomis susidūrė visos technologiškai išsivysčiusios valstybės. Elektroninės informacijos reglamentavimo klausimus pradėjo spręsti keletas tarptautinių organizacijų. Ypatingą dėmesį Europoje elektroninei informacijai skyrė Europos

Komisija, o pasaulio mastu reguliuoti šiuos procesus bando Jungtinių Tautų tarptautinės prekybos teisės komisija (UNCITRAL). Šios dvi organizacijos reglamentavimo darbą atliko tuo pat metu, daugiausia dėmesio skirdamos elektroninės informacijos naudojimui įteisinti, įrodomojo statuso elektroninei informacijai suteikti bei teisiniam reglamentavimui suvienodinti atskirose valstybėse – tai leistų sėkmingai plėstis elektroninei komercijai.

5.2.2. Elektroninės komercijos įstatymo UNCITRAL modelis

Jungtinių Tautų tarptautinės prekybos teisės komisija 1998 m. spalį patvirtino Elektroninės komercijos įstatymo modelį (toliau Modelis). Modelio tikslas – suvienodinti šalių narių įstatymus formuojant vienodą požiūrį į elektroninę komerciją, įteisinti elektroninę sutarties sudarymo formą ir prilyginti ją rašytinei.

Rengdama Elektroninės komercijos įstatymo modelį Komisija siekė, jog jis taptų efektyviu įrankiu valstybėms modernizuojant teisės aktus, pateikdamas svarbiausią informaciją bei nustatydamas orientyrus, į kuriuos turėtų atsižvelgti įstatymų, susijusių su elektroninės informacijos panaudojimu versle, kūrėjai. Todėl rengiant šį Modelį buvo keliamas tikslas ne reglamentuoti elektroninę komerciją, o pateikti reikalingas gaires valstybėms, kuriančioms savo įstatymus. Dėl šios priežasties keletas nuostatų nebuvo apibrėžtos Modelio tekste, o tik pateiktos kaip paaiškinimai aiškinamajame rašte. Jame pateikiami ne tik Modelio teisinių normų paaiškinimai, bet ir informuojama, dėl kokių priežasčių viena ar kita nuostata yra įtraukta į šį dokumentą.

Modernių komunikacijų, tokių kaip EDI, elektroninis paštas ir pan., naudojimas prekybiniuose santykiuose plečiasi. Tai lemia greitas viešų tarptautinių informacinių tinklų plitimas, leidžiantis naudotis informacija vis didesniam vartotojų skaičiui. Tuo pačiu metu, pasitelkus modernias technologijas, kuriama, siunčiama ir saugoma informacija susiduria su teisinės vertės kliūtimi, kurią sukuria teisės normos, priimtos gerokai prieš tokių technologijų atsiradimą. Modelis pateikia būdą, kaip tokias teisines kliūtis panaikinti bei įteisinti elektroniniu būdu apdorojamą informaciją. Pagrindinės tokios teisinės kliūtys nacionalinėse valstybių teisės sistemose yra **rašytinė forma**, **dokumento parašas**, **dokumento originalas** ir pan.

Rašytinė forma. Modelyje elektroninis pranešimas apibrėžiamas

kaip informacijos vienetas, sukurtas, atsiųstas, atsakytas arba saugomas elektroniniu, optiniu ar panašiu būdu, įskaitant EDI, elektroninį paštą, telegrafą, teleksą arba telekopijavimą. Taip pat numatyta, kad valstybėje, kurioje teisinė sistema reikalauja pateikti informaciją raštiškai, šią formą atitinka elektroninis pranešimas. Pradėdama vartoti elektroninio pranešimo sąvoką, Jungtinių Tautų tarptautinės prekybos teisės komisija remiasi funkcinio ekvivalento požiūriu. Remiantis šiuo požiūriu, elektroninis pranešimas neturi idealiai kartoti rašytinio dokumento rekvizitų bei atitikti rašytiniam dokumentui keliamų formalių reikalavimų. Elektroninis pranešimas turi tiesiog atlikti rašytinio dokumento funkcijas. Pavyzdžiui, rašytinis dokumentas turi atlikti šias funkcijas: dokumentas turi patikimai pateikti jame užfiksuotą informaciją, dokumentas turi nesikeisti gana ilgą laiko tarpą, dokumentas gali būti kopijuojamas, kad kiekviena sutarties šalis galėtų turėti kopiją, dokumentas privalo turėti parašą, leidžiantį patikimai nustatyti jį sukūrusį bei informaciją jame patvirtinusį asmenį, ir pan. Tokie funkciniai reikalavimai keltini ir elektroniniam pranešimui, tačiau šiuos reikalavimus galima įgyvendinti visiškai kitais naujomis technologijomis grindžiamais metodais.

Modelyje susitelkiama ne į visas įmanomas rašytinės formos funkcijas, o į tas, kurios yra susijusios su įrodomąja galia. Teigiama, jog elektroninis pranešimas atitinka rašytinei formai keliamus reikalavimus, jei informacija jame yra prieinama ir išlieka nepakitusi gana ilgą laiko tarpą. Čia žodį „pasiekiamą“ reikėtų suprasti kaip galimybę informaciją perskaityti ir interpretuoti, be to, programinė įranga, skirta informacijai perskaityti, turi būti įprasta ir lengvai įsigyjama.

Dokumento parašas. Modelis išskiria šias popierinio dokumento parašo funkcijas:

1. nustato pasirašiusį asmenį;
2. užtikrina, kad šis asmuo buvo įtrauktas į pasirašymo procesą;
3. susieja asmenį su pasirašyto dokumento tekstu.

Reikėtų pažymėti, kad šalyse tradiciškai egzistuoja ir papildomos procedūros, kartu arba atskirai nuo dokumento parašo atliekančios išvardytas funkcijas. Tai galėtų būti antspaudavimo ir perforavimo (perdūrimo) ar kitokios procedūros. Modelio kūrėjai supranta šias visas procedūras kaip pasirašymą ir įvardija jas vienu pavadinimu. Elektroninio pranešimo parašo atliekamos funkcijos turi būti tokios pačios, todėl Modelio 7 straipsnis ir formuluoja du kriterijus, kuriuos turi atitikti parašas:

1. pasirašymo metodas turi nustatyti pasirašiusį asmenį; ir
2. garantuoja asmens pasirašytos informacijos patvirtinimą.

Dokumento originalas. Tačiau teisinė sistema, kalbėdama apie įrodomąją vertę, atskirais atvejais nurodo „originalo“ buvimo būtinumą: įvairūs sertifikatai, ataskaitos ir pan. gali būti pristatomi tik originalia forma. Šiais atvejais dokumento originalas atlieka apsaugos nuo pakeitimų darant kopijas funkciją. Tačiau aiškinant dokumento originalą kaip priemonę, kurioje informacija buvo fiksuota pirmą kartą, neįmanoma būtų pateikti elektroninio pranešimo kaip originalo, nes pranešimo adresatas visuomet gauna pranešimo kopiją, pirminis variantas lieka sudarytojui. Modelis šiuo atveju teigia, jog visi elektroniniai pranešimai yra originalūs, jeigu kopijavimo metodas garantuoja informacijos vientisumą (integruotumą), palyginti su informacija, pateikta pirmine forma.

Modelyje siūloma valstybėms įteisinti elektroninį pranešimą kaip įrodymą ir nustatyti jo įrodomosios vertės kriterijus. Įtvirtinama svarbi nuostata, jog elektroninis pranešimas negali būti pripažįstamas netinkamu vien dėl jo sudarymo būdo specifikos.

Reglamentuojant elektroninės sutarties sudarymą pažymima, kad modelis įteisina ofertos ir akcepto elektroninę formą. Tai reiškia, kad sudarius elektroninę sutartį elektroniniai pranešimai negali būti pripažįstami negaliojančiais vien dėl šios priežasties, tačiau gali būti pripažinti negaliojančiais dėl kitų teisės aktuose numatytų priežasčių (pvz., Lietuvoje negalioja sandoris, sudarytas tik dėl akių, neketinant sukurti teisinių pasekmių).

Nustatomi apsaugos mechanizmai, draudžiantys sudaryti sutartį, jei tarpusavyje komunikuoja tik informacinės sistemos ir nereikalaujama įsikišti žmogui. Taip įtvirtinama laisva šalių valia, galimybė asmeniui apsispręsti sudaryti sutartį, prisiimti atsakomybę ar ne.

5.2.3. Nuotolinės prekybos sutartis

Nuotolinės prekybos direktyva buvo priimta 1997 m. ir buvo pirmoji iš direktyvų, įteisinančių elektronines sutartis. Tiesa, Europos Komisija nenustatė konkrečių sutarties reikalavimų, kaip tai buvo padaryta elektroninės komercijos įstatymo UNCITRAL modelyje. Šia Direktyva buvo siekiama apsaugoti vartotojo interesus sudarant sutartis tokiais būdais, kai sutarties šalys viena kitos nemato ir nebendrauja tiesiogiai vienoje vietoje. Tokios apsaugos tikslas pagrįstas fak-

tu, jog vartotojas nuotolinės prekybos sutartyje „yra nežinioje“, nes negali apžiūrėti ir įvertinti prekės kokybės prieš sudarydamas sutartį. Ir prekės, ir paslaugos gali būti prastesnės kokybės nei vartotojas tikėjosi, pardavėjas gali turėti prastą reputaciją arba sukčiauti. Vartotojas, įsigijęs prastos kokybės prekę, paprastai patenka į nepalankią padėtį pardavėjo atžvilgiu, todėl jo apsaugai skirtina daugiau dėmesio. Direktyva nustato, jog, be nustatytų joje garantijų vartotojui, valstybės gali savarankiškai nustatyti papildomas garantijas.

Kaip nuotolinės prekybos sutartį Direktyva apibrėžia ne tik elektroninę sutartį. **Nuotolinės prekybos sutartis** apima bet kokią prekių arba paslaugų teikimo sutartį, sudarytą pagal paslaugos teikėjo pasiūlytą mechanizmą, naudojant sutarčiai sudaryti išimtinai tik nuotolinį bendravimo būdą. Nuotolinės prekybos sutartimi ji pripažįstama būtent dėl sudarymo būdo, tai gali būti ne tik elektroninis bendravimas kompiuterių tinklu, bet ir bendravimas paštu, telefonu ir pan. Ar galima pripažinti pagal šią Direktyvą nuotolinės prekybos sutartimi sutartį, sudarytą nuotoliniu būdu, tačiau tik po to, kai buvo pristatytos prekės ir klientas galėjo jas apžiūrėti ir įvertinti? Vertinant šią padėtį reiktų atkreipti dėmesį į nuostatą „naudojant sutarties sudarymui išimtinai tik nuotolinį komunikavimo būdą“, jei sutartis buvo sudaryta nuotoliniu būdu, išankstinis tiesioginis prekės apžiūrėjimas laikytinas sutarties sudarymo formai įtakos neturinčia aplinkybe. Nuotolinės prekybos sutarties sudarymo būdas Direktyvoje suprantamas kaip nereikalaujantis vienalaikio fizinio abiejų sutarties šalių dalyvavimo sudarant sutartį.

Direktyva reikalauja, kad iki nuotolinės prekybos sutarties sudarymo pardavėjas vartotojui pateiktų savo duomenis, taip pat informaciją apie prekės savybes, prekių bei paslaugų kainas, teisę atšaukti sutartį. Pateikimą čia reikėtų suprasti kaip suteikimą galimybės vartotojui perskaityti ir įvertinti pateiktą informaciją prieš sudarant sutartį. Pateikimą galima vertinti kaip netinkamą, jei reikalingi duomenys išsiunčiami paštu ir pasiekia vartotoją tik po to, kai jis jau būna sudaręs sutartį elektroniniu paštu.

Informacija sudarant nuotolinės prekybos sutartį telefonu arba internetu yra neilgalaikė, neužtikrinanti jos patikimo saugojimo. Direktyva reikalauja, kad sudarius nuotolinės prekybos sutartį vartotojas turi gauti patvirtinimą, kad sudaryta ilgalaikė, vartotojui prieinamos formos sutartis ne vėliau kaip prekių pristatymo metu. Nėra priežasties manyti, kad patvirtinimo elektroniniu paštu forma nėra ilga-

laikė, nes žinutę galima išspausdinti ir saugoti.

Direktyva kaip vieną iš vartotojo teisių gynimo garantijų įdiegia naujovę civiliniuose teisiniuose santykiuose – sutarties atšaukimo teisę, leidžiančią vartotojui per 7 dienas atšaukti sudarytą sutartį ir nevykdyti prisiimtų įsipareigojimų, nemokant netesybų bei baudų ir sumokant tik prekės grąžinimo mokesčius, jei prekė buvo atsiųsta.

Lietuvos Respublikos civilinio kodekso 6.367 straipsnis nustato, kad vartotojas turi teisę atsisakyti pirkimo–pardavimo sutarties, sudarytos naudojant ryšio priemones, pranešdamas apie tai raštu pardavėjui per septynias darbo dienas nuo:

- daikto pristatymo dienos, kai parduodamas daiktas;
- sutarties sudarymo dienos, kai teikiamos paslaugos.

Direktyvoje numatomi atvejai, kai sutarties atšaukti negalima:

1. paslaugos vartotojo sutikimu pradėtos teikti dar nesibaigus septynių darbo dienų terminui;
2. prekių kainos yra greitai kintančios, priklauso nuo rinkos, kurios pardavėjas nekontroliuoja, pokyčių;
3. prekės buvo pagamintos pagal specialiai pirkėjo pateiktą specifikaciją arba pagal prigimtį yra skirtos konkrečiam asmeniui;
4. prekių neįmanoma grąžinti dėl jų savybių (greitai genda arba yra trumpas jų galiojimo terminas);
5. atplėšta garso arba vaizdo įrašų bei kompiuterinių programų pakuotė;
6. parduodami laikraščiai, žurnalai arba kita periodika;
7. parduodami loterijos bilietai.

Pagrindinis klausimas čia galėtų kilti dėl „prekių, kurių kainos yra greitai kintančios priklausomai nuo rinkos“. Ši išimtis yra taikoma rinkai, kuri yra labai nepastovi ir kurioje vartotojas gali gauti pelną protingai naudodamasis sutarties atšaukimo teise (pvz., užsienio valiutos rinka). Nors iš pirmo žvilgsnio šią išimtį galima būtų pritaikyti daugeliui prekių bei paslaugų, minima frazė Direktyvoje turi būti aiškinama siaurinamai. Sutarties atšaukimo teisė prarandama tik tuo atveju, kai vartotojas realiai galėjo atsisakyti sutarties dėl vėliau sumažėjusios prekės kainos.

Nors Direktyva nustato sutarties atšaukimo teisę, bet išankstinio prekės kainos apmokėjimo klausimo nereguliuoja. Vartotojas atsiduria sudėtingoje padėtyje norėdamas atšaukti sutartį, pagal kurią už prekę sumokėjo iš anksto. Vartotojui kartais lieka tik pasikliauti gera pardavėjo valia. Valstybės narės šią problemą sprendžia skirtingai. Por-

tugalijoje vartotojai neprivalo mokėti už prekes iš anksto, Olandijoje pardavėjas neturi teisės reikalauti didesnio kaip 50 proc. išankstinio mokėjimo. Kitas metodas išvengti išankstinio mokėjimo problemos – įšaldyti atitinkamą sumą vartotojo sąskaitoje, kol pasibaigs sutarties atšaukimo terminas.

Direktyva draudžia tam tikrus bendravimo būdus sudarant nuotolinės prekybos sutartį. Draudžiama sudaryti sutartis tarp automatinių fakso arba skambinimo mašinų, iš anksto neinicijuotų abiejų sutarties šalių.

5.2.4. Elektroninės komercijos direktyva

Iki Elektroninės komercijos direktyvos priėmimo daugelyje ES šalių elektroninė sutartis buvo nereglamentuota, kitur buvo įteisinta ir galiojanti. Tačiau net ir tose šalyse, kur elektroninė sutartis buvo pripažįstama, skirdavosi sutarties teksto, technologijų, įrodomosios vertės ir pan. reikalavimai.

Elektroninė komercija apima skirtingus visuomeninius santykius. Tai visuomeniniai santykiai, susiję su komerciniais pranešimais, sutartimis, skolomis, licencijavimu bei tam tikrų reikalavimų įgyvendinimu. Atsižvelgiant į visa tai Europos Komisija ėmėsi pastangų sujungti šių visuomeninių santykių reglamentavimą į vieną norminį aktą, priimdama Elektroninės komercijos direktyvą. Direktyvą pradėta rengti 1997 m. nuo Europos Komisijos elektroninės komercijos komunikato. Šią iniciatyvą labai palaikė Europos Parlamentas. Direktyva siekiama palengvinti informacinių paslaugų laisvą judėjimą tarp valstybių narių pagal kilmės šalies įstatymus.

Siekis suvienodinti valstybių narių teisės aktus elektroninių sutarčių klausimais matyti Direktyvos 9 straipsnyje, kuris teigia, jog ES valstybės narės privalo sukurti teisės aktus, kurie leistų sudaryti elektronines sutartis bei užtikrintų, kad įstatymų, reguliuojančių sutartinius teisinius santykius, reikalavimai nestabdytų elektroninių sutarčių naudojimo, o teisiniai santykiai, sukurti vykdant elektroninę sutartį, neprarastų savo galios vien dėl to, jog jie buvo sukurti sudarant elektroninę sutartį. Iš šio straipsnio bei pačios Direktyvos esmės matome, kad Europos Komisija laikosi UNCITRAL Elektroninės komercijos įstatymo modelio idėjos prilyginti elektroninę sutartį rašytinei sutarčiai.

Nuo 2006 m. liepos 1 d. įsigaliojo Lietuvos Respublikos informacinės visuomenės paslaugų įstatymas, kuris pakeitė 2002 m. balandžio

10 d. ūkio ministro įsakymą Nr. 119 „Dėl kai kurių informacinės visuomenės paslaugų, ypač elektroninės komercijos, teikimo vidaus rinkoje reglamento patvirtinimo“. Šis įstatymas visiškai įgyvendino Elektroninės komercijos direktyvos nuostatas.

Informacinės visuomenės paslaugų įstatymas reguliuoja tris pagrindinius informacinės visuomenės paslaugų ir e. komercijos aspektus:

1. informacijos apie paslaugos teikėją ir paslaugą atskleidimo reikalavimus;
2. kai kuriuos elektroninių sutarčių aspektus;
3. informacinės visuomenės paslaugų teikėjų (tarpininkų) atsakomybės klausimus.

5.2.5. Informacinės visuomenės paslauga

Šiame įstatyme, kaip ir Direktyvoje, tačiau kitaip nei Elektroninės komercijos įstatymo UNCITRAL modelyje, įvedama nauja sąvoka „informacinės visuomenės paslaugos“. **Informacinės visuomenės paslaugomis** laikomos elektroninėmis priemonėmis ir per atstumą individualiu prašymu teikiamos paslaugos. Taigi ši sąvoka apima ne tik elektroninę komerciją (prekių pardavimą tiesioginiu darbo režimu, informacijos siuntimą telekomunikacijų tinklais, kliento informacijos saugojimą tiek, kiek tai susiję su ekonomine veikla), bet ir kai kurias susijusias paslaugas, tarp jų prieigos prie elektroninio turinio (tarpininkavimo) paslaugas. Komerciniai pranešimai elektroniniu paštu taip pat pripažįstami informacinės visuomenės paslauga, išskyrus tuos atvejus, kai asmenys naudoja šį telekomunikacijos būdą verslo ar profesiniams tikslams. Sutarčių elektroniniu paštu sudarymas tarp individualių asmenų taip pat nelaikomas informacinės visuomenės paslauga. Nustatomas papildomas informacinės visuomenės paslaugos kaip paslaugos, turinčios konkretų adresatą, kriterijus. Paslaugos, teikiamos tiesioginiu darbo režimu, bet ne konkrečiam vartotojui (televizijos, radijo transliacijos), nėra informacinės visuomenės paslaugos. Nepripažįstama informacinės visuomenės paslaugomis darbdavio ir darbuotojo darbo santykiai, taip pat paslaugos, kurios negali būti kokybiškai teikiamos per atstumą dėl savo esmės, pavyzdžiui: auditas, medicinos pagalba, reikalaujanti tiesioginės kliento apžiūros ir pan.

Įstatymas netaikomas mokesčių, rinkliavų, kitų įmokų į valstybės ar savivaldybių biudžetus ir jų administravimo srityse, nereglamentuoja asmens duomenų tvarkymo ir privatumo klausimų, notarų ir analogiš-

kų veiklų, taip pat paslaugų, susijusių su teisminiu atstovavimu, azartiniais lošimais ir loterija.

Pagrindiniai informacinės visuomenės paslaugų reglamentavimo principai, deklaruojami informacinės visuomenės paslaugų įstatyme, yra: elektroninės formos nediskriminavimo principas, reiškiantis, kad teisinė informacijos galia negali būti paneigta arba apribota vien tik tuo pagrindu, jog ši informacija yra sukurta, išsiųsta, gauta arba išsaugota elektroninėmis priemonėmis; technologinio neutralumo principas, reiškiantis, kad teisės normos turi būti taikomos atsižvelgiant į tikslus, kurių siekiama atitinkamomis teisės normomis, ir stengiantis, kad, kiek tai pagrįsta, vien tik dėl jų taikymo nebūtų skatinama arba diskriminuojama naudoti konkrečių technologijų, taip pat kad teisės normos būtų taikomos kiek įmanoma neatsižvelgiant į technologijas, naudojamas informacinės visuomenės paslaugoms teikti.

5.2.6. Informacijos pateikimas elektroninėje komercijoje

Daugelio šalių įstatymuose, taip pat Europos Sąjungos elektroninės komercijos direktyvoje 2000/31/EB yra numatytos teisinės normos, reguliuojančios informacijos teikimą prieš sudarant sutartį, jos sudarymo metu ir sudarius sutartį. Lietuvoje šios normos įtvirtintos Lietuvos Respublikos civilinio kodekso 6.366 straipsnyje bei nustatytos Lietuvos Respublikos informacinės visuomenės paslaugų įstatyme.

Pagal Informacinės visuomenės paslaugų įstatymo 6–8 straipsnio nuostatas visais atvejais subjektas, vykdantis elektroninę komerciją (teikiantis informacinės visuomenės paslaugas), turi užtikrinti, kad vartotojai ir valstybės institucijos galėtų lengvai, tiesiogiai ir nuolat pasiekti šią informaciją:

1. paslaugos teikėjo pavadinimą;
2. ryšius, tokius kaip paslaugų teikėjo fizinis adresas ir informacija, kuri palengvintų greito ryšio su pardavėju / paslaugos teikėju galimybes (elektroninio pašto adresas, telefono numeris, telefakso numeris ir pan.);
3. nurodyti valstybės registrą, į kurį jis įrašytas, ir jo registracijos numerį arba analogišką identifikavimo priemonę šiame registre, jei jis užsiregistravęs įmonių arba panašiame viešajame registre;

4. pridėtinės vertės mokesčio (toliau – PVM) mokėtojo kodą (jei jis yra PVM mokėtojas);
5. atitinkamos licencijuojamos veiklos priežiūros institucijos rekvizitus, jei norint verstis veikla būtina gauti įstatymų nustatyta tvarka išduotą licenciją (leidimą);
6. profesinį vardą (pvz., mediko arba auditoriaus) ir valstybę, kurioje jis buvo suteiktas, profesinę ar panašią instituciją, kurioje jis registruotas kaip paslaugų teikėjas, nuorodą į profesinės veiklos taisykles ir priemones joms pasiekti, jei paslaugos teikėjas yra reglamentuojamos profesijos atstovas.

Elektroninės komercijos subjektai, be kitų dalykų, vartotojui taip pat turi suteikti aiškią informaciją apie:

1. svarbias produkto arba paslaugos ypatybes;
2. visus galimus pasiūlymo apribojimus, išlygas ir pan.;
3. pasirinktų prekių ir paslaugų kainas (kainos sudėtinės dalys turi būti aiškiai įvardytos ir įskaičiuotos į galutinę sumą. Tai turi būti atlikta ne vėliau kaip priimant užsakymą, paprastai perkeliant prekes į „prekių krepšelį“, o ne pirkėjui atsiskaitant);
4. laikotarpiu, kuriuo yra taikomas specialus pasiūlymas arba specialios kainos;
5. visas svarbias sutarties sąlygas ir terminus (ypač apie pristatymo, apmokėjimo sąlygas ir terminus arba nuolatinio paslaugų teikimo sąlygas);
6. specifines sąlygas, jei jas būtina išpildyti norint naudotis konkrečiu produktu arba paslauga;
7. visas įmanomas paslaugas po pardavimo bei taikomus garantinius terminus;
8. pranešimo apie sutarties nutraukimą terminus, kai sudaroma neterminuota sutartis arba ilgesnė nei vienerius metus galiojanti sutartis.

Pagal Lietuvos Respublikos civilinio kodekso 6.366 straipsnio 6 dalį iki elektroninės sutarties sudarymo, o jei daiktai tiekiami ne pardavėjo įgalioto asmens – iki daiktų pateikimo, vartotojas turi gauti informaciją raštu apie:

1. siūlomą daiktą (pavadinimas, pagrindinės savybės);
2. pardavėją, nurodant, kur ir kam vartotojas gali adresuoti bet kokį skundą;

3. vartotojo teisę atsisakyti sutarties įgyvendinimo tvarkos;
4. mokėjimo, pristatymo arba atlikimo tvarką, pardavėjo teikiamas daikto priežiūros paslaugas ir garantijas, jeigu jos suteikiamos;
5. sutarties atsisakymo sąlygas, jeigu sutartis neterminuota arba ilgesnė nei vienerių metų.

Be to, pareiga įrodyti, kad ši informacija raštu buvo įteikta pirkėjui, tenka pardavėjui. Šios nuostatos yra ypač griežtos ir sunkiai suderinamos su elektronine sandorio natūra (kadangi informaciją imperatyviai reikalaujama pateikti raštu), tačiau svarbu paminėti, jog įstatyme numatyta viena išimtis – informacijos raštu pateikti nereikia, jei ši informacija vartotojui buvo suteikta prieš sudarant sutartį. Šiuo atveju informacija vartotojui gali būti pateikta ir elektronine forma.

Paminėtina, kad informacija turi būti pateikiama vartotojui suprantama kalba, o daugeliu atvejų – valstybine kalba. Komercinė informacija turi būti aiškiai atpažįstama, iš jos turi būti galima nustatyti fizinio arba juridinio asmens, kurio vardu teikiama komercinė informacija, tapatybę. Komercinėje informacijoje turi būti aiškiai atpažįstami reklaminiai pasiūlymai, tokie kaip nuolaidos, priemokos, dovanos, o sąlygos, kurias reikia patenkinti norint gauti šias nuolaidas, priemokas ar dovanas, turi būti lengvai prieinamos ir aiškiai bei nedviprasmiškai pateiktos. Galiausiai komercinėje informacijoje turi būti aiškiai atpažįstami reklaminiai konkursai arba žaidimai, o sąlygos, kurias reikia patenkinti norint juose dalyvauti, turi būti lengvai prieinamos ir aiškiai bei nedviprasmiškai pateiktos, pavyzdžiui, netoleruotina, kad svarbi informacijos dalis pateikiama atskiruose tinklalapiuose, kurių vartotojui reikia specialiai ieškoti, arba kad informacija pateikiama smulkiu ir nekontrastingu šriftu.

5.2.7. Elektroninės sutarties teisinis pripažinimas Lietuvoje

Nepaisant skirtingos praktikos užsienio valstybėse, elektronine forma ir (arba) priemonėmis sudaromos sutartys (elektroninės sutartys) nėra aiškiai reglamentuotos Lietuvoje kaip specifinė sutarčių rūšis arba forma. Šioms sutartims iš esmės taikomi bendrieji Civiliniame kodekse nustatyti reikalavimai, kurie taikomi rašytine forma sudaromoms sutartims, tačiau keliamos ir papildomos sąlygos. Elektroninėmis priemonėmis neleidžiama sudaryti sutartis, kurioms nustatyta notarinė forma bei kurioms įstatymais nustatyta privaloma teisinė registracija. Ap-

skritai paminėtina, kad Informacinės visuomenės paslaugų įstatymo IV skyriuje vartojama „sutarties, sudaromos elektroninėmis priemonėmis“, sąvoka gali būti aiškinama dvejopai:

- kaip sutartis, kurios sąlygos pateikiamos šalims elektronine forma ir šalys išreiškia savo valią elektronine forma;
- kaip sutartis (žodinė, rašytinė ar pan.), kurios sudarymą palengvina elektroninės priemonės (pvz., sutartyje yra blanketinių nuorodų į interneto tinklalapius, sutarties sąlygas šalys derina elektroninėmis priemonėmis), tačiau šalys išreiškia savo valią neelektronine forma.

Sistemiškai nagrinėjant Informacinės visuomenės paslaugų įstatymo ir Civilinio kodekso nuostatas manytina, kad „sutartimi, sudaroma elektroninėmis priemonėmis“ laikytina tik pirmoji anksčiau nustatyta sutarčių kategorija. Deja, ši reguliavimo dviprasmybė leidžia netaikyti elektroninėms sutartims nustatytų taisyklių antros, anksčiau nustatytos kategorijos sutartims, taigi informacinės visuomenės paslaugų teikėjas gali išvengti papildomų pareigų vartotojams. Būtent tokią praktiką šiuo metu taiko finansinių paslaugų teikėjai Lietuvoje, kai rašytinėse sutartyse su vartotojais pateikiamos blanketinės nuorodos į elektroninius išteklius ir taip suteikiama galimybė paslaugos teikėjui iš esmės vienašališkai ir neinformuojant vartotojo pakeisti sutarties sąlygas ir pan. Taigi paslaugų teikėjai diskriminuoja vartotojus, kurie tiesiogine prasme sudaro sutartis elektroninėmis priemonėmis. Apskritai pažymėtina, kad paslaugų teikėjai (ypač profesionalūs paslaugų teikėjai – verslininkai) vengia sudarinėti grynai elektronines sutartis, o šalių keitimąsi elektronine informacija ir užsakymais įteisinti rašytinėmis sutartimis. Būtent tokią praktiką taiko visi be išimties Lietuvos bankai.

Išskyrus Informacinės visuomenės paslaugų įstatymą, kituose Lietuvos įstatymuose elektroninės sutartys nėra tiesiogiai įvardijamos ir išsamiai reglamentuojamos. CK 1.73 straipsnio 2 dalyje rašytinės formos dokumentui prilygina šalių pasirašytus dokumentus, perduotus telegrafinio, faksimilinio ryšio arba kitokiais telekomunikacijų galiniais įrenginiais, jeigu yra užtikrinta teksto apsauga ir galima identifikuoti parašą. CK 1.76 straipsnio 2 dalis nustato, kad jeigu sandoris buvo sudarytas naudojant telekomunikacijų galinius įrenginius, tai visais atvejais turi būti pakankamai duomenų sandorio šalims nustatyti.

Dar griežtesnės normos pateikiamos ir CK 6 knygos IV dalies XXIII skyriaus 4 skirsnyje (6.366–6.367 str.) reglamentuojant vartoto-

jiškų pirkimo–pardavimo sutarčių, sudaromų naudojant ryšio priemones (kartu ir elektronine forma), ypatumus bei jas detalizuojančiose Daiktų pardavimo ir paslaugų teikimo, kai sutartys sudaromos ryšio priemonėmis, taisyklėse, patvirtintose Ūkio ministerijos 2001 m. rugpjūčio 17 d. įsakymu Nr. 258. Šiose normose pabrėžiami du pagrindiniai funkciniai elektroniniu būdu sudaromų sutarčių reikalavimai: naudojamų ryšio priemonių saugumo bei informacijos integralumo ir asmenų, sudarančių šią sutartį, tapatybės nustatymo užtikrinimo reikalavimai.

5.2.8. Elektroninės sutarties sudarymas

Pačiame Informacinės visuomenės paslaugų įstatyme nustatyti papildomi reikalavimai dėl informacijos, susijusios su elektroninės sutarties sudarymu, pateikimo, užsakymo pateikimo, pasiūlymo sudaryti sutartį (ofertos) ir pateikto pasiūlymo sudaryti sutartį priėmimo (akcepto). Įstatymo 9 straipsnis įpareigoja informacinės visuomenės paslaugos teikėjus paslaugos gavėjui pateikti sutarčių sąlygas, taip pat sutarčių standartines sąlygas taip, kad šis galėtų šią informaciją išsaugoti ir vėliau panaudoti. Įstatymo 10 straipsnis nustato, jog elektroninio užsakymo gavimas turi būti paslaugos teikėjo nedelsiant elektroninėmis priemonėmis patvirtintas. Vienas iš tinkamų užsakymo gavimo patvirtinimų yra užsakytos informacinės visuomenės paslaugos teikimas elektroninėmis priemonėmis (pvz., prieigos prie elektroninės duomenų bazės suteikimas, galimybės parsisiųsti informaciją suteikimas ir pan.). Užsakymas ir jo gavimo patvirtinimas yra laikomi gautais, kai šalys, kurioms jie skirti, gali juos pasiekti, t. y. peržiūrėti ir patikrinti. Paslaugos teikėjas turi suteikti paslaugos gavėjui tinkamas, veiksmingas ir prieinamas technines priemones, leidžiančias jam nustatyti ir ištaisyti įvesties klaidas prieš pateikiant užsakymą. Šie reikalavimai yra privalomi, jei viena iš sutarties šalių yra vartotojas, išskyrus atvejį, kai užsakymas pateikiamas ir tvirtinamas tik keičiantis elektroninio pašto pranešimais arba analogiškais individualiais pranešimais. Ši išimtis yra pateisinama, nes pats elektroninio pašto arba individualaus pranešimo formatas suponuoja, jog atitinkama informacija bus asmeniškai atsiųsta užsakovui (vartotojui) ir išsaugota jo kompiuteryje arba elektroninio pašto bylose.

Kaip minėta, nustatytos ir pasiūlymo sudaryti elektroninę sutartį (ofertos), ir pateikto pasiūlymo sudaryti sutartį priėmimo (akcepto)

specialios taisyklės. Įstatymo 11 straipsnis pirmiausia nustato prezumpciją, kad šalis išsiuntė pasiūlymą sudaryti sutartį (oferta) ir (arba) pateiktą pasiūlymą sudaryti sutartį priėmė, jei juos išsiuntė pati šalis, jos atstovas arba informacinė sistema, kuri šalies arba jos vardu suprogramuota veikti automatiškai. Ši norma turi ypatingą reikšmę, nes pripažįstama, jog šalis gali išreikšti savo valią iš anksto suprogramuodama informacinę sistemą priimti pasiūlymus, atitinkančius tam tikras sąlygas. Pasiūlymas sudaryti sutartį (oferta) ir (arba) pateikto pasiūlymo sudaryti sutartį priėmimas (akceptas) laikomi išsiųstais, jei šalis arba jos atstovas, kurie juos išsiuntė, nebegali jų pasiekti ir kontroliuoti, t. y. neįmanoma jų vienašališkai atšaukti arba juos paneigti. Savo ruožtu pasiūlymas sudaryti sutartį (oferta) ir (arba) pateikto pasiūlymo sudaryti sutartį priėmimas (akceptas) laikomi gautais, jei šalis, kuriai jie skirti, gali juos pasiekti, t. y. gali juos įvertinti ir apsispręsti dėl jų. Įstatyme nustatytos ir elektroninių sandorių jurisdikciją lemiantis principas, laikant, jog pasiūlymas sudaryti sutartį (oferta) ir (arba) pateikto pasiūlymo sudaryti sutartį priėmimas (akceptas) laikomi išsiųstais ir (arba) gautais pasiūlymą sudaryti sutartį pateikusios šalies (oferento) ir (arba) pasiūlymą sudaryti sutartį priėmusios šalies (akceptanto) gyvenamojoje arba verslo vietoje.

5.2.9. Lietuvos teismų praktika pripažįstant elektronines sutartis

Deja, bent jau kol kas Lietuvoje nėra teismų praktikos, kuri vienareikšmiškai įteisintų elektronines sutartis, tačiau užsienio valstybių teismų praktika šias sutartis pripažįsta visateisiu civilinės apyvartos instrumentu. Artimiausi teisminiai precedentai Lietuvoje yra Lietuvos Aukščiausiojo Teismo praktika, kuria suteikiama juridinė galia dokumentų faksimilių kopijoms (faksu perduotos kopijos iš esmės yra elektroninės dokumento kopijos. Aukščiausiasis Teismas 2000 m. gegužės 29 d. nutartimi civilinėje byloje *R. Beliackas v. UAB „Sabina“ Nr. 3K-3-619/2000* konstatavo, kad „viena iš rašytinių tekstų perdavimo priemonių yra telekomunikacija, kurios techninė priemonė yra ir fakso aparatas“. Atsižvelgiant į tai, kad faksu, kaip elektroninių ryšių priemone, perduodami būtent elektroniniai duomenys, galima daryti išvadą, jog Aukščiausiasis Teismas šioje byloje iš esmės pripažino, kad elektroninė forma yra viena iš rašytinės formos rūšių. Naujesnėse bylose teismai iš esmės prilygina elektroninę informaciją rašytinei infor-

macijai, pavyzdžiui, Lietuvos vyriausiasis administracinis teismas byloje *UAB „Bitė GSM“ v AB „Lietuvos telekomas“ Nr. 3K-3-35/2003* dėl pokalbių srautų siuntimo nesutartomis kryptimis įrodymais pripažino elektroninius skambučių srautų įrašus, generuojamus telefonų stotyse, o Lietuvos Aukščiausiasis Teismas byloje *AB „Lietuvos telekomas“ v. Ž. Budros IĮ „Sėkmės vėjas“ Nr. 3K-3-35/2003* dėl nepageidaujamų elektroninių reklaminių pranešimų platinimo elektroniniams pranešimams pritaikė rašytinei informacijai reglamentuoti skirtas taisykles. Taigi pamažu, tačiau elektroniniai dokumentai (kartu ir elektroninės sutartys) yra pripažįstami įrodymais tiek civiliniame, tiek baudžiamajame procese. Todėl susidūrę su elektronine sutartimi teismai gali vadovautis Informacinės visuomenės paslaugų įstatymo 3 straipsnio 2 dalyje įtvirtintu elektroninės formos nediskriminavimo principu, kuris reiškia, kad teisinė informacijos galia negali būti paneigta arba apribota remiantis tik tuo, kad ši informacija yra sukurta, išsiųsta, gauta arba išsaugota elektroninėmis priemonėmis.

5.3. Papildoma medžiaga. Papildomos elektroninės sutarties teisinio reguliavimo nuostatos

5.3.1. Tarpininkų vaidmuo sudarant elektroninius sandorius

Direktyva apriboja informacinės visuomenės paslaugų teikėjo finansinę atsakomybę dėl informacijos, dedamos internetinėje svetainėje, turinio. Tai ypač svarbu telekomunikacines paslaugas teikiančioms organizacijoms, kurios aptarnauja informacinių paslaugų infrastruktūrą ir teikia paslaugas (šios paslaugos – informacijos perdavimo ryšio tinklo arba prieigos prie ryšio tinklo suteikimas) internetinių svetainių savininkams.

Paslaugos teikėjai yra atleidžiami nuo finansinės atsakomybės, kai jie paprasčiausiai laikinai saugo arba laiko informaciją. „Laikymas“ suprantamas kaip tarpinis informacijos saugojimas siekiant paspartinti informacijos siuntimą. Pavyzdžiui, jeigu pilietis X pasiekia puslapį Jungtinėse Valstijose iš Varviko (Didžioji Britanija) universiteto, serveris Varviko universitete paprastai saugo visą informaciją, kurią pilietis X ketina laikinai naudoti. Toks laikas paprastai būna apie vieną valandą. Jei pilietis X vėl nori prisijungti prie informacijos per valandą, informacinėse sistemoje išlikę duomenys labai sumažins lai-

ką tai informacijai pasiekti. Yra kai kurių šios bendros laikymo paslaugos išimčių. Pati svarbiausia iš jų yra, kai teikėjas nesiima skubiai užblokuoti priėjimą prie informacijos gavęs žinių, kad kompetentinga valstybės institucija įpareigojo tai atlikti.

Direktyva numato panašią nuostatą, skirtą „vadovavimui“. Tipiška „vadovavimo“ situacija yra, kai bendrovė, tokia kaip *„VirginNet“* (Didžioji Britanija), išnuomoja internetinę svetainę subjektui. Tada asmuo gali laisvai įdėti informaciją į internetą. *„VirginNet“* yra internetinės svetainės šeimininkė, bet nesistengia kontroliuoti, kokio pobūdžio informacija joje yra dedama. Taigi „vadovavimo“ paslaugos teikėjai yra atleisti nuo finansinės atsakomybės už informaciją, saugomą paslaugos gavėjo prašymu:

„1. teikėjas neturi faktinių žinių apie neteisėtą veiklą arba informaciją ir reikalavimų atlyginti žalą atžvilgiu nežino apie faktus ar aplinkybes, rodančias, kad verčiamasi neteisėta veikla arba teikiama neteisėta informacija; arba

2. teikėjas, gavęs tokių žinių arba apie tai sužinojęs, nedelsdamas panaikina šią informaciją arba atima galimybę ją pasiekti“.

Taigi paslaugos teikėjas nebus atsakingas pagal baudžiamuosius, administracinius ar civilinius teisės aktus dėl internetinėje svetainėje esančios informacijos turinio, skelbimų lentų sistemos arba naujienų programų. Tačiau tarpininkai yra skatinami kitomis priemonėmis prižiūrėti jų internetinėse svetainėse arba informacinėse sistemose esančią informaciją ir kartu su kompetentingomis valstybės institucijomis imtis priemonių, užkertančių tam kelią. Direktyva nurodo, kad Komisija aktyviai turėtų skatinti susireguliuojančių sistemų kūrimą, įskaitant elgesio kodeksus ir telefonų „karštąsias linijas“.

Vieninteliai įpareigojimai, kuriuos turi vykdyti tarpininkai, – tai valstybinių priemonių, įpareigojančių teikėjus tikrinti arba kontroliuoti trečiosios šalies turinį. Tokio pobūdžio įpareigojimų įgyvendinimas pasireiškia kompetentingų viešųjų institucijų informavimu apie įtariamą nelegalią veiklą arba informaciją, kurią pateikia jų paslaugų gavėjai, arba gavus kompetentingų institucijų prašymus, pateikti informaciją, leidžiančią nustatyti paslaugos gavėjų, su kuriais jie sudarę informacijos saugojimo sutartis, tapatybę.

Direktyva apima plačią nuostatų skalę dėl šių priemonių vykdymo ir įgyvendinimo. Komisija ir valstybės narės skatina kodeksų tobulinimą Bendrijos lygiu. Nuostatos sukurtos tam, kad padrąsintų su

šiuo reikalu susijusias šalis siųsti nacionalinių kodeksų projektus Komisijai, kad įvertinimas galėtų būti nustatytas pagal jų suderinamumą su Bendrijos teisės aktais. Tačiau kol kas dar neaišku, ar elgesio kodeksai pasiteisins kaip ganėtinai stiprus įrankis veiksmingai kontroliuoti teikėjus, ar pasižymės pastovumu Bendrijoje. Direktyva nesujungia kodeksų į jokią įpareigojančią teisinę schemą. Tyrimai rodo, kad griežtas bendras reglamentavimas gali būti didelėse, labai skirtingose rinkose, sudarytose iš mažų segmentų. Elektroninės rinkos dalis yra geras to pavyzdys.

Toliau skatindama Bendrijos elgesio kodeksų tobulinimą, Direktyva taip pat nustato, kad veiksmingas neteisminių ginčų sistemos sureguliavimas privalo būti reglamentuotas valstybės įstatymų. Pagal Komisijos rekomendaciją Dėl įstatymų, taikytinų dėl neteisminių vartotojų ginčų sureguliavimo, Direktyva įpareigoja šalis numatyti neteisminio ginčų sprendimo galimybę. Valstybės narės turi užtikrinti, kad šalims, dalyvaujančioms neteisminių vartotojų ginčų sureguliavimo procedūroje, būtų taikomi savarankiškumo ir aiškumo, konkurencijos, procedūros efektyvumo, sprendimo teisėtumo, atstovavimo ir šalių laisvės principai.

Neteisminių ginčų sureguliavimo mechanizmas yra ypač vertingas sudarant ir vykdant mažos vertės sutartis, kai viena šalis yra daug galingesnė negu kita. Tokiais atvejais daug brangaus laiko kainuojantis teismo procesas gali įbauginti tuos, kurie turi ribotus išteklius, ir visa tai gali užkirsti kelią ginčo sprendimui. Direktyvos reikalavimas veiksmingą neteisminį mechanizmą padaryti prieinamą yra teigiamas, užtikrinant vertingą vartotojų teisių apsaugą (pirmiausia turima omenyje fizinius asmenis).

5.3.2. Teisinė elektroninio parašo galia

Elektroninio parašo direktyva (1999/93/EC) nustato teisinius elektroninio parašo bei tam tikrų sertifikavimo paslaugų reikalavimus.

Direktyva buvo vienas iš pirmųjų žingsnių reglamentuojant informacinę visuomenę, o jos ašimis tapo:

- elektroninio parašo juridinis pripažinimas;
- taisyklių, kaip elektroninis parašas bus naudojamas, nustatymas;
- sertifikavimo paslaugų teikimo įteisinimas ir reglamentavimas.

Elektroninio parašo direktyvos tikslas – palengvinti elektroninio parašo naudojimą suvienodinti teisinį jo reglamentavimą Europos Są-

jungos valstybėse ir taip prisidėti prie jo teisinio pripažinimo.

Elektroninio parašo teisinė galia pagal šią Direktyvą apsiriboja tuo, jog elektroninis parašas pripažįstamas viena iš įrodinėjimo priemonių. Tačiau šis pripažinimas yra susijęs tik su *ad probatione* dalimi ir savaime nereiškia, jog pasirašyta informacija yra teisiškai galiojanti, t. y. *ad validitate* reikšmė elektroniniam parašui nėra suteikiama. Pasirašyta informacija gali būti pripažinta netinkama dėl kitų priežasčių (pvz., sudaryta neteisėta sutartis). Juridinis dokumento galiojimas, kurį reglamentuoja atitinkami įstatymai, yra apibrėžtas. Direktyva, siekdama apsaugoti vartotoją, taip pat nemini atskirų sutarčių rūšių (pvz., nekilnojamojo turto pirkimo–pardavimo).

Direktyvoje nekalbama ir apie dokumento pasirašymo vietos nustatymą. Tai ganėtinai svarbu sutartinėje teisėje. Šis aspektas minimas Elektroninės komercijos direktyvoje – teigiama, kad nustatant pasirašymo vietą reikėtų remtis tarptautinės privatinės teisės nustatytomis bendromis taisyklėmis.

Kaip jau buvo minėta, Direktyva elektroninį parašą apibrėžia kaip vieną iš įrodinėjimo priemonių. Direktyva suteikia galimybę pateikti elektroninį parašą teismui, laikant jį įrodymu. Tai nereiškia, jog elektroninio parašo nebuvo galima pateikti teismui kaip įrodymo ir iki Direktyvos priėmimo, tačiau, atsižvelgiant į atskirų ES valstybių procesinės teisės ypatumus, elektroninio parašo panaudojimas tapdavo problemiškas dviem aspektais:

- elektroninio parašo pripažinimas kaip įrodymo;
- elektroninio parašo vietos nustatymas įrodymų hierarchijoje.

Šios dvi problemos pasireiškia atskirų valstybių narių teisėje skirtingai, nelygu kokios šalyse egzistuoja įrodymų sistemos.

1. Laisvo įrodymų pateikimo sistemos (Danija, Švedija) leidžia pateikti teismui visus įmanomus įrodymus. Teisėjas laisvas vertindamas įrodymų tinkamumą. Tokioje įrodinėjimo sistemoje elektroninis parašas gali tapti įrodymu ir be papildomos reglamentacijos. Tačiau tokioje įrodinėjimo sistemoje egzistuoja hierarchija vertinant įrodymų vertingumą. Įrodymų vertė yra skirtinga, todėl esant prieštaringiems įrodymams iškyla problema, kuris iš jų turi didesnę vertę įrodymų hierarchijoje.
2. Teisinė įrodymų pateikimo sistema (Vokietija, Ispanija, Portugalija) griežtai nustato reikalavimus įrodymams, kurie yra priimtini teisme. Teismas priima ne visus įrodymus, o tik atitinkančius procesinių normų reikalavimus. Taip pat reglamen-

tuojama ir įrodymų hierarchija. Paprastai tokiose sistemose popieriniai dokumentai vertinami kaip turintys didesnę vertę nei žodžiai arba kitokie įrodymai. Tokiose sistemose elektroninis parašas gali būti pripažintas netinkamu įrodymu arba jo vieta įrodymų hierarchijoje yra labai nereikšminga.

3. Mišrios sistemos (Prancūzija, Belgija, Liuksemburgas) turi abiejų įrodymų sistemų požymių. Šioje sistemoje elektroninio parašo įrodomoji vertė skirtinga.

Būtent įrodinėjimo sistemų įvairovė paskatino įvesti Europos Sąjungos reguliavimą šiose srityse, nes įrodinėjimo bei skirtingo įrodymų vertinimo problema galėjo sudaryti didelių kliūčių elektroninės komercijos bei informacinių technologijų raidai. Dėl nevienodo elektroninio parašo, kaip įrodymo traktavimo, prekių bei paslaugų laisvas judėjimas ES vidaus rinkoje galėjo tapti labai problemiškas.

Direktyva, pripažindama elektroninį parašą įrodymu, nevienodai įvertina paprasto (klasikinio) ir saugesnio elektroninio parašo teisinę vertę. Direktyva įtvirtina nuostatą, jog saugus elektroninis parašas yra priimtinas teismui ir yra prilyginamas įrodomajai dokumento, parašyto ant popieriaus, vertei. Ši nuostata sulygina elektroninį ir įprastą parašą ant popierinio dokumento. Norint, kad elektroninis parašas įgautų tokią vertę, reikia įrodyti, jog jis atitinka Direktyvos prieduose nustatytus reikalavimus. Tam gali būti pasitelktas ir ekspertas. Tiesa, dėl to labai padidėja proceso išlaidos.

Direktyva, įvertindama klasikinio elektroninio parašo įrodomąją galią, reikalauja nedrausti pateikti teismui taip pasirašytų dokumentų, tačiau nenurodo klasikinio elektroninio parašo įrodomosios vertės palikdama šią funkciją teismui. Šalis, dalyvaujanti teisme ir besiremianti tokiu įrodymu, turės įrodyti, jog toks parašas yra patikimas. Teisėjas turės vertinti, ar elektroninis parašas yra patikimas ir kokia jo vieta įrodymų hierarchijoje.

Direktyva nereglamentuoja laisvo įrodymų vertinimo taisyklių, kurias nustato pačios valstybės narės savo nacionaliniuose norminiuose aktuose, todėl čia dar svarbesnis yra eksperto vaidmuo. Nustatydamas parašo patikimumą teisėjas turės remtis eksperto, turinčio specialių žinių atitinkamoje srityje, išvada, nes Direktyva neišaiškina sąvokos „pakankamas elektroninio parašo patikimumas“ palikdama tai ekspertui ir teisėjui. Šiuo klausimu Direktyva nustato, jog asmenys, sudarantys sutartį arba dalyvaujantys bendroje veikloje (elektroninių kor-

telių apyvarta), gali nustatyti sutartinius „pakankamo patikimumo“ reikalavimus.

Sertifikavimo paslaugų reglamentavimas

Elektroninio parašo direktyvoje kalbama ir apie trečiąjį asmenį, kurio funkcija – garantuoti elektroninio parašo galiojimą. Pasirašant elektroniniu parašu gali kilti abejonių dėl sutarties partnerio sąžiningumo. Kadangi šalys viena kitos nemato ir negali patikrinti tapatybės, reikalingas trečiasis asmuo, garantuojantis, kad elektroninis parašas yra būtent to asmens, o ne kito. Toks garantas yra trečiojo asmens – sertifikavimo centro – išduodamas dokumentas (sertifikatas), užtikrinantis, kad sertifikato turėtojas yra tas asmuo, kuriuo jis prisistato komunikavimo dalyviams.

Kalbant apie sertifikavimo paslaugas galima išvesti paraleles su notaro atliekamomis rašytinių dokumentų patvirtinimo funkcijomis. Notaro patvirtintas dokumentas turi didesnę juridinę vertę nei paprastas rašytinis dokumentas. Dėl šios priežasties kai kurios notarų kontoros Europos Sąjungos valstybėse išreiškė pageidavimą užsiimti ir sertifikavimo veikla, nes, jų manymu, tai yra toks pats patvirtinimas kaip ir rašytinio dokumento atveju.

Direktyva atskiria sertifikatų tipus bei jų reikalavimus atitinkamai pagal elektroninio parašo tipus. Sertifikavimo centrai gali išduoti kvalifikuotą ir nekvalifikuotą sertifikatą, atitinkančių klasikinį ir saugesnį elektroninį parašą. Daug griežtesni reikalavimai keliami sertifikavimo centrui, išduodančiam sertifikatą, garantuojantį saugesnio elektroninio parašo tikrumą (kvalifikuotas sertifikatas). Tai atlikta dėl to, jog saugesniu elektroniniu parašu pasirašyta informacija turi didesnę įrodomąją vertę. Saugesniu elektroniniu parašu pasirašomos informacijos įrodomoji vertė gali būti prilyginama rašytinio dokumento įrodomajai vertei.

Direktyvoje yra numatyti sertifikavimo paslaugų teikimo principai Europos Sąjungos valstybėse. Numatytas laisvas sertifikavimo paslaugų teikimo principas. Valstybės narės neturi riboti, licencijuoti arba kitaip blokuoti sertifikavimo centrų kūrimosi bei veiklos, neturi būti išduodami išankstiniai leidimai arba daromos kliūtys užsienio bendrovėms teikti sertifikavimo paslaugas valstybės teritorijoje. Valstybei palikta teisė savarankiškai nustatyti atitinkamą sertifikavimo įstaigos

akreditavimo tvarką, tačiau ji turi būti atliekama tik vienu tikslu: siekiant pagerinti sertifikavimo įstaigų paslaugų kokybę bei formuoti gerą sertifikavimo praktiką. Ypatingas elektroninio parašo patvirtinimo taisykles valstybė gali nustatyti tik valstybiniame sektoriuje, tačiau šie papildomi reikalavimai turi būti skaidrūs, aiškūs ir atitikti pasirašomų dokumentų svarbą. Priešingu atveju bus pažeistas laisvo paslaugų judėjimo principas.

Kiekvienai valstybei narei palikta teisė savarankiškai kontroliuoti sertifikavimo centro veiklą. Nacionalinės teisės normos taikomos tiems sertifikavimo centrams, kurie veikia (teikia paslaugas) atitinkamos valstybės teritorijoje.

Kontrolės pagrindu tampa antrajame Direktyvos priede nustatyti reikalavimai sertifikavimo paslaugų teikėjui ir 1995 m. Europos Komisijos direktyvos „Dėl fizinių asmenų asmeninių duomenų apsaugos“ nuostatos, nurodančios, kad asmeninių duomenų rinkimas pateisinamas tik tuo atveju, jei juos rinkti būtina, siekiant teikti geros kokybės paslaugas ir jei turimas asmens, kurio duomenys renkami, sutikimas.

Reguliuojant sertifikavimo paslaugų teikimą bei saugant asmens privatų gyvenimą, taip pat numatytas draudimas trukdyti sertifikato savininkui suteikti slapyvardį vietoje tikrosios pavardės. Direktyva iš principo leidžia naudoti slapyvardį, tačiau šiuo atveju sertifikavimo centras turi turėti tikruosius asmens duomenis bei juos pateikti nacionalinės arba ES teisės numatytais atvejais.

Tačiau bene stipriausias saugiklis reguliuojant sertifikavimo veiklą yra sertifikavimo paslaugų teikėjo atsakomybės prezumpcija. Jei padaroma žala tretiesiems asmenims pagal sertifikavimo sutartį – sertifikate nurodoma neteisinga informacija, sertifikatas atšaukiamas, neregistruojamas, atsako sertifikavimo paslaugų teikėjas. Šis principas yra palankus tretiesiems asmenims, kurie kilus ginčui turės įrodinėti tik atsiradusią dėl neteisėtos veikos žalą bei priežastinį žalos ir sertifikavimo sutarties ryšį. Sertifikavimo paslaugų teikėjas, paneigdamas savo kaltę, turės įrodyti, jog žala atsirado ne dėl jo kaltės, o dėl trečiojo asmens aplaidumo (neprotingai arba piktybiškais tikslais panaudojo sertifikatą, nepasinaudojo *on-line* pateiktu atšauktų sertifikatų sąrašu, viršijo leistinas transakcijų sumas). Papildomai sertifikavimo paslaugų teikėjas gali paminėti *force majoure* aplinkybes.

5.4. Papildoma medžiaga. Elektroninės komercijos apmokestinimas

5.4.1. Elektroninės komercijos sampratos nagrinėjant jos apmokestinimą

Siekiant pateikti tinkamą elektroninės komercijos sąvoką, kuri atspindėtų apmokestinimo ypatybes, svarbu atsižvelgti į tiesioginių ir netiesioginių mokesčių specifiką. Nagrinėdami netiesioginius mokesčius pastebėsime, kad kai kurie sandoriai buvo įmanomi dar iki kompiuterinių sistemų ir jų tinklų išplėtojimo. Naudojantis faksimilėmis, teleksais buvo galima pateikti užsakymus nuotoliniu būdu. Tačiau pirkėjui pristatyti prekes buvo įmanoma tik materialia jų forma.

Tokie komerciniai sandoriai egzistavo jau gana ilgą laiką. Tuo tikslu buvo priimti atitinkami teisės aktai, reglamentuojantys specifines minėtų sandorių sritis. Europos Sąjungoje buvo priimta Nuotolinės prekybos direktyva. Panašios nuostatos buvo įtvirtintos ir kitų valstybių teisės aktuose. Pagrindinė šių sandorių specifika, palyginti su elektroninės komercijos ypatybėmis, buvo ta, kad parduodamos prekės turėdavo materialia forma kirsti valstybių sienas. Taip buvo galima užtikrinti prekių judėjimo srautų kontrolę ir atitinkamą jų apmokestinimą.

Tik ištobulėjus informacinėms technologijoms tapo įmanoma prekes perkelti į elektroninę erdvę. Tokia galimybė atsirado po to, kai minėtomis priemonėmis kai kurias prekes buvo galima išreikšti skaitmenine forma (t. y. nematerialią išraišką turinčiais produktais). Pagrindinės prekės yra knygos, žurnalai, muzikiniai įrašai, vaizdo įrašai, kompiuteriniai žaidimai, programinė įranga ir kt.

Jei kompiuterinėmis sistemomis bei telekomunikaciniais tinklais bus atliekamos visos verslo stadijos, išskyrus paskutiniąją (prekės pristatymą pirkėjui), pažangias informacines technologijas (kompiuterines sistemas ir internetą) galėsime prilyginti faksimilėms arba teleksams. O tokių sandorių teisinis reglamentavimas yra užtikrintas iki šiol nuotolinius komercinius sandorius reglamentuojančiomis teisės normomis.

Kalbant apie prekybą elektroninėje erdvėje bei šių sandorių apmokestinimo netiesioginiais mokesčiais galimybes reikia pažymėti, kad prekės, perkeltos į elektroninę erdvę, išvengia tradicinėje komercijoje egzistuojančių kontrolės punktų. Todėl, norint analizuoti elektroni-

nės komercijos apmokestinimą netiesioginiais mokesčiais, pirmiausia reikia suformuluoti elektroninės komercijos apibrėžimą, kuris atspindėtų būtent naujų sąlygų atsiradimą tradiciniuose mokestiniuose santykiuose.

Viena iš elektroninės komercijos specifikų – tai galimybė perkelti prekes į elektroninę erdvę. Tačiau ne visos prieš tai minėtuose elektroninės komercijos apibrėžimuose pateiktos technologijos gali atlikti šią funkciją. Tik kompiuterių sistemos kartu su programine įranga gali atitinkamas prekes paversti skaitmenine jų forma. Jokios kitos technologijos šios galimybės neturi.

Kita elektroninės komercijos specifika susijusi su tuo, kad kompiuterių sistemos, kartu su globaliu telekomunikacijų tinklu leidžia nematerialią išraišką turinčias prekes persiųsti pirkėjui elektronine erdve. Tai paskutinė ir svarbiausia verslo stadija, kurios buvimas elektroninei komercijai suteikia naujų bruožų.

Atsižvelgiant į anksčiau minėtus argumentus, elektroninei komercijai apmokestinti netiesioginiais mokesčiais taikoma ši elektroninės komercijos samprata – tai elektroninėje erdvėje vykstanti prekyba prekėmis arba paslaugomis tarp mokestiniuose santykiuose dalyvaujančių subjektų, kai įgyvendinamos visos verslo stadijos – pradedant prekių ar paslaugų reklamavimu (pateikimu) ir baigiant jų pristatymu galutiniam vartotojui.

Pateiktoje sąvokoje nesiekiama nurodyti konkrečių technologijų, kurios naudojamos elektroninėje komercijoje. Kaip buvo minėta anksčiau, elektroninė erdvė gali būti sukurta tik kompiuterinėmis sistemomis ir kompiuteriniais tinklais, jokios kitos technologijos to padaryti negali. Taip pat sąvokoje nėra sukonkretinta, kad prekės turi būti išreikštos skaitmenine forma. Tačiau bet kokia prekyba elektroninėje erdvėje įmanoma tik tuomet, jei prekės yra parduodamos skaitmeniniu pavidalu. Tačiau pirkėjas nebūtinai turi naudotis kompiuterine įranga norėdamas gauti kai kurias elektronines paslaugas arba prekes. Mobiliaisiais telefonais jau dabar galima parsisiųsti logotipus, žaidimus arba melodijas bei atsiskaityti už suteiktas paslaugas. Ši elektroninės komercijos sąvoka kol kas geriausiai atspindi elektroninės komercijos apmokestinimo netiesioginiais mokesčiais įdiegtas naujoves į mokestinius santykius, o kartu ir jų teisinį reglamentavimą.

Elektroninės komercijos apmokestinimas tiesioginiais mokesčiais atskleidžia visiškai kitas ypatybes, kurias svarbu tinkamai teisiškai reglamentuoti. Šiuo atveju neturės didesnės įtakos tai, kokia forma pre-

kė pristatoma į užsienio valstybę. Norėdamos tinkamai pritaikyti tiesioginių mokesčių teisines normas, valstybių institucijos neturi kontroliuoti prekės judėjimo. Pagrindinė aplinkybė, lemianti tinkamą tiesioginių mokesčių pritaikymą elektroninėje komercijoje, – nustatyti, kaip valstybėje yra atstovaujama užsienio bendrovė. Todėl, kitaip nei taikant netiesioginius mokesčius, prekės galutiniam vartotojui gali būti pristatomos tiek materialia, tiek ir nematerialia forma.

Apibendrinant anksčiau pateiktas elektroninės komercijos sampratas, taikomas apmokestinant tiesioginiais ir netiesioginiais mokesčiais, galima atskleisti pagrindinį skirtumą, kuris priklauso nuo to, kokie mokesčiai yra taikomi. Prekių pristatymą materialia forma galima analizuoti tik nagrinėjant elektroninės komercijos apmokestinimą tiesioginiais mokesčiais. O jei elektroninė komercija apmokestinta netiesiogiais mokesčiais, galima nagrinėti tik elektronine erdve pristatomas prekes.

5.4.2. Prekės ir paslaugos apmokestinant elektroninę komerciją

Nors dauguma autorių, kalbėdami apie elektroninę komerciją, vartoja terminą „prekės“, tačiau nėra vienos nuomonės dėl to, kaip jas traktuoti – kaip prekes ar kaip paslaugas. Tradicinėje komercijoje tokia dilema neiškildavo, nes būdavo gana paprasta atskirti prekes ir paslaugas. Pagrindinis kriterijus, kuriuo buvo vadovaujamasi, tai materiali prekių išraiška. Elektroninėje komercijoje, kai prekės pristatomos elektroninėje erdvėje, šiuo kriterijumi naudotis neįmanoma. Remiantis Lietuvos Respublikos pridedamosios vertės mokesčio įstatymo 3 straipsnio nuostatomis, prekių tiekimas ir paslaugų teikimas yra laikomi PVM objektu, todėl šis klausimas ypač aktualus pridėtinės vertės mokesčio atžvilgiu, siekiant tiksliai nustatyti PVM objektą.

Elektroninės komercijos sandoriuose, tokiuose kaip programinės įrangos arba knygų pirkimas ir parsisiuntimas internetu, muzikos, filmų ar kitokių garso ar vaizdo kūrinių parsisiuntimas internetu, naudojimasis duomenų bazėmis už atitinkamą mokestį, reklama internete, nuotolinis mokymas internetu ir pan., nepatenka į tradicinės komercijos nustatytas prekių ir paslaugų kategorijas. Šiuo metu elektroninėje komercijoje pagrindinės prekės, kurias galima paversti virtualiomis prekėmis, yra knygos, žurnalai, laikraščiai, programinė įranga, filmai, muzika arba nuotraukos. Norint tinkamai taikyti PVM nuosta-

tas svarbu nustatyti, ar virtualios prekės priskirtinos prekių, ar paslaugų kategorijai.

Direktyvoje „Dėl pridėtinės vertės mokesčio“ išreikšta nuomonė, pagal kurią virtualios prekės dėl savo nematerialumo yra priskiriamos paslaugų kategorijai. Remiantis šia Direktyva bei Lietuvos teisės aktais prekė apibrėžiama taip:

> *„Prekė – bet koks daiktas (įskaitant numizmatinės paskirties pinigus), taip pat elektros energija, dujos, šilumos ir kitų rūšių energija. Preke nelaikoma kompiuterinė laikmena, jeigu jos turinį sudaro nestandartizuota programinė įranga. Nestandartizuota laikoma programinė įranga, kuri nėra masiniam naudojimui sukurta programinė įranga, kurią vartotojai galėtų savarankiškai naudoti po įdiegimo ir riboto apmokymo, reikalingo standartizuotoms operacijoms ar funkcijoms atlikti“.*

Vadovaujantis ES ir Lietuvos PVM įstatymo teisinėmis nuostatomis, virtualios prekės dėl savo nematerialumo bus priskirtinos elektroninės komercijos paslaugų teikimui. Šiai nuomonei pritaria ir Pasaulinė prekybos organizacija. Tokia pat išvada buvo padaryta ir 1998 m. Otavoje vykusioje EBPO ministrų konferencijoje.

2003 m. sausio 8 d. Europos Komisija patvirtino Pridėtinės vertės mokesčio komiteto pasiūlytas gaires dėl elektroniniu būdu teikiamų paslaugų. Šis paslaugų apibūdinimas bei pateiktas sąrašas yra ganėtinai reikšmingas norint pritaikyti tinkamą apmokestinimo būdą, nes ES direktyvoje „Dėl pridėtinės vertės mokesčio“ nėra sukonkretinta, kokios paslaugos laikomos teiktomis elektroniniu būdu. Atsižvelgiant į pateiktas gaires, elektroniniu būdu teikiamą paslaugą galima apibūdinti remiantis dviem kriterijais:

1) ši paslauga turi būti teikiama internetu arba kitu elektroniniu tinklu;
2) šios paslaugos pobūdis labiausiai turi priklausyti nuo informacinių technologijų (t. y. paslauga automatizuota, reikia minimalaus žmogaus įsikišimo, be informacinių technologijų ji negalėtų būti suteikiama).

Kaip jau minėjome apibrėždami elektroninės komercijos sąvoką, nagrinėjant netiesioginį apmokestinimą svarbu pažymėti, kad tais atvejais, kai sandorio šalys bendrauja elektroniniu būdu, tačiau pati prekė pristatoma arba paslauga suteikiama ne elektroniniu, o tradiciniu būdu, toks sandoris nelaikomas elektroniniu būdu suteikta paslauga.

Remiantis šia koncepcija galimi atvejai, kai ta pati paslauga gali būti priskiriama paslaugoms, teikiamoms elektroniniu būdu, arba paslaugoms, teikiamoms tradiciniu būdu. Tai priklausys nuo to, kokį vaidmenį tiekiant šias paslaugas vaidina informacinės technologijos. Pavyzdžiui, nuotolinis mokymas bus pripažįstamas elektroniniu būdu teikiama paslauga, jeigu ji bus visiškai automatizuota, teikiama internetu ir nereikės žmogaus įsikišimo. Tačiau jei internetas bus naudojamas kaip studento ir dėstytojo bendravimo priemonė (t. y. naudojamas elektroninis paštas reikiamai mokomai medžiagai persiųsti), tuomet tai jau nebus priskiriama elektroniniu būdu teikiamai paslaugai. Tokios pat taisyklės taikomos ir finansinėms arba teisinėms konsultacijoms.

Laikantis šių kriterijų, Europos Komisijos gairės pateikia ir konkretų elektroniniu būdu teikiamų paslaugų sąrašą: internetinių svetainių ir nuotolinis programų darbo palaikymas, programinės įrangos parsisiuntimas, duomenų saugojimas, teminių kompiuterinių sistemų darbalaukių (*desktop themes*) parsisiuntimas, knygų bei skaitmeninio formato leidinių, elektroninių žurnalų bei laikraščių prenumerata/abonentinis mokestis, elektroninėje erdvėje teikiama teisinė bei finansinė informacija (pvz., duomenys apie vertybinių popierių rinką), vietos, skirtos reklamai internete, suteikimas, mokamų paieškos sistemų naudojimas, muzikos kūrinių parsisiuntimas tiek į kompiuterius, tiek ir į mobiliuosius telefonus, vaizdo filmų parsisiuntimas, elektroninių žaidimų parsisiuntimas arba žaidimas elektroninėje erdvėje, nuotolinis mokymas, įskaitant virtualias mokymo klases, ir kt.

Be abejo, šis sąrašas nėra išsamus. Sukurti išsamų sąrašą nebūtų įmanoma, nes sparti informacinių technologijų plėtra suteikia vis daugiau galimybių įtraukti naujas paslaugas, kurios galėtų būti teikiamos elektroniniu būdu. Taip pat šiose gairėse buvo pateiktas sąrašas paslaugų, kurios nėra pripažįstamos kaip elektroniniu būdu teikiamos paslaugos:

Lietuvos PVM įstatymas nepateikia elektroniniu būdu teikiamų paslaugų apibrėžimo, tačiau 13 straipsnio 6 dalies 8 punkte pateiktas sąrašas pagrindinių paslaugų, kurios priskirtinos prie elektroniniu būdu teikiamų paslaugų:

> *„…interneto puslapių kūrimas ir jų priežiūra, kompiuterinių programų tiekimas, jų atnaujinimas ir priežiūra, prieigos prie duomenų bazių teisės suteikimas, muzikos kūrinių, filmų, žaidimų tie-*

kimas, nuotolinis mokymas ir kt. Jeigu tiekėjas ir pirkėjas bendrauja elektroniniu būdu, tačiau pati prekė patiekiama arba paslauga suteikiama ne elektroniniu būdu, toks bendravimas nelaikomas elektroniniu būdu suteiktomis paslaugomis“.

Kita koncepcija dėl virtualių prekių priskyrimo prekių arba paslaugų kategorijai teigia, kad virtualiosios prekės turi būti traktuojamos ne kaip paslaugos, o kaip prekės. Tokio požiūrio laikosi JAV ir Japonija, kurios prekių nesieja su materialia jų išraiška. Pasaulinė informacinių technologijų ir paslaugų sąjunga (toliau WITSA) vartojimo mokesčio atžvilgiu virtualias prekes taip pat linkusi priskirti prekių kategorijai. Teisinėje bazėje įtvirtintą ES požiūrį kritikuoja ir kai kurie mokslininkai.

Nors galutinėje EBPO ministrų konferencijos išvadoje virtualios prekės priskiriamos paslaugų kategorijai, tačiau buvo išreikšta ir priešinga nuomonė. Jei viena iš sandorio šalių užsako kitai sandorio šaliai sukurti turtą (elektroninėje komercijoje šiuo turtu galime laikyti programinės įrangos sukūrimą ir pan.) ir pirmoji sandorio šalis valdo šį turtą nuo jo sukūrimo momento, tuomet tokio turto pristatymas pirmajai sandorio šaliai bus traktuojamas kaip paslaugos teikimas. Jei toks turtas bus sukurtas ne vienai sandorio šaliai pagal užsakymą, o parduodamas daugeliui vartotojų (pažymėtina, kad dažniausiai būtent taip vyksta automatizuoti pardavimai elektroninėje komercijoje), jis turėtų būti traktuojamas ne kaip paslaugos teikimas, o kaip prekės pristatymas.

Kaip matyti iš anksčiau pateiktų argumentų, virtualių prekių traktavimas turi įtakos pridėtinės vertės mokesčiui. Akivaizdžiausiai tai matoma nagrinėjant sumažintus kai kurių prekių mokesčių tarifus. Standartinių ar sumažintų mokesčių tarifų pritaikymas prekėms, tiekiamoms elektroniniu būdu ar fiziškai, t. y. knyga, parduota popierine forma arba parsisiųsta iš interneto kaip tekstinis failas, lemia skirtingų mokesčių tarifų taikymą prekėms, kurių turinys toks pat, tačiau skiriasi jų išraiškos bei pristatymo forma.

Lietuvos Respublikos pridėtinės vertės mokesčio įstatymo 3 dalies 2 punktas numato vieną iš prekių rūšių, kuriai taikomas lengvatinis 5 procentų PVM tarifas:

„knygoms (įskaitant brošiūras, lapelius ir panašius spaudinius, vaikiškas knygeles su paveikslėliais, piešimo ir spalvinimo knygeles, spausdintas ar rankraštines natas, žemėlapius, hidrografijos arba pa-

našias schemas, išskyrus gaublius, kalendorius, užrašų knygeles ir kitus panašaus pobūdžio spaudinius), laikraščiams, žurnalams ir kitiems periodiniams leidiniams, išskyrus erotinio ir smurtinio pobūdžio leidinius, kuriuos tokiais pripažino teisės aktų įgaliota institucija, bei spausdintą produkciją, kurioje mokama reklama sudaro daugiau kaip 4/5 viso leidinio ploto".

Šiame punkte minimos prekės ypač aktualios elektroninėje komercijoje, nes jos gali būti išreikštos skaitmenine forma bei pristatytos elektroninėje erdvėje. Tačiau tokios virtualios prekės, kitaip nei tradicinėje komercijoje, bus traktuojamos kaip elektroniniu būdu teikiama paslauga ir joms taikomas standartinis 18 procentų PVM tarifas. Panašūs lengvatiniai PVM tarifai šioms prekėms taikomi ir kitose Europos Sąjungos valstybėse.

Nuostata dėl tokio skirtingo prekių traktavimo atsižvelgiant ne į jų turinį, o į išraiškos formą bei pristatymo būdą galėtų būti laikoma kaip principo dėl vienodo traktavimo pažeidimas. Šiuo atveju, nepriklausomai nuo minėtos prekės išraiškos (skaitmeninė ar popierinė forma), savo turiniu ji bus visiškai identiška. Nuomonei, kad savo turiniu identiškoms prekėms būtų taikomi skirtingi PVM tarifai, nepritaria ir WITSA. Jos teigimu, mokesčių srityje remtina yra tokia valstybės politika, kai taikomi atitinkamai vienodi PVM tarifai, nesvarbu, kaip šios prekės pristatomos. Tokiu atveju neutralumo principas nebus pažeistas.

Taip pat reikia atskirti, kad toks prekės įsigijimas turi būti susijęs su jos parsisiuntimu ir išsaugojimu galutinio vartotojo (t. y. pirkėjo) kompiuterių sistemos kietajame diske. Be abejo, interneto teikiama galimybė, prisijungus prie internetinių svetainių, naudotis jose esančiais atitinkamais produktais (pvz., enciklopedijomis, žodynais ir kt.) be galimybės juos parsisiųsti ir išsaugoti savo kompiuterių sistemos kietajame diske, turėtų būti traktuojama kaip paslauga.

Virtualias prekes, kaip ir daugumą prekių, mes galime saugoti, sunaikinti, kopijuoti arba perduoti kitiems asmenims ir pan. Turbūt sunkiai galime įsivaizduoti paslaugą, kurią įmanoma išsaugoti arba sunaikinti. Tokio pobūdžio operacijos būdingos prekėms.

Pagrindinis argumentas, kuriuo remiantis virtualios prekės traktuojamos kaip paslaugos, yra jų nemateriali išraiška. Tačiau reikia paminėti, kad virtualių prekių priskyrimas prekių kategorijai vartojimo mokesčio atžvilgiu nebūtų išimtis ES (kartu ir Lietuvoje). Netgi tradicinėje komercijoje galimi atvejai, kai prekėms priskiriami ir kai kurie

neturintys materialios išraiškos objektai. Minėtose PVM įstatymo nuostatose tokiais objektais jau dabar yra laikomi elektros energija, dujos, šiluma. Taigi valstybės nuožiūra kai kurioms prekėms yra suteikiamos išimtys (jei pagrindine nuostata laikysime, kad prekės turi būti materialios formos). Todėl autorių, ginančių dabartiniuose teisės aktuose įtvirtintas nuostatas, pagrindinio argumento nebuvo besąlygiškai laikomasi dar iki atsirandant elektroninei komercijai.

5.4.3. Bito mokestis

Daugiausia diskusijų ir plačiausių mokslinių tyrimų susilaukė 1994 m. pirmą kartą iškelta Arthuro Cordello ir Thomaso Ide idėja dėl naujo išskirtinai elektroninei komercijai taikytino mokesčio. Šiai idėjai pritarė ir ją išplėtojo profesorius Lucas Soete'as.

Pagrindinis bito mokesčio šalininkų argumentas yra tas, kad daugumą paslaugų įmanoma teikti elektroninėje erdvėje, o kai kurias prekes (pvz., knygas, muzikinius įrašus, programinę įrangą, filmus ir kt.) galima išreikšti skaitmenine forma ir taip pat persiųsti elektronine erdve. Tradicinėje komercijoje prekės privalėdavo kirsti valstybių sienas. Taigi jų importo bei eksporto srautai būdavo lengvai kontroliuojami. Elektroninėje erdvėje valstybių sienos išnyksta. Internetu skaitmeninė prekė per trumpą laiko tarpą gali būti persiųsta iš vienos pasaulio vietos į kitą. Tačiau iki šiol egzistavusi tarpinė kontrolės grandis kertant valstybių sienas elektroninėje erdvėje tampa neįmanoma.

Siūlymai įvesti naują elektroninės komercijos mokestį pagrįsti prielaida, kad informacinės technologijos ateityje nebus tokios sudėtingos, jog nebūtų galima nustatyti informacijos srautų. Bus galima nustatyti, kuri informacija priskiriama elektroninės komercijos sandoriams ir kokiais srautais paprasčiausiai keičiamasi informacija internetu.

Pagrindinis vartojimo mokestis Europos Sąjungos šalyse yra pridėtinės vertės mokestis. Šis mokestis priklauso netiesioginiams mokesčiams ir priskiriamas Europos Sąjungos kompetencijai. PVM sistema buvo sukurta ir daug kartų tobulinta dar iki atsirandant elektroninei komercijai. Lucas Soete'as teigia, kad PVM yra pritaikytas komercijai, kur prekės turi materialiąją savo išraišką, kai įmanoma kontroliuoti prekių judėjimo srautus, sužinoti jų pristatymo vietą. Tačiau ši sistema nėra tinkama elektroninėje erdvėje vykdomai prekybai.

Naujojo mokesčio šalininkai teigia, kad iki šiol taikomą PVM sistemą gali pakeisti duomenų perdavimo pagrindu (t. y. apskaičiuojant

siunčiamos informacijos kiekį) paremta mokesčių sistema, kuri būtų taikoma tik virtualioms prekėms bei paslaugoms, teikiamoms elektroninėje erdvėje. Tokiu atveju naujasis mokestis būtų proporcingas informacinėmis technologijomis perduodamos informacijos kiekiui.

Arthuras Cordellas pasiūlė 0,000001 cento[16] už 1 bitą mokesčio dydį (tai sudaro 1 centą už 1 megabitą informacijos). 1995 m. duomenimis, *„Hewlett–Packard“* bendrovė per metus turėtų sumokėti 4,8 milijono JAV dolerių už 480 terabitų persiųstos informacijos.

Autoriai pateikia ir papildomų argumentų, kuriais remiantis būtų priimtinas bito mokestis:

1. Papildomos pajamos, gautos taikant bito mokestį, padėtų valstybėms užtikrinti socialinę darbuotojų apsaugą, sukurtų naujas darbo vietas, leistų sėkmingiau kurti informacinę visuomenę ir užtikrinti socialinį aprūpinimą.
2. Šio mokesčio įvedimas turėtų teigiamos įtakos užtikrinant intelektinės nuosavybės apsaugą. Informacinių technologijų galimybės leidžia vartotojams sukurti skaitmeninių darbų kopijas, kurios yra visiškai identiškos originalui, ir be didelių išlaidų persiųsti dideliam skaičiui asmenų arba sudaryti sąlygas, kad šios kopijos būtų visiems prieinamos elektroninėje erdvėje, įskaitant ne tik naudojimąsi jomis, bet ir parsisiuntimą į kompiuterių sistemos kietąjį diską.
3. Bito mokestis turėtų teigiamos įtakos gerinant darbuotojų, turinčių priėjimą prie interneto, darbo kokybę. Tai apribotų darbuotojų lankymąsi internetinėse svetainėse, kurios nėra susijusios su jų vykdomu darbu. Darbdaviams tai leistų veiksmingiau naudotis elektroninėmis komunikacijomis.
4. Viena iš problemų yra ta, kad internete labai sparčiai didėja informacijos srautai, priskiriami „informacijos šiukšlėms“. Naujasis mokestis iš dalies apribotų nereikalingos informacijos plitimą ir apsaugotų internetą nuo perkrovos informacija.

Anot B. J. ter Weelo, pagrindinės kliūtys, neleidžiančios sėkmingai taikyti naujojo mokesčio, skirto tik elektroninei komercijai, yra šios:

1. Mokestis, paremtas informacijos persiuntimu, ekonomiškai nėra susijęs su prekės verte.
2. Neegzistuoja jokie mokesčiai, kurie būtų taikomi kitais meto-

[16] Autorius naudojo Jungtinių Valstijų valiutą.

dais siunčiamai informacijai (pvz., telefaksu siunčiamai informacijai).

3. Tai mokestis, kuris varžytų žodžio laisvę. Dėl šio mokesčio privatūs vartotojai atsidurtų nepalankioje padėtyje – jie būtų prilyginti verslininkams neatsižvelgiant į skirtumus, esančius tarp šių subjektų.
4. Tai ne tik neskatintų, bet ir varžytų naudojimąsi internetu. Ši pasekmė atsirastų dėl ekonominio neefektyvumo. Elektroninės komercijos neefektyvios raidos tikimybė padidėtų dėl keleto priežasčių: būtų dirbtinai mažinamas siunčiamos informacijos srautas naudojant archyvavimo programas; kitas ekonominis iškraipymas galėtų būti, kai bendrovės steigs vidinius komunikacinius tinklus, siekdamos išvengti mokesčių.
5. Bito mokestis gali turės įtakos žmonių naudojimuisi internetu. Siekiant išvengti šio mokesčio, dalis informacijos vėl bus siunčiama popierinėse arba kitose laikmenose. Tai turės neigiamų pasekmių aplinkai (pvz., padidės medienos naudojimas popieriaus gamybai).
6. Šį mokestį bus sunku įgyvendinti praktikoje. Naudojantis informacinių technologijų teikiamomis galimybėmis bus siekiama nuslėpti siunčiamų bitų skaičių.
7. Šis mokestis, jei jis nebus naudojamas visame pasaulyje, gali iškreipti konkurenciją, t. y. sandorių elektroninėje erdvėje sudarinėjimas gali būti perkeltas į tą jurisdikciją, kurioje nėra bito mokesčio.

Siūloma naujojo mokesčio sistema šiuo metu praktikoje nėra taikoma nė vienoje valstybėje. Dar 1998 m. Europos Komisijos padarytame pranešime EBPO ir Pasaulinei prekybos organizacijai buvo pažymėta, kad elektroninės komercijos atsiradimas ir siekis kuo veiksmingiau ją apmokestinti neturėtų būti paremtas naujojo mokesčio įvedimu. Tais pačiais metais birželio mėnesį šį principą patvirtino ir ECOFIN taryba. 1998 m. JAV priėmė teisės aktą, kuriame įtvirtino nuostatą, kad elektroninė komercija negali būti apmokestinama naujais mokesčiais. Žaliojoje knygoje, skirtoje Pietų Afrikos Respublikai, pažymima, kad šiuo metu nėra būtinybės įvesti naujus mokesčius elektroninei komercijai apmokestinti.

Norint veiksmingai apmokestinti naująją komercijos formą, užtektų atlikti pakeitimus dabartiniuose teisės aktuose. Tokios pat nuomonės laikosi ir Didžioji Britanija. Portugalija, savo teisės aktuose

įtvirtindama panašias nuostatas, siekia skatinti elektroninę komerciją remdamosi laisvos rinkos taisyklėmis ir apriboti valstybei galimybę piktnaudžiauti nustatant teisines taisykles, kai jos nėra būtinos norint efektyviai apmokestinti elektroninę komerciją.

Norint veiksmingai apmokestinti naująją komercijos formą, užtektų atlikti pakeitimus dabartiniuose teisės aktuose. Tokios pat nuomonės laikosi ir Didžioji Britanija. Portugalija, savo teisės aktuose įtvirtindama panašias nuostatas, siekia skatinti elektroninę komerciją remdamasi laisvos rinkos taisyklėmis ir apriboti valstybei galimybę piktnaudžiauti nustatant teisines taisykles, kai jos nėra būtinos norint veiksmingai apmokestinti elektroninę komerciją.

5.4.4. Elektroninių paslaugų apmokestinimas pridėtinės vertės mokesčiu

PVM kritika dėl neveiksmingumo elektroninėje komercijoje iš esmės buvo pagrįsta tuo, kad neįmanoma nustatyti antrosios sandorio šalies, t. y. pirkėjo. Informacinės technologijos leidžia nustatyti tik kompiuterių sistemos IP, bet jokiu būdu ne subjektą, kuris juo naudojasi.

Europos Sąjungoje priimta Šeštoji direktyva „Dėl pridėtinės vertės mokesčio“ atsižvelgė į elektroninės komercijos raidą ir įtvirtino teisines nuostatas, kurios turėtų sureguliuoti elektroninių paslaugų apmokestinimą PVM. Kaip jau minėjome, remiantis šia Direktyva bet kokios skaitmeninės prekės, parduodamos elektroninėje erdvėje, prilyginamos elektroninėms paslaugoms. Lietuvai įstojus į ES, šios teisinės nuostatos buvo užfiksuotos ir Lietuvos teisės aktuose.

Nuo 2004 m. gegužės 6 d. Lietuvos Respublikos teritorijoje įsigaliojo „Pridėtinės vertės mokesčio įstatymas“ (toliau PVM įstatymas), kurio 13 straipsnio 1 dalis įtvirtina bendrą taisyklę dėl paslaugų suteikimo vietos. Tokia vieta laikoma suteikta Lietuvoje, jei:

> *„…paslauga yra suteikta šalies teritorijoje, jeigu paslaugos teikėjas yra įsikūręs šalies teritorijoje, t. y. jeigu paslaugos teikėjo buveinė (jeigu tai ne fizinis asmuo) arba nuolatinė gyvenamoji vieta (jeigu tai fizinis asmuo) yra Lietuvos Respublikoje…“*

Atsižvelgiant į šią nuostatą, prievolė apskaičiuoti PVM ir sumokėti į biudžetą tenka paslaugų teikėjui.

Minėto straipsnio 6 dalis numato, kaip turi būti nustatoma elektro-

niniu būdu teikiamų paslaugų vieta, kai jas teikia užsienio apmokestinamasis asmuo:

> *„Jeigu šioje dalyje išvardytas paslaugas ne šalies teritorijoje įsikūręs paslaugų teikėjas arba šalies teritorijoje įsikūręs paslaugų teikėjas per padalinį užsienio valstybėje teikia Lietuvos Respublikos apmokestinamiesiems asmenims (išskyrus tuos atvejus, kai paslaugos suteikiamos šių asmenų padaliniams, esantiems už šalies teritorijos ribų) arba užsienio apmokestinamųjų asmenų padaliniams, esantiems šalies teritorijoje, laikoma, kad paslaugos suteiktos šalies teritorijoje“.*

13 straipsnio 6 dalies 8 punkte minimos elektroniniu būdu teikiamos paslaugos, kurioms taikoma anksčiau pateikta teisinė norma. Remiantis PVM įstatymo 95 straipsnio 2 dalimi, prievolė apskaičiuoti PVM ir sumokėti į biudžetą tenka paslaugų pirkėjui.

> *„Paslaugų pirkėjas, jeigu jis yra apmokestinamasis asmuo, privalo apskaičiuoti ir sumokėti į biudžetą PVM už jam užsienio asmens šalies teritorijoje teikiamas paslaugas, nurodytas šio Įstatymo 13 straipsnio 6 ir 9 dalyse“.*

Esant šioms teisinėms nuostatoms, elektroninių paslaugų teikėjai negali registruotis ES valstybėje narėje, kurioje yra taikomas mažiausias PVM tarifas. Tai aktualu, nes elektroninėje komercijoje bendrovėms ypač lengva perkelti savo verslą į kitas valstybes. Taip pat dauguma elektroninių paslaugų teikiama būtent apmokestinamiesiems asmenims. Remiantis J. Owenso apskaičiavimais, jos sudaro apie 80 proc. visų elektroniniu būdu teikiamų paslaugų. Jeigu elektroniniu būdu teikiamoms paslaugoms būtų taikoma bendra taisyklė, labai tikėtina, kad bendrovės, norėdamos mokėti mažesnius PVM mokesčius, perkeltų savo verslo buveines į mažiausią PVM tarifą taikančias ES valstybes nares.

PVM įstatymo 13 straipsnio 7 dalis taip pat įtvirtina nuostatą ir dėl paslaugų suteikimo neapmokestinamiesiems asmenims, kai jas teikia už ES ribų esantys asmenys:

> *„…elektroniniu būdu teikiamos paslaugos laikomos suteiktomis šalies teritorijoje ir tuo atveju, kai jas asmeniui, kuris nėra apmokestinamasis asmuo, kurio buveinė (jeigu tai ne fizinis asmuo) arba nuolatinė gyvenamoji vieta (jeigu tai fizinis asmuo) yra Lietuvos Respublikoje, teikia įsikūręs už Europos Bendrijų teritorijos ribų asmuo arba kai paslauga teikiama per padalinį, esantį už Europos Bendrijų teritorijos ribų“.*

Paslaugų suteikimo vietos nustatymui taip pat didelę įtaką turi ir tai, kam yra teikiamos tokio pobūdžio paslaugos – apmokestinamajam asmeniui ar ne. Pagrindiniai elektroninės komercijos modeliai yra verslas verslui (*business to business*) ir verslas vartotojui (*business to consumer*). Atsižvelgiant į atsirandančius mokestinius santykius bei teisinį jų reguliavimą, verslas verslui gali būti apibrėžiamas kaip paslaugų teikimas apmokestinamiesiems asmenims, kurie turi teisę į PVM atskaitą, o verslas vartotojui – kaip paslaugų teikimas galutiniam vartotojui.

Elektroninės komercijos modelyje *verslas verslui* nustatyti pirkėją nesunku. Identifikuojant visuomet galima pasinaudoti duomenų bazėmis, kuriose registruojami visi juridiniai asmenys, užsiregistravę kaip PVM mokėtojai. Valstybinės mokesčių inspekcijos prie Lietuvos Respublikos finansų ministerijos viršininko 2004 m. kovo 25 d. įsakymu Nr. VA – 39 buvo patvirtintos „Europos Sąjungos valstybių narių pridėtinės vertės mokesčio mokėtojų identifikacinių duomenų tikrinimo taisyklės“.

Atsižvelgiant į elektroninės komercijos specifiką buvo priimtos papildomos teisinės nuostatos, skirtos tik šiai komercijos formai. Nuo 2003 m. liepos 1 d. Europos Sąjungoje ir nuo 2004 m. gagužės 1 d. Lietuvos Respublikoje įsigaliojo speciali elektroniniu būdu teikiamoms paslaugoms taikoma apmokestinimo schema. Ši schema, įtvirtinta PVM įstatymo XII skyriaus penktame skirsnyje „Speciali elektroniniu būdu teikiamų paslaugų apmokestinimo schema“, yra taikoma tik tais atvejais, kai tokio pobūdžio paslaugas teikia apmokestinamasis asmuo, įsikūręs už ES teritorijos, o pačios paslaugos teikiamos neapmokestinamajam asmeniui, kuris yra vienoje iš ES valstybių narių. Taigi šia schema gali pasinaudoti elektroninių paslaugų teikėjai, esantys JAV, Japonijoje, Rusijoje, Australijoje ir kt.

Pridedamosios vertės mokesčio įstatymo 2 straipsnio 38 dalis užsienio apmokestinamąjį asmenį apibrėžia kaip:

> *„…bet kokio pobūdžio ekonominę veiklą vykdantis:*
>
> *1) užsienio valstybės juridinis asmuo arba organizacija, kurių buveinė yra užsienio valstybėje ir kurie įsteigti arba kitokiu būdu organizuoti pagal užsienio valstybės teisės aktus, arba*
>
> *2) bet kuris kitas užsienyje įsteigtas, įkurtas ar kitaip organizuotas vienetas, arba*
>
> *3) fizinis asmuo, kurio nuolatinė gyvenamoji vieta nėra Lietuvos Respublika“.*

Taip pat asmuo, atitinkantis šį apibrėžimą, neturi būti užsiregistravęs kurioje nors valstybėje narėje kaip PVM mokėtojas ir negali turėti padalinio arba buveinės ES teritorijoje.

Tokia registravimosi prievolė, taikoma užsienio valstybėje esančiam neapmokestinamajam asmeniui, kelia sunkumų šiam registruojantis kiekvienoje ES valstybėje narėje. Vykdant elektroninę komerciją ekonomiškai išsivysčiusiose valstybėse, kuriose piliečių kompiuterinis raštingumas ganėtinai didelis, padidėja tikimybė, kad pirkėjai bus iš daugelio ES valstybių. Siekiant palengvinti šią naštą buvo priimta speciali elektroniniu būdu teikiamų paslaugų apmokestinimo schema. Užsienio apmokestinamasis asmuo galės pats pasirinkti, kurioje ES valstybėje narėje jis nori registruotis kaip PVM mokėtojas. Pasirinkęs vieną iš ES valstybių, jis galės nebesiregistruoti kitose (tarp jų ir Lietuvoje) (PVM įstatymo 71 str. 11 d.).

> *„Už Europos Bendrijų teritorijos ribų įsikūręs apmokestinamasis asmuo arba apmokestinamasis asmuo, per padalinį, esantį už Europos Bendrijų teritorijos ribų, šalies teritorijoje elektroniniu būdu teikiantis paslaugas asmenims, kurie nėra apmokestinamieji asmenys, ir jau įsiregistravęs PVM mokėtoju kurioje nors valstybėje narėje pagal tos valstybės narės teisės aktų nuostatas…, registruotis PVM mokėtoju Lietuvos Respublikoje neprivalo, tačiau tik tuo atveju, jeigu jo prievolė registruotis PVM mokėtoju atsiranda vien dėl tokių paslaugų teikimo“.*

Esant tokioms teisinėms nuostatoms gali kilti grėsmė, kad už Europos Bendrijų teritorijos ribų įsikūręs apmokestinamasis asmuo stengsis registruotis toje ES valstybėje narėje, kur PVM tarifas yra mažiausias. Šiuo metu ES standartiniai PVM tarifai svyruoja nuo 15 iki 25 procentų.

Už ES teritorijos ribų įsikūrusiems apmokestinamiesiems asmenims, elektroniniu būdu teikiantiems paslaugas, palankiausios šalys pagal PVM yra Liuksemburgas, Malta ir Kipras. Dauguma paslaugų teikėjų, be abejo, būtų suinteresuoti registruotis PVM mokėtojais būtent tose valstybėse ir taikyti 15 proc. PVM tarifą. Siekiant išvengti tokių sukčiavimo atvejų specialioje schemoje buvo įtvirtinta taisyklė, kad užsienio šalies apmokestinamieji asmenys, užsiregistravę vienoje iš ES valstybių narių, privalo taikyti tą PVM tarifą, kuris numatytas pirkėjo šalyje. Jei Rusijos apmokestinamasis asmuo elektroniniu būdu suteikia paslaugas Švedijos neapmokestinamajam asmeniui, o pats

yra užsiregistravęs Lietuvos valstybėje, jis privalo taikyti ne 18 proc., o 25 proc. PVM tarifą. Tokiu atveju paslaugos teikėjas per Lietuvos valstybę įsipareigos vykdyti savo mokestines prievoles visose ES valstybėse, kurioms jis elektroninėmis priemonėmis teikia paslaugas.

Visose ES valstybėse taikoma panaši registravimosi procedūra. Lietuvoje šią tvarką reglamentuoja Valstybinės mokesčių inspekcijos viršininko 2004 m. kovo 10 d. įsakymas Nr. VA – 32. Valstybinės mokesčių inspekcijos internetinėje svetainėje (adresas: www.vmi.lt) sukurtas specialus internetinis puslapis, kuriuo naudodamasis paslaugų teikėjas gali registruotis kaip PVM mokėtojas. Šioje svetainėje, užpildydamas registracijos formą, subjektas nurodo: savo pavadinimą, nuolatinės buveinės adresą ir valstybę, elektroninio pašto adresą, internetinės svetainės, per kurią vykdo elektroninę komerciją, adresą, mokesčio mokėtojo numerį (jeigu turi), asmenį ryšiams, telefono numerį, datą, nuo kurios jis nori pradėti (arba jau pradėjo) specialią apmokestinimo PVM schemą. Paslaugų teikėjas taip pat turi patvirtinti, kad jis nėra įregistruotas PVM mokėtoju kurioje nors kitoje ES valstybėje narėje. Jei asmuo atitinka visus jam keliamus reikalavimus, jis įregistruojamas PVM mokėtoju, o Valstybinė mokesčių inspekcija apie tai informuoja kitų ES valstybių atitinkamas institucijas.

Taigi ši naujai sukurta apmokestinimo schema, taikoma tik už ES teritorijos ribų esantiems apmokestinamiesiems subjektams, elektroniniu būdu teikiantiems paslaugas neapmokestinamiesiems ES valstybėse narėse įsikūrusiems subjektams, nėra privaloma. Atsisakęs šio apmokestinimo modelio, paslaugų teikėjas turi registruotis PVM mokėtoju įprastine tvarka. Tai jis turės daryti kiekvienoje ES valstybėje narėje, kurioje teikia tokio pobūdžio paslaugas.

Elektroniniu būdu pateikdamas PVM deklaraciją, paslaugų teikėjas turi nurodyti, į kokias ES valstybes nares buvo teiktos paslaugos, koks taikytinas PVM tarifas arba tarifai, kiekvienai ES valstybei mokėtinas PVM bei bendrą mokėtiną PVM sumą.

Nors, palyginti su bendra elektroninės komercijos apimtimi, tokie sandoriai sudaro tik 10 – 20 proc., tačiau būtent šioje stadijoje ir sunkiausia nustatyti pirkėją. Remiantis specialia elektroniniu būdu teikiamų paslaugų apmokestinimo schema, paslaugų teikėjas turi nustatyti neapmokestinamuosius asmenis. Neapmokestinamieji asmenys gali būti ir fiziniai, ir juridiniai asmenys (pvz., biudžetinės institucijos, kurioms suteiktų paslaugų vertė praėjusiais kalendoriniais metais neviršijo 35 000 litų ir einamaisiais kalendoriniais metais nenumatoma

šią ribą viršyti). Autoriai sutaria, kad nustatyti juridinius asmenis nėra labai problemiška elektroninėje komercijoje. Tačiau paslaugų teikėjui uždėta našta nustatyti fizinį asmenį nėra taip lengvai įgyvendinama. Netgi naudojantis pažangiomis informacinėmis technologijomis neįmanoma tiksliai nustatyti fizinio asmens. Pagal šiuo metu galiojančias teisines nuostatas ES bei Lietuvoje pardavėjas turi vadovautis ta informacija, kurią pateikia fizinis asmuo. Be abejo, fizinis asmuo gali pateikti klaidingą informaciją, nurodydamas gyvenamąją vietą kitoje valstybėje. Tokiu atveju paslaugos teikėjas taikytų tos valstybės PVM tarifą, kurią nurodė klientas. Tačiau tokio pobūdžio sukčiavimų neturėtų būti, nes fiziniai asmenys nėra suinteresuoti nurodyti neteisingus duomenis. Kad ir kokios ES valstybės pirkėju save „pristatytų“ fizinis asmuo, jis vis tiek už suteiktas paslaugas turėtų mokėti tokią pat sumą. Šiuo atveju suinteresuota šalimi galėtų būti tik paslaugų teikėjas, nes galėtų taikyti mažesnius PVM tarifus. Tačiau automatizuotame paslaugų teikimo procese jis negali turėti įtakos fiziniam asmeniui, šiam pateikiant duomenis, arba kokiu nors kitu būdu keisti informacijos turinio.

5.4.5. Nuolatinės buveinės teisinis reglamentavimas elektroninėje komercijoje

Nuolatinės buveinės institutas ir su tuo susijusi teisinės jurisdikcijos nustatymo koncepcija yra vienas iš pagrindų, padedančių nustatyti atitinkamus ryšius tarp įmonės ir užsienio valstybės, kurioje ji pradeda vykdyti komercinę ūkinę veiklą siekdama išvengti dvigubo apmokestinimo. Šiuo pagrindu pasirašomos dvišalės arba net daugiašalės[17] sutartys, suteikiančios vienai ar kitai sutarties šaliai apmokestinimo teisę.

Nuolatinės buveinės koncepcija buvo suformuluota remiantis Vokietijos nacionalinės teisės nuostatomis. Manoma, kad pirmą kartą

[17] Viena žinomiausių daugiašalių sutarčių dėl dvigubo apmokestinimo išvengimo laikoma Šiaurės šalių sutartis. Pirmieji žingsniai siekiant sudaryti tokią sutartį buvo žengti dar 1960 m. Šiaurės Tarybos šalių. Pirmą kartą ji buvo pasirašyta 1983 m. kovą ir tų pačių metų gruodį įsigaliojo. Naujoji versija buvo pasirašyta 1987 m. vasarį ir įsigaliojo 1987 m. gruodį. 1989 m. rugsėjį pasirašyta trečioji sutarties versija, kuri įsigaliojo 1989 m. gruodį. Pastaroji sutarties versija buvo pasirašyta 1996 m. rugsėjį, tačiau dėl užsitęsusio ratifikavimo proceso įsigaliojo tik 1997 m. gruodį. Sutartį yra pasirašiusios šios valstybės: Danija kartu su vietine Farerų salų vyriausybe (kaip turinčia savarankišką teisę pasirašyti sutartį), Suomija, Islandija, Norvegija ir Švedija.

nuolatinės buveinės institutas tarptautinėse mokesčių sutartyse buvo paminėtas XIX a. pabaigoje. Tai buvo tarp Vokietijos ir kontinentinės Europos valstybių pasirašytos dvišalės sutartys. Nuo 1928 m. iki 1946 m. Tautų lyga pristatė tris mokesčių sutarties projektus, kuriuose buvo pateiktos trys skirtingos nuolatinės buveinės koncepcijos. 1943 m. Meksikos projekte buvo pateiktas nuolatinės buveinės apibrėžimas, kuris visiškai atspindėjo pajamų šaltinio principu pagrįsto apmokestinimo nuostatas. Meksikos projekto apibrėžimas 1946 m. buvo pakeistas ir įtvirtintas Londono projekte. Tačiau Tautų lygos pastangos pateikti perspektyvią nuolatinės buveinės koncepciją buvo nesėkmingos.

1955 m. Ekonominio bendradarbiavimo ir plėtros organizacija (toliau – EBPO) patvirtino pirmąją rekomendaciją dėl dvigubo apmokestinimo išvengimo, 1958 m. Mokesčių komitetas pateikė savo projektą dėl nuolatinės buveinės apibrėžimo. Ši koncepcija buvo įtraukta į 1963 m. EBPO dvigubo apmokestinimo išvengimo sutarties modelio (toliau – EBPO Modelinė konvencija) konvencijos projekto 5 straipsnį. 1971 m. EBPO peržiūrėjo Modelinę konvenciją ir 1977 m. patvirtino naująjį variantą kartu su komentaru. 1963 m. bei 1977 m. EBPO modelinės konvencijos tapo 1980 m. Jungtinių Tautų modelinės konvencijos modeliais ir dar reikšmingesnės buvo sudarant 1981 m. JAV modelinę sutartį.

Vėliau, ypač sparčiai plėtojantis technologijoms, įvyko esminių pokyčių dėl sandorių sudarymo tarp skirtingų valstybių. EBPO nagrinėjo bei priimdavo pataisymus dėl Modelinės konvencijos ir jos komentarų. Ši Konvencija išplito ir už EBPO narių ribų. EBPO nusprendė, kad Modelinės konvencijos pokyčiai būtų naudingi, jei būtų įtrauktos valstybės, kurios nėra EBPO narės, kitos tarptautinės organizacijos arba kiti suinteresuoti dalyviai. 1992 m. buvo pateikta „laisvų lapų“ Modelinė konvencija, kuri, kitaip nei 1963 m. ar 1977 m., nebuvo galutinė versija, o tik pirmasis žingsnis atliekant pakeitimus. 1997 m. buvo išleistas antrasis tomas, kuriame pateiktos valstybių, nesančių EBPO narėmis, pozicijos. Naujausias EBPO modelinės konvencijos apibendrintas variantas buvo paskelbtas 2000 m., tačiau jau vėliau buvo atlikti 5 straipsnio komentaro pataisymai, atsižvelgiant į elektroninės komercijos ypatybes bei praktinius sunkumus pritaikant nuolatinės buveinės institutą.

Iki XX a. pabaigos nuolatinės buveinės samprata išliko beveik nepakitusi. Pagrindinė idėja, kuria grindžiama ši koncepcija, yra ta,

kad kiekvienas, kuris gauna naudos iš tam tikros visuomenės, šiai privalo mokėti mokesčius. Nuolatinės buveinės teisinis institutas nusako būtinus kriterijus, kuriais remiantis komercinės ūkinės veiklos ryšys su tam tikra valstybe yra laikomas pakankamu, kad atsirastų reikalavimas mokėti mokesčius toje valstybėje.

Pasaulyje apmokestinimo sistemos yra grindžiamos buveinės vietos ir pajamų šaltinio principais. Paprastai mokesčių mokėtojo visame pasaulyje uždirbtos pajamos apmokestinamos toje šalyje, kurioje jis gyvena. Tačiau dauguma valstybių apmokestina ir pajamas, kurias jų teritorijoje uždirba užsieniečiai. Apmokestinimas pajamų šaltinio valstybėje mokesčių mokėtojui reikštų būtinybę laikytis užsienio mokesčių tvarkos, t. y. valstybės, kurioje uždirbtos pajamos, taikomo apmokestinimo pagrindo ir mokesčių tarifų. Jeigu pajamos yra apmokestinamos dviejose valstybėse, kurios tarpusavyje yra pasirašiusios dvigubo apmokestinimo išvengimo sutartį, apmokestinimo teisė suteikiama vienai iš jos šalių: arba buveinės valstybei (*residence – based taxation*), arba pajamų šaltinio valstybei (*source – based taxation*). Remiantis Ekonominio bendradarbiavimo ir plėtros organizacijos dvigubo apmokestinimo išvengimo sutarties modeliu bei EBPO ekspertų pastabomis, sudaryta daugelis tarptautinių sutarčių dėl dvigubo apmokestinimo išvengimo. Lietuvos Respublika nėra EBPO narė, tačiau visos sutartys dėl dvigubo apmokestinimo išvengimo grindžiamos minėta EBPO modeline konvencija. Ši Konvencija, atsižvelgiant į gautas pajamas, numato dvi taisykles, kuriomis siekiama išvengti dvigubo apmokestinimo. Pagal pirmąją taisyklę išimtinė teisė apmokestinti yra suteikiama buveinės valstybei. Pagal antrąją taisyklę šaltinio valstybė turi visišką arba dalinę teisę apmokestinti pajamas. Tuomet buveinės valstybė, siekdama išvengti dvigubo apmokestinimo, privalo atleisti nuo mokesčių.

Elektroninės komercijos išplitimas turėjo didelę įtaką tradicinei tarptautinei apmokestinimo koncepcijai, pagrįstai pajamų šaltinio valstybei suteikta apmokestinimo teise. Iš esmės pajamų šaltinis yra priskiriamas tai vietai, kurioje tiesiogiai vykdoma komercinė ūkinė veikla. Elektroninėje komercijoje dėl pirkėjų anonimiškumo bei galimybės realiuoju laiku sudaryti sandorį su bet kuria elektroninėje erdvėje prekiaujančia bendrove, neatsižvelgiant į geografinius atstumus ir skirtingas valstybių jurisdikcijas, nustatyti vietą, kur vykdoma ekonominė veikla, tampa labai sunku, o kai kuriais atvejais ir neįmanoma.

Apibendrinant galima teigti, kad apmokestinimas, grindžiamas pajamų šaltinio principu, paremtas idėja, jog valstybė turi teisę ap-

mokestinti bendrovės pajamas, kurios gaunamos iš tos valstybės subjektų, bendrovei tiesiogiai vykdant komercinę ūkinę veiklą. Apmokestinimas, grindžiamas buveinės vietos principu, paremtas koncepcija, jog valstybė turi teisę apmokestinti bendrovės pajamas, jei yra tvirtas užsienio bendrovės ir tos valstybės ryšys.

Taigi nuolatinės buveinės institutas įkurtas daug anksčiau nei atsirado elektroninė komercija, todėl daugumoje tarptautinių sutarčių, siekiant išvengti dvigubo apmokestinimo, nenurodoma, kad nuolatinės buveinės sąvoka apima ir serverį, kuriuo bendrovė vykdo komercinę ūkinę veiklą. Vienintelis bendrovę siejantis ryšys su užsienio valstybe gali būti prie interneto prijungtas serveris ir jame esanti internetinė svetainė. Bendrovėms, norinčioms pardavinėti savo prekes užsienyje, nebūtina turėti atskiras patalpas toje valstybėje. Toks bendrovės atstovavimas kitoje šalyje sukelia problemų dėl nuolatinės buveinės nustatymo. Todėl būtina nustatyti teisinį serverio statusą toje valstybėje, į kurią bendrovė, siekdama vykdyti komercinę ūkinę veiklą, jį perkelia. Taip pat turėtų būti apibrėžti kriterijai, kuriais remiantis serverį arba internetinę svetainę būtų galima traktuoti kaip nuolatinę buveinę.

1999 m. apie 19 Pietų Afrikos Respublikos (toliau – PAR) institucijų nagrinėjo įvairius elektroninės komercijos aspektus bei esančios teisinės bazės efektyvumą reglamentuojant nuolatinės buveinės institutą. PAR ryšių departamentas buvo įgaliotas pateikti elektroninės komercijos raidos strategiją. Šie darbai buvo atliekami remiantis 1996 m. Katz komisijos pateiktomis ataskaitomis. PAR iki šiol taikytas pajamų šaltinio principas bei egzistavusi teisinė sistema nenumatė jokių specifinių teisės normų, skirtų elektroninei komercijai apmokestinti. B. du Plessis nuomone, pateikta elektroninės komercijos raidos strategija bei galiojančios teisinės normos dar negreitai bus pritaikytos prie elektroninės komercijos ypatybių ir pajamų šaltinio principinių nuostatų. Autorius mano, kad apmokestinimas, paremtas buveinės vietos principu, padėtų išspręsti praktines problemas, kylančias norint elektroninę komerciją apmokestinti remiantis iki šiol PAR taikytu pajamų šaltinio principu.

Atsižvelgiant į elektroninės komercijos teikiamas naujas galimybes tarptautinėje prekyboje, per siauras nuolatinės buveinės traktavimas būtų palankus įmonėms, norinčioms mokesčius mokėti rezidavimo valstybėje. Kitu atveju per platus nuolatinės buveinės koncepcijos suvokimas ekonomiškai išsivysčiusių šalių įmonėms gali būti nepalan-

kus siekiant išplėsti komercinę ūkinę veiklą kitose šalyse.

Pagrindinius diskusijų dėl nuolatinės buveinės instituto bei apmokestinimo jurisdikcijos nustatymo šaltinius būtų galima suskirstyti į keturias rūšis:

1) EBPO plačios studijos dėl nuolatinės buveinės ir vėliau padaryti EBPO modelinės konvencijos pakeitimai;
2) pasaulio valstybių teismų praktika;
3) moksliniai darbai;
4) dvišalės ir daugiašalės tarptautinės sutartys dėl dvigubo apmokestinimo išvengimo.

Labiausiai išplėtotos studijos dėl nuolatinės buveinės, atsižvelgiant į elektroninės komercijos atsiradimą, buvo atliktos EBPO ir paskelbtos 2000 m. gruodį. Pagrindinė koncepcija yra ta, kad iki šiol egzistavusios teisinės normos dėl nuolatinės buveinės traktavimo gali būti ir toliau sėkmingai taikomos elektroninėje komercijoje. Buvo išplėstas tik šių normų aiškinimas, pagal kurį tik serveris gali būti pripažintas nuolatine buveine. EBPO siūlomoms rekomendacijoms dėl serverio pripažinimo nuolatine buveine elektroninėje komercijoje pritaria ir dauguma šalių: Lenkija, Vokietija, Švedija, Olandija ir kt.

Dauguma valstybių pritaria EBPO siūlomam komercinės ūkinės veiklos vietos interpretavimui, t. y. minėtą vietą galima apibūdinti tik kaip fizinį objektą. Tačiau kaip pirmosios nuomonės alternatyvą būtų galima laikyti Australijos pasirinktą poziciją. Šis požiūris sietinas su lankstesniu komercinės ūkinės veiklos vietos interpretavimu, pagal kurį ir fizinės išraiškos neturintis objektas galėtų būti komercinės ūkinės veiklos vieta. Tokiu atveju internetinė svetainė taip pat galėtų būti traktuojama kaip nuolatinė buveinė. Portugalija, Ispanija taip pat pareiškė, kad nėra būtina fizinė objekto išraiška norint jį traktuoti kaip nuolatinę buveinę.

Trečiąją poziciją šiuo klausimu yra pateikusios Airija ir Didžioji Britanija. Jų manymu, serveris neturėtų būti traktuojamas kaip nuolatinė buveinė. Didžiosios Britanijos vyriausybė ne tik paneigė galimybę serverį pripažinti nuolatine buveine, bet ir argumentavo, kad negali būti išvestos paralelės tarp smulkių prekių automatų bei lošimo mašinų ir elektroninės komercijos. Jos nuomone, tokie įrenginiai, kurie buvo naudojami iki atsirandant elektroninei komercijai, yra labiau nei serveris susiję su konkrečia vieta. Pardavėjai, kurie keistų savo prekybos vietą kiekvieną savaitę, greitai prarastų klientus. Dėl serverio pirkėjui nėra jokio skirtumo, nes naudodamasis internetu jis iš bet

kurios vietos gali prisijungti prie šio serverio.

Didžiosios Britanijos vyriausybės nuomone, veikla, iš kurios bendrovė gauna pelną, yra priskirtina tai vietai, kur yra bendrovės įstaiga, arba vieta, kur atliekami pagrindiniai tyrimai.

Airijos nuomone, serverį pripažinus nuolatine buveine gali būti, jog Airija praras galimybę apmokestinti bendrovių pajamas, jei bendrovės savo komercinę ūkinę veiklą iš šios valstybės perkels į kitą. Labiausiai tai nulemtų mažesni mokesčiai kitose valstybėse. Taip pat didelę įtaką turėtų ir mažos išlaidos, reikalingos bendrovei pradėti verslą kitose šalyse.

Šiek tiek kitokią poziciją šiuo klausimu yra pasirinkusi Indija. Iki elektroninei komercijai pasiekiant dabartinį mastą, Indijoje vyravo nuostata, kad subjektas, norintis turėti nuolatinę buveinę, nebūtinai turi reziduoti toje valstybėje. Pelnas būdavo apmokestinamas net jei bendrovė ir neturėdavo toje šalyje fiziškai išreikštos buveinės. Indijos kompetentingos institucijos traktuoja, kad bendrovės, teikiančios paslaugas elektroninėje erdvėje ir esančios už šalies ribų, turi virtualią nuolatinę buveinę Indijoje. Tokiu atveju mokestis, kuris gaunamas iš Indijos vartotojų, yra bendrovės pelnas ir turi būti apmokestinamas toje šalyje. Deja, virtualios nuolatinės buveinės sąvoka nėra tiksliai apibrėžta ir jos nustatymas kelia didelių sunkumų pačiai valstybei bei elektroninės komercijos sandorių šalims.

Reikia pažymėti, kad toks požiūris visiškai atitinka apmokestinimo, pagrįsto pajamų šaltinio principu, pagrindinę nuostatą – bendrovė, gaudama pelną iš Indijos piliečių, Indijai privalo mokėti mokesčius. Tačiau elektroninė komercija pasižymi tuo, kad nėra galimybių identifikuoti visus bendrovės klientus ir nustatyti pelno dalį, gaunamą iš vienos ar kitos valstybės subjektų.

Kol kas nėra galimybės nustatyti, kokia bendrovės pelno dalis yra gauta iš konkrečios valstybės piliečių. Todėl toks Indijos požiūris jokiu būdu nepadėtų išvengti dvigubo apmokestinimo, nes tą pačią pelno dalį sieks apmokestinti ir tos valstybės, kurių teritorijoje bendrovė turi serverį (šių valstybių argumentai paremti EBPO pateiktomis rekomendacijomis).

Šis Indijos pavyzdys gerai atspindi valstybės reakciją į naujai susiklosčiusią komercinę padėtį. Valstybė siekia neprarasti pagrindo apmokestinti užsienio bendrovių, kurios nereziduoja toje šalyje, bet elektroniniu būdu turi galimybę prekiauti šalies rinkoje.

5.4.6. Internetinių paslaugų teikėjas ir priklausomo agento statusas

Bendrovės savo veiklą kitoje valstybėje dažnai vykdo naudodamosi fizinių arba juridinių asmenų (toliau – agentai) paslaugomis. EBPO modelinė konvencija numato galimybę tokias agentų paslaugas pripažinti kaip užsienio įmonės nuolatinės buveinės egzistavimą toje šalyje, kur veikia agentas. Elektroninėje komercijoje tokio agento statusą daugiausia turi internetinių paslaugų teikėjai (toliau – IPT), iš kurių įmonės dažnai nuomojasi serverius, vykdydamos savo veiklą užsienio šalyje. Tačiau, norint turėti nuolatinę buveinę kitoje šalyje, susijusią su agento paslaugomis, agentas turi būti priklausomas nuo įmonės, kuriai jis teikia paslaugas. Šiuo atveju nėra taikomas pastovios komercinės ūkinės veiklos vietos reikalavimas.

Remdamiesi teisės normomis, kurios iki šiol reglamentavo agento, kaip nuo bendrovės priklausomo subjekto, statusą, galime išskirti šiuos reikalavimus, kuriuos minėtas agentas turi atitikti:

- turi būti valstybės teritorijoje (asmuo gali būti ir fizinis, ir juridinis);
- turi veikti užsienio bendrovės vardu ir jos naudai;
- turi turėti įgaliojimą sudaryti sandorius užsienio bendrovės vardu;
- turi nuolat naudotis šiuo įgaliojimu;
- turi būti priklausomas nuo užsienio bendrovės.

Reikia pažymėti, kad ne visos bendrovės gali naudotis IPT teikiamomis paslaugomis. Didžiosios bendrovės dažniausiai elektroninėje komercijoje naudojasi ne vienu, o keliais serveriais, esančiais skirtingose pasaulio šalyse, taip pat įmonės patentuota programine ar technine įranga, kuriomis veiksmingiau gali valdyti duomenų srautus. IPT personalas nėra specializuotas vykdyti tokias komercines operacijas. Jų veikla pirmiausia grindžiama techninės bazės užtikrinimu, kad galėtų tinkamai funkcionuoti serveris. Bendrovės nepatiki kitiems subjektams patentuotos programinės arba techninės įrangos. Tokiais atvejais bendrovės dažniausiai pačios nuosavybės teise valdo serverius, esančius užsienio valstybėse, o jų personalas užtikrina techninės įrangos funkcionavimą arba net ir komercinių sandorių sudarymą.

Tačiau dauguma bendrovių naudojasi IPT paslaugomis. Labiausiai paplitę elektroninės komercijos modeliai, kai užsienio bendrovės nuomoja serverį arba tam tikrą serverio atminties dalį, kur įdeda savo

internetinę svetainę, o IPT užtikrina šios įrangos funkcionavimą. Šiuo atveju IPT veiksmai atitinka EBPO modelinės konvencijos 5 straipsnio 4 dalyje numatytus pagalbinio pobūdžio veiksmus. Užsienio bendrovės internetinių paslaugų teikėjams dažniausiai nesuteikia įgaliojimų sudaryti sandorius su pirkėjais. Tačiau reikia pažymėti, kad ir pati bendrovė tiesiogiai šių sandorių taip pat nesudarinėja. Šiuos veiksmus savarankiškai atlieka automatizuota programinė įranga. Bet pagrindinę įtaką įrangos egzistavimui, jos atliekamų operacijų apimčiai bei savarankiškumui turi bendrovės sprendimai.

IPT, atlikdami savo veiklą, gali teikti paslaugas ne vienai, o kelioms užsienio bendrovėms. Dažnai kelios bendrovės iš karto viename serveryje laiko savo internetines svetaines, kurių priežiūra rūpinasi tas pats internetinių paslaugų teikėjas. Tvarkydamas įvairių bendrovių internetines svetaines, esančias jų serveryje, IPT plėtoja savo verslą ir nesiekia naudos užsienio bendrovei. Jis veikia savo interesais ir yra visiškai nepriklausomas nuo užsienio bendrovės.

Kadangi internetinių paslaugų teikėjas neatitinka šių reikalavimų ir neturi jokių įgaliojimų, susijusių su sandorių sudarymu, jis nevykdo priklausomo agento funkcijų ir gali būti traktuojamas tik kaip nepriklausomas agentas.

Tačiau EBPO neatmeta galimybės, kad IPT, esant tam tikroms aplinkybėms, gali būti traktuojamas kaip priklausomas agentas. Šiuo atveju, remiantis anksčiau nurodytais reikalavimais priklausomam agentui, IPT turi veikti užsienio bendrovės vardu bei jos naudai, turėti įgaliojimą sudaryti sandorius ir priklausyti nuo užsienio bendrovės.

Kai kurie autoriai, tradiciškai suvokdami agentą, jog tai gali būti fizinis arba juridinis asmuo, analizuoja galimybę elektroninėje komercijoje naudojamą programinę įrangą priskirti agento kategorijai. Rezervuojant kelionės bilietus tokia programinė įranga gali pateikti kainų sąrašus, parinkti tinkamą laiką, maršrutą, palyginti turimą ir kliento pateiktą informaciją, remiantis pateikta informacija parinkti optimaliausią sprendimo variantą bei sudaryti sandorį. Kad ir kiek daug funkcijų galės atlikti programinė įranga, tačiau visuomet bus reikalinga išorinio subjekto pagalba, užtikrinanti jos funkcionavimą.

Gali būti išvedama paralelė tarp programinės įrangos atliekamų operacijų apribojimo, užtikrinamo techninėmis priemonėmis, ir tradicinių agentų atliekamų veiksmų, užtikrinamų teisinėmis priemonėmis (pasirašant sutartis), apribojimo. Taigi fizinis arba juridinis asmuo sandoryje dalyvauja kaip vienas iš sandorio šalių, turi tam tikras teises bei prisiima atitinkamas pareigas, jam gali būti taikomas teisinės atsa-

komybės institutas. O programinė įranga negali būti teisinių santykių subjektas. Ji gali būti traktuojama tik kaip bendrovei nuosavybės teise priklausantis turtas.

Nors programinės įrangos atlieka ganėtinai daug veiksmų ir klientas iki galo gali užbaigti sandorio sudarymą, tačiau programinės įrangos nesavarankiškumas bei teisinio statuso nebuvimas neleidžia jos traktuoti kaip priklausomo agento, kuris sukurtų nuolatinės buveinės institutą užsienio šalyje. O IPT elektroninėje komercijoje neįgauna išskirtinių savybių, dėl kurių jam nebūtų galima taikyti tradicinių teisės normų, nekeičiant iki šiol egzistavusio jų aiškinimo.

5.4.7. Nuolatinė buveinė ir personalas

2000 m. EBPO modelinės konvencijos 5 straipsnio papildomame komentare, kuriame atsižvelgiama į elektroninės komercijos įtaką tarptautiniams mokestiniams santykiams, įtvirtinta su užsienio bendrovės personalo buvimu valstybėje susijusi nuostata, kurioje yra serveris kaip nuolatinė buveinė. Tradicinėje komercijoje sunku būtų įsivaizduoti fiksuotą verslo vietą, kuriai nereikėtų jokio žmogaus įsikišimo. Elektroninėje komercijoje automatizuoti procesai leidžia atlikti visas komercines operacijas be personalo veiksmų. Todėl EBPO, papildydama komentarą, patvirtino, kad personalo buvimas arba jo atliekami veiksmai nėra privalomi, kad serverį būtų galima traktuoti kaip nuolatinę buveinę. Tačiau panaši nuostata buvo sukurta dar iki atsirandant elektroninei komercijai. Daugiausia ji buvo taikoma lošimo ir smulkių prekių automatams. Tačiau reikia paminėti, kad ir kiti įrenginiai galėjo būti priskiriami tai įrangos kategorijai, kuri leistų atsirasti nuolatinės buveinės institutui toje šalyje. Viena iš tokių bylų buvo nagrinėjama Vokietijoje. Joje buvo priimtas sprendimas, kad užsienio bendrovė turi nuolatinę buveinę Vokietijoje, per kurią driekiasi tos bendrovės naftotiekis, nors šis yra reguliuojamas Olandijoje esančio kompiuterio. Olandijoje esanti bendrovė niekada nesamdė priklausomo agento, esančio Vokietijoje. Vokietijos teismo priimtas sprendimas neatspindi visų EBPO narių požiūrio. Olandijoje galiojo teisinės nuostatos, pagal kurias naftotiekis nebūtų priskirtas nuolatinei buveinei.

Po EBPO modelinės konvencijos komentaruose padarytų pakeitimų, susijusių su elektronine komercija, ši nuostata išliko nepakitusi. Tačiau jos taikymas buvo išplėstas ir prie šių automatinių mechanizmų (įrenginių) buvo priskiriamas ir serveris.

Norint užtikrinti automatinių įrenginių funkcionavimą, neišvengiamai reikalingas ir personalas. Tačiau savo komentaruose EBPO yra nustačiusi, kad automatinius įrenginius norint traktuoti kaip nuolatinę buveinę personalo veikla gali būti apribota tik atliekant tam tikras operacijas: surenkant įrenginius, montuojant, eksploatuojant, remontuojant ir kt. Ši personalo veikla apsiriboja tik techninės įrangos priežiūra ir visiškai nesusijusi su verslo operacijomis, kurios vykdomos automatiniais įrenginiais. Be abejo, gali būti samdomi nepriklausomi darbuotojai (neturintys priklausomo agento statuso), kad užtikrintų įrenginių funkcionavimą.

Rosemarie Portner pateikia kitą poziciją, pagal kurią pats serveris negali būti traktuojamas kaip nuolatinė buveinė, išskyrus tuos atvejus, kai toje šalyje dirba ir asmenys. Šis požiūris prieštarauja EBPO pateiktai nuostatai, kad nuolatinė buveinė gali egzistuoti ir tuo atveju, jei bendrovės verslas kitoje valstybėje vykdomas tik naudojant automatinę įrangą. R. Portner nuomone, tarp lošimo bei smulkių prekių automatų ir serverio yra reikšmingas skirtumas, todėl jų lyginti negalima. Serveriui, kitaip nei kitiems įrenginiams, reikalinga programinė įranga, kuri galėtų užtikrinti vykdomas operacijas. R. Portner taip pat teigia, kad serverio pripažinimui nuolatine buveine yra keliami ir kiti reikalavimai, susiję su personalu. Šalia esantis personalas turi atlikti ne tik pagalbinio pobūdžio darbus, užtikrinančius įrangos techninę priežiūrą, bet ir kitus darbus, kurie turėtų įtakos bendrovės vykdomam verslui.

Panašios nuomonės laikosi ir Carolis Dunahoo kartu su kitais „Pricewaterhouse Coopers“ nariais. Jų manymu, bet kurios valstybės jurisdikcijoje nuolatinė buveinė gali egzistuoti tik tuomet, jei toje valstybėje esančių darbuotojų arba bendrovei priklausančių agentų veikla yra pakankama, kad nuolatinė buveinė būtų pripažinta. Šių agentų arba personalo atliekami veiksmai turi turėti įtakos bendrovės vykdomam verslui, o neapsiriboti vien šalutinio pobūdžio darbais.

R. Portner ir C. Dunahoo oponentai teigia, kad esamų nuostatų taikymas galėtų būti išplėstas ir taikomas serveriui, kuris kai kuriais atvejais funkcionuoja panašiai kaip ir smulkių prekių automatas. Ši analogija ypač išryškėja, kai prekiaujama virtualiomis prekėmis arba kai elektroninėje erdvėje suteikiamos paslaugos. Tuomet serveris, panašiai kaip ir prieš tai minėti kiti įrenginiai, paskirstys šių prekių pristatymą pirkėjui.

Tačiau šis skirtumas nėra reikšmingas ir neturi jokios įtakos personalo atliekamiems veiksmams dėl vieno ar kito įrenginio. Pagrindi-

nis skirtumas tarp šių įrenginių turėtų būti siejamas su kitomis EBPO pateiktomis rekomendacinėmis nuostatomis. Nuolatinė buveinė gali egzistuoti tik tuomet, jei užsienio bendrovė pati arba jos priklausomas agentas valdo serverį. Kaip jau minėjome, elektroninėje komercijoje dažnai užsienio bendrovės nuomojasi tik dalį serverio atminties, todėl, remiantis EBPO, R. Portner ir C. Dunahoo argumentais, tas pats serveris būtų nuolatinė kelių bendrovių buveinė. Vienintelis objektas elektroninėje komercijoje, kuris visuomet priklausys užsienio bendrovei nuosavybės teise, yra internetinė svetainė. Todėl personalo įtaką tikslinga nagrinėti atsižvelgiant ne į serverį, o į internetinę svetainę.

Išsiskiria dvi autorių nuomonės dėl užsienio bendrovės personalo ir nuolatinės buveinės instituto elektroninėje komercijoje santykio. Vieni autoriai (R. Portner, C. Dunahoo, L. Hinneken, M. Geurts) teigia, kad personalo buvimas yra privaloma sąlyga norint serverį pripažinti nuolatine buveine. Šiuo atveju nėra pabrėžiamas serverio ir internetinės svetainės klausimas, nes daugelis mokslininkų personalo atliekamus veiksmus bei jų įtaką komerciniams procesams sieja su serverio veikla. Tačiau reikia pažymėti, kad tie patys veiksmai glaudžiai susiję su internetine svetaine. Bendrovės teikiamų paslaugų reklamavimas, prekių užsakymas, atsiskaitymas elektroninėje erdvėje, automatizuotas prekių pristatymas bei prekių pavertimas skaitmenine forma atliekamas naudojantis programine įranga. Serveris, būdamas mechanizmu ar įrenginiu, užtikrina tik aplinką, kurioje programinė įranga gali atlikti minėtus procesus. Todėl, susiejus anksčiau minėtų autorių teiginius su pozicija, kad ne serveris, o internetinė svetainė turėtų būti pripažinta kaip nuolatinė buveinė, galima teigti, jog viena bendra nuomonė bendrovės personalo klausimu yra tokia: tam, kad internetinė svetainė būtų pripažinta kaip nuolatinė buveinė užsienio šalyje, joje turi būti ir tos bendrovės personalas.

Kitos nuomonės autoriai (EBPO darbo grupės nariai) teigia, kad serveris, nesvarbu ar toje šalyje yra bendrovės personalas, gali sukurti nuolatinę buveinę. Tokia pat nuomonė buvo įtvirtinta ir Vokietijos teisminėje praktikoje: „nėra būtini darbuotojai arba žmogaus atliekami veiksmai, kad serverį būtų galima traktuoti kaip nuolatinę buveinę“.

Tradicinėje komercijoje būtų sunku įsivaizduoti užsienio bendrovės veiklą kitoje šalyje be joje esančio personalo. Tačiau iki šiol egzistavusios nuolatinės buveinės institutą reglamentuojančios teisinės normos daugelyje valstybių nenumatė imperatyvių teisės normų, reikalaujančių personalo buvimo. Elektroninėje komercijoje šis klausimas

tampa dar aktualesnis. Visos komercinės operacijos, kurios vyksta elektroninėje erdvėje, gali būti programuojamos nuotoliniu būdu. Taip pat užsienio bendrovės personalas gali būti savoje valstybėje ir naudodamasis elektroninės komercijos teikiamomis galimybėmis nustatyti prekių arba paslaugų kainas, pateikti naujas prekes skaitmenine forma, parinkti skirtingus virtualių prekių pristatymo formatus bei atlikti kitas operacijas. Asmenys, atliekantys šias operacijas, gali būti ne tik savo šalyje (t. y. šalyje, kur įsisteigusi bendrovė) arba net trečiojoje valstybėje, bet taip pat dalį operacijų atlikti vienoje šalyje, o dalį – kitoje. Norint atlikti tokius veiksmus, asmeniui užtenka turėti nešiojamąjį kompiuterį su reikiama programine įranga bei leidimą atlikti numatytas operacijas. Šiuo atveju leidimas suprantamas ne tik teisiškai, bet ir technologiškai (pvz., slaptažodžių turėjimas). Toks personalo ir kartu atliekamų veiksmų mobilumas yra labai naudingas bendrovėms: leidžia lanksčiau reaguoti į rinkos pokyčius bei operatyviai priimti sprendimus.

Elektroninės komercijos mobilumas lemia tai, kad negalima sutikti su autorių nuomone, jog serveris, kaip nuolatinė buveinė, gali būti pripažintas tik jeigu toje šalyje yra ir užsienio bendrovės personalas. Šis požiūris sietinas su serverio mobilumo problema. Siekiant ją išspręsti pasitelkiamas bendrovės personalas, kuris leistų lengviau užtikrinti stacionarumo kriterijaus įgyvendinimą. Tačiau abu minėti objektai – ir serveris, ir personalas – elektroninėje komercijoje pasižymi dideliu mobilumu ir tai teisinių normų pritaikymą įvairiems elektroninės komercijos modeliams daro labai sudėtingą, o kartais ir neįmanomą. Todėl tik internetinės svetainės traktavimas kaip nuolatinės buveinės leidžia pastarąją lengvai nustatyti. Taigi skatinama elektroninės komercijos plėtra nepaliekant bendrovėms tradicinės komercijos apribojimų, visiškai nepriimtinų elektroninei komercijai, būtent – personalo buvimo šalyje, kur yra nuolatinė buveinė, ar serverio privalomo stacionarumo.

KONTROLINIAI KLAUSIMAI

1. Kuo skiriasi elektroninės komercijos suvokimas siaurąja ir plačiąja prasmėmis?
2. Suraskite internete tiesioginės ir netiesioginės elektroninės komercijos pavyzdžių.

3. Ar gali elektorninis dokumentas būti „originalus dokumentas?“
4. Kokie teisiniai įpareigojimai internetinių paslaugų teikėjams dėl kitų subjektų dedamos informacijos?
5. Ar teisiškai pripažįstamas dokumentas pasirašytas elektroniniu parašu?
6. Kuo skiriasi elektroninės komercijos suvokimas nagrinėjant tiesioginius ir netiesioginius mokesčius?
7. Kam skirta ir kaip funkcionuoja elektroninei komercijai taikoma naujoji pridėtinės vertės apmokestinimo tvarka?
8. Kokie bito mokesčio pranašumai ir trūkumai?
9. Kas elektroninę komercija besiverčiančiai bendrovei gali atstoti nuolatinę buveinę užsienio valstybėje?
10. Ar gali internetinių paslaugų teikėjas tapti priklausomu agentu?
11. Ar elektronine komercija besiverčiančiai bendrovei būtinas personalas užsienio valstybėje, kad joje būtų įsteigtas nuolatinės buveinės institutas?

Literatūra

Teisės aktai

1. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. Official Journal L 013, 19/01/2000.
2. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce). Official Journal L 178, 17/07/2000.
3. Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts. Official Journal L 144, 04/06/1997.
4. Sixth Council Directive of 17 May 1977 (77/388/EEC) on the harmonization of the laws of the member states relating to turnover taxes - common system of value added tax: uniform basis of assessment. Official Journal L'1977 Nr. 145–1.
5. Electronically Supplied Services. European Commission, Value Added Tax Committee (Article 29 of Directive 77/388/EEC) Guidelines TAXUD/2436/02 (Working paper n°372) // http://www.belastingdienst.nl/common/dl/gui-

delines-e-services.pdf
6. Lietuvos Respublikos elektroninio parašo įstatymas // Valstybės žinios. 2000. Nr. 61-1827.
7. Lietuvos Respublikos informacinės visuomenės paslaugų įstatymas // Valstybės žinios. 2006. Nr. 65-2380.
8. Lietuvos Respublikos pelno mokesčio įstatymas // Valstybės žinios. 2001. Nr. 110-3992 (aktuali redakcija).
9. Lietuvos Respublikos pridėtinės vertės mokesčio įstatymas // Valstybės žinios. 2002. Nr. 35-1271.
10. Valstybinės mokesčių inspekcijos prie Lietuvos Respublikos finansų ministerijos viršininko įsakymas „Dėl elektroninių paslaugų teikėjų registravimo taisyklių ir elektroninių paslaugų suteikimo pridėtinės vertės mokesčio deklaracijos užpildymo ir pateikimo taisyklių patvirtinimo“ // Valstybės žinios. 2004. Nr. 40-1318.

Kiti leidiniai ir publikacijos

1. Basu S. Taxation of Electronic Commerce // The Journal of Information, Law and Technology. 2001 (1). // http://elj.warwick.ac.uk/jilt/01-2/basu1.html
2. Beynon-Davies P. E-business. Houndmills: Palgrave Macmillan, 2004.
3. Catchpole J. The Regulation of Electronic Commerce: A Comparative Analysis of the Issues Surrounding The Principles of Establishment // International Journal of Law and IT, March 2001. Vol. 9. Iss. 1.
4. Hardesty D. A. Electronic Commerce: Taxation & Planning. 2003.
5. Käbisch W. Tax Aspects of International Electronic Commerce. ESPRIT Project 27028 – Electronic Commerce Legal Issues Platform 241 p. // http://www.eclip.org/documentsII/lawtechn/tax.zip
6. Sodžiutė L., Sūdžius V. Elektroninė komercija: prielaidos, struktūra ir procesai. Vilnius: P. Kalibato LĮ „Petro ofsetas“, 2003.
7. Civilka M., Lamanauskas T., Sauliūnas D., Štitilis D., Toliušis S. Informacinių technologijų teisė. – Vilnius: NVO teisės institutas, 2004.
8. Mann R. J., Winn J. K. Electronic Commerce. Second Edition. 2005.
9. Model Tax Convention on Income and on Capital. Condensed Version / OECD Committee on Fiscal Affair. 29 April 2000, 314 p.
10. Soete L., Kamp K. The „Bit Tax”: The Case For Further Research. 1996 // http://www-edocs.unimaas.nl/abs/mer96019.htm
11. Soete L., Weel B. Cybertax // Futures. 1998. Vol. 30. Iss. 9. P. 853–871.
12. Taxation and Electronic Commerce. Implementing the Ottawa Taxation Framework Conditions / Organisation for Economic Co–operation and Development. – 2001.
13. Ter Weel B. J. Cybertax. 1997. P. 16 // http://www-edocs.unimaas.nl/abs/mer97019.htm
14. UNCITRAL Model Law on Electronic Commerce. 2001.

6. Elektroninė demokratija ir teisinė jos aplinka

6.1. Įvadinė medžiaga. Elektroninės demokratijos sąvokos ir modeliai

Informacines technologijos suteikia visuomenei kokybiškai naujas galimybes, kurios gali padėti spręsti esamas socialines problemas, priartinti valstybinę valdžią prie piliečio poreikių ir išplėsti tradicines demokratijos ribas. Internetas atveria naujas galimybes tobulinti pilietinę visuomenę modifikuojant tradicinį demokratijos institutą į elektroninę demokratiją (toliau – ir *e. demokratiją*), padedančią piliečiams aktyviai dalyvauti kasdieniame visuomenės gyvenime ir valstybės valdyme. Internetas kiekvienam piliečiui suteikia realią galimybę dalyvauti šalies valdyme nepriklausomai nuo jo buvimo vietos ir laiko. Sukūrus reikiamą IT infrastruktūrą, piliečiai galėtų dalyvauti sprendžiant neatidėliotinas visuomenės problemas ir nelikti vien pasyviais valdžios priimamų sprendimų stebėtojais ir vykdytojais.

Elektroninės demokratijos perspektyva numato informacinių ir komunikacinių technologijų atėjimą į egzistuojančius demokratijos sektorius: elektroninę vyriausybę, elektroninės žiniasklaidos ir viešųjų interneto portalų puslapius, pilietinės visuomenės iniciatyvas, kuriančias erdvę elektroniniams piliečiams, ir kt.

Šiuo metu daug piliečių yra nusivylę įprastomis įstatymų leidybos ir politikavimo formomis, kurios yra nutolusios nuo paprastų piliečių. Todėl būtina gerinti piliečių ir valdžios atstovų tarpusavio bendravimą ir bendradarbiavimą, aktyvinti jų poreikį kuo daugiau sužinoti, dalyvauti politinėse diskusijose ir politiniame gyvenime.

Elektroninė demokratija iš esmės reiškia informacinių komunikacinių technologijų naudojimą palengvinant, gerinant ir plėtojant demokratijos procesus. Taigi vienu iš esminių elektroninės demokratijos plėtros aspektų tampa praktinis elektroninių paslaugų įgyvendinimas, paremtas infrastruktūros plėtra, informacinių technologijų panaudojimo galimybėmis ir kuriamų elektroninių paslaugų įvairove, gausa ir patrauklumu.

E. demokratija visuomenėje kartais suprantama pernelyg siauriai – vien tik kaip elektroniniai rinkimai. Plačiąja prasme e. demokratija suprantama kaip platus piliečių dialogas su valdžia ir dalyvavimas priimant valdymo sprendimus. Ji skiriama į dvi skirtingas sritis: elektroninį dalyvavimą (toliau – e. dalyvavimą) ir elektroninį balsavimą (toliau – e. balsavimą). E. dalyvavimas suprantamas kaip piliečių informavimas, konsultacijos ir dialogas elektroninėje erdvėje tarp valdžios ir piliečių, o e. balsavimas – kaip piliečių valios išraiška elektroninėje erdvėje.

6.1.1. E. demokratijos modelis

Supaprastintą elektroninės demokratijos modelį sudaro keturi sektoriai: politinės grupės, privatus sektorius, žiniasklaida ir valdžia, glaudžiai sąveikaujantys su elektroniniais piliečiais (toliau – e. piliečiais) kaip elektroninės demokratijos centru. E. piliečių sąvoka skiriasi nuo įprastinės tuo, kad jie gali pasinaudoti IKT bendraudami su valdžios ir viešojo administravimo institucijomis ir šios institucijos gali juos nustatyti elektroninėje erdvėje bei autentifikuoti jų išreikštą valią.

Tiek politinės grupės, arba partijos ir interesų grupės, tiek ir privatus sektorius, žiniasklaida bei valdžia yra tradicinės demokratijos dedamosios, taigi galima teigti, kad „e.“ prieš žodį „demokratija“ lemia informacinės ir komunikacinės technologijos bei jų panaudojimas demokratijos procese.

Ne visos šalys piliečiams ir valdžiai bendrauti naudoja IKT vienodai. Tačiau reikia pabrėžti, jog viešajame gyvenime pirmiausia pradedamos teikti elektroninės viešosios paslaugos, kuriama elektroninė valdžia, o tik vėliau plėtojama ir elektroninė demokratija. **Tokiame kontekste verta atkreipti dėmesį, kad elektroninė valdžia turėtų būti suprantama kaip platesnės e. demokratijos sąvokos dalis.**

6.2.2. E. demokratijos principai

Kuriant dalyvaujamąją elektroninę demokratiją, kurioje dalyvauja dauguma piliečių (angl. *participating democracy*), reikėtų įgyvendinti šešis principus.

Pirmasis principas: *visi ar bent dauguma piliečių turi dalyvauti priimant sprendimus*

Visi piliečiai, tiesiogiai arba netiesiogiai suinteresuoti pateiktu klausimu, turi turėti teisę dalyvauti priimant valdžios sprendimus, nepriklausomai nuo rasės, religijos, amžiaus, lyties ar profesijos. Be to, turi būti sumažintas amžiaus cenzus, kad sprendžiant tam tikrus klausimus būtų galima įtraukti ir paauglius.

Antrasis principas: bendrų interesų siekis

Kad valdymas būtų sklandus ir veiksmingas, visų dalyvaujančių piliečių požiūris turi būti paremtas abipuse pagalba. Tai reiškia, kad kiekvienas žmogus sprendžia bendras problemas atsižvelgdamas į savo interesus, bet yra pasirengęs paaukoti dalį tų interesų dėl bendro gėrio. Beje, dalyvaujamosios demokratijos nereikėtų painioti su kolektyvizmu, nes ji yra paremta pagarba kiekvieno individo laisvei bei interesams.

Trečiasis principas: visa reikiama informacija turėtų būti prieinama visuomenei

Jei problemą turi spręsti visi piliečiai, jie turi gauti visą informaciją reikiamais klausimais. Dabartinėje visuomenėje informacija, labiausiai susijusi su žmonių gyvenimu, dažnai dėl įvairių priežasčių jiems yra neprieinama. Tačiau ateityje, informacijos atvirumas visuomenei turėtų būti pagrindinė demokratijos sąlyga.

Svarbu, kad visuomenė būtų informuota ne tik apie pačius faktus, bet ir apie numatomą arba galimą vieno ar kito sprendimo socialinę, ekonominę ir kitokią įtaką žmonių gyvenimui. Tik taip kiekvienas žmogus gali ne vienpusiškai, o plačiau išsiaiškinti jam rūpimas problemas, dalyvauti priimant sprendimus atsižvelgdamas ne tik į savo asmeninius, bet ir į visos visuomenės interesus.

Ateityje bus tikimąsi, kad žmonės savanoriškai suteiks reikiamą informaciją sprendžiant vieną arba kitą klausimą.

Ketvirtasis principas: visa gauta nauda turi būti padalinta piliečiams

Visos valdžios problemos iš esmės yra sudėtingos ir jų sprendimo būdai žmonėms turi skirtingą poveikį – vieni ką nors laimi, kiti pralaimi. Todėl reiktų stengtis suderinti piliečių ir jų grupių gaunamą naudą.

Penktasis principas: sprendimo reikėtų siekti sutarimu ir įtikinimu

Bet koks sprendimas rūpimu klausimu turėtų būti priimamas pri-

tarus visiems arba daugumai. Norint pasiekti sutarimą, reikia kantrybės ir pastangų. Dabartinėje parlamentinėje demokratijoje valdančiosios ir opozicinės partijos, priimdamos sprendimus svarbiais klausimais, dažnai pasiekia kompromisus. Tačiau elektroninės demokratijos visuomenėje sprendimai privalo būti priimti visų piliečių sutarimu bei įtikinimo metodu. Tačiau norint tai pasiekti reikia laikytis jau minėtųjų sąlygų – bendradarbiavimo, tarpusavio pagalbos, visos reikiamos informacijos prieinamumo bei naudos lygaus padalijimo.

Šeštasis principas: priėmus sprendimą, iš visų piliečių tikimasi bendradarbiavimo įgyvendinant sprendimą

Ši pareiga yra tiesioginio dalyvavimo priimant sprendimus išvada. Žmogus laisva valia turi apriboti savo interesus, bet tai neturėtų įgauti prievartos atspalvio, kaip yra dabartinėje visuomenėje. Dalyvavimas priimant sprendimus ir priimto sprendimo laikymasis laisva valia yra neatskiriami. Šie principai turėtų būti naujos sprendimų priėmimo ir socialinės tvarkos informacinėje visuomenėje pagrindas. Šį socialinės etikos kodeksą pažeidę piliečiai neturėtų būti baudžiami, bet iš jų turėtų būti reikalaujama kompensuoti savo veiksmus kokiu nors socialiniu įnašu arba paslauga visuomenei. Apibendrinant galima teigti, kad elektroninė demokratija yra piliečių interesų gynimo bei integracijos į sociumą priemonė ir tam tikra bendradarbiavimo su valstybe forma, paremta informacinėmis technologijomis diegiant valdžią.

6.2. Pagrindinė medžiaga. E. demokratijos teisinės problemos

6.2.1. Elektroninės demokratijos įrankiai

E. dalyvavimo modeliai

Elektroninėje demokratijoje piliečiai traktuojami kaip partneriai, aktyviai įtraukiami į politikos formavimo procedūras. Tai daugelio šiuolaikinių valstybių siekinys, kuris realiai bandomas įgyvendinti kol kas tik nedaugelyje šalių.

Galima išskirti tris piliečių įtraukimo į elektroninį dalyvavimą lygius pagal piliečiams suteikiamas galias ir įtakos mastą:

1) vienkryptis informacijos teikimas – informacija valdžios institucijų svetainėse. Keliami reikalavimai informacijai – ji turi būti su-

prantama ir prieinama kuo didesniam gyventojų skaičiui. Dėmesys sutelkiamas ir į skaitmeninę atskirtį – į tuos piliečius, kurie dar neturi galimybių naudotis internetu.

2) dvikryptis bendravimas – konsultacijos, kai piliečiai siunčia valdžios institucijoms savo atsiliepimus dėl priimamų sprendimų projektų. Čia IKT naudojamos ryšiui su piliečiais užmegzti. Dėl technologijų konsultacijos su piliečiais yra plačiau prieinamos, valdžios institucijos taip gali sužinoti visuomenės reakciją į politines iniciatyvas. Konsultacijos inicijuojamos ne pačių piliečių, o valdžios institucijų arba parlamento. Valdžios ir piliečių ryšys – „iš viršaus į apačią".

3) piliečiai suprantami kaip valdžios partneriai, pripažįstama piliečių teisė keisti svarstomų klausimų darbotvarkes, teikti politinius pasiūlymus, reikšti savo valią įvairiais klausimais. Nors piliečiams suteikiama galia siūlyti savo idėjas iš „apačios į viršų", atsakomybė už galutinį politikos formavimą tenka vyriausybei.

Siekiant užtikrinti e. dalyvavimo skaidrumą, išvengti apgavysčių, nepateikti klaidingų piliečių nuomonių, tų pačių vieno asmens pakartotinų siūlymų, būtina piliečio identifikacija ir jo reiškiamos valios bei siūlymų autentifikacija. Kartu valstybės institucijos turi daugiau dėmesio skirti asmens duomenų saugumui.

Elektroniniai dalyvavimo forumai

Dar vienas e. demokratijos įrankis, skatinantis piliečius būti aktyviais visuomenės nariais – e. forumai. E. forumai gali būti organizuojami valdžios institucijų (populiariausia vietinio lygio) arba nevyriausybinių organizacijų.

Pavyzdžiui, Vokietijos Eslingeno (*Esslingen*) miesto valdžia, pasinaudodama IKT, siekia įtraukti piliečius į sprendimų priėmimo procesus ir taip teikti geresnes paslaugas visuomenei. Pasirinkta forma – virtualūs diskusijų kambariai, kuriuose piliečiai gali diskutuoti dėl vietos politikos aktualijų, keistis informacija. Prie forumo prisijungiama užsiregistruojant, slaptažodis atsiunčiamas e. paštu. Registruojantis reikalaujama nurodyti vardą, pavardę, gimimo datą, adresą, kitus duomenis, tačiau netikrinamas jų autentiškumas. Forume dalyviai diskutuoja naudodamiesi slapyvardžiais.

Minesotos valstijoje (JAV) e. forumas paremtas e. pašto sąrašais ir diskusijos vyksta ne atskirame interneto tinklapyje, o e. paštu tarp forume užsiregistravusių dalyvių. Forumo tinklalapyje diskusijas gali-

ma tik skaityti. Forume dalyvaujančių asmenų tikslas – turėti šiek tiek įtakos realioje politikoje ir bendruomenėje. Forumas laikosi griežtų cenzūravimo taisyklių, jame reikalaujama nurodyti tikrus vardus ir pavardes. Kitiems forumo dalyviams išsiųsti savo nuomonę gali tik užsiregistravę asmenys. Registracijos procesas yra kelių pakopų: pirmiausia užsiregistruojama *yahoo groups* portale, vėliau grįžtama į tą pačią www.e-democracy.org svetainę ir registruojamasi forumuose, kurių diskusijose ketinama dalyvauti, t. y. diskusijose, susijusiose su Minesotos valstijos politika, arba diskusijoje pasaulinės politikos klausimais.

E. konsultacijos

E. konsultacijas galima apibūdinti kaip dvikrypčius santykius, kurių metu piliečiai internetu teikia atsiliepimus valdžiai. Valdžios institucijos apibrėžia pirminę informaciją, konsultacijų problematiką, nustato klausimus bei valdo procesą, kol piliečiai yra kviečiami pasidalinti savo nuomone.

E. konsultacijos inicijuojamos, kad valdžios institucijos išsiaiškintų piliečių nuomonę rūpimais klausimais. Šiuo metu e. konsultacijos laikomos pažangiausia e. demokratijos sritimi.

E. konsultacijos gali būti organizuojamos įvairiais būdais – pasinaudojant atitinkamomis internetinėmis formomis, apklausomis, e. paštu arba kitomis interaktyviomis priemonėmis.

E. konsultavimo naujovės yra:

- oficialių dokumentų internete skelbimas, taip padidinant politinių procesų skaidrumą bei palengvinant politinės informacijos prieinamumą;
- elektroninė komentarų užklausa (leidimas piliečiams užbaigti konsultacijų apklausą internetu);
- atskiras valdžios konsultacijų interneto portalas, kuriame prieinamos visos konsultacijos.
- įspėjimas apie konsultacijas e. paštu, teikiantis piliečiams informaciją apie naujas konsultacijas;
- žinučių lenta (*message board*) – galimybė perskaityti ir komentuoti ankstesnius piliečių komentarus konsultaciniame procese;
- interaktyvus diskusijų forumas, leisiantis piliečiams diskutuoti tiek tarpusavyje, tiek su valstybės tarnautojais.

E. peticijos

Peticija – tai raštiškas kreipimasis į valdžios institucijas (dažniausiai į parlamentą) reikalaujant išspręsti peticijoje pateikiamus klausimus. E. peticija – internetu prieinama elektroninė peticijos forma, kurios turiniui keliami tokie pat reikalavimai kaip ir įprastai peticijai. E. peticija turi vienodą teisinę galią, palyginti su tradicine rašytine peticija.

Internete yra nemažai tinklalapių, kuriuose galima rasti siūlymų užpildyti e. peticijos formą, tačiau dauguma iš jų neturi jokios teisinės galios, o kuriamos tam, kad atkreiptų visuomenės dėmesį.

Pavyzdžiui, tinklalapyje www.e-thepeople.org visi norintieji (prieš tai internetu užsiregistravę) gali dalyvauti diskusijoje su kitais šių svetainių lankytojais patys pasiūlę debatų temą arba prisijungę prie jau esamų. Ši svetainė taip pat suteikia galimybę sukurti savo internetines apklausas dominančiais klausimais arba užpildyti e. peticiją, kuri bus perduota valdžios institucijoms. Tik šiuo atveju e. peticijos neturi oficialios formos ir oficialaus pripažinimo. Tai piliečių neoficialaus dalyvavimo aktyvinimo forma – sukūręs peticiją asmuo gali ne tik įdėti peticiją internete, bet ir per svetainę persiųsti ją savo pateiktiems adresatams su prašymu peticiją, jei ją palaiko, pasirašyti ir pasinaudoti analogiška galimybe ją platinti ir toliau. Tokios peticijos arba forumai, nors ir nesukelia teisinių pasekmių piliečių santykiuose su valdžia, tačiau skatina žmonių pilietiškumą bei verčia valdžios institucijas atkreipti dėmesį į piliečiams rūpimus klausimus.

Kitas pavyzdys – Škotijos parlamento tinklalapyje esančios e. peticijos. Taigi e. peticijos yra prieinamos platesnei auditorijai ir visi norintieji pasirašyti peticijoje keliamus reikalavimus gali tai padaryti internetu – reikia nurodyti savo vardą, pavardę ir adresą. Beje, peticijos parašai gali būti renkami ir elektroniniu, ir tradiciniu būdu. Kiekvienas parašas patikrinamas siekiant išvengti apgavysčių. Jei tas pats asmuo pasirašo ir popieriuje, ir internetu, pasikartojantys parašai išbraukiami.

E. balsavimas

2002 m. Europos Taryba, pradėjusi ieškoti būdų, kaip galima būtų standartizuoti e. balsavimo procesą, nustatė, kad e. balsavimas gali apimti „daugybę balsavimo metodų, kuriuos sukuria naujų technologijų naudojimas, t. y. elektronines balsavimo mašinas, optinius skana-

vimo įrenginius, valdžios kontroliuojamus „rinkimų kioskus“, telefoninį balsavimą, SMS balsavimą (teksto žinutėmis), skaitmeninę televiziją, balsavimą internetu (tiesiogiai arba iš balsavimo vietų)“.

Kalbant apie visuotinius rinkimus, e. balsavimas dažniausiai yra suprantamas kaip balsavimas internetu. Tokiu atveju e. balsavimas apima sistemos duomenų bazės sudarymą ir tikslinimą, rinkėjo registraciją ir identifikaciją, e. biuletenio pateikimą rinkėjui, e. biuletenio užpildymą bei išsiuntimą į rinkimų administratoriaus duomenų bazę ir automatinį balsų skaičiavimą. Tradicinis balsavimo metodas taip pat apima visas minėtas stadijas: rinkėjų sąrašų sudarymą ir tikslinimą, rinkėjo registraciją ir identifikaciją pateikiant asmenį identifikuojantį dokumentą, biuletenio pateikimą rinkėjui, biuletenio užpildymą, įmetimą į balsavimo dėžę ir rankinį balsų skaičiavimą. Tradicinių balsavimo metodų ir e. balsavimo skirtumas yra tas, kad rinkėjui registruoti, nustatyti, biuleteniui pateikti rinkėjui ir balsams skaičiuoti nereikia žmogiškųjų išteklių – tai atlieka informacinė sistema.

Svarstant e. balsavimo įdiegimo klausimą šalyje reikia nepamiršti dviejų aplinkybių. Pirma, skaitmeninio susiskaldymo, t. y. nevienoda prieigos galimybė prie interneto yra labai svarbi vykstant visuotiniams rinkimams. Siūlomos naujos balsavimo formos ir bendradarbiavimo galimybės, pagrįstos IKT naudojimusi, tam tikrais atvejais gali sukelti priešingą poreikį dėl išskyrimo arba pašalinimo iš politinio proceso „IKT neraštingų“ balsuotojų. Antra, e. balsavimo procedūroms būdingo nepasitikėjimo, kuris priklauso nuo skaidrumo stygiaus (matomumo/apčiuopiamumo kontekste) rinkimų procese. Šis nepasitikėjimas yra labai glaudžiai susijęs su skaitmeninio susiskaldymo problema. Kai kurie paprasti tradicinės balsavimo procedūros ir dalyvavimo elementai bei reikalavimai yra visiškai skirtingi nei e. balsavimo sistemoje ir dažniausiai sunkiai suvokiami eiliniam piliečiui. Pavyzdžiui, e. balsavimas gali būti vykdomas be jokio asmens dokumento patikrinimo balsavimo vietoje ir taip pat be tradicinio ranka rašomo parašo (kaip tai daroma balsuojant paštu).

E. rinkimai

E. rinkimai suprantami kaip vienas alternatyvių teisėtų, visuotinių rinkimų arba referendumo organizavimo būdas, apimantis procedūrines rinkimų fazes iki balsavimo, balsavimo, po balsavimo, atlie-

kant auditą, rinkimų procese rinkėjui suteikiant galimybę naudotis informacinėmis technologijomis, integruotomis į rinkimų procesą.

Plačiąja prasme e. rinkimų sąvoka apima bet kokį elektroninių priemonių naudojimą rinkimų procese. Pavyzdžiui, šiuo metu galimą balsavimo biuletenių parsisiuntimą internetu iš Vyriausios rinkimų komisijos (VRK) svetainės galima laikyti kaip dalinį e. rinkimų įdiegimą fazėje iki balsavimo. Toks VRK sprendimas sumažina balsavimo biuletenio būtinumą, nes biuletenį galima atsisiųsti žinant gana plačiai paplitusius tokius asmens duomenis kaip asmens kodas, vardas, pavardė bei paso numeris. Šie asmens duomenys yra prieinami darbdaviams, personalo darbuotojams, banko darbuotojams ir daugeliui kitų valstybės arba privačių įstaigų. Dėl to kyla dvejonių, ar rinkėjo biuletenį iš interneto parsisiųs tik tas asmuo, kuriam jis yra skirtas.

Siaurąja prasme elektroniniai rinkimai apima elektroninio balsavimo fazę ir siejami su alternatyviais balsavimo būdais, pavyzdžiui, su balsavimu paštu.

Laisvų rinkimų principas reikalauja, kad visas rinkimų procesas vyktų be prievartos, manipuliavimo, spaudimo. Balsavimo vietoje (rinkimų arba referendumo metu) tarnautojai turi užtikrinti, kad rinkėjai, pareikšdami savo valią, nepatirtų jokio išorinio poveikio. Taigi ir e. balsavimas sistema turi užtikrinti rinkėjo laisvos nuomonės išraišką ir negali daryti jokio poveikio rinkėjui, skatinant jį greitai ir neapgalvotai atiduoti balsą. Žinoma, dėl saugumo turėtų būti rekomenduojama balsuotojui procedūrą atlikti per įmanomai trumpesnį laiką.

Rinkėjo apsisprendimo laisvė taip pat gali būti pažeista, jei rinkimų agitacijos medžiaga yra e. balsavimo internetinės svetainės reklamoje, kai rinkėjas pildo savo elektroninį biuletenį. Egzistuojančiuose rinkimų modeliuose neleidžiama agituoti balsavimo vietose, todėl e. balsavimo procedūra turi sudaryti techniškai neįmanomą politinę agitaciją e. balsavimo internetinėje svetainėje. Taigi balsavimo metu e. balsavimo sistema turi uždrausti bet kokią manipuliuojančią įtaką rinkėjui siekiant garantuoti e. balsavimo sistemų teisėtumą.

Dar vienas demokratinės balsavimo sistemos reikalavimas yra tas, kad ji turi užtikrinti balsavimo slaptumą. Slaptumas ir laisvė yra glaudžiai susiję principai. Slaptumas yra pradinė rinkėjo laisvo politinio apsisprendimo sąlyga. Demokratiniuose rinkimuose ryšys tarp balso ir

rinkėjo turi neturėti grįžtamojo ryšio, nes tik taip įmanoma užtikrinti rinkėjo laisvą apsisprendimo išraišką. Tradicinėse balsavimo procedūrose slaptumas yra fiziškai užtikrinamas. E. balsavimo metu slaptumą užtikrinti daug sunkiau.

Slaptumas e. balsavimo metu turi būti suderintas su kitais demokratiniais principais, taikomais rinkimams, referendumams: skaidrumu ir galimumu patikrinti visą rinkimų procesą. Balsavimo sistema turi būti sukurta taip, kad būtų galima atlikti balsų kontrolę ir perskaičiavimą be pakartotinio rinkėjų identifikavimo ir kad nebūtų jokios galimybės pažeisti balsavimo slaptumo reikalavimo.

E. balsavimo sistema turi išlaikyti balsų konfidencialumą ir laikyti juos užšifruotus iki balsų skaičiavimo procedūros. Tik Vyriausioji rinkimų komisija turėtų teisę išduoti leidimus asmenims prieiti prie centrinės sistemos infrastruktūros, serverių arba rinkimų duomenų ir tai turi būti aiškiai reglamentuota taisyklėse.

Pasak Europos Komisijos, labai svarbu plėtoti atstovaujamąją demokratiją, pagrįstą piliečių tiesioginiu įtraukimu į sprendimų priėmimo procesą, naudojant patogias e. balsavimo sistemas. Rekomenduojama, kad e. balsavimo sistema turėtų būti paremta išsamiu galimos rizikos įvertinimu, siekiant nepriekaištingai įvykdyti referendumą arba rinkimus. Sistema turi turėti savisaugos priemones, skirtas bet kokiai rizikai nustatyti bei jai kontroliuoti. Sistema turi būti sukurta taip, kad „užlūžus“ vienam sistemos elementui ji galėtų saugiai veikti.

Viena aktualiausių ne tik e. balsavimo sistemos, bet ir pačios e. demokratijos sistemos problemų – nustatyti tinkamą asmenį. Reikalavimas užtikrinti tinkamo asmens nustatymą yra sunkiai įgyvendinamas naudojant elektroninę balsavimo sistemą, nes internetas yra gana nesaugi erdvė. Elektroninės identifikacijos duomenys gali būti nuperkami arba, asmeniui nežinant, pavagiami įvairiais būdais, pavyzdžiui, naudojantis imitacinėmis interneto svetainėmis, kompiuterio viduje esančiomis kenkėjiškomis programomis, arba asmuo gali lengvabūdiškai perduoti duomenis kitam asmeniui.

Dažnai identifikacijai naudojamas elektroninis parašas, esantis ne kompiuterio kietajame diske, o išoriniame įrenginyje, kortelės

mikroschemoje ir pan. Tobulėjant technikai atsiranda įvairių papildomų identifikacijos galimybių – tai specialūs įrenginiai, veikiantys kaip saugumo raktai, kuriuose yra tam tikra programinė įranga, veikianti kaip identifikatorius.

Pastaruoju metu vis dažniau identifikacijos metu naudojamasi mobilių operatorių paslaugomis – į mobilųjį telefoną atsiunčiamas kontrolinis slaptažodis. Iš tiesų šis metodas yra inicijuotas mobiliojo ryšio bendrovių, suinteresuotų išplėsti paslaugų sektorių, todėl specialistų vertinamas gana skeptiškai, nes kiekviena SMS kainuoja, tad naudojantis tokia paslauga dažnai finansiškai labiau apsimoka naudoti kortelių identifikacines sistemas. Padėtį komplikuoja ir nesaugus GSM ryšys, kurio saugumo kodo problema dar nėra išspręsta.

Viena iš identifikavimo procedūrų gali būti pirštų anspaudų skaitytuvai. Šią technologiją numatoma panaudoti diegiant e. rinkimų sistemą Venesueloje.

Šiuo metu sukurta e. balsavimo sistemų programavimo kalba EML (*Election Markup Language*), vartojanti atvirą standartą, kad garantuotų tinkamą vidinį veikimą. Šią EML programavimo kalbą remia Europos Taryba, be to, Europos Tarybos interneto svetainėje galima susipažinti su technine jos dokumentacija. Europos Taryba kartu pabrėžia, kad būtina laikytis didelio technologinio neutralumo kuriant e. balsavimo sistemas, tačiau šiuo metu tinkamiausią programavimo kalbą pripažįsta EML.

6.2.2. Teisinės ir politinės e. demokratijos prielaidos

Taikant IKT valstybės valdyme susiduriama su įvairiomis teisinėmis ir politinėmis kliūtimis. Įstatymų leidėjai privalo užtikrinti, kad esama valstybės teisinė ir politinė sistema būtų pritaikyta e. valdžios ir e. demokratijos realijoms. Pasenęs arba netinkamas teisinis reguliavimas, bendro koordinavimo nebuvimas gali labai komplikuoti arba net sustabdyti e. valdžios ir e. demokratijos plėtrą, ypač įvertinant ypatingą visuomenės procesų raidą, kurią lemia sparti informacinių technologijų raida. Užsienio patirtis taip pat patvirtina, kad būtinas holistinis požiūris į e. valdžios ir e. demokratijos problemas, pagristas bendrais socialiniais teisiniais mechanizmais.

Bendro požiūrio į e. demokratiją principai yra:

Pagrindinių teisių ir laisvių pripažinimas elektroninėje erdvėje. Visuotinai pripažintos teisės ir laisvės turi būti vienareikšmiškai išplėstos elektroninėje erdvėje (pvz., teisė pasirinkti bendravimo su valdžia rūšį ir kanalą, laisva prieiga prie viešosios elektroninės informacijos ir žinių ir t. t.).

Minimalistinis reguliavimas. Vienas iš pagrindinių e. valdžios principų turi būti savitikslio reguliavimo ir išorinio įsikišimo į e. valdžios procesus minimizavimas.

Vyriausybės iniciatyvų ir instrumentinių procesų technologinis neutralumas. Negali būti toleruojama jokia informacinių technologijų diskriminacija arba preferencija.

Visos interneto naudotojų grupės yra svarbios – piliečiai, verslas, valstybinės įstaigos, taip pat mažumos (neįgalieji, pensijinio amžiaus asmenys, t. t.). Bet koks sprendimas turi būti visuotinai pasiekiamas, vertas pasitikėjimo ir nediskriminacinis.

Skaidrumas ir atvirumas yra modernios demokratinės visuomenės pagrindas.

Viešosios informacijos prieinamumas. Viešoji informacija turi būti lengvai prieinama internetu. Informacija yra gerai funkcionuojančio ir skaidraus sprendimų priėmimo proceso pagrindas ir būtina bet kokios demokratijos sąlyga.

Laisvai prieinamos žinios yra pagrindinis veiksnys, keičiantis ir globalią visuomeninę, ir vietines bendruomenes.

Privatumo ir duomenų apsauga. E. valdžia ir e. demokratija yra negalimi be pagarbos piliečių privatumui ir saugiai informacijos infrastruktūrai. Jei šis principas nebus užtikrintas, pasitikėjimo valdžia niekada nebus.

Padidėjusi savireguliacijos svarba. Šie instrumentai taip pat sutvirtina pagrindinį savireguliacijos vaidmenį daugelyje sričių (pvz., interneto turinio, operacijų teisėtumo, vartotojų apsaugos, elektroninių visuomenės informavimo priemonių ir t. t.).

Vyriausybes ir visuomenes bendradarbiavimas. Visuomenės dalyvavimas priimant valdymo sprendimus turi būti teisiškai pripažįstamas.

Universalaus priėjimo prieinama kaina skatinimas. Kritinis universalaus priėjimo prie informacijos ir žinių strategijos elementas yra visuotinės interneto prieigos plėtra. Visuomenės prieigos centrai ir viešosios paslaugos (tokios kaip paštas, bibliotekos, mokyklos) privalo suteikti veiksmingas universalaus priėjimo skatinimo priemones (ypač nutolusiose vietovėse) ir tapti svarbiu šių vietovių plėtros veiksniu.

Teisinis e. valdžios reglamentavimas

Teisinė aplinka yra reikšminga funkcionalumo dalis, įtvirtinanti pamatinius principus ir prielaidas, kuriomis remiantis įgyvendinami ir funkcionuoja konkretūs e. valdžios ir e. demokratijos mechanizmai. Teisinės aplinkos spragos ir trūkumai lems netinkamą ar nepakankamą valdžios funkcionalumą arba neadekvatų valdžios funkcijų įgyvendinimą.

2002 m. pabaigoje Lietuvos Respublikos Seimas, apibrėždamas pagrindinius šalies plėtros ilgalaikės perspektyvos tikslus, patvirtino ilgalaikę valstybės raidos strategiją, kuriame tiesiogiai formuluojami e. valdžios raidos prioritetai Lietuvoje. Pabrėžiama, kad veiksminga e. valdžios raida Lietuvos valstybėje besąlygiškai siejama su moderniu informaciniu ir telekomunikaciniu technologijų naudojimu viešajame administravime, numatoma įgyvendinti šalies gyventojų teisę į greitą, saugų ir pigų internetą. E. valdžia įvardinta kaip pagrindinė strateginė kryptis, padedanti gerinti šalies valdymo kokybę ir operatyvumą, sumažinti valstybės tarnautojų skaičių ir padaryti viešąjį administravimą veiksmingesnį.

Lietuvos Respublikos Vyriausybė 2002 m. gruodžio 31 d. patvirtino Lietuvos elektroninės valdžios koncepciją. Priimti ir kai kurias specifines e. valdžios ir e. demokratijos sritis reglamentuojantys elektroninio parašo, valstybės, juridinių asmenų, nekilnojamojo turto registro, autorių ir gretutinių teisių, telekomunikacijų ir kiti įstatymai. Tenka apgailestauti, kad e. valdžios koncepcija yra santykinai siaura ir nustato tik elektroninių viešųjų paslaugų teikimo gaires.

Deja, minėtuose Lietuvos teisės aktuose apie e. demokratiją tik užsimenama, tačiau apie jos sampratą ir įgyvendinimą nekalbama. Pavyzdžiui, Lietuvos nacionalinės informacinės visuomenės plėtros kon-

cepcijos 6.2. punkte teigiama, jog norint modernizuoti valstybės valdymą reikės plėtoti e. valdžią ir e. demokratiją, tačiau nenurodoma kaip. Be to, Lietuva, tapusi Europos Sąjungos nare, turi laikytis prisiimtų įsipareigojimų, taip pat ir kurdama e. valdžią bei e. vyriausybę.

Teisinės e. rinkimų problemos

Rinkimai yra kertinis politinis procesas, garantuojantis kiekvienos demokratinės valstybės valdžios legitimumą. Galimybė manipuliuoti rinkimų rezultatais yra didelė grėsmė jaunoms arba nestabilioms demokratijoms. Įvairios interesų grupės, pasinaudodamos informacinių technologijų teikiamomis galimybėmis, gali klastoti rinkimų rezultatus, manipuliuoti rinkėjų balsais.

Komunikacija elektroninėmis ryšio priemonėmis nėra nauja modernaus pasaulio praktikoje, tačiau elektroninių ryšio kanalų ir priemonių naudojimas rinkimų metu dar tik pradedamas įgyvendinti. 2005 m. Estijos Respublikoje pirmą kartą išbandytas balsavimas internetu savivaldos rinkimuose, kurio pranašumais galėjo įsitikinti daugiau nei devyni tūkstančiai rinkėjų.

Europos Tarybos Ministrų komitetas 2004 rugsėjo 30 d. patvirtino „Rekomendaciją (2004)11 dėl teisinių, operacinių ir techninių normų, taikomų rinkimams elektroniniu būdu“, kurioje smulkiai aprašomi rinkimų, vykdomų elektroniniu būdu, principai ir reikalavimai.

Įstatymų numatyta demokratinė e. balsavimo bazė pagrįsta bendrųjų demokratinės rinkimų sistemos balsavimo kriterijų užtikrinimu. Tai laikoma laisva rinkėjo valios išraiška netgi metant negaliojantį („balto popieriaus“) biuletenį. Taigi, siekiant apsaugoti apsisprendimo laisvę, e. balsavimo metu rinkėjui taip pat turi būti suteikta ir garantuota teisė sąmoningai išsiųsti negaliojantį biuletenį.

Europos Tarybos išleista rekomendacija numato šiuos e. rinkimų principus:

Universalumo principas

E. balsavimo sąsaja turi būti suprantama ir lengvai naudojama

Teisėtumo principas

E. balsavimas gali vyki tik įstatymų numatytu atveju ir metu, turi būti naudojami tik teisėti Vyriausios rinkimų komisijos nustatyti e.

balsavimo puslapiai. Už šio principo sulaužymą turi būti skiriamos griežtos sankcijos, nes imitacinės e. balsavimo svetainės gali neteisėtai surinkti identifikacinius duomenis ir vėliau panaudoti klastodamos rezultatus. Būtų tikslinga Baudžiamajame kodekse numatyti atgrasančias sankcijas asmenims, siekiantiems imituoti arba pažeisti e. balsavimo sistemą.

Lygybės principas

Rinkėjas gali atiduoti tik vieną balsą. Sistema turi būti tokia, kad neleistų balsuoti daugiau nei vieną kartą. Techniškai sistema kiekvieną kartą asmeniui atlikus balsavimo procedūrą rinkėjų duomenų bazėje turi padaryti įrašą, kad asmuo balsavo, ir blokuoti kitą mėginimą balsuoti; arba sistema turi asmeniui balsavus antrą kartą panaikinti pirmąjį balsavimo biuletenį (taip yra įdiegta Estijos e. balsavimo sistemoje). Siekiant apsisaugoti nuo rinkėjų sukčiavimo ir balsavimo keliais skirtingais balsavimo būdais, visų alternatyvių balsavimo būdų balsavimo biuleteniai turi būti saugomi iki tradicinių rinkimų balsavimo pabaigos, kai būtų sutikrinami tradiciškai balsavusių rinkėjų sąrašai su alternatyviai balsavusiųjų sąrašais, o sutampantys balsavimo biuleteniai būtų sunaikinami.

Jei paaiškėtų, kad e. balsavimo metu balsavimo biuletenis buvo užpildytas neteisėtai, turi būti galimybė atšaukti balsą. Kiekvienas balsavimo biuletenis, pakliuvęs į balsadėžę elektroniniu būdu, turi būti skaičiuojamas (tik vieną kartą), tai privalo užtikrinti sistemos programuotojai.

Laisvų rinkimų principas

E. balsavimas turi užtikrinti, kad rinkėjas laisvai formuotų ir reikštų nuomonę bei nevaržomai atiduotų balsą. E. balsavimo procesas negali daryti jokio poveikio rinkėjui, skatinant jį neapgalvotai atiduoti balsą. Rinkėjai turi turėti galimybę e. balsavimo metu keisti savo pasirinkimą prieš išsiunčiant balsą į elektroninę balsadėžę, taip pat turėti galimybę atšaukti balsavimą. Ši procedūra turėtų veikti kaip banko sąskaitos blokavimo sistemos analogija, t. y. balsas, rinkėjui pranešus, kad jis klaidingas arba neteisėtas, turėtų būti nedelsiant blokuojamas ir, gavus raštišką rinkėjo pageidavimą, naikinamas.

Balsavimo metu e. balsavimo sistema turi uždrausti bet kokią manipuliavimo įtaką rinkėjui. Pavyzdžiui, neleidžiama propaguoti interak-

tyvių reklaminių langų su politikais arba ką nors panašaus.

E. balsavimo sistema turi pateikti rinkėjui paaiškinimus, kaip atlikti balsavimo procedūrą, bet tame pavyzdyje negali būti vaizduojama priemonė, kuri paskatintų arba lemtų rinkėją balsuoti už vieną arba kitą pasirinkimą. E. balsavimo sistema turi aiškiai parodyti ir leisti suprasti rinkėjui, kad jo balsas sėkmingai buvo išsaugotas ir kad balsavimo procedūra yra baigta.

Išsiuntus balsą į e. balsadėžę, e. balsavimo sistema turi užkirsti kelią bet kokiems balsavimo rezultato pakeitimams.

Slaptumo principas

E. balsavimas turi būti organizuojamas tokiu metodu, kad balsavimo procedūra būtų atskirta nuo identifikacijos procedūros ir kad nebūtų jokios galimybės pažeisti balsavimo slaptumo reikalavimo. E. balsavimo sistema turi garantuoti, kad suskaičiuoti balsai, esantys e. balsadėžėje, yra anonimiški ir nėra jokios galimybės atkurti ryšio tarp balso ir balsavusiojo.

E. balsavimo sistema turi būti sudaryta taip, kad nuspėjamas balsų skaičius elektroninėje balsadėžėje neleistų nuspėti individualių balsuotojų balsavimo rezultatų.

Turi būti imamasi visų priemonių siekiant užtikrinti e. balsavimo metu perduodamos informacijos saugumą ir sudaryti visas sąlygas, kad balso perdavimo metu nebūtų pažeistas balsavimo slaptumas.

Viešumo principas

Diegiant e. balsavimo sistemą turi būti laikomasi viešumo principo, t. y. turi būti imamasi visų priemonių, kad rinkėjai pasitikėtų ir suprastų, kaip naudotis e. balsavimo sistema. Informacija apie *e. balsavimo* sistemų funkcionavimą turi būti viešai prieinama. E. balsavimo stebėtojams turi būti užtikrintos visos teisės stebėti, komentuoti *e. rinkimus* bei balsų rezultatų paskelbimą.

Patikrinamumo ir atskaitomybės principas

E. balsavimo sistemos komponentai privalo būti atviri susipažinti nepriklausomiems ekspertams, kad būtų galima patikrinti ir sertifikuoti sukurtą e. balsavimo sistemą. Turi būti galimybė perskaičiuoti balsus. Taip pat turi būti prieinamos priemonės, leidžiančios tikrinti balsavimo rezultatų tikslumą. E. balsavimo sistema turi užkirsti kelią

bet kokiems perbalsavimams arba rezultatų keitimams pasibaigus nustatytam elektroninių rinkimų laikui.

Patikimumo ir saugumo principas

Valdžios institucijos privalo užtikrinti e. balsavimo sistemos patikimumą ir saugumą. Turi būti imamasi visų įmanomų priemonių siekiant išvengti *e. balsavimo* sistemos pažeidžiamumo arba neteisėto įsibrovimo per visą balsavimo laikotarpį.

E. balsavimo sistema turi būti sukurta taip, kad gebėtų išsaugoti visas savo funkcijas balsavimo metu. Sistema turi atlaikyti visus ypatingus atvejus, veikimo sutrikimus, elektros smūgius, sistemos atakas. Prieš kiekvienus rinkimus arba referendumą kompetentinga rinkėjų atstovų institucija privalo įsitikinti, kad e. balsavimo sistema yra nesuklastota ir veikia nepriekaištingai.

Tik Vyriausioji rinkimų komisija gali išduoti leidimus asmenims prieiti prie centrinės sistemos infrastruktūros, serverių ar rinkimų duomenų. Tai turi būti aiškiai reglamentuota taisyklėse. Mažiausiai dviejų žmonių komanda, t. y. vienas sistemos administratorius, kitas programuotojas, turi nuolat stebėti sistemos darbą bei joje vykstančias kritines veiklos operacijas. Komandos sudėtis turi būti reguliariai keičiama, realiausiai – kas 2 valandas.

Atverta elektroninė balsadėžė turi būti saugoma mažiausiai dviejų žmonių komandos nuo bet kokio neteisėto kišimosi į sistemą. Viskas turi būti fiksuojama ir raportuojama kompetentingiems rinkimų administratoriaus (VRK) nariams ir stebėtojams.

Balsavimo ir balsuotojo informacija turi išlikti nepasiekiama taip ilgai, kaip ilgai galima susieti tuos duomenis. Identifikacijos informacija turi būti atskirta nuo balsuotojo sprendimo dar iki elektroninio biuletenio gavimo momento elektroninių rinkimų ar referendumo metu.

Estijos e. referendumų aktas

Galimybė daryti tiesioginę įtaką politiniams sprendimams dalyvaujant svarbiausių visuomenei klausimų svarstyme ir taip įgyvendinti tautai suteikiamas suverenias galias – viena iš svarbiausių konstitucinių teisių, įgyvendinamų referendumu. Referendumai pasaulinėje praktikoje organizuojami nacionaliniu, arba vietiniu, mastu.

Referendumo institutas Estijoje reglamentuojamas Estijos Respublikos referendumo įstatyme (*Referendum act*). Be įprastinio, jame

įtvirtinamas ir elektroninio balsavimo būdas. Šio įstatymo 37 straipsnis tokią galimybę suteikia asmenims, turintiems elektroninio parašo sertifikatą. Balsas „taip“ arba „ne“ atiduodamas Nacionalinio rinkimų komiteto (*nacional electoral committee*) tinklalapyje. Balsuotojas nustatomas pagal elektroninį parašą, po identifikacijos tinklalapyje balsuotojui pateikiamas balsavimo biuletenis, kuriame pažymimas ir patvirtinamas atsakymas.

6.3. Lietuvos rinkimų internetu koncepcija

Tikslai. Labai svarbi Lietuvos balsavimo internetu per rinkimus ir referendumus koncepcija, parengta vykdant Lietuvos Respublikos Seimo 2006 m. balandžio 25 d. nutarimą Nr. X-583. Koncepcijai buvo pritarta Vyriausiosios rinkimų komisijos 2006 m. birželio 17 d. posėdyje sprendimu Nr. 38. Šioje koncepcijoje pateikiami pagrindiniai elektroninio balsavimo principai, aprašomas principinis tokio balsavimo mechanizmas, nurodomi sistemos pranašumai ir trūkumai.

Koncepcijos tikslas – apibrėžti balsavimą internetu, numatyti galimybę balsuoti internetu Lietuvos Respublikoje vykstančiuose rinkimuose bei referendumuose, nurodyti balsavimo internetu pranašumus bei galimas problemas, kylančias tokio balsavimo metu.

Balsavimo internetu tikslai ir uždaviniai:

- palengvinti dalyvavimą rinkimuose suteikiant platesnes galimybes atiduoti balsą kitoje nei balsavimo apylinkė vietoje;
- skatinti rinkėjus dalyvauti rinkimuose siūlant naujas balsavimo formas;
- pritaikyti rinkimus prie naujų telekomunikacijos technologijų;
- palengvinti ir padaryti veiksmingesnį balsų skaičiavimą ir rinkimų arba referendumo rezultatų nustatymą.

Pagrindinės šioje koncepcijoje vartojamos sąvokos:

- *Balsavimas kontroliuojamoje aplinkoje* – balsavimas stebint specialioje patalpoje rinkimų komisijai išduodant biuletenius ir stebint, kad rinkėjai balsuotų slaptai.
- *Balsavimas nekontroliuojamoje aplinkoje* – balsavimas nedalyvaujant rinkimų komisijoms, pavyzdžiui, paštu, užsienyje arba internetu.
- *Elektroninis balsavimas (e. balsavimas)* – balsavimas naudojant šiuolaikines informacines technologijas. Skiriamas e. balsavi-

mas rinkimų apylinkėje naudojant įrenginius su jautriais prisilietimui ekranais, jungiklių įrenginius, standartinius kompiuterius. Rezultatai skelbiami (spausdinami) pasibaigus balsavimui, jie gali būti automatiškai perduodami telefono linijomis, gali būti spausdinami kiekvieno balsavimo duomenys. Išspausdintus arba kitaip išsaugotus kiekvieno balsavimo duomenis galima perskaičiuoti ir taip kontroliuoti balsavimo procedūrų teisingumą. Nuotolinis e. balsavimas – kai balsuojama internetu, mobiliuju telefonu (tik bandomieji balsavimai) bei balsavimo kioske, į kurį patenkama asmens tapatybę nustačius įgaliotam rinkimų komisijos pareigūnui arba konsuliniam darbuotojui.

- *Balsavimas internetu (i. balsavimas)* – nuotolinio e. balsavimo būdas, kai rinkėjas gali išreikšti savo valią per rinkimus arba referendumą naudodamasis interneto ryšiu savo namuose, darbo vietoje ar kitoje vietoje, kurioje yra interneto prieiga.
- *Viešasis raktas* – skaitmenų ir simbolių kodas, naudojamas rinkėjų balsams, saugomiems elektroninėje balsadėžėje, užšifruoti. Prieš pradedant balsavimą internetu generuojamas viešasis raktas, jis suskaldomas į keletą dalių, kurios po vieną išdalijamos keliems asmenims (pvz., keliems rinkimų komisijos nariams). Pasibaigus rinkimams ir pradedant skaičiuoti e. balsadėžėje esančius balsus, viešojo rakto dalys nustatyta tvarka suvedamos į dešifravimo įrenginį, balsai iššifruojami ir suskaičiuojami.
- *Elektroninė balsadėžė (e. balsadėžė)* – techniškai ir fiziškai apsaugota elektroninių duomenų saugykla, kurioje iki rinkimų pabaigos koduota forma saugomi i. balsavimo metu atiduoti rinkėjų balsai.

Balsuojant internetu privalo būti laikomasi Konstitucijoje nustatytų rinkimų principų: visuotinės, lygios tiesioginės rinkimų teisės ir slapto balsavimo. Balsavimas internetu turi atitikti visus tradiciniam balsavimui keliamus reikalavimus ir principus, būti ne mažiau saugus nei balsavimas rinkimų apylinkėje (balsuojama rinkimų dieną, specialiai tam skirtoje patalpoje, asmens tapatybę nustato, biuletenius išduoda, balsus suskaičiuoja ir visą balsavimo procesą kontroliuoja apylinkės rinkimų komisija, balsavimą stebi rinkimų stebėtojai) arba balsavimas paštu (išankstinis balsavimas, kai asmens tapatybę nustato, biuletenius išduoda, užklijuotus vokus su rinkėjo slapta pažymėtais biuleteniais priima rinkimų komisijos įgaliotas pašto darbuotojas, bal-

sus rinkimų dieną suskaičiuoja apylinkės rinkimų komisija, rinkimų komisijos ir rinkimų stebėtojai prižiūri, kad balsavimas paštu vyktų laikantis nustatytų reikalavimų).

Įgyvendinant rinkimų principus, turi būti užtikrinti šie i. balsavimo reikalavimai:

- *Visuotinė rinkimų teisė* – naudojimasis balsavimo sistema turi būti visiems prieinamas, suprantamas ir lengvai naudojamas; sistema turi būti sudaryta kiek įmanoma didinant galimybes, kurias galima pasiūlyti neįgaliems asmenims; internetinis balsavimas yra tik papildoma ir fakultatyvi balsavimo priemonė, neapribojanti galimybės balsuoti tradiciniais būdais – rinkimų apylinkėje arba paštu.
- *Lygi rinkimų teisė* – rinkėjas laisvas ir nevaržomas pasirenka balsavimo būdą; nepriklausomai nuo to, kokiu būdu balsuos rinkėjas, bus įskaitomas tik vienas to paties rinkėjo balsas; nepriklausomai nuo balsavimo būdo rinkėjų balsai bus skaičiuojami kaip lygiaverčiai, turintys tokią pat vertę kaip ir bet kuris kitas bet kurio kito rinkėjo balsas.
- *Tiesioginiai rinkimai ir laisvi rinkimai* – rinkėjai balsuoja už kandidatus arba kandidatų sąrašus be tarpininkų. Elektroninis balsavimas turi garantuoti laisvą rinkėjo nuomonės suformavimą ir pareiškimą, neleistina skubinti rinkėją balsuoti arba balsuoti neapgalvotai, rinkėjas turi teisę bet kuriuo balsavimo procedūros momentu pakeisti savo apsisprendimą iki jo balso įregistravimo elektroninėje balsadėžėje, o jeigu internetu leidžiama balsuoti pakartotinai, įskaitomas tik vėliausias rinkėjo balsas. I. balsavimo sistema turi aiškiai nurodyti rinkėjui, kad balsas buvo sėkmingai įskaitytas ir šio balso neįmanoma pakeisti.
- *Slaptas balsavimas* – i. balsavimas turi būti organizuojamas taip, kad balso konfidencialumas būtų išlaikytas bet kurioje procedūros stadijoje nuo pat rinkėjo nustatymo momento. Elektroninio balsavimo sistema turi garantuoti, kad į e. balsadėžę patekę balsai ir jų skaičiavimas yra ir bus anonimiški, taip pat kad nebus įmanoma nustatyti ryšio tarp balso ir jį atidavusio asmens; elektroninio balsavimo sistema turi būti tokia, kad balsų skaičius elektroninėje balsadėžėje neleistų nustatyti ryšio tarp balso ir konkretaus rinkėjo (t. y. jeigu rinkimų apylinkėje balsuoja vienas rinkėjas, jo balsas turėtų būti skelbiamas kartu su

kitų rinkėjų balsais rinkimų apygardoje, o ne rinkimų apylinkėje), techninė ir programinė balsavimo įranga turi būti patikimai apsaugota nuo neleistinų veiksmų ir poveikių. Siekiant išvengti galimo poveikio rinkėjui, kai balsuojama nekontroliuojamoje aplinkoje, tikslinga nustatyti, kad rinkėjas, naudodamasis i. balsavimo sistema, savo valią gali pareikšti keletą kartų, jo balsas bus įskaitytas tik pagal paskutinįjį valios pareiškimą. Taip pat tikslinga nustatyti galimybę rinkėjui papildomai pareikšti valią rinkimų apylinkėje balsavimo dieną, toks valios pareiškimas būtų įskaitytas kaip rinkėjo balsas, o to rinkėjo e. balsavimo rezultatai neskaičiuojami.

- *Skaidrus rinkimų mechanizmas* – informacija apie i. balsavimo sistemos funkcionavimą turi būti išplatinta viešai, įvertinta nepriklausomų specialistų ir ekspertų. Rinkėjams turi būti suteikta galimybė priprasti ir išbandyti naują i. balsavimo sistemą prieš įregistruojant balsą. Visiems stebėtojams turi būti suteikta galimybė laikantis įstatymo nustatytų ribų dalyvauti i. balsavime, taip pat ir apibendrinant rezultatus, jį stebėti ir komentuoti; i. balsavimas turi būti toks skaidrus, kad nebūtų logiškai paaiškinamų abejonių dėl jo skaidrumo (pažymėtina, kad neargumentuojančių skeptikų išvengti neįmanoma).

Rinkėjų identifikavimas

Identifikuoti rinkėją Lietuvoje ganėtinai keblu, nes nėra vienos ir visiems prieinamos identifikacijos infrastruktūros. Tokios identifikavimo priemonės kaip USB raktai, pirštų antspaudų skaitytuvai ir kitos kol kas pernelyg brangios ir neprieinamos daugeliui rinkėjų.

Nors Lietuvoje elektroninis parašas šiuo metu ir nėra taip paplitęs kaip Estijoje, tačiau vertinamas kaip vienas iš galimų rinkėjo tapatybės nustatymo būdų ateityje. Be to, mobiliojo ryšio bendrovės jau siūlo galimybę naudoti elektroninio parašo patvirtinimą mobiliuoju telefonu. Rinkėjų identifikavimas naudojat elektroninio parašo technologijas yra patikimas ir saugus būdas, tačiau dėl nedidelės šių technologijų skvarbos šiuo metu Lietuvoje jis negali būti vienintelis.

Pradinėje i. balsavimo diegimo stadijoje numatoma pasirinkti Lietuvoje veikiančią išplėtotą elektroninės bankininkystės sistemą, kuri yra gana saugus būdas rinkėjams nustatyti, nors ir mažiau patikimas negu elektroninis parašas. Lietuvoje elektronine bankininkyste akty-

viai naudojasi apie 600 000 piliečių. Be to, rinkėjų identifikavimas per elektroninės bankininkystės sistemas nereikalauja didelių investicijų į aparatinę įrangą, kortelių skaitytuvus ir kt. Papildomo pasitikėjimo bankų identifikavimo sistemomis suteikia ir Valstybinės mokesčių inspekcijos, ir komercinių bankų organizuota bei sparčiai populiarėjanti elektroninio pajamų deklaravimo sistema.

Asmuo, sudarydamas banko sąskaitos sutartį su banku, patvirtina banko darbuotojui savo tapatybę pateikdamas asmens dokumentą, savo parašo pavyzdį. Bankas, atpažinęs ir prijungęs prie sistemos savo vartotoją, perduoda vartotojo duomenis ir vartotojo sąsają į VRK serverį patvirtindamas (pasirašydamas), kad tai tikrai tas asmuo, kuris sudarė elektroninės bankininkystės sutartį. Banko perduodami duomenys: asmens kodas, vardas, pavardė.

Problemų užtikrinant patikimą rinkėjo nustatymą gali kilti dėl banko darbuotojų nesąžiningumo. Dėl to sudarant atitinkamas sutartis su bankais būtina nustatyti aiškius reikalavimus, kuriuos turi atitikti ir banko techninė įranga, ir banko personalas.

Principinė balsavimo internetu schema

Rinkėjas vienu iš galimų kanalų arba tiesiogiai prisijungia prie VRK balsavimo tinklalapio, arba prie savo banko elektroninio aptarnavimo sistemos. Jei rinkėjas naudojasi banko identifikavimo sistema, prisijungęs prie savo banko sąskaitos tvarkymo tinklalapio, jis pasirenka nuorodą „Balsavimas internetu“ ar pan. ir yra perkeliamas į VRK serverį. Kartu bankas perduoda VRK serveriui banko pasirašytą informaciją apie prisijungusį rinkėją, o pats atsijungia nuo ryšio grandinės palikdamas tiesioginį ryšį „rinkėjas – VRK“.

VRK serveris, gavęs informaciją iš banko apie prisijungusį rinkėją, patikrina, ar toks rinkėjas yra rinkimų sąrašuose, ir priskiria rinkėją atitinkamai rinkimų apygardai. Po patikrinimo VRK sistema rinkėjo „paklausia“, ar tai tikrai tas rinkėjas, kuris prisistato.

Rinkėjui ekrane pateikiamas „i. biuletenis“, kuriame rinkėjas pažymi savo pasirinkimą (pasirinkimus) ir jį patvirtina. Informacija ekrane turi būti aiški, suprantama ir kuo labiau panaši į rinkėjams įprastą balsavimo apylinkėje arba paštu biuletenį.

Rinkėjo balsas saugiu ryšio kanalu perduodamas VRK serveriui, kur nedelsiant užkoduojamas ir patenka į elektroninę balsadėžę. Rinkėjų sąraše pažymima, kad rinkėjas balsavo, o užkoduotas balsas su

rinkėjo identifikavimo duomenimis patenka į e. balsadėžę, kur yra saugomas iki tradicinio balsavimo pabaigos.

Rinkėjui nusprendus internetu pareikšti savo valią pakartotinai, procedūra pakartojama iš naujo, tačiau pirmiau priimtasis balsas išimamas iš e. balsadėžės ir į jo vietą įtraukiamas naujas.

Pasibaigus i. balsavimo laikui, e. balsadėžė „uždaroma“, t. y. atjungiama nuo išorinio ryšio kanalų, o pagal internetu balsavusių asmenų sąrašą pažymimi rinkėjai rinkėjų sąrašuose, numatytuose skirstyti apygardoms ir apylinkėms.

Rinkėjui atvykus į rinkimų apylinkę rinkimų dieną ir balsavus tradiciškai, rinkėjų sąrašuose (kuriuose apylinkės komisijos narys mato, kad rinkėjas balsavo internetu) pažymima, kad rinkėjas atvyko į apylinkę, ir apie tai informuojama rinkimų apygarda. Ši rinkimų apygarda savo ruožtu informuoja VRK serverį ir šis išima (anuliuoja) rinkėjo i. balsą.

Pasibaigus rinkimų dienai, biuleteniai ir paštu gauti vokai skaičiuojami įprasta tvarka, o VRK serveryje (e. balsadėžėje) esantys balsai atskiriami nuo rinkėjo tapatybės duomenų (sugriaunami bet kokie ryšiai), surūšiuojami pagal apygardas ir iššifruojami, Vyriausioji rinkimų komisija surašo i. balsavimo protokolą. E. balsadėžės balsai iššifruojami naudojant sudėtingą fragmentuotą šifrą, kurio skirtingus fragmentus turi skirtingi Vyriausiosios rinkimų komisijos nariai. Tik surinkus visą raktą, galima iššifruoti e. balsadėžę. Gavus apygardų rinkimų rezultatus, i. balsai pridedami prie atitinkamos apygardos ir skelbiami galutiniai (suminiai) rezultatai.

I. balsavimas – iššūkis rinkimų technologijoms, be to, jis gali susilaukti didelės skeptikų reakcijos, todėl visas i. balsavimo procesas turi būti ir saugus, ir skaidrus, kad būtų galima bet kuriame etape įsitikinti i. balsavimo proceso skaidrumu ir tikrumu. I. balsavimo technika turi būti sukurta ir visapusiškai įvertinta kompetentingų technikos specialistų. I. balsavimo sistema turi būti apsaugota nuo visų žinomų ir įmanomų įsilaužimo, klastojimo būdų arba kitokio kompromitavimo.

I. balsavimas gali būti teismo pripažintas negaliojančiu, jei sukompromituojamas bent vienas iš i. balsavimo principų: slaptumas, skaidrumas, lygi rinkimų teisė ir kt. Teismas, priimdamas sprendimą pripažinti i. balsavimą, turi remtis kompetentingų specialistų arba ekspertų išvada apie galimus i. balsavimo kompromitavimo atvejus.

Remiantis Estijos patirtimi manoma, kad bendra balsavimo internetu organizavimo kaina turėtų siekti du milijonus litų. Ši suma, reikalinga pirminiam sistemos įdiegimui ir pirmiesiems rinkimams, vėliau mažės.

Siekiant įteisinti i. balsavimą būtina atitinkamai keisti Savivaldybių tarybų įstatymą, Seimo rinkimų įstatymą, Prezidento rinkimų įstatymą, Rinkimų į Europos Parlamentą įstatymą, Referendumo įstatymą – juose įteisinti i. balsavimą kaip alternatyvų balsavimo būdą.

Techninius i. balsavimo aspektus, taip pat ir rinkėjų identifikavimo, balso autentifikavimo ir saugumo klausimus dėl jų kitimo raidos ir reguliavimo detalumo tikslinga palikti reguliuoti Vyriausiajai rinkimų komisijai.

Būtinos taip pat atitinkamos Baudžiamojo kodekso ir Administracinių teisės pažeidimų kodekso pataisos įtvirtinant bankų, kitų juridinių bei fizinių asmenų atsakomybę už i. balsavimo kompromitavimą: balsų pirkimą, slaptumo ir saugumo pažeidimą, balsavimą už kitus rinkėjus ir pan.

Literatūra

1. Clift S. E-Democracy, E-Governance and Public Net-Work. – http//www.publicus.net
2. Clift S. The E-Democracy E-Book: Democracy is Online 2.0., Online Strategist and Public Speaker. – http://www.publicus.net
3. Noble P., Brack A. Background Research „E-democracy around the world“. – http://www.begix.de/en/hintergrund/noble.html
4. Clift S. The future of E-Democracy – The 50 Year Plan. – http://www.publicus.net/articles/future.html
5. Augustinaitis A., Petrauskas R. eParticipation Development in Lithuania: Research Projects // Electronic Government. Schriftenreihe Informatik. Vol. 15. U. – Linz: Trauner Vrl., 2005. P. 233–240.
6. OECD Engaging citizens online for better policy making. – http://www1.oecd.org/publications/e-book/4204011E.PDF
7. Caldow J. e-Democracy: Putting Down Global Roots. – http://www-1.ibm.com/industries/government/ieg/pdf/e-democracy%20putting%20down%20roots.pdf
8. Chadwick A. E-Government and E-Democracy: A Case For Convergence?
9. OECD guideline „Citizens as partners guide: information, consultation and public participation in policy making“. – http://www1.oecd.org/publications/e-book/4201131.pdf

10. Macintosh A. Characterizing e.participation in policy making. – http://csdl2.computer.org/comp/proceedings/hicss/2004/2056/05/205650117a.pdf
11. Macintosh A. Using information and communication technologies to enhance citizen engagement in the policy process. – http://itc.napier.ac.uk/ITC/publications.asp
12. Coleman S. Connecting Parliament to the Public via the Internet: Two case Studies of Online Consultations Information Communication & Society. Vol. 7. No. 1. P. 3–22.
13. Council Of Europe Committee Of Ministres Recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting. – http://www.coe.int/t/e/integrated_projects/democracy/02_e-voting/ Recommendation/Rec(2004)11E_rec_adopted.asp
14. Council Of Europe. Open Technical Standards for e-voting (Nov 2002). – http://www.coe.int/t/e/integrated%5Fprojects/democracy/02%5FActivities/02%5Fe%2Dvoting.asp
15. Drechsler W. The Estonian E-Voting Laws Discourse: Paradigmatic Benchmarking for Central and Eastern Europe. – http://unpan1.un.org/intradoc/groups/public/documents/nispacee/unpan009212.pdf
16. e-Vote. Vote for the EU YOU want. – http://evote.eu2003.gr/EVOTE/en/index.stm
17. An Internet- based electronic voting system: Legal and regulatory issues on e-voting and data protection in Europe, 2002.

7. ELEKTRONINIAI NUSIKALTIMAI

7.1. Pagrindinė medžiaga. Pagrindiniai elektroninių nusikaltimų aspektai

7.1.1. Elektroninių nusikaltimų samprata

Kuriant informacinę visuomenę, visose žmogaus veiklos srityse sparčiai plinta šiuolaikinės informacinės technologijos, kuriomis naudojantis tampa prieinama elektroninė erdvė. Todėl neišvengiamai susiduriama ir su didėjančiu nusikalstamų veikų, susijusių su šios erdvės naudojimu, skaičiumi. Elektroninė erdvė suteikia naujų galimybių padaryti nusikaltimus, sudaro sąlygas naujiems nusikaltimų būdams atsirasti, be to, sudaro galimybes įvykdyti naujas, iki tol teisinėje praktikoje nežinomas veikas. Pastaruoju metu elektroniniai nusikaltimai tapo realybe, o elektroninių nusikaltėlių pajamos, kai kuriais vertinimais, yra trečioje vietoje po pajamų iš prekybos narkotikais ir ginklais.

Elektroninių nusikaltimų istorija siekia jau ne vieną dešimtmetį, tačiau dėl bendros elektroninių nusikaltimų sampratos mokslininkai ir praktikai diskutuoja iki šiol. Nors teisinės problemos, susijusios su pavojingomis veikomis naudojant kompiuterius, pradėtos nagrinėti jau prieš kelis dešimtmečius, iki šiol nėra suformuota tokio nusikaltimo samprata. Reikia paminėti, jog dažnai apibūdinant elektroninius nusikaltimus vartojami skirtingi terminai, kurie tam tikrais atvejais gali būti ir sinonimai: „kompiuteriniai nusikaltimai“ (angl. *computer crime*), „su kompiuteriais nusiję nusikaltimai“ (angl. *computer-related crime*), „aukštų technologijų nusikaltimai“ (angl. *high-tech crime*) ir kt. 2001 m. priėmus Konvenciją dėl elektroninių nusikaltimų vis dažniau vartojama elektroninio nusikaltimo sąvoka. Tačiau kelis dešimtmečius labai aktyviai buvo vartojama kompiuterinio nusikaltimo sąvoka.

Literatūroje nurodoma, kad kompiuterinio nusikaltimo terminas buvo pavartotas jau 7 ir 8 dešimtmečiuose, kai mokslinėje literatūroje pasirodė straipsnių šia tema. Vienas iš pirmųjų susidomėjęs šia problema JAV Donnas Parkeris taip apibrėžė kompiuterinio nusikaltimo

sąvoką: „visos tyčinės veikos, kurios vienaip ar kitaip susijusios su kompiuteriais ir dėl kurių asmuo patyrė ar galėjo patirti žalos, o nusikaltimo subjektas turėjo arba galėjo gauti iš to naudos". Tačiau šis apibrėžimas neapima veikų, padarytų dėl neatsargumo arba nesiekiant naudos. Be to, samprata yra pernelyg plati ir apima tokias veikas kaip kompiuterio vagystė, o tai, daugelio autorių nuomone, neturėtų būti traktuojama kaip kompiuterinis nusikaltimas. Dažnai kompiuteriniu nusikaltimu buvo laikoma veika, tiesiogiai susijusi su elektronine skaičiavimo mašina, įskaitant daug neteisėtų aktų, vykdomų arba elektroninių duomenų apdorojimo sistema, arba prieš ją.

1983 m. Ekonominio bendradarbiavimo ir plėtros organizacija sudarė ekspertų komitetą su kompiuteriais susijusių nusikaltimų problemai spręsti. Ši ekspertų grupė terminą „kompiuterinis nusikaltimas" apibrėžė kaip **bet kokį neteisėtą, neetišką ar nesankcionuotą elgesį, susijusį su automatiniu kompiuterinės formos duomenų apdorojimu ir siuntimu**. Tačiau šiame apibrėžime nepaminėta, kokias teisės šakas minėtą elgesį laiko neteisėtu.

Tai tik pirmieji bandymai apibrėžti kompiuterinius nusikaltimus. Per daugelį metų įvairios institucijos, mokslininkai bandė apibrėžti kompiuterinius nusikaltimus, tačiau prie bendros nuomonės dėl kompiuterinių nusikaltimų sampratos nebuvo prieita. Atsižvelgiant į nuomonių dėl kompiuterinio nusikaltimo sampratos įvairovę, **išskirtinos dvi pagrindinės kompiuterinių nusikaltimų sampratos kryptys:**

– *siaurąja prasme* kompiuteriniais nusikaltimais laikomos tik tos veikos, kurios nurodytos atskiruose baudžiamųjų įstatymų skirsniuose (pvz., Lietuvoje – XXIX sk. „Nusikaltimai informatikai"). Šioms veikoms būdingas bendras objektas (visuomeniniai santykiai informacijos apdorojimo procese) bei dalykas – kompiuterinė informacija;
– *plačiąja prasme* kompiuteriniais nusikaltimais laikomos baudžiamojo įstatymo nustatytos visuomenei pavojingos veikos, kai kompiuterinė informacija yra nusikaltimo dalykas arba kai kompiuteris naudojamas kaip nusikaltimo priemonė. Kitais žodžiais tariant, pasikėsinimo dalykas yra informacija, apdorojama kompiuterių sistemoje, o kompiuteris yra nusikaltimo įrankis. Šių nusikaltimų objektas skiriasi. Todėl prie tokių veikų priskiriamos ir šios veikos: sukčiavimas, autorių teisių pažeidimas naudojant kompiuterius ir kt. Paminėtina, kad kartais šios veikos vadinamos su kompiuteriais susijusiais nusikaltimais (ang. *com-*

puter-related crime), nors šis terminas turėtų apimti daugiau pavojingų veikų (pvz., šmeižtas naudojant elektroninę erdvę).

Tačiau pastaruoju metu, 2001 m. priėmus Konvenciją dėl elektroninių nusikaltimų, kompiuterinių nusikaltimų terminą pakeitė elektroninių nusikaltimų (ang. *cybercrime*) terminas.

Pirmiausia reikėtų atkreipti dėmesį į patį terminą „elektroninis nusikaltimas“. Elektroninis nusikaltimas nėra tiksliausia sąvoka, apibūdinanti nusikaltimus, vykdomus elektroninėje erdvėje. Šie nusikaltimai būdingi ne elektronikos sričiai, elektronikos mokslui, o informatikos inžinerijai, kompiuterijos mokslams. Elektronika, elektroniniai signalai, elektroniniai įtaisai plačiai vartojami televizijoje, radiofonijoje, automobiliuose, pramonėje ir pasižymi analogiška signalų forma, o *cybercrime* skiriamasis požymis – nusikaltimų dalykas yra duomenys, informacija kompiuterine, skaitmenine (angl. *digital*) forma. Terminas *cybercrime* simbolizuoja itin kompiuterizuotai interneto visuomenei būdingas nusikalstamas veikas. Jis kilęs iš termino *Cyber space*, kuris verčiamas „elektroninė erdvė“. Tačiau reikia paminėti, kad Lietuva ratifikavo Konvenciją dėl elektroninių nusikaltimų ir taip *de jure* buvo įteisintas elektroninio nusikaltimo terminas.

Pažymėtina kad iki šiol užsienio literatūroje elektroninio nusikaltimo samprata nėra išsamiai išnagrinėta. Kai kurie autoriai nurodo, jog kol kas nėra universalios elektroninio nusikaltimo sampratos, tačiau teigia, kad elektroninio nusikaltimo samprata turėtų apimti ir tokius neteisėtus veiksmus naudojant kompiuterius kaip neteisėta prieiga prie kompiuterių sistemos, neteisėtas kompiuterinės informacijos perėmimas, neteisėto turinio medžiagos siuntimas ir kt. Taip pat manoma, kad elektroniniais nusikaltimais suprantami įvairūs veiksmai, tokie kaip poveikis kompiuterių sistemai, su turiniu susiję pažeidimai (neteisėto ir žalingo turinio medžiagos panaudojimas) ir kt. Konvencijoje dėl elektroninių nusikaltimų taip pat nėra pateikiama elektroninio nusikaltimo sąvoka. Tačiau, atsižvelgiant į Konvencijoje dėl elektroninių nusikaltimų kriminalizuotinas veikas, apibrėžiant elektroninius nusikaltimus reikėtų ne tik laikytis kompiuterinių nusikaltimų sampratos plačiąja prasme krypties, tačiau tokias veikas būtų galima tapatinti su veikomis, susijusiomis su kompiuterių naudojimu (ang. *computer-related crime*) ir apimančiomis gana daug nusikalstamų veikų. Galima konstatuoti, kad Konvencijoje dėl elektroninių nusikaltimų minimos veikos yra labai skirtingos (skirtumai dėl objekto ir pan.), dėl to pateikti bendrą tokių veikų sampratą yra problemiška.

7.1.2. Konvencija dėl elektroninių nusikaltimų ir pagrindinės elektroninių nusikaltimų rūšys

Atsižvelgiant į tai, kad elektroninėje erdvėje vykdomos veikos yra pavojingos visuomenei, nusikaltėlio buvimo bei nusikaltimo padarymo vieta dažnai nesutampa, atskirų valstybių įstatymai yra apriboti jų teritorija, elektroninė erdvė leidžia atlikti naujo tipo pavojingas veikas, ir pripažįstant, kad pavojingų veikų, vykdomų elektroninėje erdvėje, teisinis reglamentavimas yra nepakankamas, siekiant apsaugoti visuomenę nuo tokių nusikaltimų, *inter alia*, priimant tam tikrus norminius aktus bei skatinant tarptautinį bendradarbiavimą, 2001 m. buvo pasirašyta Konvencija dėl elektroninių nusikaltimų (toliau – Konvencija). Konvencijos projektą parengė Europos Tarybos ekspertai kartu su JAV, Kanada, Japonija ir kitomis valstybėmis, kurios nėra šios organizacijos narės. Tai pirmasis tarptautinis norminio pobūdžio dokumentas, skirtas spręsti nusikalstamų veikų kompiuteriniuose tinkluose problemoms. 2001 m. lapkričio 8 d. Konvencijai dėl elektroninių nusikaltimų pritarė užsienio reikalų ministrai, o Europos Tarybos šalys narės šią Konvenciją pasirašė 2001 m. lapkričio 23 d. Šiuo metu Konvenciją yra pasirašiusios 26 valstybės, ratifikavusios – 17. Konvencijos įsigaliojimo sąlyga – 5 ratifikacijos (iš jų – bent 3 Europos Tarybos valstybių narių). Ši sąlyga buvo išpildyta ir Konvencija įsigaliojo 2004 m. liepos 1 d. Atkreiptinas dėmesys, kad Konvencijos kol kas neratifikavo tokios valstybės kaip JAV, Kanada, Japonija ir kai kurios didelės Europos valstybės. Lietuva Konvenciją pasirašė 2003 m. birželio 23 d., o ratifikavo 2004 m. kovo 18 d.

Konvenciją sudaro trys pagrindiniai skyriai: I. Sąvokos; II. Priemonės, kurių reikia imtis nacionaliniu lygiu; III. Tarptautinis bendradarbiavimas. Pirmojo skyriaus 1 skirsnyje (Konvencijos 2–11 str.) Konvencijos šalys įpareigojamos kriminalizuoti Konvencijoje numatytas veikas, taip pat nustatyti juridinių asmenų atsakomybę. Antrajame skirsnyje Konvencija nustato reikalavimus Konvencijos šalimis tampančių valstybių procesinėms teisės normoms, įpareigoja imtis priemonių, būtinų operatyviai išsaugoti laikomus kompiuterinius, srauto duomenis, juos atskleisti arba pateikti, surinkti srauto duomenis realiuoju laiku, įrašyti tokius duomenis ir pan. Šių proceso veiksmų atlikimas susijęs su pagrindinėmis žmogaus teisėmis ir laisvėmis, jų apsauga. Todėl pati Konvencija numato, kad minėti veiksmai turi būti suderinti su pagrindiniais tarptautiniais dokumentais žmogaus teisių

ir laisvių apsaugos srityje. Trečiajame skyriuje Konvencija įtvirtina ekstradicijos bei savitarpio pagalbos reglamentavimo nuostatas. Visos Konvencijos 2–11 straipsniuose apibrėžtos veikos yra pripažįstamos nusikaltimais, už kuriuos asmenys gali būti išduodami vienos susitariančiosios šalies kitai susitariančiajai šaliai. Konvencija taip pat įpareigoja susitariančiąsias šalis teikti skubią ir visapusišką savitarpio pagalbą tiriant arba nagrinėjant baudžiamąsias bylas dėl elektroninių nusikaltimų. Tuo tikslu Konvencijos 35 straipsnio įpareigoja susitariančiąsias šalis paskirti 24 valandas per parą ir 7 dienas per savaitę veikiančią instituciją, kuri galėtų teikti technines konsultacijas ir atlikti Konvencijoje nurodytus veiksmus.

2003 m. buvo priimtas Konvencijos dėl elektroninių nusikaltimų Papildomas protokolas dėl rasistinio ir ksenofobinio pobūdžio veikų, padarytų naudojantis kompiuterinėmis sistemomis, kriminalizavimo. Papildomo protokolo tikslas – papildyti 2001 m. Konvencijos dėl elektroninių nusikaltimų nuostatas įpareigojimais valstybėms, ratifikavusioms Protokolą, kriminalizuoti rasistinio ir ksenofobinio pobūdžio veikas, padarytas naudojantis kompiuterinėmis sistemomis, įpareigoti valstybes bendradarbiauti tarpusavyje tiriant tokius nusikaltimus. Šiuo metu Papildomą protokolą yra pasirašiusios 27, ratifikavusios – 7 valstybės. Ši tarptautinė sutartis įsigaliojo 2006 m. kovo 1 d. Šį Papildomą protokolą Lietuva pasirašė 2005 m. balandžio 7 d., ratifikavo 2006 m. spalio 12 d. Protokolas Lietuvoje įsigalios 2007 m. vasario 1 d.

Remiantis minimos Konvencijos kriminalizuotinomis veikomis galima išskirti šias pagrindines elektroninių nusikaltimų rūšis:

– Nusikaltimai, pažeidžiantys kompiuterinės informacijos ir kompiuterių sistemų konfidencialumą, vientisumą bei prieinamumą.

Neteisėta prieiga prie kompiuterių programų arba duomenų elektronine forma laikytina tokia veika, kuri pažeidžia laikomos informacijos slaptumą (t. y. kyla realios žalos grėsmė), o dėl neteisėtos prieigos vykdomas šnipinėjimas, neteisėtai kopijuojami autorių teisėmis apsaugoti kūriniai, sabotažas, sukčiavimas naudojantis kompiuteriais ir pan. laikytini savarankiškomis pavojingomis veikomis.

Baudžiamosios atsakomybės už neteisėtą prieigą problema kilo jau 1985 m., kai Vienoje kompiuterių mokslo srities studentas įsilaužė į keleto finansinių institucijų kompiuterines sistemas, bet jokios žalos nepadarė. Apie šiuos veiksmus buvo pranešta Vienos teisėsaugos institucijoms. Tačiau tyrimas buvo sustabdytas, nes nebuvo padaryta jo-

kia žala, o studento motyvacija buvo pavadinta „intelektualiu iššūkiu“. Byloje *R v Gold* taip pat buvo pademonstruota baudžiamųjų įstatymų nuostatų, susijusių su neteisėta prieiga, būtinybė. Jungtinėje Karalystėje tyrimas prasidėjo dėl to, jog be leidimo buvo įsilaužta į *„British Telecom“* kompiuterių tinklą ir pakeisti tam tikri duomenys. Be to, vienas iš įsilaužėlių asmeniniuose kompiuterio sauginiuose paliko žinutę „Laba diena, ponas Dukesai“. Kaltinamieji teigė, jog buvo įsilaužta turint tikslą „parodyti saugumo skyles“ „*British Telecom*“ kompiuterių sistemoje. Įsilaužėliai buvo apkaltinti remiantis 1981 m. Klastojimo įstatymu, vėliau buvo nuteisti. Tačiau apeliacinėje instancijoje teismo sprendimas buvo panaikintas teigiant, kad šių asmenų veiksmuose nebuvo jokio nusikaltimo sudėties. Taigi buvo padarytas egzistuojančių įstatymų netobulumas.

Įsikišimą į kompiuterinės informacijos apdorojimo procesą galima vadinti neteisėtos prieigos tąsa. Tokia veika gali pasireikšti neteisėtu kompiuterinės informacijos ištrynimu, sunaikinimu, sugadinimu arba pakeitimu. Manoma, jog kompiuterių programos ir kompiuterinė informacija, kaip ir materialūs objektai, turi būti apsaugota nuo tokio kėsinimosi siekiant užtikrinti kompiuterinės informacijos integralumą bei kompiuterių programų arba kompiuterinės informacijos tinkamą naudojimą (funkcionavimą). Kompiuterinės informacijos vagystę (iš dalies sietiną su šnipinėjimu naudojant kompiuterį) taip pat galima įvardyti neteisėtos prieigos tąsa. Šiandieninės informacinės technologijos, ypač kompiuterių tinklai, suteikia didžiulių galimybių akimirksniu nukopijuoti bet kiek informacijos. Kai kurie autoriai tokią veiką laiko savarankiška pavojinga veika, užtraukiančia baudžiamąją atsakomybę.

Su kompiuterinės informacijos vagyste susijusi ir veika perimant kompiuterinę informaciją, kai ji siunčiama elektronine erdve. Prieš keletą metų perėmimo (angl. *Interception*) veika dažniausiai būdavo tapatinama su telefoninių pokalbių perėmimu. Tačiau tobulėjant technologijoms ir komunikacijoms, į bendrą visumą susiliejant telekomunikacijoms ir kompiuterinėms sistemoms, apsaugos reikalauja ir kiti kompiuterinės informacijos tipai, siunčiami elektronine erdve.

Sabotažu naudojant kompiuterius vadinama veika, kai įdiegiant į kompiuterių sistemą „kenkėjiškas“ programas (arba padarant kompiuterių programų pakeitimus) neteisėtai sunaikinama, pakeičiama arba ištrinama kompiuterinė informacija siekiant sutrikdyti kompiuterių sistemos darbą. Duomenų, saugomų elektronine forma,

sutelktumas įmonių, organizacijų bei fizinių asmenų priklausomumas nuo elektroninės informacijos, sabotažą naudojant kompiuterius daro labai pavojinga veika. Visuomenė įvairiose gyvenimo srityse (medicinos tarnybų, transporto veikla ir pan.) tampa vis labiau priklausoma nuo kompiuterinių sistemų, kurios dažnai sujungtos su kompiuteriniais tinklais (elektronine erdve). Todėl netgi nedidelis šių sistemų funkcionavimo sutrikimas, atsiradęs dėl veikos naudojant elektroninę erdvę, gali sukelti pavojų žmonių sveikatai arba gyvybei. Atsiradus elektroninei erdvei, labiausiai populiarūs metodai padaryti žalą – specialių programų, kurios gali ištrinti daug duomenų per trumpą laikotarpį, panaudojimas. Tokios programos gali būti kompiuteriniai virusai, „Trojos arkliai“ ir kt. Daugiausia problemų kelia kompiuterinių virusų ir „kirmėlių“ paplitimas. Kompiuteriniai virusai yra programos, kurios plinta elektroninėje erdvėje bei kompiuterinėse sistemose ir greičiausiai po tam tikro laiko padaro žalos.

Pastaruoju metu pabrėžiamas *kompiuterių sistemos darbo sutrikdymas*, kai kompiuterių sistema per internetą „užverčiama“ daugybe žinučių (angl. *Denial of service attack (DoS)*). Taip sutrikdomas kompiuterių sistemos darbas, nors neteisėta prieiga prie sistemos ir neatliekama. Tokiais veiksmais buvo sutrikdytas CNN, Yahoo, E-Bay bei kitų gerai žinomų interneto svetainių darbas, dėl to buvo patirta milžiniškų finansinių nuostolių. Teisminė praktika liudija apie ne vieną bylą, kai buvo nuteisti tokias veikas padarę asmenys. Pavyzdžiui, 2002 m. pradžioje, remiantis Federaliniu sukčiavimo bei piktnaudžiavimo naudojantis kompiuteriu įstatymu, buvo nuteistas Bretas McDanelis. Šis asmuo buvo pripažintas kaltu, nes piktavališkai siuntė tūkstančius elektroninių žinučių į centrinį kompiuterį, kurio operatorius buvo „*Tornado Development*“. Taip šis centrinis kompiuteris buvo perpildytas, dėl to jo darbas sutriko. Bretas McDanelis buvo nuteistas 5 metų laisvės atėmimo bausme.

Minėtos veikos dažnai susijusios su tam tikrų įrankių (priemonių) turėjimu. Praktikoje egzistuoja net ištisos nelegalios slaptažodžių bei prieigos kodų rinkos elektroninėje erdvėje. Todėl viena iš įvardijamų internetinių nusikaltimų rūšių – neteisėtos prieigos priemonių bei įrenginių platinimas, gaminimas ir kt. Šio tipo veikų pavojingumas buvo pažymėtas jau 1994 m. Kriminalinės policijos tarptautinėje apžvalgoje dėl kompiuterinių nusikaltimų, kur nurodyta, jog veikos pavojingumas sietinas su galimybe padaryti žalą.

Kenkėjiškų programų sukūrimas, naudojimas ir platinimas taip pat laikomas pavojinga veika. Literatūroje nurodoma, jog kenkėjiškų programų sukūrimo, naudojimo bei platinimo pavojingumas visuomenei pasireiškia tuo, kad jos gali pačiu netikėčiausiu momentu sutrikdyti kompiuterių sistemos darbą, dėl to gali kilti žalingų padarinių. Atsiradus globaliai elektroninei erdvei, kenkėjiškų programų grėsmė padidėjo, nes, pavyzdžiui, paskleistas internete virusas dėl šio tinklo globalumo gali padaryti daug žalos visame pasaulyje. Kenkėjiškomis programomis laikomos kompiuterių programos, turinčios virusų (kompiuteriniai virusai) arba tam tikrų nurodymų, pavyzdžiui, „loginės bombos“, „Trojos arkliai, „asinchroninės atakos“, „liukas“, arba turinčios specifinių savybių padaryti neteisėtus arba nusikalstamus veiksmus (pagrobti pinigus iš bankų sąskaitų ir kt.). Šios programos turi savybę persikelti kompiuterių tinklu iš vienos kompiuterių sistemos į kitą, patekti į kompiuterių sistemą, taip pat daugintis kaip „virusinės ligos“.

– *Su kompiuterių naudojimu susiję nusikaltimai.*

Technologinė revoliucija padidino galimybes padaryti tokius ekonominius nusikaltimus kaip sukčiavimas. Šiandien daugelis didelių kompanijų yra prijungtos prie interneto arba kitų kompiuterių tinklų, o jų kompiuterinėse sistemose esančios bei administruojamos vertybės tapo dažnu taikiniu. Kompiuterinis sukčiavimas apibrėžiamas kaip pinigų arba kito turto grobimas naudojant kompiuterį. Ši veika apima nurodymus kompiuteriui pervesti pinigus į banko sąskaitą ar pan. Veikas atliekant sukčiavimą, susijusį su kompiuteriais, galima suskirstyti į dvi pagrindines grupes: sukčiavimas, susijęs su duomenimis, ir sukčiavimas, susijęs su kompiuterių programomis. Literatūroje nurodoma, kad terminas „sukčiavimas naudojant kompiuterį“ tam tikrais atvejais gali būti klaidinantis, nes šiuo terminu apibrėžiamos veikos gali užtraukti baudžiamąją atsakomybę ir pagal kitus straipsnius, ne vien tik pagal straipsnius, nustatančius atsakomybę už tradicinį sukčiavimą. Sukčiavimas naudojant kompiuterius gali pasireikšti turto arba paslaugų gavimu apgaule ir kt. Pastaruoju metu sukčiavimas naudojant kompiuterius apibrėžia įvairias veikas ekonominių nusikaltimų srityje ir tai, kad elektroninė erdvė suteikia ypač dideles galimybes padaryti tokio tipo nusikaltimus. Taigi iškeliamas tikslas kriminalizuoti sukčiavimo veikas elektroninėje erdvėje, manipuliuojant kompiuterine informacija arba kompiuterių programomis siekiant materialinės naudos.

Elektroninės erdvės atsiradimas atvėrė kelią ir klastojimo veikoms. Kompiuterinės informacijos klastojimas gali turėti tokių pačių pasekmių kaip ir tradicinis klastojimas. Klastojimas, susijęs su kompiuteriais, apima neteisėtą kompiuterinės informacijos sukūrimą arba sukurtos pakeitimą, dėl to ši informacija įgyja kitokią reikšmę. Todėl turi būti apsaugotas kompiuterinės informacijos patikimumas ir saugumas siekiant užkirsti kelią neigiamoms pasekmėms teisiniuose asmenų santykiuose.

– *Nusikaltimai, susiję su turiniu.*

Interneto paplitimas paskatino neteisėto ir žalingo turinio medžiagos plitimą elektroninėje erdvėje. Literatūroje nurodoma, kad tai – sparčiai plintančių nusikaltimų elektroninėje erdvėje sritis. Pornografinio turinio medžiagos internete platinimas, rasistinių nuostatų skleidimas kelia klausimus dėl baudžiamosios teisės vaidmens vertinant šias veikas. U. Sieberis taip pat mini problemas, susijusias su rasistinėmis nuostatomis, šmeižtu arba grasinimais elektroninėje erdvėje. Autorius norėtų paminėti, kad pavojingos veikos, susijusios su bendrai pornografinio turinio medžiagos naudojimu, rasistinėmis nuostatomis, šmeižtu arba grasinimais elektroninėje erdvėje, sukelia teisinės atsakomybės problemas daugiau dėl teisinių ir kultūrinių tradicijų skirtumų įvairiose valstybėse, todėl šiame darbe minimos problemos nebus nagrinėjamos. Šiuo metu daugiausia dėmesio skiriama pornografinės medžiagos apie vaikus elektroninėje erdvėje problema. Įstatymų, susijusių su pornografine medžiaga apie vaikus, kūrimo problema pabrėžiama ir Europos komisijos. Taigi siekiama apsaugoti vaikus nuo seksualinio išnaudojimo. Dėl interneto plėtros šiuo metu elektroninė erdvė tapo pagrindiniu įrankiu, kuriuo platinama tokio pobūdžio medžiaga. Todėl ši nauja pavojingos veikos forma turi būti nurodyta baudžiamuosiuose įstatymuose.

– *Pažeidimai, susiję su autorių teisėmis ir gretutinėmis teisėmis.*

Intelektualios nuosavybės teisių pažeidimai, ypač autorių teisių pažeidimai, yra vieni iš labiausiai internete paplitusių pavojingų veikų, darančių didžiulę žalą autorių teisių turėtojams. Apsaugotų darbų dauginimas ir platinimas internete be autorių teisių savininko leidimo yra ypač dažnas. Literatūroje teigiama, jog šiandieną internetas daro didžiausią įtaką neteisėtam kompiuterių programų arba kitų autorių teisėmis apsaugotų kūrinių platinimui. Tokiais apsaugotais dar-

bais laikomi literatūros darbai, fotografijos, muzikos, audiovizualiniai kūriniai ir kiti, kurie gali būti platinami naudojant FTP, elektroninį paštą, serverius, elektronines skelbimų lentas ir t. t. Didžiulės darbų kopijavimo bei platinimo galimybės, kurias suteikia elektroninė erdvė, verčia įstatymo leidėjus baudžiamuosiuose įstatymuose nustatyti tokias veikas draudžiančias normas. Trumpai paminėtina, kokios autorių teisės gali būti pažeidžiamos elektroninėje erdvėje. Internete gali būti pažeidžiamos net kelios autoriaus teisės. Gali būti pažeidžiama autoriaus teisė viešai rodyti, atgaminti kūrinį ir kt. Be to, pavojingos veikos gali pasireikšti informacijos apie autorių teisių valdymą sunaikinimu arba pakeitimu, autorių teisių techninių apsaugos priemonių pašalinimu ir pan.

Pastaruoju metu ypač pavojingi tampa *„Phishing“* tipo elektroniniai nusikaltimai. Tai duomenų vagystė, arba, kitaip tariant, „žvejojimas“ – nieko blogo neįtariančių interneto vartotojų įviliojimas į elektroninių nusikaltėlių paspęstus informacijos rinkimo tinklus, siekiant piktavališkai panaudoti šią informaciją. Tai pastaruoju metu vis labiau populiarėjantis metodas, kai, pavyzdžiui, vartotojas įrašo slaptą informaciją manydamas, kad tai daro oficialioje banko svetainėje, tačiau iš tikrųjų tai daro nusikaltėlių sukurtoje svetainėje. Priebalsių junginys „ph“ vietoje „f“ panaudotas dėl šio nusikaltimo asociacijų su aštuntajame dešimtmetyje JAV populiaria nusikaltimų rūšimi *„phone phreaking*“ – neteisėtu prisijungimu prie telefono tinklų ir mokesčio už telefoninius pokalbius nemokėjimu.

7.1.3. Elektroninių nusikaltimų latentiškumas ir daroma žala

Reikia pažymėti, kad su kompiuterinėmis technologijomis susijusios nusikalstamos veikos yra ypač pavojingos tuo, kad oficiali teisėsaugos organų statistika neatspindi tikrosios padėties. Jau Kompiuterinių nusikaltimų ir kitų su informacinėmis technologijomis susijusių nusikaltimų kolegijos susitikime Vurzburge 1992 m. buvo pateikta kompiuterinių nusikaltimų apžvalga. Ji parodė, kad yra tik 5 proc. nukentėjusių dėl su kompiuterinėmis technologijomis susijusių nusikalstamų veikų. Panaši ir FBI nacionalinės kompiuterinių nusikaltimų tyrimų grupės nuomonė, kad 85–97 proc. tokių nusikaltimų neiškyla į viešumą. Kai kurių ekspertų vertinimu, elektroninių nusikaltimų latentiškumas JAV sudaro 80 proc., Jungtinėje Karalystėje – 85 proc.,

Vokietijoje – 75 proc., Rusijoje – net 90 proc. Taip pat jau 1995 m. atliktų JAV gynybos departamento finansuotų tyrimų statistika buvo gana stulbinanti. Iš 8932 bandymų įsibrauti į informacines sistemas, kurios dalyvavo tyrime, 7860 buvo sėkmingi. Tik 390 sistemų administratoriai (iš 7860) užfiksavo įsibrovimą ir tik 19 iš jų apie tai pranešė oficialioms instancijoms.

Kaip liudija naujausia statistika, pateikiama 2005 m. Kompiuterinių nusikaltimų ir saugumo apžvalgoje, atliktoje Kompiuterių saugumo instituto*, apie neteisėtą prisijungimą prie kompiuterio ar kompiuterių tinklo teisėsaugos institucijoms pranešė tik apie 20 proc. respondentų iš 320. Didžioji dalis respondentų – beveik 80 proc. – tiesiog „užlopė padarytas skyles".

Tokį didelį elektroninių nusikaltimų latentiškumą lemia keli veiksniai:

1. Kompiuterių naudotojamas dažnai trūksta žinių, kad pastebėtų tokius nusikaltimus.

2. Aukos, aptikę kompiuterinius nusikaltimus, vengia apie juos pranešti. Verslo srityje šis nenoras susijęs su dviem dalykais:

- kai kurios aukos nenori atskleisti informacijos apie savo darbą bijodamos viešumo arba prarasti gerą vardą;
- kitos aukos bijo prarasti investuotoją, visuomenės pasitikėjimą.

Kompiuteriniai nusikaltimai kelia susirūpinimą ir dėl to, kad jų sparčiai daugėja. Kompiuterinio saugumo instituto ir FTB atliktas tyrimas, kurio metu apklausta 250 organizacijų, parodė, kad apytikriai nuostoliai 1997 m. buvo 137 mln. JAV dolerių, t. y. 37 proc. daugiau nei 1996 m.

Naujausia elektroninių nusikaltimų statistika taip pat liudija didžiulius nuostolius, elektroninių nusikaltimų įvairovę bei didėjančią tokių veikų grėsmę. Britų tyrimo kompanijos mi2g duomenimis, 2004 m. žala dėl elektroninių nusikaltimų sudarė 411 mlrd. JAV dolerių. Tai beveik du kartus viršija žalą 2003 m. 2005 m. Kompiuterinių nusikaltimų ir saugumo apžvalgoje, atliktoje Kompiuterių saugumo instituto, nurodoma, kad apklausti 639 respondentai (juridiniai asmenys) 2005 m. patyrė per 130 mln. JAV dolerių nuostolius. Iš visų 693 apklaustų respondentų 2005 m. neteisėtą kompiuterių sistemos naudojimą užfiksavo beveik 60 proc. Dažniausiai minima pavojinga veika – kompiuterių virusų platinimas. Labiausiai 2005 m. padidėjo pažeidimų, susijusių su beviele prieiga, skaičius.

* http:/www.gosci.com

Viena iš žymesnių bylų – R. T. Morriso byla, susijusi su vadinamuoju „internetiniu kirminu“. 23 metų studentas Morrisas nebuvo tipinis nusikaltėlis, jo tėvas dirbo kompiuterinio saugumo ekspertu Nacionaliniame kompiuterinio saugumo centre. Tačiau remiantis CFAA Morrisas buvo nuteistas 3 metams lygtinai, 10 000 JAV dolerių bauda ir 400 val. viešųjų darbų. Bausmė jam buvo skirta už kompiuterinės programos – „internetinio kirmino“ sukūrimą ir panaudojimą. Ši programa, anot Morriso, buvo skirta rinkti informacijai apie kompiuterius, sujungtus į pasaulinį kompiuterių tinklą, bei šių kompiuterių apsaugos priemones. Programa sukurta 1998 m., siekiant atlikti jokios žalos nedarantį eksperimentą kompiuterių mokslo srityje. Tačiau dėl klaidos, padarytos Morrisui nežinant, programa pradėjo daugintis ir sparčiai plisti. Programai patekus į internetą, po keleto valandų buvo užkrėsta apie 2000 kompiuterių (sutrikdytas kompiuterių/kompiuterinių tinklų darbas), dėl to padaryta 150 000 JAV dolerių žala vien JAV. Reikia paminėti, jog vertinimai, susiję su padaryta žala, skiriasi. J. McAfee, Kompiuterių virusų asociacijos pirmininkas, yra pareiškęs, kad Morriso „kirmino“ padaryta žala siekia 96 mln. JAV dolerių.

Tai tik vienas iš daugelio precedentų, iškilusių į viešumą. Labai daug elektroninių nusikaltimų iš viso neiškyla į viešumą, nes ši nusikaltimų kategorija yra viena latentiškiausių, t. y. dažnai nepatenka į oficialią nusikaltimų statistiką. Elektroninių nusikaltimų kriminalizavimo prasme reikėtų paminėti, jog ilgą laiką atsakomybė už kai kuriuos elektroninius nusikaltimus, pavyzdžiui, neteisėtą prieigą prie kompiuterinės informacijos, iš viso nebuvo nustatyta. Ir tik didžiulėmis pastangomis, koordinuojant atskirų valstybių baudžiamuosius įstatymus daugumai nacionalinių įstatymų leidėjų, pavyko kriminalizuoti pagrindines elektroninių nusikaltimų rūšis. Tačiau iki šiol problemos kyla ne tik dėl netinkamo kai kurių elektroninių nusikaltimų kriminalizavimo nacionaliniuose baudžiamuosiuose įstatymuose, bet ir dėl kvalifikacijos arba techninės įrangos stokos tiriant elektroninius nusikaltimus bei elektroninių įrodymų įtvirtinimo problemų.

7.2. Papildoma medžiaga. Elektroninių nusikaltimų subjektai

Informacinės technologijos suteikia unikalias galimybes žmonėms, turintiems kriminalinius tikslus. Pradeda atsirasti organizuotos elek-

troninių nusikaltėlių grupės, kurias sudaro nariai iš viso pasaulio.

Elektroniniai nusikaltėliai, beje, yra pelnę didesnį visuomenės palankumą nei tradiciniai nusikaltėliai. Nuomonė, kad elektroninis nusikaltėlis yra mažiau pavojingas, neteisinga. Manoma, kad ateities grėsmė bus beveik proporcinga informacinių technologijų pranašumams.

Kodėl reikia žinoti, kas yra elektroninių nusikaltimų subjektai? Atskirų kategorijų tipinių nusikaltimų išskyrimas, šių žmonių pagrindinių bruožų žinojimas leidžia optimaliai išskirti žmones, tarp kurių reikėtų ieškoti nusikaltėlio. Tai taip pat leidžia nustatyti konkretaus nusikaltėlio išaiškinimo būdus.

Daugelis elektroninių nusikaltimų tyrinėtojų šios rūšies nusikaltimų atsiradimą sieja su vadinamųjų programišių (hakerių) atsiradimu. Programišius – tai elektroninės skaičiavimo mašinos vartotojas, ieškantis neteisėtų būdų gauti nesankcionuotą prieigą prie kompiuterinės technikos priemonių bei duomenų, kad galėtų juos naudoti savanaudiškais tikslais. Kartais literatūroje ir žiniasklaidoje jie vadinami „piratais“, „sukčiais“, „elektroniniais vagimis“, „elektroniniais banditais“ ir t. t. Programišiams priklauso kompiuterine technika besidomintys asmenys, daugiausia jaunimas. Yra duomenų, kad Rusijoje programišiai buriasi į regionines grupes, leidžia regionines žiniasklaidos priemones (laikraščius, žurnalus, elektronines lentas su skelbimais), rengia elektronines konferencijas, turi savo žargonų žodyną ir jį nuolat atnaujina. Rusijos programišiai glaudžiai bendradarbiauja su užsienio programišiais, naudodamiesi pasauliniais telekomunikacijų kanalais keičiasi patirtimi.

Nors elektroninius nusikaltėlius reikėtų vertinti kaip visumą, tačiau pagal tam tikrus požymius išryškėja atskiros jų rūšys ir grupės. Kaip matyti iš istorijos, elektroniniai nusikaltėliai yra studentai, mėgėjai, teroristai, nusikalstamų grupuočių nariai, tačiau skiriasi jų padarytų nusikaltimų pobūdis. Asmuo, kuris įsilaužia į kompiuterių sistemą be nusikalstamų ketinimų, skiriasi nuo finansinės institucijos darbuotojo, kuris vagia pinigus iš klientų sąskaitų. Labai prieštaringai vertinamas elektroninių nusikaltėlių tipiškas įgūdžių lygis.

Elektroniniai nusikaltėliai yra iš skirtingų visuomenės sluoksnių. Jų amžius vidutiniškai svyruoja nuo 10 iki 60 metų, įgūdžių lygis – nuo naujoko iki profesionalo.

Remiantis dauguma tyrimų, galima teigti, kad didžiausią grėsmę kelia darbuotojai. Todėl elektroniniai nusikaltimai dažnai yra vadinami vidiniais nusikaltimais. Tyrimo duomenimis, apie 90 proc. ekono-

minių elektroninių nusikaltimų buvo padaryta nukentėjusios firmos arba įstaigos darbuotojų. Šiaurės Amerikos ir Europos tyrimai rodo, kad 73 proc. rizikos kompiuterių saugumui buvo priskirta vidiniams veiksniams ir tiktai 23 proc. – išoriniams. Ir atvirkščiai – kitų tyrimų duomenimis, dauguma grėsmių kompiuterinėms sistemoms kyla iš išorės. Dėl to elektroniniai nusikaltimai daugiausia gali būti laikomi „išoriniais“ nusikaltimais. Manytina, jog tokius skirtingus duomenis lemia elektroninių nusikaltimų latentiškumas.

Dauguma elektroninių nusikaltimų arba saugumo pažeidimų įvyksta dėl vidinių klaidų arba vidinių tyčinių veikų. Tačiau plintant kompiuteriniams tinklams išorinių grėsmių lygis turėtų padidėti.

Egzistuoja daug elektroninių nusikaltėlių skirstymo būdų. Vienas iš jų:

1. programišiai;
2. tipiniai nusikaltėliai;
3. vandalai.

Šios kategorijos tam tikrais atvejais susikerta. Geriausiai juos atskirti galima pagal motyvus. Programišiai dažniausiai nori tik patekti į sistemą, o štai pagrindinis nusikaltėlių motyvas yra nauda, pinigai. Vandalai dažniausiai nori padaryti žalą.

1. Programišiai

Šie žmonės labai gerai išmano programas bei tinklų kūrimo procesus, jų trūkumus. Labai didelė jų dalis yra kompiuterinės technikos fanatikai, nuolatos ieškantys kompiuterinės įrangos trūkumų, kurių nežino net patys įrangos kūrėjai. Dėl šios priežasties tokie nusikaltimai yra vadinami „baltųjų apykaklių“ nusikaltimais. Jiems padaryti nereikia stiprių raumenų arba ginklų, šio tipo nusikaltimai padaromi pasitelkus intelektą: įsibrauti į banką per atstumą gali asmuo, neturintis kojų, tačiau gerai išmanantis kompiuterinę techniką ir turintis priėjimą prie kompiuterių tinklo.

Bet kokios kategorijos nusikaltėliai gali padaryti tą patį, ką ir programišiai, tačiau programišiai yra unikali grupė. Istoriškai jie buvo privilioti prie savo „profesijos“ iš nuobodulio arba norėdami pademonstruoti savo intelektualinius sugebėjimus. Jie gali veikti ištisą naktį, nes dažniausiai dieną būna mokykloje arba dirba.

Dauguma šių nusikaltėlių yra paaugliai, tačiau jie sėkmingai gali įsilaužti į bet kokios rūšies kompiuterines sistemas – bankų, kompanijų, gamyklų, karines sistemas. 1989 m. keturiolikmetis, naudodamasis

kompiuteriu, įsilaužė į JAV karinių pajėgų navigacinę palydovų sistemą. Vėliau tiriant bylą buvo išsiaiškinta, kad įsilaužėlio karjerą jis pradėjo nuo 8 metų.

Kai kurie programišiai veikia grupėmis, bet yra ir vienišių. Nors programišiai pasižymi protiniais sugebėjimais, dauguma jų prastai mokosi arba visai nelanko mokyklos. Kai kurie, be savo bičiulių programišių, turi mažai draugų. Didesnė sąveikos forma, kai jie bendrauja su kitais programišiais nebūdami kartu, yra kompiuteriniai tinklai. Susikūrusios programišių grupės siekia būti neformalios. 1990 m. pirmas organizuotas programišių suvažiavimas buvo surengtas Europoje. Programišiai iš viso pasaulio rinko dalijamas idėjas, mokėsi kitų dalykų, pavyzdžiui, kaip įsiveržti į kitų šalių kompiuterines sistemas. Nuo to laiko papildomi suvažiavimai buvo surengti Amerikoje ir kitose šalyse.

Pagal priklausomybę programišius galima suskirstyti į dvi grupes:

- vidiniai darbuotojai;
- svetimieji.

Programišiai taip pat skirstomi į kitas dvi pagrindines grupes:

- diletantai;
- profesionalai.

Diletantai – paprastai jauni žmonės (17–25m.). Jie mėgaujasi kompiuteriais, savo intelektualinėmis galimybėmis, padedančiomis įveikti kliūtis, kurių negali įveikti paprasti vartotojai.

Programišius diletantas paprastai siekia šių tikslų:

1. įsibrauti į sistemą, kad nustatytų jos paskirtį;
2. prieiti prie žaidimų programų;
3. modifikuoti ir ištrinti duomenis, tyčia palikti savo pėdsakus.

Dauguma diletantų nėra pavojingi firmos ar organizacijos kompiuterių sistemai. Vieniems rūpi paprasčiausiai prisijungti prie kompiuterių tinklo, nes legaliai tai padaryti trūksta lėšų, kiti skaito informaciją iš duomenų banko. Jiems įdomu surasti ir ištaisyti programinės priežiūros klaidas arba sumaniai naudotis tokiomis klaidomis ar programos darbo šalutiniais efektais. Tikėtina, kad jie yra didelės dalies virusų ir „Trojos arklių“ autoriai.

Dažnai paprasčiausiai dėl malonumo, o kai kada dėl asmeninio komforto tokie programišiai prasiskverbia per įvairių operacinių sistemų, turinčių daugiapakopę apsaugą, apsaugos sistemas. Šių programišių motyvai paprasti: arba prieiti prie žaidimų, arba parodyti save. Antruoju atveju pasekmės gali būti daug sunkesnės, nes jie gali palikti sistemoje įsilaužimo žymes, sugadinti kokius nors failus arba pa-

prasčiausiai palikti žinutes. Pavojingi bet kokie įsilaužimai į kompiuterių sistemą. Įsilaužėlis gauna priėjimą prie vartotojų failų, kuriuose gali būti konfidenciali informacija. Kiekvienas programišius, turintis nemenką kvalifikaciją, supranta, kad jį sugauti labai sunku. Toks asmuo, patrauktas atsakomybėn, neretai atsiperka nedidelėmis baudomis.

Daug pavojingesni programišiai profesionalai, kurie aktyviai panaudoja savo žinias, kad padarytų žalą kitiems arba kad gautų asmeninę naudą. Veikti jie gali savo iniciatyva, taip pat kaip nusikalstamos grupuotės nariai arba vykdydami nurodymus. Dažniausiai programišių profesionalų objektais tampa bankai, draudimo kompanijos, firmos.

Programišiai profesionalai skirstomi į šias grupes:

- nusikaltėlių grupuotės, siekiančios politinių tikslų;
- asmenys, besistengiantys gauti informaciją pramoninės žvalgybos tikslais;
- asmenų grupuotės pasipelnymo tikslais.

Dvi pastarosios grupės beveik nesiskiria nuo „tipinių nusikaltėlių“. Programišiai profesionalai – tai pereinamoji programišių ir tipinių nusikaltėlių grandis. Programišius, kai jo pagrindinė veikla tampa susijusi su naudos gavimu, tampa nusikaltėliu.

Siekdamas prasibrauti į kompiuterių sistemą, programišius negaili pastangų ir naudoja visas priemones, kad rastų trūkumą. Galima išvardyti keletą iš daugelio įsibrovimų į kompiuterių sistemą metodų:

1. nužiūrimas klaviatūra renkamas slaptažodis (galima net naudojant žiūronus). Kai kurie vartotojai užrašo slaptažodžius matomoje vietoje ir tai labai palengvina programišių darbą;
2. slaptažodis parenkamas naudojantis labiausiai paplitusiais slaptažodžių sąrašais arba žiniomis apie konkrečius asmenis. Daugelis vartotojų pasirenka trumpus ir labai paprastus slaptažodžius, vardų arba pavardžių sutrumpinimus, neretai – gimimo datą arba kitą viešai prieinamą informaciją;
3. į kompiuterių sistemas įdiegiamos specialios programos, kurios „sugauna“ įrašomą kodą;
4. naudojamos kodo parinkimo programos;
5. atliekama vidinės dokumentacijos, kurioje kalbama apie sistemos apsaugą, analizė;
6. nagrinėjama pirminių tekstų ir dvejetainių kodų programų registracija ir apsauga ir ieškoma klaidų jose;
7. tokios programos pakeičiamos savomis;
8. naudojamos specialios techninės priemonės siekiant perimti pranešimus, esančius vietos tinkluose.

Tinka ir tokie tradiciniai metodai kaip pokalbių, pokalbių telefonu klausymasis, pažinčių užmezgimas (daug galima sužinoti iš nepatenkinto darbuotojo). Pažintis programišiai užmezga su tarnautojais siekdami sumažinti riziką. Dažniausiai pasirenkami turintys finansinių ir šeimos problemų tarnautojai. Tada tarnautojai šantažu verčiami rizikuoti ir atlikti nusikaltimą veltui arba už minimalų atlyginimą.

Kad programišiai pasiektų savo tikslus, jiems reikalingas tiesioginis priėjimas arba priėjimas per kompiuterinius tinklus. Tiesiogiai prieiti prie kompiuterių sistemos programinius gali tada, kai tam tikras pastatas yra blogai saugomas. Kai kurių darbuotojų, paliekančių savo kompiuterius be priežiūros, nerūpestingumas labai palengvina įsilaužėlių darbą. Pasirengusiam programišiui nereikia daug laiko, kad įsibrautų į kompiuterių sistemą: 15–20 min. gali užtekti prasiskverbti į kompiuterių sistemą, turinčią daugiapakopę apsaugą. Duomenų, gautų iš pirmo įsilaužimo, užtenka tam, kad būtų galima nustatyti, kaip greitai galima prasiskverbti į kompiuterių sistemą bet kuriuo metu.

Profesionalūs nusikaltėliai visuomet stengiasi maksimaliai sumažinti riziką, todėl tapo beveik nesugaunami. Neretai kartu su jais dirba ir firmos darbuotojai arba neseniai iš firmos atleisti darbuotojai. Profesionalūs nusikaltėliai siekia tokių buvusių darbuotojų pagalbos, ypač jei firmos kompiuterių tinklas yra gerai saugomas.

2. „Tipiniai nusikaltėliai“

Tai daugiausia suaugę žmonės. Jie susitelkia ties dviem pagrindinėmis veikomis: šnipinėjimu ir sukčiavimu bei piktnaudžiavimu.

Šnipinėjimas. Ši elektroninių nusikaltimų kategorija apima asmenis, kurie pavagia slaptą informaciją iš strategiškai svarbių ir kitų objektų, taip pat iš teisėsaugos kompiuterių. Ji taip pat apima pramoninį agentų, dirbančių konkurentų firmoms arba užsienio vyriausybėms, pasiruošusioms sumokėti už informaciją, šnipinėjimą.

Sukčiavimas ir piktnaudžiavimas. Apgavysčių ir piktnaudžiavimo atvejų naudojant kompiuterius sparčiai daugėja. Kriminalinės grupuotės – ir vietinės, ir tarptautinės – įsitraukia į elektroninius nusikaltimus kaip į tiesioginį nelegalių pajamų šaltinį. Nusikaltėliai supranta, kad jie gali uždirbti daugiau pinigų vykdydami kompiuterinį sukčiavimą ir kad tai daryti daug saugiau už kitus įprastus nusikaltimus. Bankai visada traukė kompiuterinius nusikaltėlius. 1988 m. septynių įsilaužėlių grupė atliko operaciją, nukreiptą į vieną iš stambių vakarų bankų. Jie neteisėtai pervedė 70 mln. dolerių, priklausiusių trim kom-

panijoms, iš pradžių į vieną Niujorko bankų, po to į du Europos bankus. Pinigų pervedimai buvo sankcionuoti telefonu, todėl bankas atlikdavo kontrolinius skambučius, kad patvirtintų užklausą. Tačiau nusikaltėliai padarė esminę klaidą: visus skambučius jie nukreipė į namus vienam iš bendrininkų. Kai pinigai buvo pervesti, trys kompanijos susisiekė su banku, kad išsiaiškintų, kas įvyko. Prasidėjo tyrimas ir telefono numeris, kuriuo buvo daromi kontroliniai skambučiai, „užvedė“ ant nusikaltėlių pėdsakų.

3. Vandalai

Ši kategorija dažniausiai nedaro nusikaltimų, kad parodytų savo intelektualinius sugebėjimus (kaip tai daro programišiai) arba finansiniais, politiniais sumetimais (kaip tai daro elektroniniai nusikaltėliai). Vandalizmo motyvas dažnai būna kerštas už tikrą ar išgalvotą įžeidimą. Dažniausiai šios kategorijos žmonės būna pikti ant tam tikros organizacijos, bet kartais tai būna žmonės, kurie apskritai nusivylę gyvenimu. Vandalai apytikriai gali būti padalyti į dvi grupes, kurias būtų galima pavadinti naudotojais ir svetimšaliais. Naudotojai yra tie, kurie piktnaudžiauja galėdami teisėtai prieiti prie kompiuterių sistemos. Svetimieji yra tie, kurie negali prieiti prie sistemos.

Reikėtų paminėti ir elektroninių nusikaltėlių klasifikaciją, paplitusią Rusijoje. Čia elektroninių nusikaltimų subjektai skirstomi į tris grupes:

1. Pirmajai elektroninių nusikaltėlių grupei priklauso žmonės – kompiuterinės technikos profesionalai, programavimo žinovai. Jiems taip pat būdingas tam tikras fanatizmas bei išradingumas. Kai kurių autorių manymu, šie subjektai kompiuterinės technikos priemones vertina kaip tam tikrą iššūkį jų profesionalioms žinioms. Būtent tai ir yra pagrindinė paskata padaryti veikas, daugelis iš kurių yra nusikalstamos. Reikia paminėti dar vieną šios grupės požymį – šie nusikaltėliai neturi kokių nors konkrečių tikslų pažeisti įstatymą. Beveik visus veiksmus jie atlieka norėdami parodyti savo intelektualinius ir profesinius sugebėjimus. Šios grupės atstovai yra gana smalsūs, aukšto intelekto, be to, turi tam tikro „sportinio azarto“. Jie bet kokiomis priemonėmis nori įrodyti, kad yra pranašesni už kompiuterius. Paprastai tai ir paskatina juos padaryti nusikaltimą.

Kartais, bėgant laikui, šios kategorijos žmonės ne tik įgauna patirties, bet keičiasi ir jų interesai. Savo veikloje jie pradeda ieškoti materialinės naudos. Taigi mėgėjas programuotojas tampa profesio-

naliu nusikaltėliu.

Nagrinėjamai grupei galima priskirti šiuos požymius:

- nėra tam tikro išankstinio pasirengimo padaryti konkretų nusikaltimą;
- nusikaltimas padaromas originaliu būdu;
- nusikaltimui padaryti naudojamos buitinės kompiuterinės technikos priemonės;
- nusikaltimo pėdsakai neslepiami.

2. Kaip artimą šiai grupei būtų galima priskirti ir kitą nusikaltėlių grupę, sergančią naujomis psichikos ligomis – informacinėmis ligomis ir kompiuterinėmis fobijomis.

Ši ligų kategorija kyla dėl sistemingo žmogaus informacinio režimo pažeidimo: informacinio bado, informacinės perkrovos. Šių klausimų tyrimu užsiima gana nauja medicinos šaka – informacinė medicina. Žiūrint iš šios šakos pozicijų, žmogus suprantamas kaip universali save reguliuojanti informacinė sistema, turinti nustatytą biologinės informacijos pusiausvyrą. Šios pusiausvyros pažeidimas dėl vidinių ar išorinių destabilizuojančių veiksnių sukelia įvairias informacines ligas, tarp kurių labiausiai paplitusios informacinės neurozės. Kitais žodžiais tariant, žmogui reikia ir fizinės, ir informacinės pusiausvyros. Kai jos mažai, ateina informacinis badas, kai daug – žmogus kenčia nuo informacinių perkrovų (pasireiškia įvairūs stresai ir emociniai protrūkiai). Visa tai gali sukelti informacinę ligą. Esant dabartiniam darbo kompiuterizavimui, daugelis darbuotojų papuola į stresines situacijas ir kartais tai baigiasi kompiuterine fobija. Tai ne kas kita kaip profesinė liga. Jos požymiai yra greitas nuovargis, staigūs kraujo spaudimo šuoliai fiziškai ir audiovizualiai kontaktuojant su kompiuteriu, galvos svaigimas ir skausmas, galūnių drebėjimas ir t. t. Faktiškai baiminamasi prarsti savo veiksmų kontrolę.

Taigi elektroninius nusikaltimus gali padaryti ir žmonės, sergantys minėtomis psichikos ligomis. Tiriant tokį elektroninį nusikaltimą būtina skirti teismo psichiatrinę ekspertizę, kad būtų galima nustatyti kaltinamojo psichinę būklę nusikaltimo metu (ar tai buvo afekto būsena, ar nepakaltinamumas).

Dažniausiai šios grupės nusikaltėliai, iš dalies arba visiškai praradę kontrolę, fiziškai naikina kompiuterius (neturėdami nusikalstamų ketinimų).

3. Trečią grupę sudaro profesionalūs elektroniniai nusikaltėliai. Šiai grupei priklauso žmonės, turintys aiškių nusikalstamų ketinimų.

Kitaip nei pirmosios dvi grupės, jų veikos nebūna vienkartinės. Dažniausiai jie slepia savo nusikaltimus. Paprastai šie žmonės būna gerai organizuotų grupių, turinčių specialią techniką (neretai operatyvinę), nariai. Tai kvalifikuoti specialistai, turintys techninį, aukštąjį juridinį arba ekonominį išsilavinimą. Būtent ši grupė visuomenei kelia didžiausią grėsmę. Pavyzdžiui, 79 proc. pinigų grobimų stambiu mastu įvykdo būtent šie asmenys.

Pastaruoju metu paplitusi elektroninių nusikaltėlių pagal elektroninių nusikaltimų padarymo būdus klasifikacija:

1) krekeriai (nuo angliško žodžio „*cracker*“) – asmenys, įsilaužiantys (įskaitant duomenų modifikavimą, blokavimą arba sunaikinimą) į įstatymo saugomas informacines sistemas;

2) frekeriai (nuo angliško žodžio „*phreacker*“) – asmenys, darantys elektroninius nusikaltimus naudodamiesi elektroniniais ryšiais, kai specialiomis priemonėmis slapta perimama konfidenciali informacija;

3) karderiai (nuo angliško žodžio „*card*“) – asmenys, vykdantys elektroninius nusikaltimus, susijusius su mokėjimo kortelių apyvarta.

7.3. Papildoma medžiaga. Teisiniai elektroninių nusikaltimų aspektai

7.3.1. Pagrindiniai tarptautiniai dokumentai dėl elektroninių nusikaltimų

Tarptautiniu mastu elektroninių nusikaltimų sritį reguliuoja (teisines priemones koordinuoja) šios organizacijos: Europos ekonominio bendradarbiavimo ir plėtros organizacija (OECD), Europos Taryba, Jungtinių Tautų Organizacija, Pasaulio prekybos organizacija, kitos organizacijos. Galima pateikti keletą minimų organizacijų veiklos kovojant su elektroninių nusikaltimų fenomenu pavyzdžių.

Dėmesys elektroninių nusikaltimų problemai tarptautiniu mastu buvo parodytas jau 1983 m. 1983–1985 m. Ekonominio bendradarbiavimo ir plėtros organizacijos paskirti ekspertai atliko baudžiamųjų įstatymų dėl nusikaltimų, susijusių su kompiuteriais, derinimo tyrimą. Atlikus tyrimą valstybėms narėms buvo pateiktas minimalus pavojingų veikų, susijusių su kompiuteriais, sąrašas. Prie tokių veikų buvo priskirta:

– tyčinis kompiuterinių duomenų ir (arba) kompiuterių progra-

mų įvedimas, pakeitimas, ištrynimas ir (arba) slopinimas siekiant nelegaliai pasisavinti lėšas arba kitas vertybes;
– tyčinis kompiuterinių duomenų ir (arba) kompiuterių programų įvedimas, pakeitimas, ištrynimas ir (arba) slopinimas klastojimo tikslais;
– tyčinis kompiuterinių duomenų ir (arba) kompiuterių programų įvedimas, pakeitimas, ištrynimas ir (arba) slopinimas arba kitoks kišimasis į kompiuterių sistemos darbą siekiant sutrikdyti kompiuterių ir (arba) telekomunikacijų sistemos funkcionavimą;
– išskirtinės savininko teisės į saugomą kompiuterinę programą pažeidimas siekiant naudoti ją komerciniais tikslais arba paleisti į rinką;
– patekimas į kompiuterį arba kompiuterio ir (arba) telekomunikacijos sistemos perėmimas be asmens, atsakingo už šią sistemą, leidimo, pažeidžiant apsaugos priemones arba dėl kitų nesąžiningų ar žalingų paskatų.

Valstybėms buvo siūloma užtikrinti, kad baudžiamieji jų įstatymai būtų pataisyti pagal išvardytą veikų sąrašą. Dauguma Informacijos, kompiuterių ir ryšių politikos komiteto narių taip pat buvo už tai, kad baudžiamosiomis normomis turėtų būti uždraustos ir kitos veikų rūšys, pavyzdžiui, neteisėtas kompiuterinių sistemų naudojimas ir kt.

1994 m. Jungtinės Tautos išleido „Su kompiuteriais susijusių nusikaltimų kontrolės ir prevencijos vadovą“, kuris aptarė kompiuterinių nusikaltimų fenomeną, teisinį jų reguliavimą, prevenciją ir tarptautinį bendradarbiavimą šiuo klausimu.

Nuo 1985 iki 1989 m. Europos Tarybos su kompiuteriais susijusių nusikaltimų ekspertų komitetas nagrinėjo teisines kompiuterinių nusikaltimų problemas. Europos Tarybos Ministrų komitetas 1989 m. priėmė Rekomendaciją Nr. R(89)9 [12], kurioje Europos Tarybos šalių narių vyriausybės kviečiamos atsižvelgti į ekspertų komiteto parengtą ataskaitą kuriant įstatymus, susijusius su kompiuteriniais nusikaltimais. Šią ataskaitą sudaro penkios dalys. Pirma dalis aprašo kompiuterinio nusikaltimo fenomeną. Antroje dalyje išdėstyti vadinamieji principai nacionaliniams įstatymų leidėjams (minimalus ir neprivalomas nusikalstamų kompiuterinių veikų sąrašai). Kitos dalys susijusios su procesinių normų taikymu: kompiuterinių įrodymų leistinumas, įrodymų rinkimas ir kt. Galutinėje dalyje kalbama apie kompiuterinių nusikaltimų prevenciją, latentiškumo mažinimą ir kt.

Kaip minėta, pranešime pateikiami du veikų, susijusių su tokiais nusikaltimais, sąrašai. Europos Sąjungos šalims leidžiama savarankiškai spręsti, kaip ir kiek pasinaudoti šiuo pasiūlymu. Minimaliame sąraše išvardytos 8 pavojingos veikos, susijusios su kompiuterinėmis technologijomis. Papildomas sąrašas apima keturias mažiau pavojingas veikas, kurios įtraukiamos į įstatymų leidybą, bet nėra privalomos. Šie sąrašai reikalingi Europos Sąjungos šalių teisinėms sistemoms suvienodinti pagal kompiuterinius nusikaltimus.

Pasiūlytas minimalus sąrašas:

– sukčiavimas, susijęs su kompiuteriu (kompiuterinių duomenų arba kompiuterinių programų įvedimas, ištrynimas, pakeitimas ar paslėpimas arba kitoks įsikišimas į duomenų apdorojimo procesą. Dėl to padaroma žala kitam asmeniui turint tikslą gauti materialinę naudą sau arba kitam asmeniui);
– klastojimas naudojant kompiuterį (kompiuterinių duomenų arba kompiuterių programų įvedimas, ištrynimas, pakeitimas ar paslėpimas arba kitoks įsikišimas į duomenų apdorojimo procesą. Dėl to įvykdomas tradicinis klastojimas);
– kompiuterinių duomenų ar programų sunaikinimas arba sugadinimas (kompiuterinių duomenų ar kompiuterių programų ištrynimas, sunaikinimas, sugadinimas neturint tam teisės);
– sabotažas naudojant kompiuterį, kompiuterinių duomenų ar kompiuterių programų įvedimas, ištrynimas, pakeitimas ar paslėpimas arba kitoks įsikišimas į duomenų apdorojimo procesą siekiant sutrikdyti kompiuterio arba telekomunikacijų sistemos darbą);
– neteisėta prieiga prie kompiuterių sistemos (prieiga prie kompiuterių sistemos arba kompiuterių tinklo neturint tam teisės ir pažeidžiant saugumo priemones);
– neteisėtas informacijos perėmimas kompiuterių sistemoje (neteisėtas susirašinėjimo perėmimas į, iš arba viduje kompiuterių sistemos ar tinklo, atliktas techninėmis priemonėmis);
– neteisėtas apsaugotų kompiuterinių programų dauginimas ir platinimas;
– neteisėtas kompiuterinių lustų (mikroschemų) topografijų dauginimas ir platinimas.

Pasiūlytas neprivalomas sąrašas: kompiuterinių duomenų arba programų pakeitimas, kompiuterinis šnipinėjimas, neteisėtas kompiuterio naudojimas (laiko vagystė), neteisėtas apsaugotų kompiuterinių programų naudojimas.

Priimtos ir dvi Europos Tarybos kompiuterinių nusikaltimų komiteto rekomendacijos, susijusios su baudžiamojo proceso teisės taikymu tiriant elektroninius nusikaltimus: Nr. R(85)S ir Nr. R(95)13. Pastarojoje valstybių narių vyriausybėms rekomenduojama, peržiūrint nacionalinius teisės aktus, atsižvelgti į prie Rekomendacijos pridedamus principus:

– *krata ir poėmis.* Nacionaliniai įstatymai kratai ir poėmiui elektroninėje erdvėje turi sudaryti vienodas sąlygas. Be to, įstatymai turi sudaryti sąlygas „išplėsti“ kratą arba poėmį kitose kompiuterių sistemose, sujungtose per kompiuterių tinklą;
– *telekomunikacijų kontrolė*. Procesiniai įstatymai turi būti peržiūrėti. Siekiant sudaryti galimybę teisėsaugos institucijoms, tiriančiomis sunkius nusikaltimus, kontroliuoti telekomunikacijų srauto duomenis arba telekomunikacijų turinį;
– *pareiga bendradarbiauti su teisėsaugos institucijomis.* Teisės aktai telekomunikacijų operatoriams turi nustatyti specialias pareigas teikti informaciją, reikalingą pradėtam tyrimui;
– *elektroniniai įrodymai*. Teisės aktų nuostatos dėl tradininių įrodymų turi būti vienodai taikomos ir įrodymams elektronine forma;
– *šifravimo naudojimas*. Turi būti apsvarstytas šifravimo naudojimas, turint omenyje teisėsaugos institucijų galimybę prieiti prie informacijos turinio;
– *tyrimas, statistika ir mokymai*. Turi būti apsvarstyta galimybė steigti specialius padalinius, tiriančius pavojingas veikas elektroninėje erdvėje ir turinčius pakankamai patirties;
– *tarptautinis bendradarbiavimas*. Valstybių sienos neturi trukdyti atlikti numatytus tyrimo veiksmus, pavyzdžiui, kratą ar poėmį, siekiant paimti reikiamą informaciją elektronine forma.

Dalis anksčiau minėtų principų jau yra įgyvendinti, tačiau po rekomendacijos priėmimo praėjus daugiau nei dešimtmečiui kelios esminės problemos nebuvo išspręstos: veiksmingo tarptautinio bendradarbiavimo, elektroninių įrodymų ir kt.

Anksčiau jau buvo aptarta pagrindinė informacija dėl Konvencijos priėmimo aplinkybių bei struktūros. Toliau atskirai bus aptariamos Konvencijos nuostatos dėl materialinės bei proceso teisės.

7.3.2. Konvencijos dėl elektroninių nusikaltimų nuostatos dėl materialinės teisės

Konvencijos pirmojo skyriaus pirmajame skirsnyje, susijusiame su materialine teise, siūloma nustatyti teisinės atsakomybės pagrindus už šias pavojingų veikų rūšis:

– 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));
– su kompiuteriais susijusius pažeidimus (sukčiavimas, susijęs su kompiuteriais; klastojimas, susijęs su kompiuteriais);
– pažeidimus, susijusius su turiniu (pažeidimai, susiję su pornografine medžiaga apie vaikus);
– pažeidimus, susijusius su autorių teisėmis arba gretutinėmis teisėmis.

Konvencijos nuostatos, susijusios su materialine teise (t. y. teisinės atsakomybės pagrindų už pavojingas veikas elektroninėje erdvėje nustatymu):

1) konfidencialumo, duomenų vientisumo, kompiuterinių duomenų ir sistemų pažeidimai

Neteisėta prieiga. Konvencijos 2 straipsnyje numatyta, jog „turi būti priimtos įstatymų normos, pagal kurias būtų nustatyti baudžiamosios atsakomybės pagrindai už tyčinę prieigą prie kompiuterių sistemos neturint tam teisės“. Šia nuostata siekiama, kad būtų nustatyta baudžiamoji atsakomybė už veikas, keliančias pavojų kompiuterinių sistemų ir duomenų saugumui (konfidencialumui, integruotumui ir prieinamumui), t. y. už vadinamąsias „*Hacking*“, „*Cracking*“, „*Computer trespass*“. Tame pačiame Konvencijos straipsnyje nurodoma, jog nustatant baudžiamosios atsakomybės pagrindus gali būti reikalaujama, kad nusikaltimas būtų padaromas pažeidžiant saugumo priemones, siekiant gauti kompiuterinę informaciją arba turint nesąžiningą tikslą, arba kai veika yra susijusi su kompiuterių sistema, sujungta su kita kompiuterių sistema. Anksčiau minėta formuluotė valstybėms narėms palieka tam tikrą veikimo laisvę nustatant baudžiamosios atsakomybės pagrindus už neteisėtą prieigą. Galima konstatuoti, kad Konvencijoje laikomasi nuostatos, jog tyčinė prieiga prie kompiuterių

sistemos neturint tam teisės turi būti įvardijama kaip neteisėta veika.

Neteisėtas perėmimas. Konvencijos 3 straipsnyje nurodyta, kad *„turi būti priimtos teisės normos, nustatančios baudžiamosios atsakomybės pagrindus už tyčinį informacijos perėmimą neturint tam teisės, kai tai padaroma naudojantis techninėmis priemonėmis ir kai informacija perimama neviešai siunčiant kompiuterinę informaciją į, iš kompiuterių sistemos arba jos viduje (įskaitant ir elektromagnetinį kompiuterių sistemos spinduliavimą)“*. Šia nuostata siekiama apsaugoti duomenų komunikacijų privatumą, kuris apsaugotas Europos žmogaus teisių konvencijos 8 straipsniu. Minėta veika gali būti vykdoma neteisėtai perimant kompiuterinę informaciją, siunčiant ją elektroniniu paštu, persiunčiant kompiuterines bylas (sauginius) ir kt. Minėtos nuostatos tekstas buvo beveik perkeltas iš Rekomendacijos (89) 9. Pažymėtina, jog remiantis Konvencijos komentaru sąvoka „neviešas“ turėtų būti vartojama kalbant apie informacijos perdavimo neviešumą, o ne pačios perduodamos informacijos neviešumą. Tame pačiame Konvencijos straipsnyje nurodyta, jog nustatant baudžiamosios atsakomybės pagrindus už minėtą veiką gali būti reikalaujama nesąžiningo tikslo arba kad veika būtų susijusi su kompiuterių sistema, prijungta prie kitos kompiuterių sistemos. Konvencijos formuluotė valstybėms narėms palieka tam tikrą veikimo laisvę nustatant baudžiamosios atsakomybės pagrindus už neteisėtą kompiuterinės informacijos perėmimą. Reikia paminėti, jog formuojant pažeidimo aprašymą buvo atsisakyta techninių apsaugos priemonių pažeidimo požymio, nes tokiu atveju būtų saugoma tik koduota kompiuterinė informacija.

Įsikišimas į duomenų apdorojimo procesą. Konvencijos 4 straipsnyje nustatyta, kad *„turi būti priimtos teisės normos, nustatančios baudžiamąją atsakomybę už tyčinį kompiuterinės informacijos sunaikinimą, ištrynimą, pakeitimą, sugadinimą, neturint tam teisės“*. Šios nuostatos tikslas – apsaugoti tinkamą kompiuterinės informacijos apdorojimą, tinkamą išsaugotos kompiuterinės informacijos arba kompiuterinių programų naudojimą. Konvencijoje taip pat nurodoma, jog nustatant baudžiamosios atsakomybės pagrindus už minėtą veiką gali būti reikalaujama didelės žalos. Taigi ši Konvencijos formuluotė valstybėms narėms palieka tam tikrą veikimo laisvę.

Įsikišimas į kompiuterių sistemos darbo procesą. Konvencijos 5 straipsnyje nustatyta, kad *„turi būti priimtos teisės normos, nustatančios baudžiamosios atsakomybės pagrindus už tyčinį pavojingą kom*piuter*ių sistemos darbo trukdymą, kuris pasireiškia kompiuterinės*

informacijos įvedimu, perdavimu, sunaikinimu, ištrynimu, sugadinimu, pakeitimu“. Ši nuostata panaši į Rekomendacijos (89) 9 nuostatą „Sabotažas, susijęs su kompiuteriais“ ir turi tikslą kriminalizuoti trukdymą teisėtai naudoti kompiuterių sistemą, įskaitant telekomunikacijų įrenginius, naudojant arba darant įtaką kompiuterinei informacijai. Šiame Konvencijos straipsnyje nesiūloma įrašyti jokių papildomų požymių nustatant baudžiamosios atsakomybės pagrindus už anksčiau minėtą veiką. Pažymėtina, jog Konvencijos formuluotė valstybėms narėms nepalieka veikimo laisvės nustatant baudžiamosios atsakomybės pagrindus už neteisėtą įsikišimą į duomenų apdorojimo procesą.

Piktnaudžiavimas kompiuterinėmis priemonėmis (įrenginiais) (*angl*. – Misuse devices). *Konvencijos 6 straipsnyje nustatyta, kad „turi būti priimtos teisės normos, nustatančios baudžiamosios atsakomybės pagrindus už tyčinį:*

a) įrenginio (priemonės), įskaitant kompiuterio programą, sukurto arba pritaikyto bet kokiam iš pažeidimų, nurodytų Konvencijos 2–5 straipsniuose, padaryti, taip pat kompiuterinio slaptažodžio, priėjimo kodo ar panašių duomenų, kuriais pasinaudojus galima prieiti prie kompiuterių sistemos, gaminimą, pardavimą, parūpinimą, importą, platinimą arba kitu būdu padarymą prieinamų;
b) *įrenginio (priemonės), įskaitant kompiuterio programą, sukurto arba pritaikyto bet kokiam iš pažeidimų, nurodytų Konvencijos 2–5 straipsniuose, padaryti, laikymą“.* Tačiau Konvencijoje nurodyta, jog galima nustatyti, kad baudžiamoji atsakomybė kyla tik tuo atveju, jei turima keletas tokių įrenginių (priemonių), taip paliekant valstybėms narėms tam tikrą pasirinkimo laisvę.

Ši nuostata skirta tyčiniam specifinių neteisėtų veikų, susijusių su įrenginiais (priemonėmis) ar prieigos informacija, padarymui įvardyti atskiru nusikaltimu, siekiant padaryti kitus Konvencijoje paminėtus nusikaltimus pažeidžiant kompiuterinių sistemų arba duomenų konfidencialumą, integruotumą arba prieinamumą. Reikia paminėti, jog Konvencijoje paliekama teisė iš viso nenumatyti baudžiamosios atsakomybės pagrindų už kompiuterinio slaptažodžio, priėjimo kodo arba panašių duomenų, kuriais pasinaudojus galima prieiti prie kompiuterių sistemos, pardavimą, platinimą arba kitu būdu padarymą prieinamu. Paminėtina, jog siekiant atriboti pavojingas veikas nustatytas svarbus požymis – tikslas įvykdyti pažeidimus, susijusius su kompiuterių naudojimu. Tokiomis nuostatomis aiškiai įvardijama, kad tei-

sinės priemonės kompiuterinėms sistemoms testuoti nepriklauso teisinės atsakomybės pagrindų veikimo sričiai.

2) Su kompiuteriais susiję pažeidimai

Klastojimas, susijęs su kompiuteriais. Konvencijos 7 straipsnyje nustatyta, jog „*turi būti priimtos teisės normos, nustatančios baudžiamosios atsakomybės pagrindus už tyčinį (taip pat neturint tam teisės) kompiuterinių duomenų įvedimą, pakeitimą, ištrynimą, dėl to gaunami neautentiški duomenys (informacija), siekiant kad jie būtų laikomi autentiškais*“. Šios nuostatos tikslas – nustatyti paralelią atsakomybę, kaip ir atsakomybę už materialių dokumentų klastojimą, t. y. pašalinti baudžiamųjų įstatymų „skyles“, susijusias su atsakomybės pagrindų nustatymu už tradicinį klastojimą, kai atitinkami įstatymai netaikomi elektroniniams duomenims. Autoriaus nuomone, kadangi vis daugiau sandorių sudaroma elektronine forma, vis daugiau žmonių veiklos perkeliama į elektroninę erdvę, tokia paminėta nuostata yra ganėtinai svarbi. Reikia taip pat paminėti, jog šiame straipsnyje valstybėms narėms palikta pasirinkimo laisvė nustatant baudžiamosios atsakomybės pagrindus už minėtą veiką reikalauti tikslo apgauti arba kito nesąžiningo tikslo.

Sukčiavimas, susijęs su kompiuteriais. Konvencijos 8 straipsnyje nustatyta, kad „*turi būti priimtos teisės normos, nustatančios baudžiamosios atsakomybės pagrindus už tyčinį (taip pat neturint tam teisės):*

a) kompiuterinės informacijos įvedimą, ištrynimą;

b) bet kokį įsikišimą į kompiuterių sistemos funkcionavimą, jei

dėl to padaroma žala turint apgavikišką ar nesąžiningą tikslą gauti materialinę naudą sau arba kitam“. Ši nuostata susijusi su naujos technologinės revoliucijos, dėl kurios atsirado unikalios galimybės vykdyti ekonominius nusikaltimus elektroninėje erdvėje, atėjimu. Kadangi kompiuterinėse sistemose apdorojama informacija (pvz., susijusi su pinigais) pasidarė labai vertinga, kai kuriais atvejais netgi vertingesnė už nekilnojamąjį turtą, šią nuostatą įgyvendinti pasidarė būtina. Reikia paminėti, jog šiame straipsnyje nepaliekama jokios veikimo laisvės nustatant baudžiamosios atsakomybės pagrindus už nurodytą veiką.

3) Su turiniu susiję pažeidimai

Pažeidimai, susiję su pornografine medžiaga apie vaikus. Konvencijos 9 straipsnyje nustatyta, jog „*turi būti priimtos teisės normos, nusi-*

kalstamomis veikomis įvardijančios tyčines (taip pat neturint tam teisės) veikas:

a) Medžiagos, susijusios su vaikų pornografija, gaminimą siekiant ją platinti per kompiuterių sistemą;

b) medžiagos, susijusios su vaikų pornografija, padarymą prieinama (taip pat siūlymą) per kompiuterių sistemą;

c) medžiagos, susijusios su vaikų pornografija, platinimą arba siuntimą per kompiuterių sistemą;

d) medžiagos, susijusios su vaikų pornografija, siuntimą per kompiuterių sistemą sau arba kitam;

e) medžiagos, susijusios su vaikų pornografija, turėjimą kompiuterių sistemoje arba įrenginyje, galinčiame saugoti kompiuterinę informaciją".

Šiomis nuostatomis siekiama sustiprinti teisines vaikų apsaugos priemones, įskaitant jų apsaugą nuo seksualinio išnaudojimo, modernizuojant baudžiamosios teisės normas, siekiant kovoti su veikomis, kai naudojantis kompiuterinėmis sistemomis bei kompiuterių tinklais seksualiai išnaudojami vaikai. Konvencijos komentare pažymima, jog nors daugelis valstybių yra kriminalizavusios tradicines veikas, susijusias su pornografinės medžiagos apie vaikus naudojimu ir platinimu, tačiau nauja tokios nelegalios veiklos forma (pvz., internetu) taip pat turėtų būti numatyta baudžiamuosiuose įstatymuose. Šiame straipsnyje nustatyta pasirinkimo laisvė nenustatyti baudžiamosios atsakomybės už išvardytas veikas, nurodytas d ir e punktuose.

4) Pažeidimai, susiję su autorių teisėmis arba gretutinėmis teisėmis

Konvencijos 10 straipsnyje nustatyta, jog „turi būti priimtos teisės normos, nustatančios baudžiamosios atsakomybės pagrindus už autorių teisių ir gretutinių teisių pažeidimą (pagal įstatymus, priimtus remiantis tarptautiniais dokumentais (Berno konvencija dėl literatūros ir meno kūrinių apsaugos ir kt.)), padarytą naudojant kompiuterių sistemą komerciniais tikslais". Tačiau tame pačiame straipsnyje nustatoma, jog už tokias veikas baudžiamoji atsakomybė gali būti ir nenumatyta, jei yra numatyta kitų pakankamų priemonių ir laikomasi visų tarptautinių įsipareigojimų autorių teisių ir gretutinių teisių srityje. Svarbios yra PINO (Pasaulio intelektualios nuosavybės organizacijos) autorių teisių bei PINO atlikimų ir fonogramų sutartys, nes jos itin pakeičia tarptautinę intelektualios nuosavybės apsaugą, ypač susijusią su apsaugotos medžiagos padarymu prieinamos internetu „pagal

pareikalavimą“. Pavyzdžiui, 1996 m. PINO autorių teisių sutarties 6 straipsnyje platinimo teisė apibrėžiama taip: literatūros ir meno kūrinių autoriai turi išimtinę teisę suteikti leidimą padaryti jų kūrinių originalus arba jų kopijas viešai prieinamas juos parduodant ar kitaip perduodant nuosavybėn.

7.3.3. Konvencijos dėl elektroninių nusikaltimų nuostatos dėl proceso teisės

Vienas iš pagrindinių Konvencijos tikslų – ne tik unifikuoti nacionalinius baudžiamuosius įstatymus dėl elektroninių nusikaltimų, bet ir tobulinti nacionalinę baudžiamojo proceso teisę. Tokie elektroninių nusikaltimų požymiai kaip globalumas, elektroninė veikos forma sukuria gana dideles kliūtis minimiems nusikaltimams tirti. Vienas iš pagrindinių problemų kovojant su elektroniniais nusikaltimais yra nusikaltimo subjekto nustatymas, taip pat nusikalstamos veikos masto ar poveikio įvertinimas. Iššūkį meta ir elektroninės informacijos, kuri gali tapti nusikalstamos veikos įrodymu, pažeidžiamumas, galimybė ją pakeisti arba sunaikinti. Užsienio valstybių praktika rodo, kad dažnai neužtenka galiojančių procesinių normų, kurios istoriškai pritaikytos tradiciniams nusikaltimams tirti (pvz., kratos išplėtimo kompiuteriniuose tinkluose problema).

Konvencijoje išskirtas atskiras I skyriaus 2 skirsnis, skirtas valstybių nacionalinių įstatymų proceso normoms suvienodinti. Šiuo skirsniu siekiama tradicines procesines priemones, tokias kaip krata ir poėmis, pritaikyti elektroninei aplinkai. Taip pat, siekiant tradicines įrodymų rinkimo priemones, pavyzdžiui, kratą, poėmį, padaryti veiksmingas besikeičiančioje elektroninėje aplinkoje, nustatomos tokios naujos priemonės kaip operatyvus laikomųjų kompiuterinių duomenų išsaugojimas ir pan. Išskirtinos šios toliau nagrinėtinos pagrindinės proceso teisės skirsnio nuostatos dėl procesinių priemonių: operatyvus laikomųjų kompiuterinių duomenų išsaugojimas, laikomųjų kompiuterinių duomenų paieška ir poėmis bei kompiuterinių duomenų surinkimas realiuoju laiku.

Operatyvus laikomųjų kompiuterinių duomenų išsaugojimas. Konvencijos dėl elektroninių nusikaltimų 16 straipsnio 1 dalyje teigiama, kad „*kiekviena šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti įgalinant jos kompetentingas institucijas nurodyti arba panašiai pasirūpinti operatyviu konkrečių kompiuterinių duomenų, įskai-*

tant srauto duomenis, laikomus kompiuterių sistemoje, išsaugojimu, ypač kai galima pagrįstai manyti, jog tie kompiuteriniai duomenys gali būti nesunkiai prarasti arba pakeisti“. Konvencijos 17 straipsnyje taip pat reglamentuojamas minimų išsaugotų duomenų atskleidimo galimybės užtikrinimas, o 18 straipsnyje – nurodymas dėl duomenų pateikimo.

Poreikis išsaugoti kompiuterinius duomenis gali kilti tais atvejais, kai tyrimo nustatyta, jog tam tikri kompiuterių duomenys kitų duomenų srauto sudėtyje yra laikomi atitinkamo paslaugų teikėjo serveryje, kur teikėjas verslo tikslais kaupia tam tikrą laikotarpio srautą. Tam, kad būtų galima išskirti reikiamą informaciją iš duomenų srauto bei ją paimti, reikalinga laikina duomenų apsauga. Tai gali būti įmanoma įgyvendinti tik tuo atveju, jei tyrimo organai turės atitinkamas teises įpareigoti paslaugų teikėją išsaugoti saugomus kompiuterių duomenis.

Ši priemonė taikytina tuo atveju, kai kompiuteriniai duomenys jau išsaugoti. Tačiau tyrimui svarbūs kompiuteriniai duomenys, nors ir išsaugoti, per trumpą laiką gali būti ištrinami. Pavyzdžiui, praktikoje galima situacija, kai paslaugos teikėjo užfiksuoti kompiuteriniai duomenys kompiuterių sistemoje saugomi ne ilgiau nei kelias valandas arba kelias paras.

Paminėtina, jog, Konvencijos rengėjų nuomone, teisė įpareigoti subjektą išsaugoti laikomuosius kompiuterinius duomenis nacionalinėje teisėje turi būti įtvirtinta ir siekiant sudaryti galimybę pagelbėti kitai valstybei tarptautiniu lygiu, išsaugant svarbius kompiuterių duomenis savo teritorijoje. Taip būtų užtikrinta, kad svarbūs kompiuterių duomenys nebūtų prarasti iki to laiko, kol bus nustatyta tvarka gautas teisinės pagalbos prašymas suteikti informaciją. Atsižvelgiant į tai, kad nusikaltimo tyrimo procese skirtingų valstybių teisėsaugos institucijos privalo bendradarbiauti viena su kita ir oficialiai, ir neoficialiai, gali kilti tam tikrų problemų. Jei valstybės teisės normos nenustato konkrečių elektroninės informacijos rinkimo įgaliojimų, tokia valstybė iš esmės gali būti nepajėgi adekvačiai reaguoti į prašymą suteikti pagalbą.

Ar nurodymas išsaugoti kompiuterinius duomenis, laikomus kompiuterių sistemoje, gali būti traktuojamas kaip nauja procesinė prievartos priemonė? Kaip rodo teisinė praktika, toks duomenų išsaugojimas daugelyje valstybių laikytinas nauja teisine priemone arba procedūra pagal nacionalinę teisę.

Laikomųjų kompiuterinių duomenų paieška ir poėmis. Konvencijos dėl elektroninių nusikaltimų 19 straipsnio 1 dalyje teigiama, jog „*kiekviena šalis priima tokius teisės aktus ir kitas priemones, kurių gali pri-*

reikti įgaliojant jos kompetentingas institucijas apieškoti arba panašiai ištirti:

a) kompiuterių sistemą arba jos dalį ir joje laikomus kompiuterinius duomenis;

b) kompiuterinių duomenų atmeniąją terpę, kurioje tos šalies teritorijoje gali būti laikomi kompiuteriniai duomenys".

Kaip nurodyta Konvencijos 19 straipsnio 2 dalyje, *„Kiekviena šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti užtikrinti, kad jos institucijoms pagal šio straipsnio 1 dalies a punktą apieškant ar panašiai tiriant konkrečią kompiuterių sistemą arba jos dalį ir turint priežasčių manyti, kad ieškomi duomenys laikomi tos šalies teritorijoje esančioje kitoje kompiuterių sistemoje arba jos dalyje ir kad tokie duomenys yra teisėtai prieinami naudojant pirmąją sistemą, tokios institucijos galėtų operatyviai išplėsti paiešką arba panašų tyrimą kitose sistemose".*

Vienas iš pagrindinių anksčiau minėtų Konvencijos normų tikslų – kad informacijos elektronine forma paėmimas iš apieškomos vietos nebūtų diskriminuojamas kitų materialių daiktų arba dokumentų atžvilgiu. Kitaip tariant, turi būti vienodai veiksminga tiek materialių, tiek nematerialių objektų krata.

Konvencijos rengėjų nuomone, nacionalinėje teisėje svarstytini keli kratos kitoje kompiuterių sistemoje išplėtimo variantai:

1) išduota sankcija yra papildoma ją išdavusios institucijos, t. y. „išplečiama" apimant ir kompiuterių sistemą, kurioje laikoma informacija, prieinama iš tiriamosios kompiuterių sistemos;
2) sankciją gavusiai institucijai (pareigūnui) suteikiami įgaliojimai ją papildyti.

Nors pirmuoju atveju nereikėtų kreiptis dėl naujos sankcijos, šio varianto neigiama savybė yra ta, jog tyrėjui, prieš „išplečiant" kratos veiksmus kitoje kompiuterių sistemoje, reikėtų kreiptis dėl sankcijos papildymo[18]. Turint omenyje kitoje kompiuterių sistemoje saugomos informacijos pažeidžiamumą ir tai, jog sankcija negali būti papildoma tiesiogiai (t. y. tyrėjas turėtų atlikti veiksmus, kurie pagal laiko sąnaudas prilygintini naujos sankcijos gavimui) būnant kratos vietoje, šis būdas yra diskutuotinas.

Antruoju atveju tyrėjas nesikreiptų dėl sankcijos papildymo, o

[18] Tokio procesinio veiksmo galimybė Lietuvos Respublikos baudžiamajame proceso kodekse iš viso nėra numatyta.

būtų traktuojama, jog išduota sankcija leidžia tyrėjui savarankiškai „išplėsti“ paiešką su tiriamąja kompiuterių sistema sujungtoje kompiuterių sistemoje, esančią Lietuvos Respublikos teritorijoje, jei būtų manoma, kad toje kompiuterių sistemoje yra tyrimui svarbi informacija. Šiuo atveju būtų tiesiogiai „išplečiama“ krata ir iki minimumo sumažinama galimybė pakeisti arba ištrinti informaciją iš atitinkamos kompiuterių sistemos, kol bus gauta nauja sankcija arba esama sankcija papildyta.

Paminėtina, jog Konvencijos paaiškinamajame rašte įvardijama, kad kratos „išplėtimo“ galimybė nebūtinai turi būti reglamentuojama naujais teisės aktais pagal nacionalinę teisę. Jei egzistuojantys teisės aktai suteikia galimybę „išplėsti“ kratą, nėra būtinybės priimti naujas teisės normas, reglamentuojančias kratos „išplėtimą“.

Kompiuterinių duomenų surinkimas realiuoju laiku. Konvencijoje numatyta, jog „*kiekviena šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti įgaliojant jos kompetentingas institucijas:*

a) tos šalies teritorijoje surinkti arba techninėmis priemonėmis įrašyti;
b) priversti paslaugos teikėją pagal jo technines galimybes:
   – tos šalies teritorijoje surinkti arba techninėmis priemonėmis įrašyti arba
   – bendradarbiauti su kompetentinga institucija ir padėti jai surinkti arba įrašyti

realiuoju laiku srauto duomenis, susijusius su konkrečia informacija, jos teritorijoje perduodama naudojantis kompiuterių sistema“ (Konvencijos 20 str.) arba „*realiuoju laiku turinio duomenis, susijusius su konkrečia informacija, jos teritorijoje perduodama naudojantis kompiuterių sistema*“ (Konvencijos 21 str.).

Kalbant apie kompiuterinių duomenų surinkimą realiuoju laiku, turimas omenyje įrodymų rinkimas iš dabartiniu metu vykdomų komunikacijų, kurios generuoja tam tikrus duomenis. Reikėtų atskirti, jog šiuo atveju galimi dviejų tipų duomenys: srauto duomenys[19] bei turinio duomenys[20]. Manoma, jog procesiniai srauto ir turinio duo-

[19] Pagal Lietuvos Respublikos elektroninių ryšių įstatymo 3 str. 52 p. srauto duomenimis laikytini duomenys, tvarkomi siekiant perduoti informaciją elektroninių ryšių tinklu ir (arba) tokio perdavimo apskaitai. 2002 m. rugsėjo 19 d. Konstitucinio Teismo nutarime telekomunikacijų įvykis apibūdinamas kaip „informacijos perdavimo, siuntimo, priemimo telekomunikacijų tinklais faktas“. Pavyzd•iui, srauto duomenimis laikytina informacija apie sujungimo laiką, trukmę, naudotus protokolus ir pan.

menų surinkimo reikalavimai turėtų skirtis, nes turinio duomenys neteisėtai atskleidžia komunikacijų turinį ir tai daro didesnę žalą, palyginti su neteisėtu srauto duomenų atkleidimu. Todėl turinio duomenų kontrolės sankcionavimas turėtų būti griežtesnis. Tačiau reikėtų paminėti, jog nors tradicinėse telekomunikacijose sąlyginai lengva atskirti turinio duomenis nuo srauto duomenų, kitos susižinojimo formos, pavyzdžiui, internetas, tokį atskyrimą padaro gana komplikuotą. Turinio ir srauto duomenų atskyrimas nulemtas tradicinių telekomunikacijų procesų, kur takoskyra tarp srauto duomenų (kas skambino, kur skambino, kiek truko skambutis) ir turinio duomenų (pokalbio turinio) buvo gana aiški, tačiau toks atskyrimas internete yra gana sudėtingas, o gal ir iš viso įmanomas. Neaišku, ar turinio duomenimis laikytinas visas elektroninių paketų turinys, ar srauto duomenys yra tik elektroninių paketų antraštės, taip pat ar srauto duomenimis laikytinos *clickstreams* ar *http* tipo užklausos. Tokiu atveju užklausa „http://searchengine/com/++aids++homosexuality++symptoms“ būtų laikoma srauto duomenimis, o minima užklausa susijusi su susižinojimo turiniu. Galima pateikti ir kitą pavyzdį – DTMF kodų rinkimą elektroninių komunikacijų metu. Pavyzdžiui, surinkus atitinkamą telefoninės bankininkystės numerį, po sujungimo atsiranda galimybė paslaugas valdyti DTMF kodais. Kadangi DTMF kodai renkami jau įvykus sujungimui, galima teigti, kad tai telekomunikacijų turinys. Tačiau, kita vertus, DTMF kodais siekiama inicijuoti tam tikras paslaugas (veiksmus), todėl šios komandos gali turėti ir srauto duomenų požymių. Kai kurie telekomunikacijų operatoriai Valstybinės duomenų apsaugos inspekcijos tinklapyje adresu http://www.ada.lt skelbiami deklaravę technines komandas pradėti sujungimus kaip tvarkomus asmens, t. y. srauto, duomenis. Todėl diskusija dėl minimų duomenų priskyrimo turinio arba srauto duomenų kategorijoms arba dėl šių kategorijų sutapatinimo ypač aktuali.

---

[20] Nei Konvencijoje, nei Lietuvos Respublikso teisės aktuose nėra apibrėžta, kas laikytina turinio duomenimis, tačiau šie duomenys susiję su susižinojimo (komunikacijų) turiniu (išskyrus srauto duomenis). Pagal 2002/58/EB direktyvos 2 (d) straipsnį „pranešimas“ – tai informacija, kuria apsikeičiama arba kuri perduodama baigtinio skaičiaus šalims, naudojantis viešai prieinamomis elektroninių ryšių paslaugomis. Kitaip tariant, turinio duomenimis laikytinas pokalbio telefonu arba elektroninio pašto žinutės turinys.

7.3.4. Elektroninių nusikaltimų kriminalizavimas Lietuvoje

Lietuvos Respublikos prisijungimas prie Konvencijos turėjo didelę įtaką Lietuvos nacionalinei baudžiamajai teisei. Nors dar iki Konvencijos pasirašymo priimtame naujajame Lietuvos Respublikos baudžiamajame kodekse jau buvo naujas skirsnis „Nusikaltimai informatikai“[21], kuriame nustatyta atsakomybė už nusikaltimus, keliančius grėsmę saugiam kompiuterinės informacijos apdorojimui, svarbūs Baudžiamojo kodekso papildymai buvo atlikti 2004 m. pradžioje. Įgyvendinant Konvenciją, nuo 2004 m. vasario 14 d. įsigaliojo nauji Baudžiamojo kodekso papildymai, kuriais į minėtą skirsnį įvestos dvi naujos veikos: neteisėtas prisijungimas prie kompiuterio arba kompiuterių tinklo (198-1 str.) bei neteisėtas disponavimas įrenginiais, kompiuterinėmis programomis, slaptažodžiais, prisijungimo kodais ir kitais duomenimis, skirtais nusikaltimams daryti (198-2 str.). Buvo papildyti ar pakeisti ir kiti kodekso straipsniai, pavyzdžiui, 309 straipsnis, nustatantis atsakomybę už disponavimą pornografinio turinio dalykais.

Atsakomybė už pavojingas veikas, pažeidžiančias kompiuterinės informacijos ir kompiuterių sistemų konfidencialumą, vientisumą bei prieinamumą.

Baudžiamoji atsakomybė už neteisėtą prieigą (su tam tikromis realiomis pasekmėmis (žala)) gali kilti pagal kelis Baudžiamojo kodekso straipsnius. Tik įsigaliojus naujajam Baudžiamajam kodeksui, Lietuvos įstatymo leidėjas, nustatydamas baudžiamąją atsakomybę už neteisėtą prieigą, buvo pasirinkęs tokį veikos elektroninėje erdvėje kriminalizavimo būdą – reikalaujama realios žalos, t. y. sunaikinti ar pakeisti kompiuterinę informaciją (Baudžiamojo kodekso 196 str.), sunaikinti ar pakeisti kompiuterinę programą (Baudžiamojo kodekso 197 str.) arba pasisavinti kompiuterinę informaciją (Baudžiamojo kodekso 198 str.).

Tačiau kėsinantis į įstatymo saugomus teisinius gėrius gali būti ne tik daroma reali žala, bet kilti ir tos žalos grėsmė. Tais atvejais, kai reali žala neatsiranda, o yra tiktai tokios žalos grėsmė, objekte irgi vyksta tam tikri pokyčiai. Pavojingumo pobūdį paprastai apibūdina

---

[25] Iki 2004 m. vasario šį skirsnį sudarė trys straipsniai, numatantys baudžiamąją atsakomybę už kompiuterinės informacijos sunaikinimą ar pakeitimą (196 str.), kompiuterinės programos sunaikinimą ar pakeitimą ir kompiuterių tinklo, duomenų banko ar informacinės sistemos darbo sutrikdymą (197 str.) bei kompiuterinės informacijos pasisavinimą ar skleidimą (198 str.).

kėsinimosi objekto vertingumas. Nusikaltimo objekto, į kurį kėsinamasi atliekant neteisėtą prieigą, – visuomeninių santykių saugant, apdorojant kompiuterinę informaciją vertingumą yra pabrėžę U. Sieberis, D. Baibridge'as ir kt. Šio objekto apsaugos baudžiamosiomis normomis praktika (kai nepadaroma reali žala) nustatoma vis daugiau valstybių. Be to, kriminalizuoti neteisėtą prieigą, kai nepadaroma reali žala, rekomenduojama ir tarptautiniuose norminiuose aktuose. Dėl to 2004 m. sausio 29 d. įstatymu Nr. IX-1992 Baudžiamasis kodeksas buvo papildytas nauju 198-1 straipsniu „Neteisėtas prisijungimas prie kompiuterio ar kompiuterių tinklo".

Lietuva baudžiamosios teisės normomis saugo formalią kompiuterinės informacijos ir kompiuterinių programų integralumo sritį, nustatydama atsakomybę Baudžiamojo kodekso 196 bei 197 straipsniuose. Šioms veikoms įvykdyti gali būti panaudojamos tokios kenkėjiškos programos kaip „Trojos arkliai", virusai, „kirmėlės" ir kt. Beje, 2004 m. papildžius Baudžiamojo kodekso 196 straipsnį buvo kriminalizuotos ir vadinamosios „DoS" atakos.

Baudžiamojo kodekso 197 straipsnyje taip pat nustatyti baudžiamosios atsakomybės pagrindai už vadinamąsias sabotažo naudojantis kompiuteriu veikas. Kompiuterių tinklo, duomenų banko arba informacinės sistemos darbo sutrikdymas arba pakeitimas siejamas su kompiuteryje esančios programos sunaikinimu, sugadinimu, pakeitimu ar tokios programos įdiegimu į kompiuterį ar kompiuterių tinklą. Kad kiltų baudžiamoji atsakomybė pagal Baudžiamojo kodekso 196 bei 197 straipsnių pirmąsias dalis, įstatymo leidėjas reikalauja, kad būtų padaryta didelė žala.

Baudžiamasis kodeksas saugo privatumą bendraujant elektroniniais ryšiais – pavojingos veikos šioje srityje kriminalizuotos 166 straispnyje „Neteisėtas susirašinėjimo, kitokių pranešimų, siuntų ar pokalbių telefonu slaptumo pažeidimas". Šio straipsnio, garantuojančio laisvą, normalų žmonių socialinį bendravimą, 1 dalyje nurodyta, kad baudžiamas yra *„tas, kas neteisėtai pažeidė asmens susirašinėjimo ar kitokiu paštu ar techninėmis priemonėmis siunčiamų pranešimų, siuntų slaptumą arba klausėsi pokalbių telefonu, arba naudojo kitas jų perėmimo formas*". Informacijos perėmimą elektroninėje erdvėje galima laikyti „kita perėmimo forma", todėl galima preziumuoti, jog ši nuostata taikoma pasikeitimams informacija elektroniniu paštu bei kitiems būdams.

Pavojingos yra veikos, kai tyčia atliekami tam tikri neteisėti veiks-

mai, susiję su įrenginiais arba prieigos duomenimis turint tikslą padaryti kitus kompiuterinius nusikaltimus, buvo kriminalizuotos 2004 m. sausio 29 d., papildžius Baudžiamąjį kodeksą 198-2 straipsniu „Neteisėtas disponavimas įrenginiais, kompiuterinėmis programomis, slaptažodžiais, prisijungimo kodais ir kitokiais duomenimis, skirtais nusikaltimams daryti“. Tai veikos, kai kuriami, platinami, panaudojami ir t. t. neteisėti įrenginiai/prieigos duomenys (slaptažodžių „nulaužimo“ programos, neteisėtu būdu gauti slaptažodžiai ar pan.), skirti kompiuterinių sistemų arba duomenų konfidencialumui, integruotumui ir prieinamumui pažeisti.

Atsakomybės pagrindai, susiję su neteisėtu turiniu elektroninėje erdvėje

Įstatymo leidėjas yra pasirinkęs veikų, susijusių su vaikų pornografijos platinimu internetu, kriminalizavimo tradiciniais straipsniais variantą. Lietuvos Respublikos baudžiamojo kodekso 309 straipsnis nustato baudžiamosios atsakomybės pagrindus už pornografinio turinio dalykų apie vaikus viešą demonstravimą įsigijimą, platinimą, gaminimą ir net laikymą. Beje, šiuo straipsniu kriminalizuotos ir veikos platinant vadinamąsias „pseudofotografijas“, kuriose tam tikras asmuo pateikiamas kaip vaikas.

Atsakomybės pagrindai už veikas, susijusias su kompiuteriais

Lietuvos įstatymo leidėjas Baudžiamajame kodekse sukčiavimo ir klastojimo veikas, vykdomas naudojantis elektronine erdve, kriminalizuoja tradicinėmis teisės normomis. Baudžiamoji atsakomybė už sukčiavimą nurodyta Baudžiamojo kodekso 182 straipsniyje. Šio straipsnio 1 dalyje nurodoma, jog baudžiamojon atsakomybėn traukiamas tas, kas apgaule savo arba kitų naudai įgijo svetimą turtą arba turtinę teisę, išvengė turtinės prievolės arba ją panaikino.

Baudžiamajame kodekse baudžiamoji atsakomybė už klastojimą nurodyta XLIII skyriuje „Nusikaltimai ir baudžiamieji nusižengimai valdymo tvarkai, susiję su dokumentų ar matavimo prietaisų klastojimu“. Baudžiamoji atsakomybė už dokumento klastojimą nustatyta Baudžiamojo kodekso 300 straipsnyje, kur nurodoma, jog baudžiamojon atsakomybėn traukiamas tas, kas pagamino netikrą dokumentą, suklastojo tikrą dokumentą arba netikrą ar suklastotą dokumentą panaudojo.

Atsakomybė, susijusi su autorių teisių bei gretutinių teisių pažeidimais

Autorių teisių bei gretutinių teisių pažeidimo elektroninėje erdvėje veikas galima kvalifikuoti pagal Baudžiamojo kodekso XXIX skyriaus „Nusikaltimai intelektinei ir pramoninei nuosavybei straipsnius. Šiame skyriuje nusikaltimais įvardytas autorystės pasisavinimas (191 str.); literatūros, mokslo, meno ar kitokio kūrinio neteisėtas atgaminimas, neteisėtų kopijų platinimas, gabenimas ar laikymas (192 str.); informacijos apie autorių teisų ar gretutinių teisių valdymą sunaikinimas arba pakeitimas (193 str.) bei neteisėtas autorių teisių ar gretutinių teisių techninių apsaugos priemonių pašalinimas (194 str.). Baudžiamojo kodekso 192 straipsnyje nurodyta, jog baudžiamojon atsakomybėn traukiamas tas, kas neteisėtai atgamino literatūros, mokslo, meno ar kitokį kūrinį ar jo dalį arba importavo, eksportavo, platino, gabeno ar laikė komercijos tikslais neteisėtas jų kopijas, jeigu bendra kopijų vertė pagal teisėtų kopijų mažmenines kainas viršijo 100 MGL dydžio sumą.

KONTROLINIAI KLAUSIMAI

1. Kuo skiriasi sąvokos „elektroninis nusikaltimas“ ir „kompiuterinis nusikaltimas?“
2. Kokios yra pagrindinės elektroninių nusikaltimų latentiškumo priežastys?
3. Įvardinkite pagrindinius elektroninių nusikaltėlių programišių požymius.
4. Kokie yra pagrindiniai elektroninių nusikaltimų požymiai, skiriantys šiuos nusikaltimus nuo kitų nusikaltimų?
5. Kokie elektroninių nusikaltimų padarymo būdai gali būti panaudoti siekiant įvykdyti elektroninės informacijos vagystę?
6. Kokie yra pagrindiniai tarptautiniai ir regioniniai dokumentai, reglamentuojantys elektroninių nusikaltimų sritį?
7. Kada buvo priimtas pirmasis įpareigojančio pobūdžio tarptautinis dokumentas elektroninių nusikaltimų srityje?
8. Ar Lietuva savo teisinėje sistemoje yra įgyvendinusi Konvencijos dėl elektroninių nusikaltimų proceso teisės dalies nuostatas?
9. Kokia atsakomybė Lietuvoje yra numatyta už neteisėtą prisijungimą prie kompiuterio arba kompiuterių tinklo?

Literatūra

1. Akdeniz Y., Walker C., Wall D. The Internet, Law and Society. – Pearson Education Limited, 2000.
2. Baibridge D. Introduction to Computer Law / Fifth edition. – Longman Pub Group, 2000.
3. Brenner S. W. Cybercrime and jurisdiction: a global survey (Information technology and law). – Aser press, 2006.
4. Broderick T. R. Regulation of Information Technology in the European Union. – London: Kluwer Law International, 2000.
5. Convention on Cybercrime. Budapest, 23. XI. 2001 // http://convention.coc.int.
6. Explanatory Report – Convention on Cybercrime // http://convention.coc.int.
7. Gahtan A. M., Kratz M. P. J. Internet Law: A Practical Guide to Legal and Business Professionals. – Carswell: Thomson Proffesional Publishing, 1998.
8. Icove D., Seger K., VonStorch W. Computer Crime: A Crimefighters Handbook. – Oreilly&Associates, Inc., 1995.
9. Civilka M., Lamanauskas T., Sauliūnas D., Štitilis D., Toliušis S. Informacinių technologijų teisė. – Vilnius: NVO teisės institutas, 2004 (Vilnius: Ciklonas).
10. Moreau D. Cybercrime: the investigation, prosecution and defence of a computer-related crime. – Karolina academic press, 2006.
11. Nathanson N., Gringras C. The Laws of the Internet. – Butterworths, 1997.
12. Petrauskas R., Štitilis D. Kompiuteriniai nusikaltimai ir jų prevencija. – Vilnius: Lietuvos teisės akademijos Leidybos centras, 2000 (2nd edition).
13. Sieber U. Legal Aspects of Computer-Related Crime in the Information Society. Comcrime study, prepared for European Commission // 1998. http://europa.eu.int/ISPO/legal/en/comcrime/sieber.html.
14. Štitilis D., Petrauskas R. Lietuvos Respublikos baudžiamasis kodeksas Nusikaltimų elektroninėje erdvėje konvencijos kontekste // Jurisprudencija. 2002. Nr. 24(16).
15. Štitilis D. Kai kurie neteisėtos prieigos prie kompiuterinės informacijos kriminalizavimo aspektai // Jurisprudencija, 2003. Nr. 47(39).
16. Štitilis D., Krikščiūnas R., Petrauskas R. Kai kurie Konvencijos dėl elektroninių nusikaltimų proceso teisės skirsnio įgyvendinimo Lietuvoje aspektai // Jurisprudencija. 2005. Nr. 67(59).
17. United Nations Manual on Computer-Related Crime. International Review of Criminal Policy Nos. 43/44 // http://www.uncjin.org/Documents/irpc4344.pdf

Kiškis, Mindaugas; Petrauskas, Rimantas; Rotomskis, Irmantas; Štitilis, Darius

TEISĖS INFORMATIKA IR INFORMATIKOS TEISĖ: vadovėlis. – Vilnius: Mykolo Romerio universiteto Leidybos centras, 2006. – 268 p., 2 schemos.

Te23

Bibliogr. 69, 113, 150, 203, 228, 267 p.

ISBN 9955-19-048-5

Vadovėlis skirtas visų lygių teisės studijų programų studentams, gali būti skaitomas informatikos, informacinių technologijų, verslo vadybos, viešojo administravimo ir kt. specialybių studentų bei specialistų.

Vadovėlyje aptariama informacinių technologijų ir teisės sąveika bei socialinė teisinė reikšmė, analizuojamos svarbios teisėje informacinių technologijų kategorijos, nagrinėjami interneto teisinio reguliavimo ypatumai, aptariamos intelektinės nuosavybės elektroninėje erdvėje teisinės apsaugos problemos. Vienas skyrius skirtas teisiniams privatumo ir asmens duomenų elektroninėje erdvėje klausimams. Vadovėlyje taip pat nagrinėjami elektroninės komercijos teisiniai aspektai, elektroninės demokratijos reiškinys, jo teisinė aplinka ir elektroniniai rinkimai. Paskutiniame vadovėlio skyriuje nagrinėjami nusikaltimai elektroninėje erdvėje: jų apibrėžimas, ypatumai, sudėtis, teisiniai aspektai ir elektroninių nusikaltimų tyrimo problemos.

UDK 34:004(075.8)

Mindaugas Kiškis, Rimantas Petrauskas,
Irmantas Rotomskis, Darius Štitilis

TEISĖS INFORMATIKA IR INFORMATIKOS TEISĖ

Vadovėlis

Redaktorės *Vesta Adomaitienė ir Jūratė Balčiūnienė*
Viršelio dailininkė *Stanislava Narkevičiūtė*
Maketavo *Aušrinė Ilekytė*

SL 585. 2006 11 30. 13,44 leidyb. apsk. l.
Tiražas 500 egz. Užsakymas
Išleido Mykolo Romerio universiteto Leidybos centras,
Ateities g. 20, LT–08303 Vilnius
Puslapis internete www.mruni.eu
Elektroninis paštas leidyba@mruni.lt
Spausdino UAB „Baltijos kopija“, Kareivių g. 13b, Vilnius
Puslapis internete www.kopija.lt
Elektroninis paštas info@kopija.lt