Interneto ir technologijų

teisė

MRU
MYKOLO ROMERIO UNIVERSITETAS

INTERNETO IR TECHNOLOGIJŲ TEISĖ


MYKOLO ROMERIO
UNIVERSITETAS

INTERNETO IR TECHNOLOGIJŲ TEISĖ

Vadovėlis

VALSTYBĖS ĮMONĖ
REGISTRŲ CENTRAS

Vilnius, 2016

UDK 004.738.5(094)(075.8)
In-156

Recenzavo:

Prof. dr. **Eglė Bilevičiūtė**
Mykolo Romerio universiteto Teisės fakulteto
Konstitucinės ir administracinės teisės institutas

Prof. dr. **Vida Davidavičienė**
Vilniaus Gedimino technikos universiteto
Verslo vadybos fakulteto Verslo technologijų katedra

Rekomendavo spausdinti:

Mykolo Romerio universiteto Mokslinių ir mokomųjų leidinių aprobavimo leidybai komisija 2015 m. rugpjūčio 17 d. (posėdžio protokolas Nr. 2L-13)

Autorių kolektyvo indėlis:

Prof. dr. **Darius Štitilis** – II, VII–X skyriai

Prof. dr. **Mindaugas Kiškis** – I, VI, XI skyriai

Doc. dr. **Tadas Limba** – IV, V, XII skyriai

Doc. dr. **Irmantas Rotomskis** – III skyrius

Konstantin Agafonov – XII skyrius

Gintarė Gulevičiūtė – V skyrius

Karolis Panka – įvadas, IV skyrius

ISBN 978-9955-30-214-8 (spausdinta)
ISBN 978-9955-30-213-1 (el. knyga)

TURINYS

Santrumpos

A2K (angl. *Access to knowledge)* – žinių prieinamumas
ACTA (angl. *Anti-counterfeiting trade agreement)* – prekybos sutartis dėl kovos su klastojimu
ADTAĮ – Asmens duomenų teisinės apsaugos įstatymas
AGATA – Lietuvos gretutinių teisių asociacija
AIPPI – Tarptautinė pramoninės nuosavybės apsaugos asociacija
ATGTĮ – Autorių teisių ir gretutinių teisių įstatymas
ATM (angl. *Activity transaction model)* – finansinių operacijų aktyvumo modelis
ATPK – Administracinių teisės pažeidimų kodeksas
B2B (angl. *Business to business)* – verslas verslui
B2C (angl. *Business to customer)* – verslas vartotojui
B2G (angl. *Business to government)* – verslas valdžios institucijoms
BEREC (angl. *Body of European regulators for electronic communications)* – Europos elektroninių ryšių agentūra
BK – Baudžiamasis kodeksas
C2B (angl. *Customer to business)* – vartotojas verslui
C2C (angl. *Customer to customer)* – vartotojas vartotojui
C2G (angl. *Customer to government)* – vartotojas valdžios institucijoms
CA (angl. *Certification authority)* – sertifikavimo institucija
CERN – Europos dalelių fizikos laboratorija
CERT (angl. *Computer emergency response team)* – reagavimo į kompiuterių incidentus komanda
CFAA (angl. *Computer fraud and abuse act)* – aktas dėl kompiuterinio sukčiavimo ir kenkiamųjų paskatų
CK – Civilinis kodeksas
CRL (angl. *Certificate recall list)* – sertifikatų atšaukimo sąrašas
CSS (angl. *Contents scrambling system)* – turinio kodavimo sistema
DDoS (angl. *Distributed Deny of Service)* – paskirstytas atsisakymas aptarnauti
DHT (angl. *Distributed hash table)* – išskirstytosios maišos lentelės
DĮR – didelė įtaka rinkoje
DNR – rekombinantinė dezoksiribonukleino rūgštis
DNS (angl. *Domain name server)* – domeno vardo serveris
DoS (angl. *Deny of Service)* – atsisakymas aptarnauti
EB – Europos Bendrija
EBPO – Ekonominio bendradarbiavimo ir plėtros organizacija
EDI (angl. *Electronic Data Interchange)* – elektroninių duomenų mainai
EERRI (angl. *Eastern European Research Reactor Initiative)* – Europos elektroninių ryšių reguliuotojų institucijos

EGAS – „Sodros“ elektroninė gyventojų aptarnavimo sistema
eID – elektroninė asmens tapatybės kortelė
EK – Europos Komisija
ELPA – Europos laisvosios prekybos organizacija
EMISARI (angl. *Emergency management information system and reference index)* – Ekstremalių situacijų valdymo ir nuorodų puslapių informacinė sistema)
EML (angl. *Electronic markup language)* – elektroninė aprašų kalba
ENISA (angl. *European network and information security agency)* – Europos tinklų ir informacijos apsaugos agentūra
EP – Europos Parlamentas
ERG (angl. *European Regulators Group)* – Europos reguliuotojų grupė
ES – Europos Sąjunga
ESTT – Europos Sąjungos Teisingumo Teismas
EŽTT – Europos Žmogaus Teisių Teismas
FDA – Maisto ir vaistų administracija
FTP (angl. *File transfer protocol)* – failų perdavimo protokolas
FTTB (angl. *Fiber to the building)* – optinis ryšys į pastatą
FTTH (angl. *Fiber to the home)* – optinis ryšys į namus
FTTN (angl. *Fiber to the node)* – optinis ryšys į ryšių mazgą
G2B (angl. *Government to business)* – valdžios institucijos verslui
G2C (angl. *Government to customer)* – valdžios institucijos vartotojui
G2G (angl. *Government to government)* – valdžios institucijos valdžios institucijoms
GM – genetiškai modifikuotas
GMO – genetiškai modifikuoti organizmai
GNU GPL (angl. *GNU General public licence)* – bendroji viešoji licencija
GPL (angl. *General public licence)* – žr. GNU GPL
HTML (angl. *Hypertext markup language)* – hiperteksto aprašų kalba
HTTP (angl. *Hypertext transfer protocol)* – hiperteksto perdavimo protokolas
ICANN (angl. *Internet corporation for assigned names and numbers)* – Interneto korporacija paskirtiems vardams ir skaičiams
IETF (angl. *Internet engineering task force)* – Interneto inžinerijos darbo grupė
IKT – informacinės ir komunikacinės technologijos
IPT – interneto paslaugų teikėjai
IRC (angl. *Internet relay chat)* – momentinė internetinių pokalbių ir pranešimų sistema
IRT – informacinės ir ryšių technologijos
ISM – interneto srauto mainai
ISO (angl. *International Organization for Standardization)* – tarptautinė standartizacijos organizacija

IT – informacinės technologijos
JAV – Jungtinės Amerikos Valstijos
JK – Jungtinė Karalystė
JT – Jungtinės Tautos
JTAP – Jungtinių Tautų aplinkos apsaugos programa
KTU – Kauno technologijų universitetas
LAN (angl. *Local area networks)* – vietos kompiuterių tinklas
LAT – Lietuvos Aukščiausiasis Teismas
LATGAA – Lietuvos autorių teisių gynimo asociacijos agentūra
LITEKO – Lietuvos teismų informacinė sistema
LITNET – Lietuvos mokslo ir studijų kompiuterių tinklas
LNRTC – Latvijos nacionalinis radijo ir televizijos centras
LOS (angl. *Low orbit satellite)* – žemos orbitos palydovas
LR – Lietuvos Respublika
LR ABTĮ – Lietuvos Respublikos administracinių bylų teisenos įstatymas
LR CK – Lietuvos Respublikos civilinis kodeksas
LR CPK – Lietuvos Respublikos civilinio proceso kodeksas
LRV – Lietuvos Respublikos Vyriausybė
LVAT – Lietuvos vyriausiasis administracinis teismas
MAC (angl. *Media access control)* – fizinis tinklo plokštės adresas
MŽŪO – Maisto ir žemės ūkio organizacija
NATO (angl. *North Atlantic Threat Organization)* – Šiaurės Atlanto sutarties organizacija
NCCUSL (angl. *National Conference of Commissioners on Uniform State Law)* – Jungtinių Amerikos Valstijų nacionalinės konferencijos dalyviai, atsakingi už bendrą šalies teisę
NETAIS – nacionalinės elektroninės atpažinties informacinės sistemos
NGN (angl. *New generation network)* – naujosios kartos tinklas
NIST (angl. *National Institute of Standards)* – Nacionalinis standartizacijos institutas
NKP – naujosios kartos prieigos
NRA (angl. *National regulatory authority)* – Nacionalinė reguliavimo institucija
NTP (angl. *Network time protocol)* – tinklo laiko protokolas
OTT (angl. *Over the top)* – operatoriai, kurie teikia paslaugas naudodamiesi kitų operatorių sukurta ir palaikoma elektroninių ryšių infrastruktūra
P2P (angl. *Peer to peer)* – tinklo modelis, kuriame keitimasis ištekliais vyksta tiesiogiai tarp vartotojų
PAR – Pietų Afrikos Respublika
PeX (angl. *Peer Exchange)* – tiesioginis apsikeitimas adresais
PINO – Pasaulinė intelektinės nuosavybės organizacija

PKI (angl. *Public key infrastructure)* – viešojo rakto infrastruktūra
PPO – Pasaulinė prekybos organizacija
PSO – Pasaulinė sveikatos organizacija
PVM – pridėtinės vertės mokestis
RAM (angl. *read-ahead memory)* – darbinė kompiuterio atmintis
RRT – Ryšių reguliavimo tarnyba
SCENIHR (angl. *Scientific committee on emerging and newly identified health risks)* – Besivystančių ir naujai identifikuotų rizikų sveikatai mokslo komitetas
SEO (angl. *Search engine optimization)* – tinklalapių optimizavimas paieškos rezultatams
SLD (angl. *Second level domain)* – antrojo lygio domenas
TCP/IP – (angl. *Transmission control protocol/internet protocol)* – standartinis duomenų perdavimo protokolų rinkinys
TLD (angl. *Top level domain)* – aukščiausio lygio domenas
TRIPS (angl. *Trade-related aspects of intellectual property rights)* – susitarimas dėl su prekyba susijusių intelektinės nuosavybės teisių aspektų
TSA (angl. *Time stamping authorities)* – laiko žymos institucija
TSM (angl. *Telecom single market)* – bendroji telekomunikacijos rinka
TSP (angl. *Time Stamp Protocol)* – laiko žymos protokolas
TST (angl. *Time Stamp Token)* – laiko žymos kodas
TTP (angl. *Third Trusted Party)* – trečioji patikima šalis
UAB – uždaroji akcinė bendrovė
UDRP (angl. *Uniform domain-name dispute resolution policy)* – unifikuota domeno vardų ginčų sprendimo politika
UETA (angl. *Uniform electronic transactions act)* – bendrasis Jungtinių Amerikos Valstijų elektroninių finansinių operacijų aktas
UNCITRAL – Jungtinių Tautų tarptautinės prekybos teisės komisija
UNESCO – Jungtinių Tautų švietimo, mokslo ir kultūros organizacija
UNIDO – Jungtinių Tautų pramonės plėtros organizacija
URL (angl. *Unified resource rocator)* – universalus informacijos šaltinio adresas
VDAI – Valstybinė duomenų apsaugos inspekcija
VĮ – valstybės įmonė
VoIP (angl. *Voice over IP)* – balso perdavimas per interneto protokolą
VSAT (angl. *Very small aperture terminal)* – labai mažos apertūros terminalai
WAN (angl. *Wide area networks)* – didelės aprėpties kompiuterių tinklas
WIPO (angl. *World Intellectual Property Organization*) – Pasaulinė intelektinės nuosavybės organizacija
WWW (angl. *World wide web)* – pasaulinis interneto tinklas

Įvadas

Sparti praėjusių kelių dešimtmečių technologijų plėtra, didėjanti konkurencija ir globalizacijos procesai stipriai pakeitė ir toli į priekį pastūmėjo telekomunikacijų, elektronikos bei informacinių technologijų ir jų teikiamų paslaugų pramonės sektorius. Šią nepaprastą plėtrą labiausiai skatina kompiuterinė įranga, puslaidininkiai, programinė įranga ir informacinių technologijų bei telekomunikacijų paslaugos. Sunku įsivaizduoti šiuolaikinę visuomenę, neturinčią modernių informacijos apdorojimo, kaupimo ir perdavimo priemonių. Informacinės technologijos yra neatskiriama šiuolaikinės visuomenės dalis. Internetu visame pasaulyje naudojasi daugiau kaip 3,2 mlrd. vartotojų[1], socialinis tinklas *Facebook* turi per 1,55 mlrd. vartotojų[2], pasaulyje egzistuoja per 3,9 mlrd. el. pašto adresų[3], mobiliojo ryšio operatoriai visame pasaulyje turi apie septynis milijardus abonentų[4], pasaulyje itin spačiai daugėja mobiliųjų mokėjimų operacijų, su internetu susijusias paslaugas teikiančios bendrovės 2014 m. sulaukė 11,9 mlrd. JAV dolerių investicijų. O programinės įrangos bendrovės, kuriančios programėles ir pan., pritraukė vienuolika milijardų JAV dolerių investicijų[5]. Visa tai patvirtina, kad pasaulis nebegali gyventi be interneto ar kompiuteriuose esančių programų ir išmaniuosiuose bei mobiliuosiuose įrenginiuose veikiančių programėlių.

Be to, reikia pabrėžti, kad technologijų prigimtis ir vaidmuo itin sparčiai vystosi ir keičiasi. Mes gyvename tarpinėje eroje tarp *Web 2.0* (antrosios kartos žiniatinklio) ir *Web 3.0* (trečiosios kartos žiniatinklio). *Web 2.0* terpėje beveik kiekvienas vartotojas, nors ir nėra informacinių technologijų specialistas, turi galimybę tiesiogiai prisidėti prie interneto turinio formavimo. 1997 m., kai internetu naudojosi maždaug 40 ar 50 mln. vartotojų, jie galėjo būti tik pasyvūs bet kokios informacijos, kurią

[1] Toks vartotojų skaičius prognozuojamas 2015 m. Prieiga per internetą: <http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf>.

[2] 2015 m. lapkričio duomenys. Prieiga per internetą: <http://expandedramblings.com/index.php/by-the-numbers-17-amazing-facebook-stats>.

[3] Toks skaičius prognozuojamas 2015 m. Prieiga per internetą: <http://www.radicati.com/wp/wp-content/uploads/2013/04/Email-Statistics-Report-2013-2017-Executive-Summary.pdf>

[4] Toks vartotojų skaičius prognozuojamas 2015 m. Prieiga per internetą: <http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf>.

[5] 2015 m. sausio duomenys. Prieiga per internetą: <http://nvca.org/pressreleases/annual-venture-capital-investment-tops-48-billion-2014-reaching-highest-level-decade-according-moneytree-report>.

tinklalapių savininkai pasirinkdavo į juos įkelti, gavėjai. Šiandien vartotojai yra tapę turinio teikėjais. Skaitytojai yra autoriai. Gavėjai yra tinklo dalyviai, kurie pateikia informaciją ir vienas su kitu bendradarbiauja, pvz., tinklaraštininkai, socialinių tinklų[6] naudotojai arba bendrų tinklo išteklių (angl. *shared resource)* bendraautoriai (pvz., nemokama laisvoji interneto enciklopedija *Wikipedia*, kuriama jos lankytojų – interneto vartotojų arba interneto tinklalapis *YouTube*, kuriame kiekvienas įsiregistravęs vartotojas gali įkelti, žiūrėti vaizdo įrašus ar jais dalytis su kitais vartotojais). Informacinių technologijų ir interneto plėtros finišo tiesioji neegzistuoja, nes kiekvieną dieną yra sukuriama daugybė naujų programų (pvz., nuotraukų redagavimo programa *Instagram* buvo paleista 2010 m. spalį, o 2015 m. lapkritį jau turėjo daugiau kaip 400 mln. aktyvių vartotojų[7]). Nuo 2006 m. netyla kalbos ir apie *Web 3.0* (trečiosios kartos žiniatinklį), kuris būtų paremtas tuo, kad pačios interneto naršyklės galėtų „suprasti“ ir apdoroti joms pateikiamas užklausas. Kai kurie autoriai *(Susskind*, 2013) teigia, kad mes šiuo metu esame informacijos substruktūros pokyčio visuomenėje liudininkai. Informacijos substruktūra – tai pagrindinis būdas, kuriuo informacija yra užfiksuojama, ja dalijamasi ir ji platinama. Žmonija yra perėjusi keturis informacijos substruktūros etapus: žodinis amžius, kai kalba buvo pagrindinė komunikacijos priemonė, rašto amžius, spaudos amžius ir žinių visuomenė, kurioje informacinės technologijos yra pagrindinė komunikacijos priemonė. Šiuo metu žmonija yra pereinamosios fazės pabaigoje tarp trečiojo ir ketvirtojo etapų, tarp spausdintu žodžiu grindžiamos industrinės visuomenės ir internetu bei informacinėmis technologijomis paremtos žinių visuomenės. Prognozuojama, kad po 30–40 metų žmonijos laukia penktasis etapas – nanotechnologijų, robotikos, genetikos ir informacinių technologijų konvergencija.

Savo ruožtu teisė, kaip socialinis reiškinys, negalėjo ir toliau negali atsilikti nuo sparčios informacinių technologijų plėtros ir naujų technologijų radimosi, o tai kelia naujų iššūkių ir problemų tiek tarptautinėms insitucijoms, Europos Sąjungos ir atskirų valstybių įstatymų leidėjams inicijuojant naujų teisės aktų, kurie atspindi įvykusius technologinius pokyčius, leidimą, tiek verslo subjektams, tiek teisėsaugos institucijoms bei, ko

[6] Internetiniai socialiniai tinklai gali būti suprantami kaip socialinė struktūra, vienijanti tam tikras interesų grupes, kurių nariai (vartotojai) tarpusavyje susiję įvairiais ryšiais (draugyste, giminyste, ekonominiais santykiais, simpatija ar antipatija, seksualiniais ryšiais, religija, išsilavinimu, pomėgiais, socialine padėtimi), motyvuoti dalytis turima informacija, diskutuoti aktualiais klausimais, keistis muzika, vaizdo medžiaga, prisistatyti elektroninėje erdvėje bei viešai demonstruoti socialinį aktyvumą.

[7] 2015 m. lapkričio duomenys. Prieiga per internetą: <http://expandedramblings.com/index.php/important-instagram-stats>.

gero, kiekvienam iš mūsų, nes šiuolaikinio žmogaus gyvenimas yra beveik neįsivaizduojamas be informacinių technologijų (interneto, elektroninio pašto, mobiliojo ryšio, socialinių tinklų ir t. t.). Jau 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 (angl. *cyberlaw)*, informatikos teisė ir kt. Pabrėžtina, kad teisės informatika ir informatikos teisė yra netapatūs dalykai. Teisės informatikos paskirtis – informacinių technologijų pritaikymo ir naudojimo teisėje susisteminimas bei struktūrizavimas. Tuo metu informacinių technologijų teisės reguliavimo dalykas yra specifiniai santykiai, susiklostantys informacinių technologijų pagrindu[8].

Autorių nuomone, atsižvelgiant į esamą patirtį ir itin sparčią technologijų plėtrą, Lietuvoje vartotini trys 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;
- *naujų technologijų teisė* – nagrinėjant tik socialinių santykių, susijusių su ne tik su informacinėmis technologijomis (elektronine erdve), bet ir su nanotechnologijomis, biotechnologijomis, robotika ir kitomis pažangiomis technologijomis, teisinio reglamentavimo specifiką.

Ši teisinė sprecifika taip pat pagrindžia būtinybę studijuoti teisės informatiką ir naujų technologijų teisę kaip specifinių teisės institutų ir reiškinių kompleksą. Šiame vadovėlyje nagrinėjamos pagrindinės bendrosios informacinių technologijų bei teisės sąveikos problemos ir pateikiami naujų technologijų teisės pagrindai.

---

[8] Plačiau žr.: Civilka, M.; Lamanauskas, T.; Nosinaitė, G.; Sauliūnas, D.; Štitilis, D.; Toliušis, S.; Ulevičius, L. Informacinių technologijų teisė. Vilnius: NVO teisės institutas. 2004, p. 25–29.

Vadovėlis yra skirtas visų lygių teisės studijų programų studentams, tačiau interneto, elektroninių ryšių, elektroninės komercijos, elektroninių sutarčių, elektroninių įrodymų, nano ir biotechnologijų bei robotikos teisinio reglamentavimo principai, intelektinės nuosavybės ir privatumo bei asmens duomenų apsaugos elektroninėje erdvėje, elektroninių nusikaltimų ir kibernetinio saugumo pamatinės nuostatos, kurios nagrinėjamos šiame vadovėlyje, turėtų sudominti ne tik studentus ir praktikuojančius teisininkus, bet ir informacinių technologijų specialistus bei visus tuos, kuriems kiekvieną dieną tenka naudotis informacinėmis technologijomis darbo ar asmeniniams tikslams.

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

Antrame skyriuje apžvelgiamas elektroninių ryšių teisinis reguliavimas: apibūdinama elektroninių ryšių kaitos ir teisinio reguliavimo raida, ES elektroninių ryšių reguliavimo sistema, apžvelgiami pagrindiniai ES elektroninių ryšių reguliavimo institutai ir analizuojami kiti su elektroninių ryšių teisiniu reguliavimu susiję klausimai.

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

Ketvirtame skyriuje aptariami su elektroninių įrodymų teisiniu reguliavimu susiję klausimai: atskleidžiama elektroninių įrodymų samprata, jų svarba teismo procese, analizuojami elektroninių įrodymų pateikimo teismui, vertinimo ir įrodomosios galios klausimai.

Penktame skyriuje apibūdinamos elektroninių dokumentų ir elektroninių sutarčių techninės apsaugos priemonės, analizuojami su elektroninio parašo ir laiko žymos naudojimu susiję klausimai.

Šeštame skyriuje aptariamos intelektinės nuosavybės elektroninėje erdvėje teisinės apsaugos problemos, taip pat atskirai nagrinėjama kompiuterių programų ir duomenų bazių teisinė apsauga, intelektinės nuosavybės kolektyvinio administravimo problemos elektroninėje erdvėje, atviro kodo ir kūrybinių bendrijų judėjimai, laikmenų ir įrangos mokesčiai ir prekių ženklų apsauga elektroninėje erdvėje.

Septintame skyriuje apžvelgiamas privatumas ir asmens duomenų apsauga elektroninėje erdvėje, apibūdinama ES duomenų apsaugos reforma, analizuojami su privatumu ir asmens duomenų apsauga elektroniniuose ryšiuose, elektroninėje darbo vietoje, virtualiuose socialiniuose tinkluose, teikiant nuotolinės kompiuterijos paslaugas, susiję klausimai.

Aštuntame skyriuje aptariamas teisinis asmens identifikavimo elektroninėje erdvėje reguliavimas.

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

Dešimtame skyriuje atskleidžiama kibernetinio saugumo samprata, principai, apžvelgiama ES kibernetinio saugumo strategija, aptariami kiti su kibernetiniu saugumu susiję klausimai.

Vienuoliktame skyriuje apibūdinamas biotechnologijų teisinis reglamentavimas, teisės principai, atskleidžiama nanotechnologijų samprata, teisinio reguliavimo prielaidos, ypatumai ir principai, aptariami robotikos teisiniai aspektai.

Dvyliktame skyriuje yra nagrinėjamas naujųjų technologijų poveikis šalių demokratiniams ir visuomenės dalyvavimo procesams, aptariami šiuolaikinėmis technologijomis pagrįsti visuomenės įtraukimo į šalies politinius procesus aspektai, e. balsavimo sistemos, jų pažeidžiamumo ir apsaugos klausimai.

Teisė ir informacinės technologijos

1. Elektroninė erdvė, jos savybės ir įtaka teisiniams reiškiniams

Elektroninės informacijos erdvė (angl. *cyber space)* – globaliai integruota, viešai ir visuotinai prieinama kompiuterių tinklų sistema, kuria naudojantis keičiamasi informacija.

Prieiga prie informacijos ir keitimasis ja yra svarbiausios e. erdvės funkcijos. Technologinis progresas lemia, kad e. erdvės techninė realizacija darosi vis sudėtingesnė, tačiau tuo pat metu visuomenei, verslui ir individualiems vartotojams informacija tampa vis lengviau prieinama ir naudojama. Dėl šių priežasčių socialinių santykių apimtis e. erdvėje ypač sparčiai didėja, o kai kuriose srityse (pvz., elektroniniuose atsiskaitymuose) jau pralenkia analogiškos veiklos apimtį fizinėje erdvėje. Elektroninė erdvė gali būti naudojama:

- vienpusei komunikacijai, kai vartotojai tarpusavyje pasikeičia elektroninio pašto pranešimais, skaito interneto tinklalapiuose pateiktą informaciją;
- daugiapusei komunikacijai, kai vartotojai aktyviai diskutuoja ir keičiasi informacija įvairiuose forumuose, interneto tinklalapių

komentarų skiltyse, naujienų grupėse, tinklaraščiuose, socialiniuose tinkluose ir pan.;

- įvairioms finansinėms operacijoms, kai e. erdvėje atliekami finansiniai atsiskaitymai, teikiamos įvairios paslaugos, sudaromi ir tvirtinami sandoriai;
- įvairioms veiklos rūšims, automatizuotiems įrengimams valdyti per atstumą.

Elektroninė erdvė gali būti naudojama ir tiesioginei interaktyviajai komunikacijai virtualiose darbo grupėse, bendradarbiavimo erdvėse, tampa įprastu verslo instrumentu, viešosios valdžios institucijų ir interesų grupių bendravimo su piliečiais ir visuomene priemone. Elektroninėje erdvėje vyksta konvergencija – dar XX a. devintajame dešimtmetyje televizoriai ir kompiuteriai buvo visiškai atskiri prietaisai ir nebuvo galimybių tarpusavyje keistis informacija. Dabar įmanoma žiūrėti televizijos programas per kompiuterį, o kai kurie televizoriai gali atlikti intelektualųjį informacijos apdorojimą. Taigi ribos tarp televizijos ir informacinių technologijų nyksta. Panašus ribų susiliejimas vyksta per visą skaitmeninę vertės grandinę – nuo turinio šaltinio iki pat kliento. Yra du konvergencijos tipai: substitutų ir komplektuojamųjų produktų. Substitutų konvergencija pasireiškia, kai skirtingos įmonės įdiegia produktus, kurių savybės panašios į kitų produktų, pvz., tai gali būti televizorius, turintis tas pačias intelektualaus apdorojimo savybes, kaip ir asmeninis kompiuteris, arba asmeninis kompiuteris, kuris gali priimti televizijos transliacijas. Laikui bėgant produktai, įgyjantys vis daugiau bendrųjų savybių, taps sukeistini. Komplektuojamųjų produktų konvergencija pasireiškia, kai produktai savo funkciją geriau atlieka kartu nei atskirai, pvz., televizorius, kuriuo transliuojama informacija, gali būti tuojau pat perkeliamas į asmeninį kompiuterį.

Būtina atkreipti dėmesį, kad e. erdvė iš esmės neturi nei fizinių, nei teisinių sienų, nėra jokios „centrinės valdžios“, kuri valdytų informacijos kaitą internete. Todėl informacija e. erdvėje akimirksniu tampa visuotinai vienu metu (lygiagrečiai) prieinama ja susidomėjusiems viso pasaulio vartotojams. Prieigos prie informacijos ir jos platinimo sąnaudos e. erdvėje yra nedidelės, palyginti su kitomis informacijos sklaidos formomis (pvz., tradicinės žiniasklaidos priemonėmis: televizija ar spauda). Iš esmės e. erdvė atvėrė dideles galimybes valdžios institucijoms, verslui ir plačiajai visuomenei skelbti jiems aktualią informaciją ir ją gauti, teikti elektronines paslaugas, siūlyti savo prekes ir paslaugas bei jų įsigyti.

Pabrėžtina, kad e. erdvė ne tik atveria naujų rinkų tradiciniams produktams ir paslaugoms, bet ir leidžia kurti visiškai naujus elektroninius

produktus bei paslaugas, kurie pristatomi ir dažniausiai vartojami elektroniniu būdu (pvz., elektroniniu būdu parsisiunčiami muzikos įrašai[9], elektroninės knygos ir žurnalai[10], kompiuterių programos, prieiga prie elektroninių duomenų bazių ir pan.).

Dar viena svarbi e. erdvės savybė – vadinamasis globalaus kaimo efektas, t. y. visa e. erdvėje pateikiama informacija bus iškart ir tuo pat metu prieinama viso pasaulio vartotojams, todėl ją reikėtų kritiškai įvertinti ir atsižvelgti į įvairias etines, religines ir politines normas bei požiūrius. Globalaus kaimo efektas lemia ir tai, kad e. erdvėje gali būti laisvai pateikiama informacija, prekės ir paslaugos, kurių platinimas kai kuriose šalyse ribojamas ar net apskritai griežtai draudžiamas, pvz., ksenofobinio pobūdžio (antisemitinė, rasistinė ir pan.) informacija, azartinių lošimų, alkoholio, narkotinių medžiagų[11], vaistų reklama ir kita. Dėl techninių e. erdvės savybių tokia informacija, prekės ir paslaugos yra laisvai prieinamos viso pasaulio vartotojams ir netgi griežtomis fizinės kontrolės priemonėmis beveik neįmanoma iki galo sureguliuoti jų platinimo. Netgi nedemokratinėse valstybėse, tokiose kaip: Iranas, Kinija ar Baltarusija, iš esmės negalima visiška e. erdvėje skelbiamos informacijos kontrolė.

Akivaizdu, kad minėtosios e. erdvės savybės atvėrė iš esmės naujos kokybės elektroninės demokratijos ir socialinės bei ekonominės plėtros galimybių. Dėl e. erdvės plėtros tapo galimas unikalus piliečių dalyvavimas priimant visuomenei svarbius administracinius bei teisinius sprendimus ir teisės aktus, padaugėjo galimybių naudotis viešosiomis paslaugomis net atokiausiuose šalies kampeliuose. Kartu didėja ir viešųjų paslaugų pasiūla bei kokybės kontrolė, atveriama vartotojiškų elektroninių produktų ir paslaugų rinka, kuriami socialiniai tinklai ir diegiamos naujos socialinio bendravimo formos.

---

[9] Pvz., internete veikiančios elektroninių muzikos įrašų parduotuvės *Beatport* ir *iTunes Music Store*.

[10] Jau 2012 m., vienos didžiausių internetinių parduotuvių *www.amazon.co.uk* duomenimis, elektroninių knygų pardavimas Jungtinėje Karalystėje viršijo įprasto popierinio formato knygų pardavimą.

[11] Pvz., internetinė prekybos platforma „Šilko kelias“ (angl. *Silk road)*, kuri veikė nuo maždaug 2011 m. sausio iki 2013 m. rugsėjo. Joje buvo prekiaujama nelegaliais narkotikais ir kitomis prekėmis bei paslaugomis, kurias nuolat pirko ir pardavinėjo tinklalapio vartotojai. Pirkėjų ir (ar) pardavėjų anonimiškumas joje buvo užtikrinamas tuo, kad puslapis buvo pasiekiamas tik per TOR tinklą, o atsiskaitant naudojama virtuali *BitCoin* valiuta. Pasak JAV federalinio tyrimų biuro (FTB), per 2011–2013 m. apyvarta šioje platformoje siekė 1,2 mlrd. JAV dolerių, o jos savininkas, kuris FTB buvo sulaikytas 2013 m. spalį, gavo 79,8 mln. JAV dolerių komisinių. Platforma turėjo beveik milijoną registruotų vartotojų, kurie atliko 1,2 mln. mokėjimo operacijų.

Naujosios informacinės komunikacinės technologijos, sparti e. erdvės – kompiuterių tinklų ir interneto – plėtra lėmė didelius teisės pokyčius. Praėjusio šimtmečio pabaigoje teisininkai vis plačiau pradėjo naudoti naujausias informacines technologijas. Kita vertus, pasaulinė elektroninė komunikavimo erdvė sukėlė daug teisinių problemų, kurioms išspręsti neužteko esamų teisės normų, todėl atsirado naujų teisės institutų ir teisės mokslo bei teisės šakų – teisės informatika, informatikos (informacinių technologijų) ir naujųjų technologijų teisė. Be to, informacinių technologijų plėtra atvėrė naujų erdvių suvokiant, aiškinant ir taikant teisę. Teisės normų gausa bei jų sudėtingumas paskatino net ir teisiniams procesams pasitelkti technologinių priemonių (teisės aktų paieška, sisteminimas, aiškinimas ir t. t.), o tai lėmė technologijų bei technologinio reguliavimo ir tradicinių teisės normų konkurenciją. Elektroninėje erdvėje teisė tampa veiksminga tik tuo atveju, jeigu jai įgyvendinti pasitelkiamos techninės priemonės (pvz., informacijos privatumas yra užtikrinamas ją šifruojant), kita vertus, ir pačios techninės priemonės gali pažeisti teisės normas (pvz., suteikti galimybę neteisėtai naudotis privačia informacija, sunaikinti elektroninius duomenis arba apriboti teisių išimtis), arba pačios būti pažeidžiamos (pvz., naudojant neteisėtus dekoderius koduotų televizijos programų peržiūrai). Išplėtotos ir toliau plėtojamos naujosios kartos technologijos – teisinių sprendimų paramos sistemos, teisinės duomenų bazės (pvz., *LexisNexis* ir *Westlaw)*, teisinių dokumentų analizės ir automatinio apdorojimo, procesinių dokumentų pateikimo teismui sistemos – dar glaudžiau susieja technologijas ir teisės normas. Visa tai lemia teisės suvokimo ir tapatumo e. erdvėje klausimus.

Globalus e. erdvės pobūdis lemia, kad nacionalinės teisinės iniciatyvos reglamentuojant e. erdvę ir su ja susijusius socialinius teisinius reiškinius (elektroninę komerciją, nusikaltimus internete ir t. t.) gali būti neveiksmingos dėl valstybių fizinių sienų, skirtingo teisinio reguliavimo atskirose valstybėse, valstybės įstaigų ir pareigūnų kompetencijos bei techninių galimybių. Elektroninėje erdvėje kylančios problemos sprendžiamos tarptautiniu lygiu (pvz., 2001 m. priimta Konvencija dėl elektroninių nusikaltimų), regioniniu lygiu (pvz., 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, 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privataus gyvenimo apsaugos elektroninių ryšių sektoriuje, 2013 m. gegužės 21 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 524//2013 dėl elektroninio vartotojų ginčų sprendimo, kuriuo iš dalies keičiami Reglamentas (EB) Nr. 2006/2004 ir

Direktyva 2009/22EB) bei nacionaliniu lygiu (pvz., Filipinų Aukščiausiojo Teismo elektroninių įrodymų vertinimo taisyklės).

Kita išryškėjusi tendencija – specialių internetą reguliuojančių normų vengimas. Informacinės technologijos ir socialiniai teisiniai reiškiniai e. erdvėje su tam tikromis išimtimis turėtų būti reglamentuojami remiantis tokiais pat teisės principais, kaip ir jų tradiciniai analogai (pvz., interneto žiniasklaidai turėtų būti taikomos tos pačios taisyklės kaip ir tradicinei). Specialus papildomas reglamentavimas turėtų būti pasitelkiamas tik tais atvejais, kai pasireiškia specifiniai, išskirtinai e. erdvei ar informacinėms technologijoms, būdingi ypatumai, priešingu atveju nebus išvengta diskriminavimo ir nevienodų verslo bei konkurencijos sąlygų.

2. Teisinio informacinių technologijų reglamentavimo principai

Informacinių technologijų ir socialinių teisinių reiškinių e. erdvėje reguliavimas turėtų būti griežtai pagrįstas šiais pagrindiniais principais[12]:

- 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. Šio principo esmė – elektroninių duomenų nediskriminavimas vien tik dėl jų formos. Jeigu elektroniniai duomenys atlieka tas pačias funkcijas kaip ir rašytiniai dokumentai – nėra jokio teisinio pagrindo jais nesivadovauti sprendžiant teisinius klausimus.

Technologinio neutralumo principas užtikrina lygiavertį technologijų vertinimą, nes draudžia teikti pirmenybę kuriai nors vienai iš jų. Pagal šį principą prioritetas, aiškinant su technologijomis susijusias sąvokas, turėtų būti teikiamas jų funkcijoms, o ne pačioms konkrečiai įvardijamoms technologijoms. Atsižvelgiant į teisės ir technikos sąveikos perspektyvas, tai leidžia išvengti teisės normų taikymo apribojimų, atsirandančių dėl jose vartojamų specifinių terminų. Teisinis reguliavimas, laikantis technologinio neutralumo principo, teisėkūros metu naudojamų technologijų

[12] Plačiau apie principus žr.: Civilka, M.; Lamanauskas, T.; Nosinaitė, G.; Sauliūnas, D.; Štitilis, D.; Toliušis, S.; Ulevičius, L. Informacinių technologijų teisė. Vilnius: NVO teisės institutas. 2004, p. 30–33.

atžvilgiu yra ne tik abstraktus procesas, bet ir siejamas su galimomis jų ateities perspektyvomis. Jis apima ir tas technologijas, kurių išradimas ar plėtra negali būti numatomi iš anksto.

Funkcinio lygiavertiškumo principas reiškia, kad vertinant elektroninio dokumento teisinę galią yra atsižvelgiama į tradicinių dokumentų, surašytų popieriuje, tikslus bei funkcijas ir tik tada sprendžiama, kaip tie tikslai ir funkcijos yra įgyvendinami konkrečiu elektroniniu pranešimu. Be to, taikant šį principą elektroninės komercijos naudotojams neturėtų būti keliami didesni saugumo (ir su tuo susijusių didesnių išlaidų) reikalavimai nei neelektroninėje aplinkoje. Tačiau Lietuvos teisėje nusistovėjęs šio principo apibrėžimas skiriasi nuo to, kuris įtvirtintas tarptautiniuose dokumentuose. Lietuvos Respublikos informacinės visuomenės paslaugų įstatymo 3 str. 4 d. teigiama, kad funkcinio lygiavertiškumo principas reiškia, jog teisės normos turėtų būti kuo vienodžiau taikomos informacinės visuomenės paslaugoms, atliekančioms analogiškas funkcijas. Taigi šia norma nustatomas lygiavertis informacinės visuomenės paslaugų, o ne lygiavertis popierinės ir elektroninės formų vertinimas. Tokios diskutuotinos funkcinio ekvivalentiškumo principo sampratos įtvirtinimas Informacinės visuomenės paslaugų įstatyme gali būti viena iš priežasčių, dėl kurių nacionalinėje teisėje yra atsiradę nemažai elektroninės formos reglamentavimo neaiškumų[13].

Esant darniam teisiniam reguliavimui, savireguliacija gali funkcionuoti kaip ypač veiksmingas e. erdvės ir informacinių technologijų kontrolės mechanizmas, veiksmingesnis už valstybinio reguliavimo priemones. Dėl šios priežasties valstybinis reguliavimas neturėtų užkirsti kelio savireguliacijai, o visapusiškai ją skatinti ir galiausiai palikti erdvės pačių rinkos dalyvių ir vartotojų teisėkūrai, nes būtent rinkos dalyviai ir vartotojai gali realiausiai įvertinti savo poreikius ir proporcingai pasidalyti riziką.

Atskirai paminėtina ir tai, kad naujosios e. erdvės technologijos įgalina kurti naujus informacijos kontrolės ir socialinių santykių reguliavimo mechanizmus. Tokioms technologijoms priskiriama: elektroninio turinio techninės apsaugos ir 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 e. erdvėje.

Remiantis moksliniais tyrimais informacinių technologijų ir teisės srityje, pvz., L. Lessigo teorija, galima įžvelgti tam tikrą informacinių

[13] Plačiau žr.: Kalinauskaitė, A. Elektroninė forma ir elektroninis parašas: Lietuvos teisinė bazė globaliame kontekste. Teisės problemos, 2012, Nr. 1 (75).

technologijų ir teisės konvergenciją, teigiama, kad žinių visuomenėje informacinės technologijos ir teisė negali egzistuoti vienos nuo kitų atskirai. Informacinėms technologijoms būtina teisinė apsauga ir socialinį interesą užtikrinančios reglamentavimo išimtys, o teisė vis dažniau remiasi technologiniais teisės normų įgyvendinimo mechanizmais.

3. Teisės informatikos sąvoka ir turinys

Teisės informatiką galima apibrėžti kaip mokslą, nagrinėjantį informacinių technologijų, teisės sistemos ir teisinių reiškinių sąveiką. Praktiniu požiūriu teisės informatika apima informacinių technologijų teisinio reglamentavimo modelius ir institutus, teisinės informacijos teoriją, jos tvarkymo (kaupimo, sisteminimo ir saugojimo) klausimus bei paieškos sistemas (tarp jų ir automatizuotas). Teisės informatiką galima suprasti ir kaip teisės mokslo šaką, kurios objektas – informacinis teisės 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, lemia ir teisinės informacijos ypatumus, išskiriančius šią informaciją į atskirą socialinės informacijos rūšį, ir teisės informatikos tikslus bei principus.

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

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

Siekiant minėtųjų tikslų, atsižvelgiama į šiuos svarbiausius teisės informatikos ir teisinės informacijos principus:

1) teisinės informacijos viešumą: teisės šaltinis gali būti tik viešai paskelbtas norminis teisės aktas (šis principas yra įtvirtintas Lietuvos Respublikos Konstitucijoje);

2) teisinės informacijos patikimumą: informacijos patikimumas priklauso nuo jos šaltinio ir transformavimo patikimumo. Šaltinio patikimumas išreiškiamas tam tikrais rekvizitais, kurie turi būti išsaugoti perrašant dokumentą iš vienos laikmenos (pvz., popieriaus) į kitą (pvz., USB atmintinę). Transformavimo patikimumas priklauso nuo informacijos kanalo kokybės;
3) teisinės informacijos galiojimą: teisinės informacijos vartotojui turi būti teikiama informacija apie galiojančią teisę, t. y. teisės aktų tekstuose būtini visi jų pakeitimai ir papildymai, todėl teisinės informacijos apdorojimo priemonės turėtų būti tokios, kurios leidžia operatyviai padaryti tokių pakeitimų ir papildymų;
4) informavimo spartą: būtina įvairių valdymo sprendimų, veiksmingo teisės aktų taikymo, priėmimo ir poveikio sąlyga – greitas reikalingos informacijos suradimas. Todėl teisinės informacijos bazė (bankas) abonentui turi būti prieinamas bet kuriuo jo darbo metu;
5) informavimo išsamumą ir tikslumą: teisinės informacijos gali būti per daug, bet jos negali būti per mažai, todėl turėtų būti siekiama gauti kuo išsamesnės informacijos ir kartu užtikrinti kuo mažiau netikslumų.

Be to, svarbu yra atsižvelgti į tokius bendruosius principus:

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. nė vienai iš esamų technologijų neteikiama teisinė pirmenybė;
3) naujausių techninių priemonių naudojimą (aprūpinant įvairias įstaigas techninėmis priemonėmis prioritetas turėtų būti teikiamas naujausioms techninėms priemonėms ir technologijoms).

4. Teisinė informacija ir jos tvarkymas

Teisinė, kaip ir bet kuri kita, informacija yra vienas iš svarbiausių žinių visuomenės įrankių ir išteklių. Siekiant apibrėžti teisinės informacijos sampratą, būtina identifikuoti bendruosius jos požymius ir koncepcijas.

Filosofiniu požiūriu galimos trys pagrindinės informacijos koncepcijos:

1) semiotiniu požiūriu informacija sietina su ženklų sistemomis ir jų struktūromis;

2) funkciniu požiūriu informacija tapatintinama 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, nes jis dažniausiai būna susijęs su teisės pažeidimais ir jų atskleidimu. Teisiniu požiūriu yra svarbus ir kitas – ontologinis – informacijos aspektas, kuris yra mažiau matomas ir gana dažnai pamirštamas. Ontologinis aspektas atspindi informacijos suvokimą, taip pat teisės kaip informacijos suvokimą ir įsisąmoninimą. Ontologinis teisinės informacijos aspektas atskleidžia teisės sistemos esmę ir dėl to yra ypač svarbi teisės filosofijos dalis.

Pagrindinės teisinės informacijos rūšys skiriamos minėtuoju filosofiniu pagrindu:

1) ontologinė teisinė informacija – pozityvioji teisinė informacija – teisės normos;
2) gnoseologinė teisinės 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 ir pagrindines jų savybes:

1) informacija apie galiojančią teisę – tai žinios apie pačias teisės normas; norint pabrėžti šią informaciją, galimą ją vadinti teisės informacija;
2) informacija apie teisės vykdymą – tai įvairios kriminologinės ir kitokios teismų, arbitražų, notarų kontorų ir kitų teisinių institucijų žinios, duomenys apie teisės normų taikymą;
3) teisinė mokslinė informacija – tai žinios, pateikiamos teisiniuose mokslo žurnaluose, knygose, straipsniuose ir kt.

Kaip jau minėta, ontologiniu požiūriu pati teisė yra informacija, o gnoseologiniu – teisinė informacija yra žinios apie teisę ir su ja susijusius socialinius reiškinius. Teisinė informacija yra viena svarbiausių teisės informatikos ir teisės sistemos kategorijų. Ji gali būti klasifikuojama įvairiais pagrindais, svarbiausi iš jų yra šie:

I. Pagal teisės šakas:
   1) informacija apie baudžiamąją teisę;

2) informacija apie civilinę teisę;
3) informacija apie proceso teisę ir t. t.

II. Pagal šaltinius:
1) informacija apie įstatymus;
2) informacija apie įstatymo aiškinamuosius (įstatymo įgyvendinamuosius) teisės aktus;
3) informacija apie teisės taikymo aktus (teismų ir administracinius sprendimus);
4) informacija apie teisės jurisprundenciją (mokslo darbus) ir pan.

III. Pagal informacijos laikmenas:
1) neautomatinės teisinės informacijos rinkmenos;
2) automatinės teisinės informacijos rinkmenos.

IV. Pagal priklausomybę:
1) visuotinės teisinės informacijos paieškos sistemos;
2) žinybinės teisinės informacijos paieškos sistemos (pvz., Lietuvos teismų informacinė sistema *LITEKO)*;
3) komercinės teises aktų paieškos sistemos (pvz., *LITLEX, LexisNexis, Eur-Lex, CEDEX* ir kt.) ir t. t.

Šiuolaikinių teisės sistemų požymis yra informacinės teisės krizės gilėjimas, t. y. nuolat didėjanti formaliosios teisės apimtis ir jos sudėtingumas, be paliovos spartėjantys teisiniai informaciniai procesai ir teisinės informacijos mainai. Pabrėžtina, kad nuolat plečiama ir tobulinama tarptautinė ir regioninė teisėkūra dar labiau gilina informacinę teisės krizę. Deja, išsamesnis teisinis reguliavimas ir teisinės informacijos gausa ne tik neišsprendžia visų visuomenės socialinių problemų, bet neretai dar sukuria naujų (pvz., problemos dėl teisėkūros spragų ir klaidų) arba pasunkina esamos teisės taikymą ir suvokimą (pvz., prieštaringi teisės aktai arba nekompetentingas teisės aiškinimas). Daug kur vyrauja požiūris, kad kai kurių socialinių problemų kilo dėl nepakankamo teisinio reglamentavimo, todėl buvo stengiamasi dar išsamiau reguliuoti atitinkamus visuomeninius santykius, tačiau neskirta reikiamo dėmesio reglamentavimo kokybei užtikrinti. Kaip rodo sėkmingos užsienio valstybių praktikos pavyzdžiai, kokybiškas, nors kartais ir labai minimalus (principinis), reglamentavimas (pvz., paliekantis galimybę veikti savireguliacijos mechanizmams) yra socialiai veiksmingiausias.

Pagrindinės teisinės informacijos savybės yra susijusios su pačios informacijos savybėmis:

1) informacijos fiksuojamumu;
2) informacijos perduodamumu;
3) informacijos nekonkurencingumu, kuriam būdinga tai, kad informacija, perduota į kitą sistemą, gali pasilikti ir pirmojoje.

Pirma bendroji informacijos savybė reiškia, kad šiuolaikinė teisinė informacija apskritai gali egzistuoti tik išreikšta tam tikra objektyvia forma – teisės šaltiniuose. Antra bendroji informacijos savybė – teisinė informacija gali išlikti tik nuolat perduodama, o jai įsisavinti reikia energijos, lėšų ir laiko. Trečioji, svarbiausia, informacijos savybė yra ypač aktuali sprendžiant teisinės informacijos laikymo, apsaugos ir platinimo klausimus.

5. Pagrindinės teisinės informacinių technologijų kategorijos

Kompiuteris

Enciklopedinis kompiuterijos žodynas kompiuterį apibrėžia kaip duomenų apdorojimo įrenginį, kuris priima duomenis, juos apdoroja pagal programą ir pateikia rezultatus. Tai bendras visų kompiuterių požymis, pradedant dideliais (pagal užimamą vietą, o ne pagal galimybes) pirmaisiais kompiuteriais, tada dar vadintais elektroninėmis skaičiavimo mašinomis, ir baigiant šiuolaikiniais asmeniniais kompiuteriais ir superkompiuteriais. Kompiuterių sistema – tai iš vieno ar daugiau kompiuterių, išorinių įrenginių ir programinės įrangos sudaryta visuma, atliekanti duomenų apdorojimo funkciją. Ji dažniausiai susideda iš:

- kompiuterinės įrangos (angl. *hardware)* – tai kompiuterių technikos fizinių priemonių visuma, kuri gali būti sudaryta iš:
  - fizinių komponentų, kurie gali būti atskirti nuo pagrindinio kompiuterio arba integruoti į mažesnį įrenginį (pvz., nešiojamąjį kompiuterį): klaviatūra, pelė, vaizduoklis, vidinis kietasis diskas, vidinis optinių duomenų laikmenų skaitytuvas (pvz., *CD, DVD, Blu-ray)*, kiti išorinio duomenų saugojimo įrenginiai (pvz., išorinis kietasis diskas, USB atmintinė) ir periferiniai įrenginiai (tokie kaip spausdintuvas ir skaitytuvas);
  - procesoriaus – pagrindinės dalies, valdančios visą kompiuterį. Procesorius skaito komandas iš operatyviosios atminties, jas iššifruoja, daugelį operacijų vykdo pats, o kitoms vykdyti siunčia atitinkamus signalus į kitus kompiuterio įtaisus;
  - vidinės atminties (pvz., *RAM)*.
- programinės įrangos (angl. *software)* – tai visuma programų, naudojamų kompiuteriui valdyti ir jame esantiems duomenims apdoroti.

Šnekamojoje kalboje programinė įranga kartais sinonimiškai vadinama programomis. Ji skirstoma į dvi dideles grupes: sisteminę ir taikomąją programinę įrangą:

- sisteminė programinė įranga – tai programų, valdančių kompiuterio arba kompiuterinės sistemos veikimą, visuma. Paprastai šiuo terminu apibūdinama operacinė sistema drauge su dar kai kuriomis kompiuterio veiksmus valdančiomis (dažniausiai – paslaugų) programomis. Kadangi įvairūs programinės įrangos gamintojai nevienodai nubrėžia ribą tarp sisteminės ir taikomosios programinės įrangos, pastaruoju metu „sisteminės programinės įrangos“ terminas vartojamas kur kas rečiau – apsiribojama „operacinės sistemos“ sąvoka;
- taikomoji programinė įranga – visuma programų, padedančių kompiuterio vartotojams atlikti reikiamus veiksmus: rašyti raštus, piešti piešinius, kurti muziką, sudaryti įvairių duomenų lenteles, braižyti grafikus ir pan. Prie taikomosios programinės įrangos priskiriamos ir darbo internete (pvz., *Internet Explorer, Google Chrome, Mozilla Firefox)*, elektroninio pašto (pvz., *Microsoft Outlook)* ir kitos komunikacinės programos, taip pat kompiuterinės enciklopedijos ir mokomosios programos. Šiuo metu taikomosiomis laikomos ir programavimo kalbų sistemos (anksčiau dar buvo mėginama išskirti jas į atskirą programinės įrangos grupę).

- duomenų ir (ar) informacijos;
- procedūrų;
- žmogaus, dirbančio su kompiuterine sistema.

Šiuolaikinių kompiuterių tobulėjimo sparta pranoksta bet kokius lūkesčius. Tai didina informacijos apdorojimo galimybes ir greitį, kartu skatindama nuolat tobulėti ir pačius kompiuterių vartotojus. Spėjama, kad iki 2020 m. vidutinis stalinis kompiuteris savo informacijos apdorojimo galia prilygs žmogaus smegenims, kurios, pasak neurologų, sugeba atlikti 10^{16} skaičiavimo veiksmų per sekundę *(Susskind*, 2013).

Kompiuterių tinklai

Dauguma šiuolaikinių kompiuterių sujungti informaciniais tinklais. Jeigu reikiamos informacijos darbo vietoje nėra, jos galima gauti naudojantis informaciniais kompiuteriniais tinklais. Tinklas gali turėti nuolatinę jungtį (pvz., kabeliu) arba laikinąją (pvz., komutuojamąja telefono linija, belaidžiu ryšiu). Kompiuterių tinklus galima klasifikuoti pagal įvairius požymius.

Vienas labiausiai paplitusių skirstymų – remiantis geografiniu išsidėstymu. Pagal šį požymį skiriami du tinklų tipai:

1) regioniniai tinklai, kartais dar vadinami globaliniais – *(WAN-Wide Area Networks)*, jie apima didelę geografinę teritoriją, tokią kaip valstija, šalis ar net visas pasaulis. Regioniniai tinklai naudojami vietiniams tinklams sujungti;
2) vietiniai (lokaliniai) tinklai – įstaigų, ministerijų, žinybų, įmonių, universitetų ir kitų organizacijų vidiniai tinklai *(LAN-Local Area Networks)*.

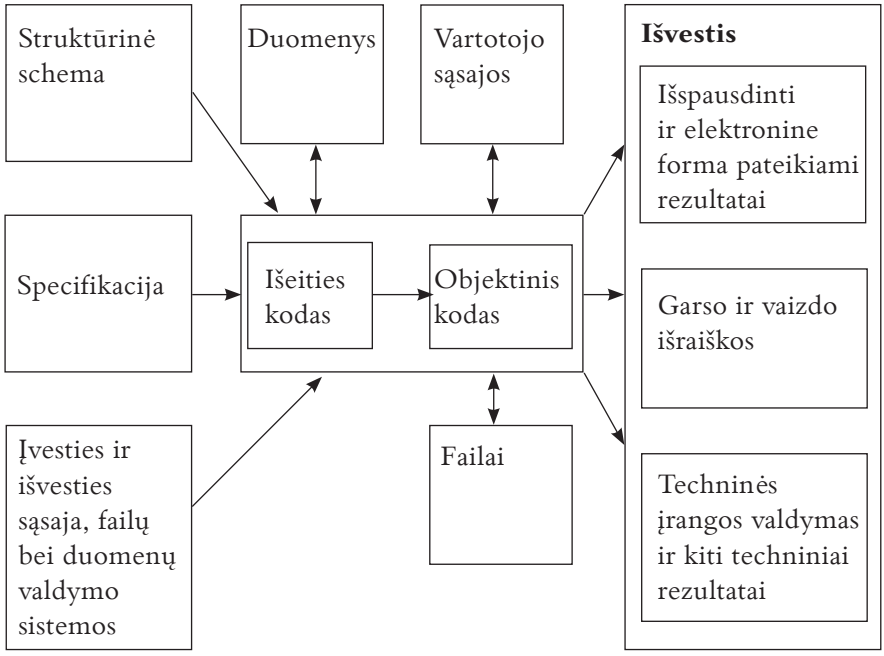
Įmonė arba organizacija savo pagrindinėje būstinėje gali turėti centrinį serverį (tarnybinę stotį), užtikrinantį ryšį su centrine organizacijos duomenų baze. Šis centrinis serveris regioniniu tinklu gali būti sujungtas su įmonės filialų ir įstaigų vietiniais tinklais, kurie turi savo vietinius serverius ir duomenų bazes. Pagal nustatytą procedūrą vietiniai serveriai perduoda duomenis centriniam serveriui, kokią informaciją būtina atnaujinti. Centrinis serveris savo ruožtu analogiškai sąveikauja su vietiniais serveriais ir nurodo, kokią vietinių serverių ir ten esančių duomenų bazių informaciją reikia atnaujinti ir kaip tai padaryti. Taip sudaromos prielaidos įmonei turėti efektyviai veikiantį kompiuterių tinklą. Tam, kad kompiuterių tinklai tinkamai funkcionuotų, būtina patikimai ir greitai elektroniniu būdu perduoti informaciją iš vienos vietos į kitą. Tai gali būti paprastas informacijos perdavimas iš vienos to paties pastato patalpos į kitą, tačiau ji gali būti paskleidžiama ir po visą pasaulį. Ryšiui gali būti naudojami tiek uždarieji, tiek ir atvirieji komunikacijos kanalai. Uždariesiems ryšio kanalams priskirtinos susuktosios laidų poros, bendraašiai ir optiniai kabeliai, o atviriesiems – mikrobangų, palydovinio ryšio, radijo transliacijos ir infraraudonųjų spindulių sistemos. Paprastai vietiniais tinklais duomenys perduodami greičiau negu regioniniais. Duomenims perduoti kompiuterių tinkluose gali būti naudojama ir tokia neįprasta duomenų perdavimo sistema kaip elektros tiekimo linijos. Tai aktualu tiems vartotojams, kurie prie kompiuterių tinklo negali prisijungti nei per įprastinį telefono, nei per specializuotą duomenų perdavimo sistemos kabelių tinklą, nei per radijo ryšį arba kabelinę televiziją.

Kompiuterių programos

Svarbiausias kompiuterių sistemų ir jų tinklų komponentas, įgalinantis juos veikti, yra kompiuterių programos. Techniniu požiūriu jos yra suprantamos kaip programavimo kalbomis užrašyti matematiniai (loginiai) algoritmai. Dažniausiai kompiuterių programoms priskiriamos kompiuterio darbui naudojamos operacinės sistemos, taikomoji programinė įranga

ir tam tikras kiekis įvairių elektroninių duomenų: skaičių, tekstų, piešinių, garsų ir kt. Visa ši informacija kompiuterio viduje yra skaitmenizuota ir išreikšta dvejetaine skaičiavimo sistema (nuliukais ir vienetukais). Būtent programinė įranga suteikia kompiuteriui dirbtinio intelekto elementų ir jis tampa intelektualiu informacijos dorokliu.

Plačiąja prasme kompiuterių programos suprantamos kaip visuma elementų ir efektų, susijusių su kompiuterių programos kūrimu ir veikimu, išskyrus reikalingą techninę įrangą. Šiuolaikinė kompiuterių programos samprata apima ir duomenų struktūras, taip pat šiuolaikinius įvesties ir išvesties elementus – sąsajas, kaip savarankiškas kompiuterių programos sudėtines dalis. Šiandien kompiuterių programa galima laikyti kompiuterių programos elementų visumą ir jų tarpusavio sąveikas, taip pat pirminį ir objektinį programos kodą, jos specifikacijas ir veikimo schemą, elektroniniu būdu išsaugotą informaciją (rinkmenas), duomenis, kompiuterių programa valdomo kompiuterio veikimo rezultatus – išpausdintą medžiagą, garso ir vaizdo išraiškas, grafinę vartotojo sąsają, rinkmenų ir grafinių vaizdų struktūras bei įvesties ir išvesties elementus – sąsajas kaip savarankiškas kompiuterių programos sudėtines dalis (žr. 1 pav.).



1 pav. Kompiuterių programos elementai

Svarbu suvokti dvejopą kompiuterių programų pobūdį. Jas apibūdina tiek jų tekstinė išraiška (pirminis kodas, objektinis kodas), tiek kompiuterių programa valdomo kompiuterio veikimo rezultatai (vartotojo ir kitos sąsajos, rinkmenų ir grafinių vaizdų išdėstymas, vaizdinės ir garsinės programos pateikimas). Tekstinė kompiuterių programos išraiška tiesiogiai lemia kompiuterių programos veikimo rezultatus ir, priešingai, kompiuterių programos tekstinė išraiška ir veikimo rezultatai tuo pat metu yra nepriklausomi, nes analogiškų veikimo rezultatų įmanoma pasiekti pasitelkiant kitokios tekstinės išraiškos kompiuterių programą, o visiškai skirtingų išraiškų kompiuterių programos gali atlikti tas pačias užduotis (pasiekti tokių pat rezultatų). Kūrybinis procesas apima abu kompiuterių programos aspektus.

Atsižvelgiant į kompiuterių programų dvilypumą, jas galima apibūdinti kaip techninius mechanizmus, išreikštus tekstinėmis priemonėmis. Tokiais „tekstiniais mechanizmais“ galima pasiekti konkrečių naudingų rezultatų, sudarytų iš visumos veiksmų, kuriuos gali atlikti kompiuteris, vykdydamas programos instrukcijas. „Tekstiniams mechanizmams“, kaip ir bet kokiems kitiems techniniams mechanizmams, gali būti taikomi inžineriniai sprendimai ir naujovės. Kompiuterių programas, kaip ir techninius mechanizmus, sudaro visuma tarpusavyje suderintų ir sąveikaujančių elementų – algoritmų bei duomenų struktūrų, ir kurio nors vieno iš jų „gedimas“ dažniausiai lemia viso mechanizmo funkcijų sutrikimą. Be to, rezultatai, gauti naudojantis kompiuterių programomis, gali būti pasiekiami ir vien techninėmis priemonėmis.

Kompiuterinės duomenų bazės

Dideliems duomenų ir informacijos kiekiams tvarkyti bei sisteminti naudojami specialūs duomenų formatai ir programų paketai, vadinamosios duomenų bazių valdymo sistemos. Jos leidžia kurti įvairių duomenų rinkinius, peržiūrėti ir (ar) keisti duomenis, rengti ataskaitas. Techniniu požiūriu duomenų bazę sudaro jos turinys (patys duomenys) ir duomenų bazės sąsaja (duomenis valdančios programos). Populiariausios duomenis valdančios programos yra šios: *MySQL*, *Oracle Database*, *Microsoft SQL Server*, *Microsoft Access* ir kt.

Šiuo metu duomenų bazės yra svarbiausia informacijos tvarkymo forma ir priemonė, vienas iš dažniausių modernių informacinių technologijų pritaikymo kasdienei aplinkai pavyzdžių. Šiuolaikinės įmonės, valstybinės institucijos ir kitos organizacijos susiduria su nuolat didėjančiais informacijos srautais ir būtinybe kuo efektyviau juos valdyti, todėl duomenų bazės yra tapusios vienu svarbiausių informacijos valdymo ir kontrolės įrankių, būtinu informacijos valdymo elementu.

Duomenų bazės yra būtinos atliekant daugumą verslo valdymo funkcijų, tokių kaip apskaita ir sąskaityba, atsargų planavimas, ryšių su klientais palaikymas, pardavimo bei personalo vadyba ir t. t. Kai kurios verslo rūšys yra tiesiogiai priklausomos nuo duomenų bazių, pvz., įmonių katalogai, kredito biurai, įdarbinimo ir personalo paieškos agentūros, bankai ir draudimo bendrovės.

Duomenų bazę galima apibrėžti tiesiog kaip informacijos rinkinį ar kompiliaciją, išdėstytą (organizuotą) sisteminiu ar metodologiniu būdu, kai pavieniai duomenys susiejami į kokybiškai naują informacijos visumą. Pabrėžtina, kad duomenų bazę turi sudaryti informacijos daugetas, t. y. turi būti tam tikras minimalus sistemiškai sutvarkytos informacijos kiekis. Duomenų baze laikytinas tiek automatiškai, tiek ir neautomatiškai (net ranka užrašytas) surinktas bei tvarkomas informacijos rinkinys, jeigu jis išreikštas kokia nors forma.

Duomenų bazės santykis su kompiuterių programomis gali būti dvejopas. Jeigu duomenų bazėms tvarkyti naudojama 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). Jeigu kompiuterių programa yra tik duomenų bazės kūrimo ir (ar) tvarkymo (prieigos, keitimo, išsaugojimo) priemonė, tokia programa nelaikoma duomenų bazės dalimi.

Internetas – socialinių ir teisinių santykių erdvė

Interneto samprata ir veikimo principas

Šiuolaikiniams komunikacijos tinklams naudojami telefoninio, radijo, kabelinio, optinio ir palydovinio ryšio kanalai. Ypač didelį vaidmenį plėtojant komunikacijas atliko interneto tinklo paplitimas. Atsiradęs daugiau nei prieš dvidešimt metų, internetas tapo svarbiausiu pasauliniu informacijos tinklu, kuriuo komunikacijai ir informacijos paieškai naudojasi dauguma įvairių pasaulio šalių gyventojų. Lietuvos teisės aktuose internetas apibrėžiamas kaip viešojo naudojimo kompiuterių tinklas, t. y. bendrosios prieigos informacinis tinklas, tarptinklinės sąveikos protokolais vienijantis techninę įrangą (kompiuterius) ir tinklus, priklausančius informacijos išteklių ir telekomunikacijų paslaugų teikėjams, kitiems juridiniams ir fiziniams asmenims. Tarpusavyje sujungti vidaus kompiuterių tinklai irgi laikomi viešojo naudojimo kompiuterių tinklais. Internetas dar gali būti apibrėžiamas kaip keitimosi informacija, bendravimo aplinka, kurią galima skirstyti į techninį ir paslaugų lygius. Pirmasis lygis apibūdina, kaip tarpusavyje sąveikauja kompiuteriai, antrasis – kokių galimybių bendrauti internetu turi asmenys.

Interneto kompiuterių tinklą sudaro labai išplėtota kelių lygių ryšio kanalų visuma. Bendroji interneto elektroninė komunikavimo erdvė šiuolaikiniais ryšio kanalais aprėpia visą pasaulį ir neturi geografinių sienų. Kartu ji lengvai prieinama per bet kurį prie interneto prijungtą kompiuterį. Vadinasi, kiekvienas asmuo, dirbantis su interneto ryšį turinčiu kompiuteriu, patenka į bendrąją elektroninę komunikavimo erdvę ir gali keistis informacija su kuo tik nori beveik nekontroliuojamas. Interneto tinklo informacija kaupiama milijonuose tinklo mazgų – tarnybinėse stotyse (serveriuose). Šios tarnybinės stotys prijungtos prie greitaeigių ryšių kanalų (palydovinių, optinių, kabelinių ir kt.). Prie kiekvienos iš jų paprastesnėmis ryšio linijomis (telefoninio, kabelinio ir pan.) prijungiama nuo keliasdešimt iki kelių tūkstančių interneto vartotojų kompiuterių. Visose minėtosiose stotyse kaupiama informacija nuo kitų pašalinių vartotojų nepriklauso. Šis procesas nėra kaip nors reguliuojamas ar koordinuojamas ir užtikrina keitimosi informacija laisvę. Todėl internete galima rasti daug pasikartojančios, neteisingos ar menkavertės (kartais net pavojingos visuomenei) informacijos. Pagrindinius interneto informacijos srautus perneša vadinamasis interneto kamienas (angl. *backbone*), sudarytas iš didžiausių potinklių, kurie priklauso pagrindinėms interneto paslaugų teikėjoms – bendrovėms: A*T&T, GTE, MCI, Sprint, UUNet, AOL*. Šie tarpusavyje sujungti palydoviniai tinklai sudaro itin greitas palydovinio ryšio linijas, kurios aprėpia Šiaurės Ameriką, Europą, Japoniją, žemyninę Azijos dalį ir kitas pasaulio šalis. Tačiau ne visose pasaulio dalyse šis tinklas yra vienodai gerai išplėtotas. Pavyzdžiui, JAV yra tiek daug tinklo susikirtimo taškų, kad nutrūkus ryšiui ar sulėtėjus duomenų perdavimui vienoje linijoje, informacijos srautas iškart persiunčiamas kita. Tačiau esama vietų, kur nutrūkus vienai ryšio linijai gali nebūti atsarginių kelių, ir interneto ryšys gali labai sulėtėti arba išvis nutrūkti. Palydovinis ryšys nuo XX a. septintojo dešimtmečio naudojamas tarptautiniam telefono ryšiui ir tarptautinėms televizijos transliacijoms. Norėdami palaikyti Ryšį *VSAT* tinklais, palydovais gali naudotis įvairūs vartotojai. *VSAT* (labai mažas apertūrinis terminalas) yra palydovinio ryšio sistema, transiveris priima signalą arba siunčia jį erdvėje esančiam palydovo atsakikliui. Palydovas siunčia signalus ir juos priima iš Žemės stoties kompiuterio, kuris veikia kaip sistemos šakotuvas (angl. *hub)*. Tam, kad vienas galutinis vartotojas susisiektų su kitu, kiekvienas siunčiamas signalas pirmiausia turi eiti į sistemos šakotuvo stotį, kuri per palydovą jį retransliuoja į kito galutinio vartotojo *VSAT*.

Dar vienas palydovo tipas, kuris turėtų išplėsti palydovinio ryšio tinklą, yra žemos orbitos palydovas *(LOS)*. Tradicinių geosinchroninių palydovų orbita yra 22 300 km nutolusi nuo Žemės paviršiaus. Šis aukštis

leidžia jiems nukreipti signalus į stabilią plačią sritį, tačiau sukelia ir perduodamų duomenų vėlavimo problemų. Žemos orbitos palydovai nuo Žemės paviršiaus nutolę maždaug 1 800 km atstumu; tai duoda mažesnę aprėptį, tačiau sumažina vėlavimą ir suteikia galimybę lengvai prie interneto prisijungti žmonėms, gyvenantiems atokiuose regionuose, kur nėra telefono ar kabelinio tinklo. Vartotojai prie interneto jungiasi įvairiais ryšio (laidinio, kabelinio, belaidžio, mobiliojo ir kt.) kanalais per interneto paslaugų teikėjus (angl. *Internet Service Providers)*. Smulkesnieji interneto paslaugų teikėjai savo klientus prijungia prie kito interneto teikėjo tinklo, išnuomodami prieigą prie pagrindinių interneto palydovinių potinklių. Keitimosi informacija internetu pigumą lemia faktas, kad internetas – ne pelno siekianti organizacija. Informacija perduodama paketiniu režimu, o tai kainuoja gerokai pigiau negu telefonu, paštu ar faksu.

Informacijos mainams internete bendrai naudojamas paprastas 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 kompiuterių tinklu siunčiama informacija iš pradžių kam nors adresuojama, paskui išsiunčiama tiksliai tuo adresu. *TCP/IP* susideda iš dviejų protokolų – *TCP* (angl. *Transmission Control Protocol)* ir *IP* (angl. *Internet Protocol)* – samplaikos. Visi duomenys perduodami paketais, dėl to labai sumažėja galimybė prarasti informaciją. Visų pirma *TCP* protokolas visą siunčiamą informaciją suskaido porcijomis (paketais), sudeda juos į elektroninius vokus ir ant jų užrašo gavėjo bei siuntėjo adresus. Tada IP protokolas suranda optimalų kelią paketams siųsti internetu. Numatoma, per kokius interneto mazginius punktus (maršrutizatorius) bus siunčiamas duomenų paketas. Kiekvienas maršrutizatorius perskaito gavėjo adresą ir siunčia paketą kitam. Taigi kiekvienas interneto elektroninis laiškas gali būti padalytas į kelis duomenų paketus, kurie gali judėti pas adresatą atskirai vienas nuo kito tiek pagal maršrutą, tiek ir laiko prasme, nes tai priklauso nuo reikiamos tinklo dalies apkrovos. Vėliau *TCP* protokolas surenka visus atskirus paketus ir vėl atkuria pirminę informaciją.

Interneto tarnybinės stotys duomenimis keičiasi greitaeigiais ryšio kanalais paketiniu režimu, todėl komunikavimo greitis internete yra labai didelis ir iš esmės priklauso nuo to, kaip dažnai suformuojami ir siunčiami duomenų paketai. Šis laikas apytikriai svyruoja nuo kelių minučių iki kelių valandų, išskyrus atvejus, kai atsiranda tarnybinės stoties ar ryšio kanalo gedimų. Todėl pasitaiko atvejų, kai į kitą pasaulio kraštą (pvz., Australiją) laiškas interneto elektroniniu paštu patenka per kelias minutes, o į miestą, esantį už keliasdešimties kilometrų, keliauja kelias valandas. Labiausiai

komunikavimo internetu greitį mažina siauri ryšio kanalai tarp tarnybinių stočių ir vartotojų. Tai ypač būdinga ekonomiškai atsilikusioms šalims, kur dar naudojamas pasenęs analoginio telefono ryšys.

Unikali interneto adresavimo sistema yra bendra visiems vartotojams, ir kiekvienam prie interneto prijungtam kompiuteriui suteikia išskirtinį iki dvylikos skaitmenų ilgumo *IP* adresą (pvz., 301.15.52.2). Vienas svarbiausių reikalavimų – interneto adresas turi būti unikalus ir niekada nesikartoti. Todėl tinklo tarnybinėms stotims (serveriams) išskirtinius *IP* adresus suteikia ir juos užregistruoja *ICANN* organizacija ar jos įgaliotieji atstovai. *IP* adresas yra išreiškiamas skaitmenimis, kuriuos sunku ir nepatogu įsiminti, todėl *IP* adresų sistema iš esmės pakeičiama simboline ir vartotojams patogia interneto domenų vardų sistema *DNS* (angl. *Domain Name System)*, kur pasitelkus serverius beveik kiekvienas *IP* adresas internete yra susiejamas su domeno vardu. Įvedus domeno vardą į kompiuterį, *DNS* serveriai jį automatiškai konvertuoja į skaičiais išreikštą *IP* adresą. Techniniu požiūriu domeno vardas visų pirma suprantamas kaip interneto adresas ir apibrėžiamas kaip interneto adresų srities simbolinis pavadinimas. Patys interneto adresai yra skaitmeniniai, tačiau žmonių patogumui jie susiejami su domenų vardais (pvz.: *www.google.com)*. Domenų (apibrėžtų interneto sričių pavadinimų) sukūrimas – dar viena pažangi interneto adresų indeksavimo sistema, apimanti specialius domenų vardo serverius, esančius visame pasaulyje. Ji leidžia interneto mazgus (tarnybines stotis – serverius), jau turinčius *IP* adresą, pavadinti žmogui suprantamais pavadinimais. „Šaknies“ domenas – tai atskiros įmonės, institucijos ar organizacijos tarnybinei stočiai (serveriui) priskirtas identifikavimo vienetas, kuris jungia tam tikrą kiekį galinių vartotojų kompiuterių. Pavyzdžiui, domeno vardas *www.name.com* pagal *IP* adresą nurodo *WWW* serverį, skirtą *name.com*. Kartais po domeno vardo gali eiti dvitaškis ir skaičius, pavyzdžiui, *www.yahoo.com:8080*. Tai rodo, kad serveris pasiekiamas per prievadą (angl. *port)* 8080, o ne tinklo serveriams numatytą 80 prievadą. Adresui identifikuoti svarbiausi dešinieji taškais atskirti jo elementai. Kraštutinis dešinysis dviejų ar trijų raidžių adreso elementas parodo interneto tarnybinės stoties šalį arba paskirtį. Lietuvos tarnybinėms interneto stotims skirtos raidės *.lt*, Rusijos – *.ru*, JAV – *.us* ir t. t. Registruojamai tarnybinei stočiai pagal paskirtį suteikiamos adreso galūnės: *.edu* – švietimo ir mokymo įstaigos, *.gov* – JAV vyriausybinės organizacijos, *.net* – tinklai, *.com* – komercinė organizacija ir t. t. Vienas ar keli gretimi adreso elementai pateikia unikalų tarnybinės stoties pavadinimą. Konkretūs kitų interneto galinių vartotojų adresai suteikiami per tarnybines stotis. Kai kurios tarnybinės interneto stotys teikia adresus visiems norintiesiems, nereikalaudamos asmens

identifikavimo. Todėl iš interneto adreso negalima tiksliai nustatyti, kokiai šaliai ar kokiam asmeniui jis priklauso. Kiekvieno dokumento vieta interneto tinkle nurodoma jo bendruoju informacijos šaltinio lokatoriumi *URL* (angl. *Unified Resource Locator)*, nes vien serverio pavadinimo neužtenka, dar reikia žinoti, kokioje to serverio vietoje yra reikiama informacija. Kiekvienas *URL* turi tris pagrindines dalis: protokolą, serverio įrenginį ir laikmeną, dėl kurios pateikiama užklausa. Protokolas apima tai, kas yra iki dvitaškio ir pirmųjų dviejų brūkšnių. Tinklalapio naršyklių atveju populiariausi protokolai yra šie: *http://, ftp://, gopher:// ir news://*. Po protokolo ir dvigubo pasvirojo brūkšnio prieš kitą pasvirąjį (vieną) brūkšnį nurodomas to serverio įrenginio, kuriame yra dokumentas, vardas. Tai gali būti arba interneto srities (domeno) vardas, arba *IP* adresas. Po protokolo ir serverio įrenginio *URL* eina užklaustos laikmenos pavadinimas, dėl kurios pateikta užklausa. Pavyzdžiui, *www.name.com/customer/bill* kreipiasi į failą, vadinamą „bill“, kuris yra aplanke „customer“.

Interneto paslaugos

Tinklo vartotojui teikiamas interneto paslaugas galima suskirstyti į dvi pagrindines grupes – ryšio ir informacines.

Interneto ryšio paslaugos leidžia naudotis įvairiomis interneto ryšio priemonėmis: elektroniniu paštu, failų siuntimu *(FTP)*, prisijungimu prie nuotolinio kompiuterio *(Telnet)*, pokalbiu naudojantis internetu *(Talk)*, interneto konferencija *(IRC)*, telefonija, vaizdo konferencija, vietinių tinklų *(LAN)* sujungimu ir kt.

Pati populiariausia ir moderniausia interneto informacinė paslauga yra saitynas (angl. *World-Wide Web)*. Tai duomenų saugykla, kurią sudaro daugybė po visą pasaulį išsidėsčiusių tarpusavyje sujungtų kompiuterių. Saitynas apima nemažą dalį viso interneto duomenų srauto, todėl daugelis žmonių šį terminą vartoja kaip interneto sinonimą. Tačiau tai iš esmės neteisinga, nes internetas yra tinklas, leidžiantis keistis informacija tarp kompiuterių, o saitynas – didelė atskirų informacijos failų sankaupa. Kitaip tariant, interneto tinklas egzistuoja atskirai ir nepriklauso nuo saityno, tačiau be interneto tinklo nebūtų galimybės naudotis saityne sukaupta informacija. Šią duomenų saugyklą sukūrė *CERN* (Europos dalelių fizikos laboratorija) tyrinėtojai, kurie susidūrė su problema, kaip susieti ir sekti dokumentus, esančius skirtingose pasaulio vietose. 1989 m. buvo sukurtas hiperteksto perdavimo protokolas *HTTP* (angl. *Hypertext Transfer Protocol)*. Šis protokolas leidžia dinamiškai susieti failus, laikomus skirtinguose kompiuteriuose. Sąsajos tarp dviejų dokumentų gali būti sudaromos taip, kad spragtelėjus vieno dokumento kurioje nors teksto dalyje esančią

nuorodą (angl. *hyperlink)* vartotojas būtų automatiškai nukreipiamas į informaciją, esančią kitame dokumente. Šis dokumentas nebūtinai turi būti laikomas tame pačiame kompiuteryje, jis gali būti bet kurioje tinklo vietoje. Saityną sudaro atskiri interneto mazguose (tarnybinėse stotyse – serveriuose, kartais vadinamuose *Web* serveriais) esantys puslapiai. Jie yra parašyti specialiąja kalba – *HTML* (angl. *Hypertext Markup Language)*. Informacijos paieškai internete sukurta speciali lengvai suprantama ir labai efektyvi programinė įranga – interneto naršyklės, šiuo metu iš jų tarp vartotojų populiariausios yra šios: *Internet Explorer, Google Chrome, Safari* ir *Mozilla Firefox*. Informaciją iš interneto galima lengvai nukopijuoti į kompiuterio atmintį, ją išspausdinti ar išsaugoti. Naršyklės pritaikytos suprasti *HTML* kalbą ir vienodai teisingai atvaizduoti interneto puslapius.

Norint be vargo naudotis milžinišku milijonuose interneto kompiuterių sukauptos informacijos kiekiu, būtinos centralizuotos efektyvios ir greitos informacijos paieškos galimybės. Todėl buvo sukurtos specialios informacijos paieškos sistemos, turinčios didžiulius kompiuterinius išteklius. Šiuo metu internete plačiausiai naudojamos šios informacijos paieškos sistemos: *Google Search, Yahoo, Bing, Baidu* ir kt. Pagal vieną ar kelis užklausos raktinius žodžius per trumpą laiką peržvelgiami milijonai interneto puslapių ir pateikiamas tinklalapių, kuriuose rasti ieškomi žodžiai, sąrašas.

/ I / *skyrius*

Interneto teisė

1 skirsnis. Interneto teisės samprata ir pagrindiniai klausimai

Interneto teise siaurąja prasme vadinami interneto jurisdikcijos klausimai, o plačiąja – šis terminas naudojamas bendrai apibrėžiant teisės institutus, susijusius su svarbiausiais teisės taikymo internete klausimais, kurie nėra priskiriami kitiems teisės institutams ar šakoms, iš jų – interneto jurisdikcijai, e. erdvės tarpininkų veiklai (atsakomybei), interneto domeno vardams, turiniui ir informacinės visuomenės paslaugoms (teikiamoms internete) reglamentuoti, interneto administravimo teisiniams klausimams.

Domeno vardai – interneto adresų srities simboliniai pavadinimai, identifikuojantys jo turinio teikėją, prekes, paslaugas ar informaciją.

Interneto turinį sudaro visa jame pateikiama informacija, prekės ir paslaugos, įskaitant žalingą (ribojamą) turinį (pvz., smurtinio, erotinio ar pornografinio pobūdžio informaciją, prekes ir paslaugas) bei neteisėtą (draudžiamą, nepageidaujamą) turinį (pvz., vaikų pornografiją, neteisėtas intelektinės nuosavybės kopijas ir pan.).

Interneto jurisdikcijos klausimus sudaro du pagrindiniai institutai – internete taikomos teisės ir valstybinių institucijų galios reguliuoti (spręsti ginčus, priimti privalomus sprendimus, taikyti sankcijas) visuomeninius santykius internete.

Informacinės visuomenės paslaugų (teikiamų internete) teikėjais laikytini visi informacinės visuomenės paslaugų teikėjai, t. y. paprastai už atlyginimą elektroninėmis priemonėmis ir per atstumą individualiu informacinės visuomenės paslaugos gavėjo prašymu paslaugas teikiantys asmenys.

Interneto tarpininkais galima laikyti subjektus, užtikrinančius interneto infrastruktūros funkcionavimą, teikiančius interneto prieigos, prieglobos, turinio publikavimo ir perdavimo paslaugas. Tokie yra ir informacinės visuomenės paslaugų (teikiamų internete) teikėjai. Iš tiesų interneto tarpininkai yra interneto prieigos paslaugų teikėjai, įvairiausi interneto portalai, kuriuose vartotojai gali pateikti savo informaciją (pvz., failus, komentarus ir pan.). Universitetas irgi yra interneto tarpininkas, nes teikia interneto prieigos, elektroninio pašto, tinklalapių įdėjimo paslaugas darbuotojams ir studentams. Asmuo, kuris įdeda savo arba paties atrinktą žinomą kitų asmenų informaciją, nelaikomas interneto tarpininku.

Interneto tarpininkas nėra įpareigotas kontroliuoti ir tikrinti informacijos, kurią interneto tarpininko paslaugų gavėjai (vartotojai), naudodamiesi interneto tarpininko infrastruktūra, siunčia, gauna, skelbia, saugo ir pan.

Interneto administravimas yra bendrųjų interneto standartų (tokių kaip interneto adresų ir domenų sistema, duomenų perdavimo protokolai ir kt.) bei kitų bendrųjų klausimų, susijusių su globaliu interneto funkcionavimu, sprendimas.

2 skirsnis. Interneto jurisdikcija

Jurisdikcija nusprendžia, kurios valstybės teisė bus taikoma ir kurios valstybės teismai nagrinės ginčą. Nors e. erdvės prigimtis ir yra globali, valstybių teisės taikymas internete yra viena svarbiausių ir iki šiol vienareikšmiškai dar neišspręstų teisės problemų.

Pagrindinis bendrasis jurisdikcijos nustatymo principas – geografinio teritorialumo – visiškai netinkamas internete, nes e. erdvė yra *per se* globali ir neturinti jokių apribojimų. Elektroninio turinio ir paslaugų sklaidą internete riboja ne valstybių sienos ar geografinė jų teikėjų ar vartotojų buvimo vieta, o tik pastarųjų noras gauti tam tikrą turinį ar paslaugas.

Interneto kasdienybė yra tokia:

1) platinama informacija, prekės ir paslaugos, kurios tam tikroje valstybėje yra visiškai draudžiamos ar ribojamos;
2) informaciją, prekes ir paslaugas teikiantys, tarpininkaujantys ir jas įsigyjantys asmenys yra skirtingose valstybėse;
3) deliktą ar kitokį teisės pažeidimą internete darantis ir žalą patiriantis asmenys yra skirtingose valstybėse.

Nevienodas asmenų, kurie yra teisinių santykių internete šalys, teritorialumas iš esmės yra taisyklė, o ne išimtis. Primintina, kad veikimas e. erdvėje nepanaikina asmenims pareigų pagal tos valstybės, kurioje jie veikia, įstatymus, tačiau internete tai reiškia, kad kiekviena teisinių santykių šalis vadovaujasi savo valstybės teise, kuri daugeliu klausimų gali būti radikaliai priešinga.

Esant tokiai situacijai, būtina aiškiai suvokti nacionalinės teisės taikymo internete ribas ir specifinės interneto jurisdikcijos perspektyvas.

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

Tarptautinė teisė pripažįsta du svarbiausius jurisdikcijos principus:

- pilietybės;
- teritorialumo.

Esami tarptautiniai jurisdikcijos sprendimai – tokie kaip universaliosios jurisdikcijos principas, pagal kurį ginčas gali būti nagrinėjamas bet kurioje pasaulio valstybėje, internetui yra netinkami, nes, skirtingai nei

kosminė erdvė ar Antarktida, internetas yra įprasta kasdienybės dalis. Kai kuriose valstybėse (pvz., Suomijoje) nevaržoma teisė naudotis internetu jau oficialiai pripažįstama savarankiška žmogaus teise, kuri yra kildinama iš tradicinių komunikacijos ir žiniasklaidos laisvių. Be to, e. erdvė neturi „centrinės valdžios“, jos funkcionavimas visiškai nesusijęs su valstybių suvereniteto įgyvendinimu, nėra visuotinių tarptautinių susitarimų dėl jos statuso (tokių kaip dėl kitų bendrųjų erdvių – kosmoso ar Antarktidos teritorijos statuso). Netgi visiškai nedemokratinėse valstybėse, kur visais įmanomais būdais mėginama kontroliuoti internetą, ši kontrolė nėra absoliuti ir apeinama sąlygiškai nedidelėmis pastangomis. Primintina, kad net ir tradicinių geografinių erdvių atveju tarptautinėje viešojoje, baudžiamojoje ir privatinėje teisėje jurisdikcijos principai yra skirtingi. Nors esama šimtametės praktikos, net ir geografinės jurisdikcijos klausimai dažnai gali būti itin sudėtingi.

Tarptautinėje praktikoje esama pavyzdžių, kai valstybė nacionalinę jurisdikciją įgyvendina asmenų, nesusijusių teritorialumo saitais, atžvilgiu. JAV ir kitos valstybės taiko savo jurisdikcijos taisykles asmenims, kurie vykdo itin pavojingus nusikaltimus ar antivalstybinę veiklą (pvz., terorizmą), neatsižvelgdama į tai, kur šie asmenys yra. Vis dėlto tokia praktika yra tik išimtinė, o ne visuotinė.

Tradicinių teritorialumo ar pilietybės jurisdikcijos principų besąlygiškas taikymas internete iš tiesų reikštų, kad kiekviena valstybė savo jurisdikcijos taisyklėmis galėtų remtis pasauliniu lygiu, taip būtų sukuriama visiško teisinio neapibrėžtumo ir nesaugumo situacija.

Tradicinės jurisdikcijos teorijos požiūriu, bet kurį teisinį santykį galima lokalizuoti, t. y. vadovaujantis iš anksto apibrėžtais kriterijais susieti jį su konkrečios valstybės teisės teritorija ir sistema. Toks susiejimas atliekamas per kilusio ginčo objektą, subjektą, veiką ir papildomus kriterijus. Internete toks lokalizavimas irgi yra įmanomas, nes visi subjektai veikia naudodamiesi tam tikru adresu *(IP* adresu) ir (ar) domeno vardu, kurie iš esmės gali būti susieti su tam tikra teritorija. Be to, nekyla jokių abejonių, kad valstybė gali taikyti jurisdikciją asmenims, esantiems ar veikiantiems toje valstybėje, net jeigu visa tų asmenų veikla yra vykdoma e. erdvėje.

Vis dėlto lokalizavimo nauda e. erdvėje yra ribota, nes jis nepadeda išspręsti jurisdikcijos kolizijų, kurių internete kyla kasdien, be to, platus lokalizavimas sudarytų prielaidas taikyti valstybinę teisę pasauliniu mastu (žr. žemiau komentarą dėl neigiamų padarinių atsiradimo vietos principo).

Vadovaujantis funkcinio lygiavertiškumo principais, analogiška jurisdikcija turėtų būti taikoma ir elektroniniams, ir įprastiniams teisiniams santykiams, jeigu jų esmė yra tokia pati. Funkcinio lygiavertiškumo principas

iš tiesų priimtas reglamentuojant didelę dalį tradicinių teisinių santykių, kai šie vyksta e. erdvėje. Pvz., baudžiamojoje teisėje iš esmės priimtas principas, kad jeigu asmuo padarė teisės pažeidimą e. erdvėje, jis gali būti paduodamas į tos valstybės, kurioje būdamas jis įvykdė tą nusikaltimą, teismą ir teisiamas pagal jos įstatymus. Kitaip tariant tai – nusikaltimo, akto atlikimo vietos principas (lot. *lex loci actus)*. Deja, visiškas jo taikymas e. erdvėje nėra paprastas, įvertinant nusikaltimo vietos fakto nustatymo problematiką ir galimybes dirbtinai išvengti atsakomybės, specialiai atliekant veiksmus toje vietoje, kur jurisdikcija yra paranki (tai įprasta praktika vien dėl noro paslėpti nusikaltimo pėdsakus).

Kitas nacionalinėms teisės sistemoms įprastas bendrasis principas – atsakovo ar vienos iš sutarties šalių gyvenamoji vieta (buveinė). Tradiciškai taikant šį principą civiliniam procesui ginčas bus sprendžiamas toje valstybėje ar net vietovėje, kur gyvena atsakovas. Deja, e. erdvėje, kur tarp ieškovo ir atsakovo galimi milžiniški atstumai, kartais šį principą taikyti būtų tiesiog neracionalu ar išvis neįmanoma.

Matoma tendencija, kad tarptautinė teisė nuo griežto, formalaus reglamentavimo pereina prie lanksčių kolizinių normų, vis labiau toleruojamas glaudžiausio ryšio *(lex conveniens*, angl. *proper law)*, šalių valios autonomijos *(lex voluntatis)* taisyklių taikymas. Pagal pirmąjį, glaudžiausio ryšio, principą kilęs ginčas turėtų būti sprendžiamas toje valstybėje, kuri labiausiai susijusi su teisiniu santykiu. Pagal antrąjį principą, ginčas bus sprendžiamas šalių susitarimu pasirinktoje valstybėje. Šie principai yra bene vieninteliai, kurie yra lengvai pritaikomi e. erdvei, tačiau jie nėra tinkami sprendžiant viešosios teisės jurisdikcijos klausimus. Atsižvelgiant į teisinio santykio rūšį ir konkrečias aplinkybes, e. erdvėje galėtų būti taikomos ir kitos tradicinės jurisdikcijos taisyklės, tarp jų ir neigiamų padarinių atsiradimo, žalos padarymo, daikto buvimo vietos teisė ir kt.

Minėtieji tarptautinės teisės jurisdikcijos principų pavyzdžiai rodo ir galimybes juos taikyti e. 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 e. erdvės globalumo, t. y. pasireiškia vadinamasis globalaus kaimo efektas. Šią situaciją puikiai iliustruoja 2000 m. spręsta teisminė byla Prancūzijoje – *Yahoo! Inc. v. La Ligue Contre le Racisme et l'Antisemitisme* (LICRA). Šioje byloje Prancūzijos teismo sprendimas siekė apriboti JAV bendrovės *Yahoo!* teisę savo internetiniuose puslapiuose skelbti informaciją apie galimybes įsigyti fašistinės atributikos, nes tokia atributika ir su ja susijusi informacija yra neteisėtos pagal Prancūzijos teisę – ir nors tai skelbiama *Yahoo!* vartotojų JAV ir kitose valstybėse, atitinkamas prekes bei

informaciją gali matyti ir Prancūzijos gyventojai. Minėtosios šalies teismas argumentavo, kad jeigu žmogus gali matyti internetinį puslapį Prancūzijoje, tinklalapio operatorius turėtų atsakyti pagal Prancūzijos teisę, todėl įpareigojo *Yahoo!* pašalinti ginčą sukėlusią informaciją arba užblokuoti prieigą prie jos. Deja, toks Prancūzijos teismo sprendimas techniškai buvo ir yra neįgyvendinamas. Atsižvelgdamas į tai, JAV teismas (į kurį kreipėsi *Yahoo!,* siekdama išvengti Prancūzijos teismo sprendimo vykdymo) konstatavo, kad toks Prancūzijos teismo sprendimas nėra nei pripažįstamas, nei įgyvendinamas JAV, nes jis prieštarauja Pirmajai JAV Konstitucijos pataisai (žodžio ir išraiškos laisvei). Abu teismai iš esmės teisingai nustatė jurisdikcijos klausimą ir taikė savo nacionalinius įstatymus, nors dėl to ir kilo didžiulė neišsprendžiama kolizija.

Spręsdamas *Yahoo! Inc. v. LICRA* Prancūzijos teismas pritaikė neigiamų padarinių atsiradimo vietos principą. Tarptautinėje praktikoje tai bene dažniausiai taikomas principas nustatant jurisdikcijos taisykles internete, tačiau, kaip matyti iš aptartosios bylos, reali šio principo nauda yra ribota, o jo taikymo teisėtumas yra abejotinas.

Neigiamų padarinių atsiradimo vietos principas internete gali būti suprantamas plačiąja ir siaurąja prasmėmis. Plačiąja prasme šis principas reiškia, kad gali būti taikoma bet kurios valstybės, kurioje prieinamas atitinkamas interneto išteklius, teisė. Toks interpretavimas iš tiesų buvo panaudotas *Yahoo! Inc. v. LICRA* ir reiškia globalų valstybės jurisdikcijos išplėtimą, kuris yra labai abejotinas ir menkai pagrįstas. Siaurąja prasme neigiamų padarinių atsiradimo vietos principas reiškia, kad gali būti taikoma tos valstybės, į kurią specialiai orientuotas atitinkamas interneto išteklius, teisė, nors tas pats išteklius yra laisvai prieinamas ir kitose valstybėse. Specialiai orientuotas išteklius yra tas, kuris yra lokalizuotas arba pritaikytas konkrečios valstybės vartotojams, pvz., pateikiamas nacionaline kalba, naudojant tam tikros šalies domeną ar prasminį domeno vardą (šis tam tikros šalies ar regiono gyventojams turi kalbinę ar simbolinę prasmę), skelbia geografiškai pritaikytą reklamą arba yra reklamuojamas asmenų, plačiai žinomų tam tikroje valstybėje ar regione, ir pan.

Neigiamų padarinių atsiradimo vietos principas siaurąja prasme yra kur kas tinkamesnis sprendžiant tam tikrų interneto išteklių jurisdikcijos klausimą ir kelia gerokai mažiau kontroversijų. Vis dėlto, taikant šį principą, būtina įvertinti realias šalių nacionalinės teisės žinias (ar atsakinga šalis žinojo, turėjo ar galėjo žinoti apie nacionalinės teisės taisykles), ar interneto išteklius ir (ar) veikla internete yra nuolatinio ar trumpalaikio pobūdžio, ar šalies, kuriai norima taikyti jurisdikciją, vaidmuo nagrinėjamuoju metu yra svarbiausias ar ne, ir pan.

Valstybės institucijoms ir teismams prieš imantis spręsti konfliktinę situaciją, irgi dėrėtų kiekvieną kartą individualiai įvertinti šalių galimybes dalyvauti procese ir ginti savo teises, t. y. būtina nepamiršti proceso teisingumo ir ekonomiškumo principų.

Nors esamų jurisdikcijos principų taikymas, atsižvelgiant į interneto realijas, yra labiausiai paplitęs jurisdikcijos problemų sprendimo būdas internete, dėl minėtųjų keblumų teisės moksle jau senokai diskutuojama apie specialiosios interneto teisės ir jurisdikcijos perspektyvas, nustatant analogiją su tarptautinėmis taisyklėmis, taikomomis tarptautiniams vandenims, kosmosui ar Antarktidos teritorijai. Dar naujesnė analogija, cituojama specialiosios interneto teisės ir jurisdikcijos šalininkų, yra tarptautinė aplinkos teisė.

Nustačius specialiąją interneto jurisdikciją, valstybės neturės spręsti, ar jų įstatymai yra taikomi sprendžiant konkretų ginčą, bus užtikrintas didesnis saugumas ir labiau apibrėžta atsakomybė. Deja, praktiškai *sui generis* tarptautinė interneto teisė įgyvendinama tik kaip tarptautinės teisės institutas. Dėl valstybių kultūrinių skirtumų ir globalaus šių taisyklių įgyvendinimo pasauliniu lygiu negalimumo artimiausiu metu to tikėtis neverta.

Kita vertus, speciali interneto jurisdikcija iš esmės jau įsitvirtino tose srityse, kuriose valstybių nacionalinė jurisdikcija (ir nacionalinis reglamentavimas) tik sekė interneto bendruomenės nustatytas taisykles ir bendrųjų teisės principų taikymą, pvz., sprendžiant ginčus dėl interneto domenų vardų.

Jurisdikcijos praradimą valstybės kompensuoja taikydamos įvairias teritorines interneto techninės kontrolės priemones, ypač blokavimo ir filtravimo mechanizmus.

3 skirsnis. Interneto jurisdikcijos reglamentavimas ES ir Lietuvoje

Remiantis tradiciniais jurisdikcijos principais, jos klausimams spręsti Europos civilinėje teisėje naudojami du modeliai. Pirmasis iš jų yra grindžiamas esamais tarptautiniais dokumentais, pvz., 1980 m. balandžio 11 d. Vienos konvencija dėl Tarptautinio prekių pirkimo–pardavimo sutarčių, ji taikoma privatiems subjektams. Antrasis modelis, kuris yra taikomas dažniau, yra grindžiamas tarptautinės privatinės teisės principais. Pats paprasčiausias ir efektyviausias būdas tarptautinėje privatinėje teisėje išspręsti jurisdikcijos klausimus – teisinio santykio šalims pačioms pasirinkti taikomą teisę ir ginčą sprėsiantį teismą. Deja, prievolių, kylančių iš deliktų, ir kai kuriais sutartinių prievolių atvejais tai yra neįmanoma.

Tokiais atvejais jurisdikcijos klausimai Europoje sprendžiami pagal 1968 m. rugsėjo 29 d. Briuselio konvenciją dėl jurisdikcijos ir teismų sprendimų vykdymo civilinėse ir komercinėse bylose, ji yra pirminis teisės šaltinis, kuriuo remiamasi nagrinėjant jurisdikcijos klausimus visose civilinėse bylose. Konvencija reguliuoja tris jurisdikcijos aspektus: nustato teisminės jurisdikcijos normas; nurodo prielaidas ir veiksmus užsienio teismų sprendimų pripažinimo ir vykdymo klausimais; reglamentuoja *lis pendens* bylose, iškeltose vienos iš Konvencijos šalių teisme. Ši Konvencija yra taikoma tik civilinėse ir komercinėse bylose (Briuselio konvencijos 1 str. 1 p.).

Briuselio konvencija leido suderinti procedūras, pripažįstant ir vykdant sprendimus Europos Bendrijoje, taikant vienodai interpretuojamas Konvencijos nuostatas ir nepaisant valstybių narių teisinių sistemų skirtumų. Pagal 1971 m. birželio 3 d. papildomą protokolą, šalių narių aukščiausieji teismai gali prašyti Europos Sąjungos Teisingumo Teismo (toliau – *ESTT*) išaiškinimo dėl Briuselio konvencijos normų taikymo.

Teigiama patirtis, susijusi su šios konvencijos veikimu, paskatino šalis, kurios nebuvo narės, tačiau priklausė Europos laisvosios prekybos asociacijai *(ELPA)*, remtis Briuselio konvencija, net ir formaliai jos nepasirašius. Siekiant išspręsti šią problemą, buvo priimta nauja konvencija, lygiavertė Briuselio – 1988 m. rugsėjo 16 d. Lugano konvencija. Abiejų konvencijų pavadinimai tapatūs, ir tai dar kartą patvirtina jos pirmtakės – Briuselio konvencijos – taisyklių svarbą bei aktualumą.

Abiejų konvencijų panašumas pasireiškia identiškai suformuluotomis nuostatomis ir tokia pat straipsnių numeracija. Lugano konvencija yra atvira sutartis, sudaryta iš trijų protokolų. Pirmasis protokolas yra susijęs su jurisdikcijos klausimais, procedūromis ir jos vykdymo užtikrinimu; antrasis – su vienodu konvencijos aiškinimu; trečiasis reglamentuoja ryšius su kitomis konvencijomis. Skirtingai nei Briuselio konvencijos atveju, *ESTT* nėra kompetentingas aiškinti Lugano konvencijos nuostatų, nes *ELPA* valstybės nedavė tam sutikimo. Antrasis, papildomas, konvencijos protokolas nustato išaiškinamąjį sprendimą – kiekvienos iš besitariančiųjų šalių teismai, atsižvelgdami į precedentus ir taikydami konvencijos nuostatas, turi atsižvelgti į kitų valstybių teismų išaiškinimus. Siekiant užtikrinti informacijos sklaidą, buvo suformuluota pareiga persiųsti pagal Lugano ir Briuselio konvencijas priimtus sprendimus. Lugano konvencija gali būti taikoma neatsižvelgiant į procesiniuose veiksmuose dalyvaujančių šalių pilietybę. Minėtoji konvencija apima civilines ir komercines bylas, tačiau „civilinės ir komercinės bylos“ definicija joje nėra apibrėžta.

Tačiau Lugano konvencija gali būti taikoma tik tada, kai atsakovas gyvena valstybėje, kuri yra Konvencijos šalis, tačiau nėra ES narė. Jurisdikcija galima ir tuo atveju, kai Lugano konvencija tai tiesiogiai numato. Konvencija iš esmės pakeičia kitus šalių sudarytus tarptautinius susitarimus, kurie susiję su jos reguliuojamais klausimai. Jos nuostatos pakeičia valstybių narių nacionalinius teisės aktus, kurie yra susiję su Konvencijos reguliuojamais klausimais.

Jurisdikcijos taisyklės Lugano konvencijoje visų pirma remiasi *actor sequitur forum rei* principu. Todėl, sprendžiant jurisdikcijos klausimą, turėtų būti atsižvelgiama į su atsakovu susijusias aplinkybes, ypač jo gyvenamąją vietą. Vienos šalies, pasirašiusios Konvenciją, asmenys gali būti atsakovais kitos valstybės teismuose tik konkrečiais Konvencijoje nustatytais atvejais. Nacionalinių įstatymų normos, apibrėžiančios kitus jurisdikcinius kriterijus (pvz., gyvenamąją vietą), šiais atvejais netaikomos. Tik jeigu atsakovas negyvena tos valstybės teritorijoje, užsienio šalies teismų jurisdikcija jo atžvilgiu yra nustatoma pagal pačios valstybės nacionalinius įstatymus. Vis dėlto Lugano konvencija neapibrėžia gyvenamosios vietos kriterijaus. Asmeniui, gyvenančiam vienoje iš Lugano konvencijos valstybių narių, gali būti taikoma kitos valstybės teismų jurisdikcija, vadovaujantis Konvencijos taisyklėmis, susijusiomis su alternatyviąja jurisdikcija (Lugano konvencijos 5 ir 6 str.).

Lugano konvencija pirmenybę teikia šalių susitarimui dėl jurisdikcijos, o *actor sequitur forum rei* principas taikomas tik tuo atveju, jeigu pačios santykio šalys nesutaria dėl jurisdikcijos. Primintina, kad *actor sequitur forum rei* principas iš esmės leidžia ieškovui rinktis palankiausią jurisdikciją, o tai gali paskatinti jį piktnaudžiauti.

ES reglamentas Nr. 44/2001, kuris visose ES šalyse, išskyrus Daniją, pakeitė 1968 m. Briuselio konvenciją, yra fundamentaliai svarbus ES narėms sprendžiant civilinės jurisdikcijos klausimą. Ir Lugano konvencija, ir Reglamentas Nr. 44/2001 yra sukurti remiantis Briuselio konvencija ir pateikia analogiškus sprendimus. Minėtieji teisės aktai taikomi tik civilinėms ir komercinėms byloms. Abu kaip pagrindinį pabrėžia bendrąjį teritorialumo principą, pagal kurį bendru sutarimu nustatomas sutartinių santykių teisinis reglamentavimas, kai pačios šalys negali išspręsti jurisdikcijos klausimų. Pagal Briuselio arba Lugano konvencijų 16 str., valstybėje narėje ar susitariančiojoje valstybėje nuolat gyvenantiems arba veikiantiems asmenims, neatsižvelgiant į jų pilietybės ar registracijos vietas, gali būti iškelta byla šios šalies teismuose. Šios nuostatos iš esmės įgyvendina bendrąjį *actor sequitur forum rei* principą. Šalių sąveika e. erdvėje arba sutartinių santykių elektroninis pobūdis nei modifikuoja, nei kaip nors specialiai išaiškina šį principą ar jo taikymą.

Nuolatinė šalių gyvenamoji vieta yra kriterijus, kuriuo abiejuose teisės aktuose vadovaujamasi visais atvejais, įskaitant ir civilinius, ir komercinius santykius e. erdvėje. Pagal Lugano konvencijos 5 str. 4 p., vienintelė ir pakankama prielaida vietoj nacionalinės teisės aktų nuostatų taikyti Konvencijos taisykles yra nuolatinės gyvenamosios vietos nustatymas valstybės narės teritorijoje. Tačiau nė vienas aktas nenumato nuolatinės gyvenamosios vietos apibrėžimo. Greta bendrojo principo formulavimo abu dokumentai suteikia galimybę taikyti alternatyviąją jurisdikciją.

Nesant šalių susitarimo dėl taikytinos teisės ir sutartinių santykių reglamentavimo, atsižvelgiant ir į Lugano konvencijos ir Reglamento 44/2001 5 str., šaliai gali būti iškelta byla bet kurios valstybės, išskyros tos, kurioje yra šalies nuolatinė gyvenamoji vieta arba joje yra užregistruota buveinė, teisme. Atitinkama prievolės vykdymo valstybė gal būti laikoma tinkama jurisdikcija bylai nagrinėti. Dėl tokių nuostatų gali kilti nesutarimų, taikant jas elektroninėms sutartims. Reglamentas 44/2001 paaiškina koncepciją prievolės atlikimo vieta taip: „Prekių pardavimo pagal sutartį atveju vieta, kur prekės turi būti pristatytos arba buvo pristatytos“ (5 str.). Paslaugų teikimo atveju tai yra vieta, kurioje paslaugos pagal sutartį buvo suteiktos arba turėtų būti suteiktos.

Internetas yra tapęs įprasta elektroninių deliktų terpe. Be tradicinių civilinės teisės pažeidimų, atsiranda ir naujų, kurie yra būdingi tik internetinei erdvei, tokie kaip teisių pažeidimai *P2P* tinkluose, elektroninis šmeižtas ir informacijos pasisavinimas, nepageidaujami elektroniniai laiškai, raktažodžių pažeidimai ir pan.

Ir Lugano konvencijos, ir Reglamento 44/2001 5 str. 3 d. suteikia jurisdikciją delikto bylose teismams, kompetentingiems toje šalyje, kurioje buvo atlikti žalą sukėlę veiksmai. Kenkiamosios veiklos vykdymo vieta gali būti fizinė (teritorinė jurisdikcija), kurioje pasireiškė žala, nulemta atliktų veiksmų arba neveikimo, ir vieta, kurioje buvo padaryta žala (veikimo jurisdikcija). Tokiu atveju ieškovas gali rinktis, kokiam teismui pateikti bylą – kompetentingam toje srityje, kurioje kaltininkas veikė (ar neveikė), ar tam, kuris yra kompetentingas toje srityje, kur buvo patirta žala.

Atsižvelgiant į e. erdvės pobūdį, žala gali būti taip paplitusi, kad iš esmės lemia pasaulinę jurisdikciją, t. y. plačiąja prasme žala padaroma visose valstybėse, kuriose yra prieinamas atitinkamas išteklius. Veiksmo atlikimo vieta gali būti ta, kur kaltininkas įkėlė duomenis į interneto išteklių, tačiau konkrečią žalos internetu padarymo vietą yra kur kas sunkiau nustatyti. Vietos, kurioje yra padaryta žala, koncepcijos taikymas, atsižvelgiant į globalų veiklos poveikį, kylantį iš bet kokių veiksmų internete, turėtų būti apribotas.

Potencialus elektroninės informacijos prieinamumas konkrečioje šalyje dar nesuteikia pagrindo teigti, kad žala yra padaryta būtent šioje valstybėje. Minimalūs reikalavimai, taikomi žalos atsiradimo vietos institutui, turėtų būti grindžiami remiantis žalingo turinio autoriaus ketinimais – būtina nustatyti, ar kaltininkas numatė galimybę, kad jo žinutė gali lemti tam tikrus konkrečios jurisdikcijos rezultatus, ir ar to siekė, jeigu taip, jis turėtų prisiimti atsakomybę.

Paprasčiausias būdas nustatyti jurisdikciją elektroninių deliktų atžvilgiu būtų jos apribojimas ta vieta, iš kurios buvo įkeltas žalingas turinys. Verslo atveju turėtų būti taikomi valstybės, kurioje jis yra vykdomas, įstatymai, neatsižvelgiant į tai, kad paslaugos yra prieinamos internete. O fizinių asmenų atveju – jeigu fizinis asmuo nevykdo jokios ekonominės veiklos, jam turėtų būti taikomi įstatymai tos šalies, kurioje yra asmens nuolatinė gyvenamoji vieta.

ES reglamentas (EK) 593/2008 (dažniausiai vadinamas Romos I reglamentu) irgi yra svarbus sprendžiant jurisdikcijos klausimus. Minėtieji teritoriniai principai negali būti taikomi, jeigu deliktą ar sutartinius įsipareigojimus lemianti veikla negali būti susieta su rezidencijos šalimi, tačiau iš aplinkybių visumos matyti, kad sutartis ar deliktas yra labiau susiję su kita valstybe. Analizuojant šias nuostatas elektroninių sandorių ir deliktų atžvilgiu, turėtų būti atsižvelgiama į tokias aplinkybes: elektroninės sutarties sudarymo būdas, tinklalapio kalba, domenas, kuriame tinklalapis yra užregistruotas, elektroninės prekybos valiuta, pačiame tinklalapyje nustatytos veiklos sąlygos, su kuriomis turi sutikti jo vartotojai, ir pan. Serverių, kuriuose yra saugomas tinklalapis arba jo dalys, vieta yra visiškai nesvarbi.

ES direktyva 2000/31/EB dėl elektroninės komercijos yra vienas iš pirminių specialių interneto jurisdikcijos principų šaltinių. Šioje Direktyvoje formuluojamas svarbiausias informacinės visuomenės paslaugų kilmės jurisdikcijos principas, jis teigia, kad paslaugų teikėjui (asmeniui, teikiančiam paslaugas e. erdvėje) paprastai taikomi tos valstybės, kurioje jis iš tikrųjų veikia (yra įsisteigęs), bet ne tos valstybės, kur fiziškai yra veiklai vykdyti pasitelkiamas interneto serveris ar tinklalapis, įstatymai. Šis principas nėra absoliutus.

Pati Direktyva numato kilmės principo išimčių, pvz., jurisdikcijos kilmės principas gali būti netaikomas pagrindžiant:

- viešąja tvarka ir saugumu, visuomenės sveikata ir vartotojų apsauga; paslaugos yra žalingos arba daro žalą vienam ar daugiau iš išvardytųjų objektų;
- valstybių narių taisyklės yra būtinos ir proporcingos minėtųjų objektų atžvilgiu.

Direktyvoje nustatyti principai yra įgyvendinti Lietuvos Respublikos civiliniame kodekse (toliau – CK).

Jurisdikcija internetinių išteklių atžvilgiu yra nustatoma konkuruojant kilmės ir paskirties šalių principams. Pirmasis (kilmės šalies principas) taikomas internete siekiat pateikti bylą tos šalies, kurioje buvo įkeltas skaitmeninis turinys, teismui. Antrasis principas yra paremtas informacijos gavimo (žalos padarymo) vietos kriterijumi išlaikant sąsają su asmeniu, gavusiu konkrečios informacijos – jo nuolatine arba nenuolatine gyvenamąja vieta. Akivaizdu, kad pirmasis principas yra palankesnis vienai šaliai, o antrasis – kitai, t. y. skirtingoms civilinio santykio šalims.

Visos taikytinos tarptautinės sutartys (Briuselio konvencija, Lugano konvencija, Reglamentas 44/2001 ir Romos I reglamentas), kurios reglamentuoja tarpvalstybinę jurisdikciją, be tradicinio kilmės valstybės principo, numato pagrindines taisykles, kai gali būti taikoma paskirties šalies jurisdikcija. Išimtis kilmės valstybės principo naudai, taikant specifinę vidaus rinkos sąlygą, yra nustatoma pagal ES elektroninės komercijos direktyvos 3 straipsnį. Remiantis minėtuoju šaltiniu, informacinės visuomenės paslaugos turi būti vertinamos pagal tų valstybių, kuriose yra įsikūręs verslas (kilmės valstybės principas), įstatymus.

Informacinės visuomenės paslaugos apima elektroninio turinio prieigą ir prieglobą, jo perdavimą, paiešką ar pardavimą. Elektroninės komercijos direktyvos 3 str. 1 ir 2 d. nustato dvi kilmės šalies principo taikymo prielaidas. Visų pirma tos valstybės, kurioje yra įsikūręs paslaugos teikėjas, valdžios institucijos privalo užtikrinti, kad jo veiksmai atitiktų tos valstybės vidaus teisės nuostatas. Be to, valstybė turi nediskriminuoti užsienio paslaugų. Elektroninės komercijos direktyvos 3 str. 2 d. aiškinimas (Europos Tarybos aprobuotas išaiškinimas) teigia, kad bet koks laisvės teikti informacinės visuomenės paslaugas, išskyrus nurodytąsias priede, suvaržymas yra draudžiamas. Šio principo tikslas – besilaikantiems šalies įstatymų verslininkams neturėtų būti taikoma papildomų apribojimų toje valstybėje, kurioje jie teikia savo paslaugas. Pagal Elektroninės komercijos direktyvą, kilmės valstybės principas yra pagrindinis elektroninės komercijos jurisdikcijos principas ES.

Elektroninės komercijos direktyvoje prioritetas, teikiamas kilmės valstybės principui, ES jurisdikcijos reglamentų atžvilgiu yra naujovė, pagrįsta elektroninių paslaugų teikimo Bendrojoje rinkoje laisvės principu. Pagal Elektroninės komercijos direktyvą, šio principo taikymo sritis ribojama tik teikiant informacinės visuomenės paslaugas. Speciali išimtis iš kilmės valstybės principo, nustatyta Elektroninės komercijos direktyvos preambulės 57 punkte, yra tie atvejai, kai valstybėms narėms paliekama teisė

imtis priemonių prieš paslaugų teikėjus, kurie yra įsikūrę kitoje valstybėje narėje, tačiau visą arba didžiąją dalį savo veiklos vykdo pirmosios valstybės narės teritorijoje. Išimties *ratio legis* yra užkirsti kelią apeiti valstybės įstatymus sukuriant verslą už valstybės, kurios teritorijai yra skirtos verslo teikiamos paslaugos, ribų.

Elektroninės komercijos direktyvos nuostatos nukrypsta nuo tradicinės tarptautinės privatinės teisės principų, nes jos yra specialios normos tradicinės privatinės tarptautinės teisės atžvilgiu.

Naujausias ES žingsnis sprendžiant jurisdikcijos kolizijas Bendrojoje rinkoje nesutartinių prievolių atžvilgiu yra Reglamentas Nr. Nr. 864/2007 – vadinamasis Romos II reglamentas. Pagal jo 3 str., Reglamentas turi būti universalus, t. y. taikomas, neatsižvelgiant į tai, ar valstybės narės arba trečiosios šalies teisė buvo pasirinkta kaip taikytinoji. Šis Reglamentas toliau tikslina su deliktu susijusių prievolių jurisdikcijos principus. Jo 4 str. pateikta bendroji taisyklė – teisė, taikoma nesutartinėms prievolėms, atsirandančioms dėl civilinės teisės pažeidimo, yra tos valstybės, kurioje yra padaroma žala, teisė, neatsižvelgiant į tai, kurioje valstybėje ar valstybėse gali būti pastebėta netiesioginių delikto padarinių. Nors šį formuluotė susiaurina potencialias taikytinas jurisdikcijas, ji nepateikia termino „vieta, kur buvo padaryta žala“ išaiškinimo, taip vis dar suteikdama ieškovams galimybę rinktis palankiausią jurisdikciją. Neįmanoma nustatyti vienos kolizinės normos, kuri būtų tinkama naudoti visiems globaliame tinkle padaromiems deliktams. Tokiu būdu žalos padarymo vietos principas, kuris dažnai yra svarbiausias kriterijus nustatant jurisdikciją, yra nepakankamas įvairaus tipo naujų galimų deliktų kontekste. Todėl kitos Reglamento taisyklės daugiausia dėmesio skiria ne žalingai veiklai, o padaromai žalai ir būdams jai ištaisyti.

Apibendrinant minėtąją trumpą Europos jurisdikcijos taisyklių apžvalgą, svarbu atkreipti dėmesį, kad jurisdikcijos taisyklių taikymas didele dalimi priklauso nuo to, kaip nacionalinės institucijos supranta ir aiškina bendrąsias tarptautines taisykles ir principus. Dažniausiai taikomas kriterijus – sutarties sudarymo vieta *(lex loci contractus)*. Prievolės vykdymo vietos *(lex loci solutionis)* ir paslaugos teikimo vietos (*lex loci originalis*) kriterijai irgi gana dažnai pasitelkiami nustatant jurisdikciją.

Dėl didelio lankstumo pats praktiškiausias internetinių įsipareigojimų principas yra teisės taikymo pagal artimiausios ir natūraliai su sutartimi labiausiai susijusios teisės taikymo teorija. Taikant šį principą būtina sąlyga, kad bylos faktus analizuojantis teisėjas turėtų užtektinai patirties ir galėtų pateikti pakankamą ir motyvuotą įvertinimą.

Lengviausias būdas išvengti jurisdikcinių problemų kilus su e. erdve susijusių ginčų – sutartyje nurodyti, kokios šalies teisė reglamentuoja teisinius sutarties santykius. Jeigu sutarties šalys nepasinaudoja šia galimybe, ES teisė suteikia daug laisvės teismams patiems nustatyti jurisdikciją ir palieka daug neaiškumų bylų, susijusių su internetu, atsakovams. Iš to kyla didelis teisinis neaiškumas dėl galimų teisinių padarinių, atlikus tam tikrus veiksmus internete, ir daug galimybių potencialiems ieškovams elgtis savanaudiškai bei siekti nagrinėti ginčą taikant jiems palankiausią jurisdikciją.

Dabartinė teismų praktika ES rodo, kad ten, kur kilmės valstybės nuostatos nėra taikomos (Elektroninės komercijos direktyvoje) ir kur sutarties šalys nenurodo taikytinos valstybės teisės, atsižvelgiant į konkretaus elektroninio turinio pobūdį, turėtų būti taikomas kilmės valstybės (tos valstybės, kur į elektroninę erdvę įkeltas turinys, teisę) principas. Turi būti atsižvelgiama, ar elektroninė svetainė, kurioje yra turinys, yra pasyvi (paprastai netikslinė ir niekuo nesiskirianti nuo vietos spaudos, radijo ir televizijos, naudojama kaip priemonė teikti reikalingą aktualią informaciją, bet nenaudojama kaip aktyvi verslo vykdymo priemonė toje valstybėje, kurioje yra neigiamų padarinių patirianti šalis), ar ji yra akyvi, t. y. konkreti, paslauga arba tinklalapio turinys yra skirtas konkrečiai valstybei (atsižvelgiant į tinklalapio kalbą, turinį, valiutą ir pan.). Turi būti vertinama ir tai, ar yra reali sąveika su valstybe ir ar padaroma faktinės žalos. Vien tik tam tikro turinio prieinamumas valstybės teritorijoje neturėtų būti laikomas jurisdikcijos nustatymo pagrindu.

Lietuvoje, kuri yra ES narė, interneto jurisdikcijos klausimai iš esmės sprendžiami remiantis minėtojoje ES direktyvoje 2000/31/EB dėl elektroninės komercijos įtvirtintu kilmės principu, nacionaline teise, dvišalėmis ir daugiašalėmis tarptautinėmis sutartimis. Atskirai reikėtų paminėti CK esančias tarptautinės privatinės teisės nuostatas, nurodančias konkretiems teisiniams santykiams taikytiną teisę. Nors daugelyje šių taisyklių nėra paminėti teisiniai e. erdvės santykiai, jomis turėtų būti remiamasi ir reguliuojant teisinius santykius internete. Bendrųjų jurisdikcijos principų tęstinumas taikomas ir pagal Lietuvos baudžiamuosius bei administracinius įstatymus.

Lietuva yra ratifikavusi 2001 m. lapkričio 23 d. Europos Tarybos konvenciją dėl elektroninių nusikaltimų, kurioje nustatytos specialios jurisdikcijos taisyklės dėl nusikaltimų e. erdvėje – iš esmės įtvirtinamas pažeidimo vietos padarymo principas, o ypač sunkiems nusikaltimams suformuluojama universalios jurisdikcijos taisyklė, pagal kurią kiekviena valstybė turi teisę taikyti atsakomybę.

4 skirsnis. Interneto tarpininkų veiklos reglamentavimas

Interneto tarpininkai yra laikytini informacinės visuomenės paslaugų teikėjais, t. y. asmenys, paprastai už atlyginimą elektroninėmis priemonėmis ir per atstumą individualiu informacinės visuomenės paslaugos gavėjo prašymu teikiatys tam tikras paslaugas.

Interneto tarpininkais galima laikyti visus subjektus, užtikrinančius interneto infrastruktūros funkcionavimą, iš jų ir subjektus, teikiančius interneto prieigos, prieglobos, turinio skelbimo ir perdavimo paslaugas. Iš esmės interneto tarpininkai yra interneto prieigos paslaugų teikėjai, įvairiausi interneto portalai, kuriuose vartotojai gali pateikti savo informacijos (pvz., failų, komentarų ir pan.). Universitetas irgi yra interneto tarpininkas, nes teikia interneto prieigos, elektroninio pašto, tinklalapių skelbimo paslaugas darbuotojams ir studentams. Įmonė yra savo darbuotojų interneto tarpininkė, nes teikia jiems interneto prieigos, elektroninio pašto ir kitų naudojimosi internetu galimybių.

Nesant tarpininkų, paties interneto funkcionavimas būtų nelabai įmanomas, nes jo vartotojai gali prisijungti, siųsti ir skelbti informaciją tik per interneto tarpininkus, tiesioginis vartotojo prisijungimas iš esmės yra neįmanomas. Kita vertus, pats interneto vartotojas, kuris sudaro galimybes savo administruojamame tinklalapyje kitiems asmenims skelbti ar saugoti informaciją (pvz., komentarus), jau savaime tampa interneto tarpininku. Asmuo – interneto vartotojas, kuris skelbia savo arba paties atrinktą ir žinomą kitų asmenų informaciją, t. y. pats ją įkelia, siunčia, saugo arba kontroliuoja, nelaikomas interneto tarpininku, nes minėtaisiais veiksmais tarpininkavimas yra eliminuojamas.

Interneto tarpininkui nenumatyta bendra pareiga kontroliuoti ir tikrinti informacijos, kurią jo paslaugų gavėjai (vartotojai), naudodamiesi interneto tarpininko infrastruktūra, siunčia, gauna, skelbia, saugo ir pan. Todėl interneto tarpininko ir jo paslaugų vartotojo santykiai iš esmės yra anonimiški. Jeigu interneto tarpininkas žino ir kontroliuoja jo infrastruktūroje esantį interneto turinį, jis pats tampa už jį atsakingas. Tik kilus konfliktinei situacijai interneto tarpininkas privalo įsikišti ir imtis interneto turinio reguliavimo veiksmų. Jis laikomas infrastruktūros teikėju ir pagal analogiją su telekomunikacijų operatoriumi iš esmės neatsako už vartotojų neteisėtą naudojimąsi šia infrastruktūra.

Atsižvelgiant į direktyvoje 2000/31/EB dėl elektroninės komercijos įtvirtintus principus, interneto tarpininkai yra atsakingi už visą medžiagą, kuri priklauso jų interneto ištekliams – serveriams ar tinklalapiams, tik tuo atveju, jeigu paslaugų teikėjai apie šią informaciją žino ir ją kontroliuoja.

Išimčių yra nustatyta tik interneto tarpininkams (kaip informacinės visuomenės paslaugų teikėjams), kurie teikia informacijos perdavimo ar skelbimo paslaugas, t. y. iš esmės tarpininkauja tarp vartotojų ir interneto turinio teikėjų. Tačiau ir tokiems interneto tarpininkams gali tekti prisiimti atsakomybę, jeigu jie žinojo apie pažeidimą, tačiau nesiėmė jokių veiksmų šiam pažeidimui pašalinti ar kitaip prie jo prisidėjo. Tokie principai pirmąkart suformuluoti JAV teisėje, vėliau priimti ir kitose valstybėse, iš jų ir ES. Šuo metu Lietuvoje minėtieji principai išsamiai reglamentuoti LR informacinės visuomenės paslaugų įstatymu.

Minėtajame įstatyme ir ES elektroninės komercijos direktyvoje vartojama „informacinės visuomenės paslaugų tiekėjo“ 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 prekes, ir pan. Informacinės visuomenės paslaugų teikėjo sąvoka yra gerokai platesnė, apimanti įvairias paslaugas, teikiamas per atstumą e. erdvėje, tačiau svarbiausi reglamentavimo principai, susiję su atsakomybe už interneto vartotojų (informacinės visuomenės paslaugos gavėjų) siunčiamą ar saugomą interneto turinį, iš esmės yra taikomi interneto tarpininkams.

Interneto tarpininkai neįpareigoti tikrinti ir kontroliuoti jų tinklais perduodamo bei jų serveriuose skelbiamo turinio ir už jį neatsako, jeigu informacinės visuomenės paslaugų (prieigos ar skelbimo 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 prieigą prie jos.

Šie atsakomybės ribojimo principai taikomi ir tuo atveju, kai perduodamos informacijos saugojimas yra automatinis, tarpinis ir trumpalaikis, t. y. skirtas tik tam, kad ji 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 perdavimas kitiems jos prašantiems paslaugos gavėjams būtų efektyvus, jeigu paslaugos teikėjas atitinka minėtąsias sąlygas, be to, laikosi savo verslo sričiai įprastų informacijos atnaujinimo taisyklių, netrukdo teisėtai naudotis technologija, kuri šioje verslo srityje yra pripažįstama ir naudojama siekiant gauti duomenų apie informacijos naudojimą.

Galimybės pasiekti neteisėtu būdu įgytos, sukurtos, pakeistos ar naudojamos informacijos panaikinimo tvarka ir 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 suinteresuotųjų asmenų pretenzijas dėl neteisėtos informacijos saugojimo ir (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) vartotojui skirtą informaciją pateikia naudodamasis nuorodomis į kitos elektroninės komercijos įmonės internetinio puslapio turinį (pvz., pateikia nuorodą į gamintojo puslapyje esantį produkto aprašymą), jis tampa atsakingas ir už šios medžiagos turinį. Jeigu informacinės visuomenės paslaugų teikėjas (ir interneto tarpininkas) pastebi, kad tie internetiniai puslapiai, į kuriuos yra pateikiamos nuorodos jo internetiniame puslapyje, pažeidžia įstatymus, jis turi nedelsdamas pašalinti šias nuorodas. Tuo atveju, kai internetiniame puslapyje yra nuorodų į kitus puslapius, vartotojui turėtų būti visiškai aišku, kada yra išeinama iš pirminio puslapio. Analogiškos taisyklės taikomos ir tuo atveju, kai interneto puslapiuose naudojami daugialypiai rėmeliai ar kitos priemonės, leidžiančios virtualiai pasiekti kituose puslapiuose esančią informaciją.

Interneto tarpininkų atsakomybės taisykles Lietuvoje šiuo metu reglamentuoja Informacinės visuomenės paslaugų įstatymas, šiems klausimams yra skirtas minėtojo įstatymo V skyrius. Pagal šio įstatymo 12 str. nuostatas, informacinės visuomenės paslaugos teikėjas, perduodantis paslaugos gavėjo pateiktą informaciją elektroninių ryšių tinklu arba suteikiantis galimybę šiuo tinklu naudotis, neatsako už teikiamą informaciją, jeigu paslaugos teikėjas:

1) neinicijuoja informacijos perdavimo;

2) neparenka perduodamos informacijos gavėjo;

3) neparenka ir nekeičia perduodamos informacijos.

Šie apribojimai ypač aktualūs tuo atveju, kai informacijos perdavimas ar galimybės naudotis elektroninių ryšių tinklu suteikimo veikla apima

automatinį, tarpinį ir trumpalaikį perduodamos informacijos saugojimą (pvz., tarpiniai serveriai (angl. *proxy servers)*, kurie skirti interneto greitaveikai padidinti). Šis saugojimas skirtas tik tam, kad informacija būtų perduota elektroninių ryšių tinklu, jeigu ji nėra saugoma ilgiau, negu pagrįstai būtina jai perduoti. Dėl to Informacinės visuomenės paslaugų įstatymo 13 str. atskirai pabrėžiama, kad paslaugos teikėjas, elektroninių ryšių tinklu perduodantis paslaugos gavėjo pateiktą informaciją, neatsako už automatinį, tarpinį ir laikiną tos informacijos saugojimą, skirtą tik tam, kad vėlesnis perdavimas kitiems jos prašantiems paslaugos gavėjams būtų efektyvus, jeigu jis:

1) nepakeitė informacijos;
2) nepakeitė prieigos prie informacijos sąlygų;
3) laikosi šioje verslo srityje įprastų informacijos atnaujinimo taisyklių;
4) nekliudo teisėtai naudotis technologija, kuri šioje verslo srityje yra pripažįstama ir naudojama siekiant gauti duomenų apie informacijos naudojimą;
5) skubiai imasi priemonių pašalinti saugotą informaciją arba panaikinti galimybę ją pasiekti, sužinojęs, kad pradinis perdavimo šaltinis yra pašalintas iš elektroninių ryšių tinklo ar panaikinta galimybė pasiekti pradinį perdavimo šaltinį arba jį pašalinti iš elektroninių ryšių tinklo ar panaikinti galimybę jį pasiekti nurodė teismas ar įstatymų numatytais atvejais kita valstybės ar savivaldybės institucija ar įstaiga.

Specialios taisyklės dėl interneto prieglobos (informacijos saugojimo) paslaugų teikėjų atsakomybės yra nustatytos Informacinės visuomenės paslaugų įstatymo 14 straipsnyje. Paslaugos teikėjas, paslaugos gavėjo prašymu saugantis jo pateiktą informaciją, už ją neatsako, jeigu:

1) neturi faktinių duomenų apie neteisėtą paslaugos gavėjo veiklą arba apie tai, kad paslaugos gavėjo pateikta informacija įgyta, sukurta, pakeista ar naudojama neteisėtu būdu ir, kai reikalaujama atlyginti žalą, nežino apie faktus ir aplinkybes, rodančius neteisėtą paslaugos gavėjo veiklą arba tai, kad paslaugos gavėjas teikia neteisėtu būdu įgytą, sukurtą, pakeistą ar naudojamą informaciją;
2) sužinojęs arba gavęs žinių apie neteisėtą paslaugos gavėjo veiklą arba apie tai, kad paslaugos gavėjo pateikta informacija įgyta, sukurta, pakeista ar naudojama neteisėtu būdu, skubiai imasi veiksmų, kad panaikintų galimybę tokią informaciją pasiekti.

Savaime suprantama, kad tuo atveju, kai paslaugos gavėjas veikia paslaugos teikėjo įgaliotas arba jo kontroliuojamas, šios atsakomybės apribojimo sąlygos yra nekeliamos. Tokiu atveju kontroliuojančiajam asmeniui bus taikoma tiesioginė atsakomybė.

Pagal Informacinės visuomenės paslaugų įstatymo 14 str. 3 d. galimybė pasiekti neteisėtu būdu įgytos, sukurtos, pakeistos ar naudojamos informacijos panaikinimo tvarką ir kriterijus, kai paslaugos teikėjas laikomas sužinojęs apie neteisėtą paslaugos gavėjo veiklą arba apie tai, kad paslaugos gavėjo pateikta informacija įgyta, sukurta, pakeista ar naudojama, gali būti papildomai reglamentuojama įstatymo įgyvendinamaisiais teisės aktais. Vienintelis šiuo metu galiojantis įstatymo įgyvendinamasis teisės aktas yra 2007 m. rugpjūčio 22 d. Lietuvos Respublikos Vyriausybės nutarimu Nr. 881 patvirtintas Galimybės pasiekti neteisėtu būdu įgytą, sukurtą, pakeistą ar naudojamą informaciją panaikinimo tvarkos aprašas. Įstatymo įgyvendinamųjų aktų, reglamentuojančių, kada paslaugos teikėjas laikomas sužinojęs apie neteisėtą paslaugos gavėjo veiklą arba apie tai, kad paslaugos gavėjo pateikta informacija įgyta, sukurta, pakeista ar šiuo metu nėra naudojama.

Galimybės pasiekti neteisėtu būdu įgytą, sukurtą, pakeistą ar naudojamą informaciją panaikinimo tvarkos aprašas iš esmės nustato interneto tarpininkų informavimo apie pastebėtą numanomai neteisėtą kopiją arba informaciją, atsiradusią dėl paslaugos gavėjo veiksmų, formą ir taisykles, taip pat reagavimo būdą, t. y. atitinkamų įstatymus pažeidžiančių interneto išteklių blokavimą (galimybės juos pasiekti panaikinimą).

Nors, kaip jau minėta, patys interneto tarpininkai nėra įpareigoti aktyviai stebėti ar kontroliuoti vartotojų perduodamos ir skelbiamos informacijos arba išteklių, jeigu interneto tarpininkas, pastebėjęs galbūt neteisėtą informaciją ar išteklius, įpareigotas apie tai nedelsiant informuoti atsakingą instituciją – Informacinės visuomenės plėtros komitetą prie LR susisiekimo ministerijos. Ši pareiga yra įtvirtinta Informacinės visuomenės paslaugų įstatymo 15 straipsnyje. Informacinės visuomenės paslaugų teikėjai privalo informuoti apie įtariamą neteisėtą paslaugos gavėjo veiklą arba tai, kad paslaugos gavėjo pateikta informacija gali būti įgyta, sukurta ar pakeista neteisėtu būdu. Be to, pagal Informacinės visuomenės paslaugų įstatymo 15 str. 2 d., paslaugų teikėjai Informacinės visuomenės plėtros komiteto reikalavimu privalo pateikti informaciją, leidžiančią nustatyti paslaugų gavėjus, su kuriais atitinkami paslaugų teikėjai yra susitarę dėl informacijos saugojimo.

Iš esmės pastaroji nuostata reiškia įpareigojimą interneto tarpininkams – informacinės visuomenės paslaugų teikėjams – fiksuoti informaciją apie

šių paslaugų gavėjus (bent jau tuos, kurie naudojasi informacijos saugojimo paslaugomis) ir leidžiančią juos identifikuoti. Kitais žodžiais tariant, šios nuostatos nustato sekimo pareigą. Iš tiesų jos yra menkavertės, nes interneto tarpininkai – informacinės visuomenės paslaugų teikėjai – dėl pasirinkto verslo modelio apie paslaugų gavėjus gali fiksuoti tik neesminę informaciją, kuri neleidžia identifikuoti konkretaus informaciją skelbiančio fizinio ar juridinio asmens. Tiek Lietuvoje, tiek užsienio šalyse apstu interneto tarpininkų – informacinės visuomenės paslaugų teikėjų, kurie sąlygiškai nedidelį informacijos kiekį saugo neatlygintinai, arba leidžia atsiskaityti anoniminėmis priemonėmis (pvz., išankstinio mokėjimo abonentų *SMS* žinute), todėl neturi užtektinai informacijos tikrajam paslaugų gavėjui identifikuoti. Be to, pagal LR Konstitucinio Teismo 2002 m. rugsėjo 19 d. nutarimą „Dėl telekomunikacijų, operatyvinės veiklos įstatymų ir Baudžiamojo proceso kodekso“ interneto tarpininkai, fiksuodami ir saugodami duomenis apie paslaugų gavėjus, patiria papildomų išlaidų ir sunkumų, todėl gali būti įpareigojami teikti tik tokią informaciją, kurią jie gauna įprastinių verslo operacijų metu ir ją saugo.

Apskritai Informacinės visuomenės paslaugų įstatymo 15 str. 2 d. nuostatos kelia abejonių dėl jų konstitucingumo ir suderinamumo su konstitucinėmis privatumo teisėmis bei nekaltumo prezumpcija. Panašios nuostatos iš esmės neturi analogų ES šalyse, tačiau lygiuojasi į Azerbaidžane ar Turkmėnistane taikomas interneto teisės taisykles. Dėl panašių nuostatų Europos Parlamentas 2012 m. liepą atmetė Prekybos sutarties dėl kovos su klastojimu (angl. *Anti-Counterfeiting Trade Agreement)* (toliau – *ACTA)* ratifikavimą. Pagal *ACTA* 27 str. 4 dalį, interneto paslaugų teikėjai gali būti įpareigoti atskleisti informaciją apie abonentus, kurių paskyros buvo naudojamos intelektinės nuosavybės teisių pažeidimams, kad tokius abonentus būtų galima patraukti atsakomybėn. Šios nuostatos labiausiai buvo kritikuojamos dėl jų nekonkretumo. Iš esmės, norint atskleisti informaciją apie abonentą, būtina prieš tai ją surinkti ir sutvarkyti, todėl kyla klausimų, kokios apimties informacija, kokiomis sąlygomis ir kaip ilgai turėtų būti saugoma. Tvarkant minėtuosius duomenis, atsirastų daugiau galimybių juos neteisėtai naudoti kitiems tikslams, be to, tokios informacijos tvarkymas pakenktų viešųjų tinklų infrastruktūrai, interneto paslaugų teikėjai patirtų nuostolių dėl didesnių ekonominių sąnaudų, kurios tikriausiai būtų perkeltos vartotojams. Kyla pagrįstų abejonių, ar tokios nuostatos neprieštarauja pagrindinėms žmogaus teisėms, ypač teisei į privataus gyvenimo neliečiamumą ir žodžio laisvę.

Jeigu interneto tarpininkas netenkina minėtųjų atsakomybės apribojimo sąlygų, jis tampa pats atsakingas už trečiųjų asmenų teisių ir interesų

pažeidimą. Kai kuriais atvejais interneto tarpininkui gali būti taikoma ir civilinė, ir net baudžiamoji atsakomybė (žr. *P2P* tinklų valdytojų atsakomybės klausimų analizę skyriuje „Intelektinė nuosavybė elektroninėje erdvėje“). Atkreiptinas dėmesys, kad atsakomybės taikymas interneto tarpininkams yra savarankiškas teisių gynimo būdas, pvz., jis savarankiškai taikomas tarpininkui, neatsižvelgiant į tai, ar buvo patrauktas atsakomybėn asmuo, kuris, naudodamasis tarpininko paslaugomis, išplatino neteisėtą turinį, o tarpininkas, turėdamas apie tai informacijos, nereagavo. Be to, tarpininkų atsakomybė yra atskirta nuo draudimų tarpininkams taikymo galimybių. Tam tikrais atvejais tarpininkai gali būti įpareigoti taikyti draudimus tiems interneto ištekliams, kurių jie nekontroliuoja (pvz., nutraukti interneto paslaugų teikimą serveriui, kuris yra vartotojo patalpose arba patalpose, kurias gali būti sunkiau kontroliuoti, (primintinas atvejis, kai kontroversiška interneto svetainė „Kavkaz Center“ buvo serveryje, esančiame LR Seimo nario tarnybiniame bute, LR Seimo viešbutyje). Šiais atvejais gali būti aktualu nedelsiant nutraukti informacinės visuomenės paslaugų teikimą, t. y. įpareigoti interneto tarpininką nebeteikti vartotojui atitinkamų paslaugų, nors pats tarpininkas nėra ir nebus atsakingas už vartotojo veiksmus ir platinamą turinį. Būtent tokia taisyklė yra įtvirtinta Informacinės visuomenės paslaugų įstatymo 15 str. 3 d. nuostatose. Asmenys, kurių teises pažeidžia paslaugų teikėjo perduodama ir (ar) saugoma informacija ar su ja susijusi veikla, turi teisę kreiptis į teismą su prašymu įpareigoti paslaugos teikėją imtis veiksmų, kad būtų nutrauktas pažeidimas, vykdomas naudojant informacinės visuomenės paslaugas, ar jam užkirstas kelias, nors už tokį pažeidimą pats informacinės visuomenės paslaugos teikėjas neatsako. Bendrosios interneto tarpininkų atsakomybės apribojimo sąlygos šiuo atveju – reiškiant reikalavimus dėl įpareigojimo, kad būtų sustabdytas pažeidimas, vykdomas naudojant informacijos perdavimo paslaugas, ar jam užkirstas kelias – tarpininkams nėra taikomos. Draudimai ir įpareigojimai, kaip teisių gynimo būdas, interneto tarpininkams gali būti taikomi, neatsižvelgiant į tai, ar siekiama traukti juos atsakomybėn, tačiau teismų vaidmuo šiuo atveju turi būti kontrolinis, siekiant užtikrinti, kad draudimais ir įpareigojimais nebūtų piktnaudžiaujama.

Manytina, kad draudimai ir įpareigojimai interneto tarpininkams (kai nėra sąlygų pačių tarpininkų atsakomybei) turėtų būti taikomi tik esant *prima facie* teisių ir teisėtų interesų pažeidimų, ypač sunkiems nusikaltimams ir atvejams, kai kyla pavojus visuomenės saugumui. Draudimų ir įpareigojimų kaip laikinųjų priemonių taikymas nepriimtinas tada, kai nėra aiškių įrodymų, kad interneto ištekliai, dėl kurių kyla konfliktinė situacija, yra neteisėti.

5 skirsnis. Teisiniai interneto domenų vardų aspektai

1. Domeno vardo samprata

Domeno vardas informatikos moksle visų pirma suprantamas kaip interneto adresas ir apibrėžiamas kaip interneto adresų srities simbolinis pavadinimas. Panašus apibrėžimas priimtas ES elektroninės komercijos direktyvoje ir 2002 m. birželio 22 d. Europos Parlamento ir Tarybos reglamento Nr. 733/2002 dėl .eu Aukščiausio lygio domeno įdiegimo. Šis apibrėžimas priimtinas objektyviąja prasme, tačiau jis neprarado jokių subjektyvinių teisių, kurios gali būti susijusios su domeno vardu. Teisiniu požiūriu domenų vardai turi panašumų su intelektinės nuosavybės objektais, prievolinėmis ar net daiktinėmis teisėmis. Teisinis domenų vardų supratimas atspindi jų socialinę vertę ir funkciją, nes šiuo metu domenų vardai atlieka ne tik fizinio adreso, bet ir identifikatoriaus funkciją.

Domeno vardas yra simbolinis *IP* adreso atitikmuo, jis, kaip ir *IP* adresas, nurodo kompiuterio lokaciją internete. *IP* adresas yra išreiškiamas skaitmenimis, kuriuos įsiminti sunku ir nepatogu, todėl *IP* adresų sistema iš esmės pakeičiama simboline ir vartotojams patogia interneto domenų vardų sistema. Pasitelkus *DNS* (angl. *Domain Name System)* serverius, beveik kiekvienas *IP* adresas internete yra susietas su domeno vardu. Įvedus domeno vardą į kompiuterį, *DNS* serveriai jį automatiškai konvertuoja į skaičiais išreikštą *IP* adresą.

Domenų vardus, *IP* adresus, *TCP* duomenų perdavimo protokolą ir kitus bendruosius interneto aspektus administruoja *Internet Corporation for Assigned Names and Numbers (ICANN)* – juridinis asmuo, įsteigtas pagal JAV Kalifornijos valstijos įstatymus.

Domeno vardas turi būti sudarytas bent iš dviejų dalių:

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

Kaip jau minėta, aukščiausio lygio domenų vardai gali būti:

1) rūšiniai arba generiniai (gTLDs); pvz., bendriniai aukščiausiojo lygio domenų vardai yra tokie: „.com“, „.org“, „.net“, „.edu“, „.int“, „.info“, „.biz“ ir kt.;
2) teritoriniai ar regioniniai (ccTLDs). Pasaulyje egzistuoja daugiau kaip 244 šalies kodo aukščiausiojo lygio domenų vardai, kurie suteikti remiantis Tarptautinės standartizacijos organizacijos (ISO)

standartu – 3166. Pavyzdžiui, „.lt“ (Lietuvos kodas), „.pl“ (Lenkijos kodas), „.eu“ (ES regioninis kodas).

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

2. Domeno vardo reikšmė

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

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

- prekės, paslaugos ir (ar) informacijos kilmės (šaltinio) identifikavimo;
- kokybės užtikrinimo.

Kaip jau minėta, domenų vardai gali aiškiai identifikuoti interneto tinklalapio kilmės regioną (šiuo požiūriu jie yra panašūs į geografines nuorodas) ar net konkretų asmenį (įmonę), kuriam priklauso interneto tinklalapis. Kita vertus, būtina pabrėžti, kad ši indikacija nėra vienareikšmė, nes valstybių aukščiausiojo lygio domenus gali registruoti ir užsienio subjektai, pvz., televizijos bendrovėms įvairiose valstybėse registruojami aukščiausiojo lygio domenai „.tv“, kurie priklauso Ramiojo vandenyno salų valstybei Tuvalu. Visais atvejais domenų vardai atskiria skirtingų asmenų e. erdvėje pateikiamą informaciją. Be to, domeno vardas gali tapti ir kokybės simboliu (pvz., „ebay.com“ yra įgijęs patikimiausio ir patogiausio naudoti interneto aukcionų operatoriaus reputaciją; „google.com“ visuotinai laikomas kokybiškiausiu ir išsamiausiu interneto paieškos įrankiu). Kaip jau minėta, domeno vardas dažnai tampa visos įmonės rinkodaros strategijos ašimi ir prekės ženklu.

3. Teisinis domeno vardo statusas

Teisinio domenų vardų statuso klausimas nėra vienareikšmis. Prieš dešimtmetį dėl panašumo į kai kuriuos intelektinės nuosavybes teisių objektus (ypač prekių ženklus) dominavo požiūris į domenų vardus kaip naujai atsirandančius intelektinės nuosavybės teisių objektus. Šiuo metu vis labiau

įsigali nuostatos, kad domenų vardai yra daugiau prievolinio pobūdžio teisės, t. y. sutartimi tarp domeno turėtojo ir jo registratoriaus nustatytos teisės, leidžiančios naudoti domeno vardą, jį valdyti ir juo disponuoti.

Vis dėlto, kaip ir daugelis kitų intelektinės nuosavybės teisių objektų, domenų vardai gali būti originalūs, t. y. iš esmės įmanomas tik vienas tam tikro vardo domenas. Savaime suprantama, kad originalūs domenų vardai, turintys kūrinio požymių, lygiagrečiai gali būti saugomi ir intelektinės nuosavybės teisėmis (pvz., autorių teisėmis). Nors tarp domeno vardo bei intelektinės nuosavybės objektų ir esama tam tikros koreliacijos, akivaizdu, kad domenų vardai nėra tiesiogiai susiję su kūryba ar inovacijomis ir šiems socialiniams procesams nedaro jokios įtakos. Domenų vardai nelaikytini intelektine nuosavybe, nes jie netenkina jokių originalumo ar naujumo reikalavimų ir daugeliu atvejų yra antriniai, t. y. asmens vardo ar pavadinimo, veiklos rūšies ir pan. atkartojimas. Dėl šių priežasčių domeno vardas gali būti laikomas tik kvazi-intelektine nuosavybe (tokia kaip geografinės nuorodos).

Domeno vardo kaip prievolinės teisės statusą apibrėžia jo registracijos sąlygos ir sutartys, sudaromos registruojant domeno vardus. Subjektyvines teises į domeno vardą riboja ir techninės galimybės veikti savarankiškai, nes tiesiogiai nedalyvaujant domenų administratoriui (registratoriui), t. y. tarpininkui, domeno vardas negali funkcionuoti.

Domenų vardai, kaip ir kitos civilinės teisės, gali būti civilinės apyvartos objektas. Gana dažnai jie vertinami nemažomis sumomis, yra perparduodami, nuomojami ar net įkeičiami. Kai kuriose valstybėse (pvz., JAV, Vokietijoje) domenų vardai teisės aktuose aiškiai įvardijami kaip savarankiškas civilinių teisių objektas. Ši nuostata atėjo iš JAV teismų praktikos, kurioje aiškiai pripažinta domenų vardų turtinė vertė, teisės jais disponuoti ir tam tikros pirmenybės teisės juos registruoti. Domeno vardą kaip civilinių teisių objektą įvardija ir *ICANN* (svarbiausios tarptautinės institucijos, reguliuojančios interneto funkcionavimą) Bendrosios domenų vardų ginčų sprendimo taisyklės.

Praktika pripažinti domenų vardus prievolinio pobūdžio civiline teise šiuo metu įsigalėjo daugelyje valstybių, taip pat ir teismų praktikoje. Paminėtina, kad daugelyje valstybių, iš jų ir Lietuvoje, domenų vardai nėra įstatymais reglamentuotos teisės. Jos yra nustatomos išimtinai sutartiniais ir savireguliaciniais (interneto registratorių tarpusavio konkurencijos) instrumentais.

Kaip jau minėta, 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 ar Belgijos teisės aktuose, kuriuose akcentuojama, kad domeno vardas nėra kieno nors nuosavybė, jis niekam nepriklauso – suteikiama tik sąlygiška teisė juo naudotis. Domeno vardo kaip prievolinės teisės supratimas pagrįstas tuo, kad šie vardai visose pasaulio valstybėse yra suteikiami už tam tikrą registracijos mokestį, dar taikomi ir metiniai palaikymo mokesčiai, be to, domeno vardo registratorius turi sutartimis nustatytas teises apriboti domeno naudojimą ar net panaikinti jo registraciją. Kita vertus, galima teigti, kad konkretų domeno vardą (prievolės turinį) yra laisvas rinktis pats pareiškėjas, kuris siekia identifikuoti save internete.

Apibendrinus aukščiau aptartus domeno vardo aspektus, tampa akivaizdu, kad tai yra kompleksinis teisinis institutas. Šio negalima painioti su interneto adresu, nes domeno vardas atlieka ne tik interneto adreso, bet ir kitas funkcijas, būdingas socialiniams žymenims, o ne adresams. Kaip jau minėta, domenų vardai *per se* nelaikytini intelektinės nuosavybės teisių objektu, tačiau minėtosios nuosavybės objektu gali būti originalūs žymenys, kurių pagrindu sudaromi domenų vardai.

4. Domenų vardai Lietuvoje

Interneto domenas „.lt“ įkurtas 1992 metais. Iki 2003 m. Lietuvoje domenų zoną „.lt“ administravo Lietuvos mokslo ir studijų kompiuterių tinklas LITNET, šiuo metu šias funkcijas atlieka KTU Informacinių technologijų plėtros institutas. 2013 m. rugpjūtį buvo sukurta daugiau kaip 158 tūkst. „.lt“ domenų vardų.

Lietuvoje domenų vardai „.lt“ suteikiami pasirašius sutartį su KTU Informacinių technologijų plėtros institutu (šis yra *ICANN* įgaliotasis „.lt“ domenų registratorius), sumokėjus nustatytą registracijos mokestį ir vadovaujantis pirmumo principu, t. y. asmuo, pateikęs paraišką registruoti tam tikrą domeną anksčiau už kitą asmenį, įgyja pirmumo teisę įregistruoti atitinkamą domeną.

Nors formaliai KTU Informacinių technologijų plėtros institutas nereikalauja, jog užsakovas patvirtintų savo teisę naudotis konkrečiu pavadinimu, iš tiesų sekama, kad domenų vardais „.lt“ zonoje nebūtų registruojami Lietuvoje ar užsienyje žinomi prekių ženklai, nesant jų savininkų sutikimo. Sudarydamas sutartį dėl domeno registracijos, asmuo patvirtina, kad jis domeną registruoja žinodamas, jog nepiktnaudžiauja ir nepažeidžia trečiųjų asmenų teisių bei interesų. Visais atvejais KTU Informacinių technologijų plėtros institutas atsiriboja nuo bet kokios atsakomybės tretiesiems asmenims ir visą šią atsakomybę sutartimi perduoda užsakovui.

KTU Informacinių technologijų plėtros instituto ir užsakovo sutartis sudaroma pagal patvirtintą tipinę formą. Minėtojo instituto tipinėje sutar-

tyje pabrėžiama, kad domeno vardas – adresų srities simbolinis pavadinimas – sudaromas vartotojų patogumui; adresų srityje esantys duomenys atitinka tarnybinių stočių *IP* skaitmeninius adresus arba aprašo žemesniojo lygio adresų sritis; adresų sričių simboliniai pavadinimai nusako vartotojo vietą interneto tinkle, todėl jie 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 įsitvirtinęs prievolinis teisių į domeno vardą pobūdis, specialia forma nepripažįstant jo intelektinės nuosavybės teisių.

Be to, KTU Informacinių technologijų plėtros instituto tipinėje sutartyje pabrėžiama, kad domeno vardas – adresų srities simbolinis pavadinimas – yra viešojo pobūdžio, todėl sudaromas atsižvelgiant į moralės normas ir neklaidinant 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 rinktis savo pavardę. Sudarant domenų vardus, nedraudžiama vartoti bendrinių žodžių. Apskritai ribojamas (bet nedraudžiamas) tik dviejų raidžių (ar skaičių) kaip domeno vardo, taip pat informacijos (žymenų), kurių vartojimas ribojamas ar draudžiamas Lietuvos įstatymais, registravimas. Maksimalus adresų srities simbolinio pavadinimo ilgumas – 63 simboliai. 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, turintį specifinių lietuviškos abėcėlės raidžių.

KTU Informacinių technologijų plėtros institutas iš esmės neprisiima jokios atsakomybės, susijusios su domenų vardų registravimu. Šio 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, kad užsakovas pažeidė trečiųjų asmenų teises, gali vienašališkai ne ginčo tvarka apriboti adresų srities naudojimą, kol bus išspręstas ginčas tarp užsakovo ir pretenzijas pareiškusių trečiųjų asmenų. Be to, sprendžiant klausimą dėl adresų sričių simbolinio pavadinimo naudojimo teisėtumo, KTU Informacinių technologijų plėtros institutas nėra ginčo šalis. Užsakovas privalo užtikrinti, kad domeno vardas nebūtų naudojamas kaip įrankis vykdant neteisėtą veiklą. Esant įtarimų dėl neteisėtos veiklos, KTU Informacinių

technologijų plėtros institutas gali vienašališkai įspėti užsakovą apie galimus padarinius, apriboti domeno vardo naudojimą arba išvis nutraukti sutartį. Minėtasis institutas iš esmės neturi nuoseklios teisių į domeno vardą gynimo praktikos ir apskritai vengia veltis į ginčus dėl domenų vardų. Atsižvelgiant į šias priežastis, teisės į domenų vardus Lietuvoje gali būti efektyviai ginamos tik tuo atveju, jeigu jie yra tinkamai įregistruoti kaip prekių ženklai, firmų vardai ar yra originalūs autoriniai kūriniai. Bendrinio pobūdžio domenų vardai iš esmės yra pasisavinami tų asmenų, kurie juos pirmieji įregistravo. Ši praktika Europos valstybėse (ypač Vokietijoje) pamažu pripažįstama nesąžininga, tačiau efektyvios domenų vardų suteikimo pagal paraiškų datos pirmumą alternatyvos kol kas nėra.

5. Ginčai dėl domenų vardų

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

Bendroji ginčų dėl domeno vardų sprendimo politika *(UDRP)* yra ginčų dėl interneto domeno vardo registracijos sprendimo ir intelektinės nuosavybės teisių domenų varduose gynimo internete teisinis pagrindas. *UDRP* taisyklės nustato tiek teisių gynimo procedūras ir tvarką, tiek pažeidėjams taikomą specialią sankciją – domenų vardų kontrolės priverstinį perdavimą, bei šios sankcijos įgyvendinimo tvarką. Šiuo metu *UDRP* taikoma visiems aukščiausiojo lygio domenams: „.aero“, „.asia“, „.biz“, „.cat“, „.com“, „.coop“, „.info“, „.jobs“, „.mobi“, „.museum“, „.name“, „.net“, „.org“, „.pro“, „.tel“ bei „.travel“ ir kai kuriems šalies (nacionaliniams) aukščiausiojo lygio domenams, taip pat ir ES regioniniam domenui „.eu“. 2012 m. gruodžio 1 d. duomenimis, 65 šalių nacionalinių aukščiausiojo lygio domenų *(ccTLDs)* taisyklės yra pagrįstos *UDRP* taisyklėmis ar jų variantu. Sprendžiant ginčus dėl šių domenų varduose esančių prekių ženklų ir asmenvardžių teisių pažeidimų, taikoma *UDRP* taisyklėmis nustatyta procedūra. *UDRP* taisykles ir minėtųjų tarptautinių domenų vardų ginčų procedūrą administruoja Pasaulinės intelektinės nuosavybės organizacijos *(WIPO)* Šalių aukščiausiojo lygio domenų vardų arbitražo ir tarpininkavimo centras *(ccTLDs)*. Ginčus dėl teisių į regioninius ar nacionalinius

domenų vardus gali nagrinėti ir kitos institucijos (iš jų ir nacionalinės), tačiau jos vadovaujasi *UDRP* taisyklėmis ar bent pagrindiniais jų principais, o svarbiausia – taiko efektyvią ir internete veikiančią specialią teisinę priemonę (specialią sankciją) – priverstinį domeno vardo kontrolės perdavimą.

UDRP taisyklės veikia kaip privatinės teisės institutas, iš esmės sutartiniu pagrindu. Kai suinteresuotasis asmuo (registruotojas) kreipiasi dėl domeno vardo registravimo, jis, be abejo, privalo įsipareigoti (tai yra viena iš *UDRP* taisyklių sąlygų), jog jo prašomas registruoti domeno vardas „jokiais būdais nepažeis trečiųjų asmenų teisių", ir sutikti, kad jam būtų taikomos *UDRP* taisyklės, jeigu bet kuris trečiasis asmuo pareikštų pretenziją dėl teisių (taip pat ir intelektinės nuosavybės) pažeidimo. Iš esmės asmuo pats sutinka su minėtosios sankcijos priverstinio taikymo galimybe.

Pabrėžtina, kad *UDRP* išskirtinumas – specifinė tiesioginį poveikį internete turinti sankcija. Visos tradicinės privatinės teisės teisminės sankcijos iš esmės yra nukreiptos į asmenį ar jo turtą. Internete jos labai sunkiai įgyvendinamos dėl prigimtinio interneto globalumo ir ekstrateritorialumo. Tiesiog internetas yra tapęs tariamai savarankiška jurisdikcija, nors įvairios valstybės aktyviai mėgina teisinius santykius, atsirandančius internete, reglamentuoti savo nacionaliniais įstatymais (net ir tais atvejais, kai tradiciniai jurisdikcijos ir taikytinos teisės principai neleistų taikyti nacionalinės teisės). Doktrinoje aiškėja nuomonė, kad internetas turėtų būti savarankiškos teisės – *Lex Informatica* arba *Lex Internetica* – reguliavimo objektas, pagal tarptautinės privatinės ir tarptautinės paprotinės teisės analogiją *(Lex Mercatoria)*. *Lex Informatica* viena iš ryškesnių apraiškų yra būtent domenų vardų sistemos taisyklės, dar nebuvusios kurios nors valstybės nacionalinės teisės reguliavimo objektu. Domenų vardų sistema iki šiol tebėra esminė ir labiausiai centralizuota interneto atraminė dalis, kurią vienašališkai valdo *ICANN* ir sąlygiškai nedaug aukščiausiojo lygio domenų registratorių. *ICANN* yra supranacionalinė organizacija, nepavaldi nacionalinėms vyriausybėms, nors JAV įtaka *ICANN* visada buvo juntama. *ICANN* būstinė yra JAV, ji kaip juridinis asmuo yra įregistruota Kalifornijos valstijoje.

Bendrosios domenų vardų ginčų sprendimo taisyklės iš esmės yra procedūrinis ir neprivalomojo pobūdžio dokumentas. Procedūra yra panaši į arbitražinę, tačiau artimiausia tarpininkavimo procedūroms. Priimtas sprendimas yra neprivalomas, juo nepatenkinta šalis ginčą gali perduoti spręsti kompetentingoms teisminėms institucijoms. Bendrosios domenų vardų ginčų sprendimo taisyklės kildinamos iš domeno vardų registracijos sutarčių nuostatų, vienašališkai įtrauktų į sutartį ir paskelbtų registro tvarkytojo, kuris neturi kito pasirinkimo dėl *ICANN* akreditavimo politikos.

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

Bendrosios domenų vardų ginčų sprendimo taisyklės iš pareiškėjo, siekiančio pagrįsti savo reikalavimą, reikalauja įrodyti tris būtinas aplinkybes:

- atsakovo domeno vardas yra tapatus arba klaidinamai panašus į pareiškėjo žymenį, į kurį pareiškėjas turi oficialias teises;
- atsakovas neturi pagrįstų teisių arba teisėtų interesų į domeno vardą;
- atsakovo domeno vardas buvo registruotas ir nesąžiningai naudojamas pareiškėjo atžvilgiu.

Pagal tipinę KTU Informacinių technologijų plėtros instituto sutartį, ginčai dėl „.lt“ zonos domeno vardo gali būti sprendžiami teismuose, o ne *UDRP* institucijose. Bendrosios domenų vardų ginčų sprendimo taisyklės Lietuvoje iš esmės netaikomos, tačiau jos ir *UDRP* precedentai gali būti pasitelkiami kaip netiesioginis teisės šaltinis sprendžiant ginčus, susijusius su domenų vardais. Siekiant modernizuoti ir suvienodinti praktiką, *UDRP* precedentų taikymas yra skatintinas.

Vadovaudamiesi *UDRP* praktika, Lietuvos teismai, spręsdami ginčus dėl domenų vardų, pradėjo ne tik konstatuoti pažeidimą, bet ir tiesiogiai spręsti domeno perdavimo klausimą tarp bylos šalių, pripažindami, kad ieškovas turi ankstesnes teises į domeno vardą, o atsakovas jį registravo ir veikia nesąžiningai.

Iki 2009 m. Lietuvos teismai atsisakydavo spręsti domeno priverstinio perdavimo klausimą motyvuodami tuo, kad Lietuvos teisėje nėra tokio pažeistų teisių gynimo būdo, tačiau, spręsdami domeno „burgerking.lt“ bylą (bylos Nr. 2-846-553/2008 *Burger King corporation v. SC Burger King SR)*, nusprendė taikyti priverstinį domeno perdavimą. Teismų praktikoje susiformavo pozicija vadovautis „.eu“ Reglamentu Nr. 874/2004.

Apskritai manytina, kad tarptautinės arbitražinės praktikos kaip teisės šaltinio taikymas, sprendžiant ginčus dėl domenų vardų, Lietuvoje yra leistinas ir net skatintinas, nes dėl globalaus interneto pobūdžio tik taip galimas tolygus ir nediskriminacinis teisių gynimas internete.

Naujausia teismų praktika dėl domenų vardų Lietuvoje pripažino, kad teisės į domeno vardą gali būti ginčijamos ir teisių į firmos vardą pagrindu (civilinė byla Nr. 23853585/2010, *UAB „Mano duomenys“ v. UAB „Matrix“)*.

6 skirsnis. Interneto turinio reguliavimas

Nors internete gausu naudingos medžiagos, susiduriama ir su nepageidaujamais dalykais – informacija, darančia žalingą poveikį pažeidžiamoms socialinėms grupėms ar visai visuomenei, taip pat informacija, kurios viešą skelbimą riboja įstatymai arba ji išvis draudžiama. Nevaržomas tokios informacijos platinimas kelia pavojų demokratinėms teisėms ir laisvėms ar net tiesioginę grėsmę visuomenei. Dėl šių priežasčių prireikia interneto turinio reglamentavimo priemonių.

Naujausioje Europos Žmogaus Teisių Teismo (toliau – EŽTT) jurisprudencijoje žmogaus teisė pasiekti informaciją internetu pripažįstama savarankiška teisine vertybe. 2011 m. byloje *Pravoye Delo and Shtekel v. Ukraine* Nr. 33014/05 teismas pripažino, kad „Internetas yra informavimo ir komunikacijos įrankis, kuris turi esminių skirtumų nuo spausdintinės žiniasklaidos, ypač kiek tai susiję su informacijos saugojimo ir perdavimo apimtimi ir masteliu. Elektroninis tinklas, kuriuo naudojasi milijardai vartotojų visame pasaulyje, nėra ir negali būti tokio pat reguliavimo kaip spausdintinė žiniasklaida objektas. Rizikos, kurias kitų žmonių teisėms sukelia interneto turinys ir komunikacija, internete yra ženkliai didesnės nei rizikos, kurias kelia tradicinė spausdintinė žiniasklaida“.

Kita vertus, bet kokia interneto turinio kontrolė kelia akivaizdžių asociacijų su cenzūra, gali riboti žodžio ir išraiškos laisvę, teisę į informaciją ir yra ypač mėgstama nedemokratinėse valstybėse, tokiose kaip Sirija, Saudo Arabija, Šiaurės Korėja ar Baltarusija. Interneto turinio kontrole galima naudotis ir mėginant daryti įtaką visuomenės nuomonei, palaikyti tam tikrą politinę jėgą ir pan.

Paminėtina ir tai, kad interneto turinio reglamentavimas galiausiai susiduria su reguliuotino turinio apibrėžimo problema. Toks turinys skirtingose valstybėse ir kultūrose vertinamas labai nevienodai. Aukščiau minėtasis *Yahoo! Inc. v. La Ligue Contre le Racisme et l'Antisemitisme* konfliktas iš esmės yra nulemtas nevienodo to paties interneto turinio vertinimo.

1. Tarptautinis interneto turinio reguliavimas

Dėl interneto turinio reglamentavimo konfliktiškumo šis klausimas iš esmės nėra reglamentuotas tarptautiniu mastu. Priimta tik regioninio ir rekomendacinio pobūdžio teisės aktų, kuriais siekiama nustatyti interneto turinio reglamentavimo gaires. ES lygiu yra priimta tik keletas su interneto turinio reglamentavimu susijusių rekomendacinių teisės aktų:

– 1996 m. Europos Komisijos komunikatas apie neteisėtą ir žalingą interneto turinį;

- 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 ir kartu kovoti su neteisėtu bei 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);
- Europos Tarybos 2008 m. lapkričio 28 d. bendrasis sprendimas Nr. 2008/913/JHA dėl kovos su tam tikromis rasizmo ir ksenofobijos apraiškomis baudžiamosios teisės priemonėmis.

ES, sprendžiant interneto turinio reguliavimo problemą, daugiausia dėmesio yra skiriama savireguliacijai, akcentuojama, kad interneto turinio reglamentavimas turėtų būti efektyvus, objektyviai pagrįstas ir proporcingas, tinkamai derinant teisinius ir techninius instrumentus.

Vienas svarbiausių interneto turinio reglamentavimo principų – informacinės visuomenės paslaugų teikėjų atsakomybės už interneto turinį apribojimas. Šis principas aiškiai įtvirtintas ES direktyvoje 2000/31/EB dėl elektroninės komercijos ir detaliau nagrinėtas aukščiau.

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

- 1997 m. spalio 30 d. rekomendacija Nr. (97) 20 „Dėl nepakančių pasisakymų“;
- 1997 m. spalio 30 d. rekomendacija Nr. (97) 21 „Dėl smurto rodymo elektroninėje žiniasklaidoje“;
- 2001 m. rugsėjo 5 d. rekomendacija 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. deklaracija „Dėl teisės komunikuoti internetu“;
- 2001 m. lapkričio 23 d. Europos Tarybos konvencija dėl nusikaltimų elektroninėje erdvėje;
- 2002 m. lapkričio 7 d. konvencijos dėl nusikaltimų elektroninėje erdvėje papildomasis protokolas.
- 2007 m. Europos Tarybos konvencija dėl terorizmo prevencijos *(CETS* Nr. 196).

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

2001 m. lapkričio 23 d. Europos Tarybos konvencija dėl nusikaltimų e. erdvėje specialiai reglamentuoja veikas, susijusias su draudžiamu interneto turiniu, konkrečiai – vaikų pornografija. Šiai pornografijos rūšiai priskiriama pornografinė medžiaga, vizualiai vaizduojanti 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, skelbimą 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 papildomas Europos Tarybos konvencijos dėl elektroninių nusikaltimų protokolas. Jame rasinę ir tautinę neapykantą kurstanti informacija apibrėžiama kaip bet koks rašytinis, vizualinis ar kitoks minčių ir teorijų, propaguojančių diskriminaciją ar smurtą prieš individą ar jų grupes, išsiskiriančius dėl savo rasės, tikėjimo, politinių pažiūrų ir pan., pateikimas. Papildomas protokolas įsigaliojo 2006 m. kovą ir iki šiol yra pagrindinis tarptautinis teisės šaltinis, reglamentuojantis neteisėtą interneto turinį.

Reguliuotinu interneto turiniu laikytina ir nepageidaujama komercinė komunikacija (angl. *spam)*, kuri išsamiau aptariama skyriuje apie teisinį elektroninių ryšių reglamentavimą.

2. Bendrieji interneto turinio reguliavimo principai

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

Žalinga ir nepageidaujama yra laikoma informacija, susijusi su turiniu, kuris gali daryti neigiamą poveikį nepilnamečiams ar kitoms jautrioms socialinėms grupėms, pvz., pornografija, erotinio ar smurtinio pobūdžio informacija, duomenys 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, taikymas internete publikuojamai ir tvarkomai informacijai;
- interneto paslaugų teikėjų atsakomybės reglamentavimas;
- savireguliacijos priemonių skatinimas;
- specifinių teisių ir pareigų interneto paslaugų teikėjams nustatymas specialiaisiais norminiais teisės aktais, siekiant užtikrinti veiksmingą nusikaltimų tyrimą, kovą su tarptautiniu terorizmu, efektyvią nacionalinio ir visuomenės saugumo bei kitų interesų apsaugą.

3. Interneto turinio reguliavimas Lietuvoje

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

- 2000 m. rugpjūčio 29 d. Lietuvos Respublikos visuomenės informavimo 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;
- 2010 m. liepos 21 d. Lietuvos Respublikos Vyriausybės nutarimas Nr. 1121 „Dėl neigiamą poveikį nepilnamečių vystymuisi darančios viešosios informacijos žymėjimo ir skleidimo tvarkos aprašo patvirtinimo“.

Minėtieji teisės aktai yra ne kartą keisti ir tobulinti. Vienas svarbiausių Lietuvos Respublikos teisės aktų, reglamentuojančių neskelbtinos ir žalingo turinio informacijos naudojimą, yra Lietuvos Respublikos visuomenės

informavimo įstatymas, kurio 19 str. nurodyta, kad draudžiama skelbti informaciją, kuria:

1) raginama prievarta keisti Lietuvos Respublikos konstitucinę santvarką;
2) skatinama kėsintis į Lietuvos Respublikos suverenitetą, jos teritorijos vientisumą ar politinę nepriklausomybę;
3) kurstomas karas ar neapykanta, tyčiojimasis, niekinimas, raginama 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 skelbiamos 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 ir kliudoma teisminės valdžios nešališkumui.

Viešoji informacija, susijusi su erotiniu, smurtiniu turiniu, alkoholio ar tabako reklama ir vartojimu, kita nepilnamečių fiziniam, protiniam ir doroviniam vystymuisi kenkianti informacija, priskiriama ribojamai viešajai informacijai.

Erotinio pobūdžio informacija įstatyme įvardijama kaip tokia, kuria skatinamas lytinis geismas, rodomas tikras ar suvaidintas lytinis aktas ar kitoks seksualinis pasitenkinimas arba sekso reikmenys. Pornografinio pobūdžio informacijai priskiriama: atviras 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 svarbiausias tokios informacijos tikslas. Smurtinio pobūdžio informacija laikoma: detaliai rodomas žmonių ar gyvūnų žudymas, žalojimas, kankinimas ar kitoks prieš žmogų ir 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 šiais dalykais.

LR visuomenės informavimo įstatyme internetinėmis visuomenės informavimo priemonėmis (informacinės visuomenės informavimo priemonėmis) laikomos visos informavimo priemonės, dažniausiai už tam tikrą

atlygį elektroniniu būdu per atstumą individualiu vartotojo prašymu teikiančios informaciją. Lietuvos Respublikos Vyriausybės 2003 m. kovo 5 d. nutarimu Nr. 250 patvirtintoje viešojo 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, platinama įprastu būdu, nesvarbu, ar į interneto tinklalapį būtų perkeliamas visas turinys, ar tik jo dalis. Elektronines visuomenės informavimo priemones įstatymų nustatyta tvarka gali kurti ir kiti fiziniai bei juridiniai asmenys, pageidaujantys vykdyti arba faktiškai vykdantys visuomenės informavimo veiklą viešojo naudojimo kompiuterių tinkluose. Elektroninėmis visuomenės informavimo priemonėmis nelaikomi valstybės institucijų ir įstaigų, valstybės pareigūnų ir valstybės tarnautojų (darbuotojų) interneto tinklalapiai, skirti oficialiems dokumentams ir informacijai apie valstybės institucijos darbą platinti, bei asmenų privatūs interneto tinklalapiai, į kuriuos dedama informacija apie pačius 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 pateikiama neskelbtina ar ribojama informacija, lieka neprižiūrimi.

Viešojo naudojimo kompiuterių tinkluose neskelbtinos informacijos kontrolės ir ribojamos viešosios informacijos platinimo tvarkos 5 punktas draudžia viešojo naudojimo kompiuterių tinkluose viešinti ir platinti neskelbtiną ar žalingo turinio informaciją, nustatytą Lietuvos Respublikos įstatymais.

Be to, pagal šią tvarką, neskelbtiną ar ribojamą viešąją informaciją draudžiama laikyti laisvai prieinamą Lietuvos Respublikos teritorijoje esančiose tarnybinėse stotyse, skleisti per elektronines konferencijas, neapibrėžtam gavėjų skaičiui siųsti elektroniniu paštu arba kaip nors kitaip platinti viešojo naudojimo kompiuterių tinkluose, kai ribojama viešoji informacija gali tapti laisvai prieinama nepilnamečiams. Prie interneto tinklalapiuose pateikiamos ribojamos viešosios informacijos turėtų būti pridėtas įspėjamasis užrašas lietuvių ir anglų kalbomis, kad minėtoji informacija skiriama tik pilnamečiams, ir laikomasi kitų 2010 m. liepos 21 d. Lietuvos Respublikos Vyriausybės nutarimu Nr. 1121 patvirtinto Neigiamą poveikį nepilnamečių vystymuisi darančios viešosios informacijos žymėjimo ir skleidimo tvarkos aprašo nustatytų sąlygų.

Viešojo 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, ir asmenų, kuriems informacijos prieglobos paslaugų teikėjas teikia nuolatines paslaugas, duomenis.

Pagrindinis Lietuvos Respublikos vaiko teisių apsaugos ir Lietuvos Respublikos nepilnamečių apsaugos nuo neigiamo viešosios informacijos poveikio įstatymų principas – apsauga nuo neigiamos socialinės aplinkos įtakos. Pagal šį įstatymą, neigiamą poveikį nepilnamečiams darančia informacija laikoma tokia viešoji informacija, kuri gali būti žalinga nepilnamečių psichinei ar fizinei sveikatai, fiziniam, protiniam, dvasiniam ar doroviniam vystymuisi.

Lietuvos Respublikos nepilnamečių apsaugos nuo neigiamo viešosios informacijos poveikio įstatymo 4 str. nurodoma informacija, kuri turi būti draudžiama arba ribojama.

Neigiamą poveikį nepilnamečiams darančiai priskiriama ši viešoji informacija:

1) smurtinio pobūdžio, kurstanti agresyvumą ir nepagarbą gyvybei;
2) skatinanti turto naikinimą ar gadinimą;
3) stambiu planu rodomas mirusio, mirštančio arba žiauriai sužaloto žmogaus kūnas, išskyrus atvejus, kai tai reikalinga asmens tapatybei nustatyti;
4) erotinio pobūdžio;
5) kelianti baimę ar siaubą;
6) skatinanti lošti, raginanti ar siūlanti dalyvauti azartiniuose lošimuose ir kituose žaidimuose, kai sudaromas lengvo laimėjimo įspūdis;
7) palankiai vertinanti priklausomybę nuo narkotinių, toksinių, psichotropinių medžiagų, tabako ar alkoholio ir nuo kitų medžiagų, kurios vartojamos arba gali būti vartojamos svaiginimosi tikslams, ir kuria skatinamas jų vartojimas, gamyba, platinimas ar įsigijimas;
8) skatinanti savęs žalojimą ar savižudybę, detalizuojanti savižudybės priemones ir aplinkybes;
9) teigiamai vertinanti nusikalstamą veiką ar idealizuojanti nusikaltėlius;
10) susijusi su nusikalstamos veikos modeliavimu;
11) skatinanti žmogaus orumą žeminantį elgesį;

12) kai tyčiojamasi iš žmogaus ar žmonių grupės arba žmogus ar žmonių grupė niekinami dėl tautybės, rasės, lyties, kilmės, neįgalumo, seksualinės orientacijos, socialinės padėties, kalbos, tikėjimo, įsitikinimų, pažiūrų ar kitais panašiais pagrindais;
13) demonstruojanti inscenizuotus paranormalius reiškinius, kai sudaromas jų tikrumo įspūdis;
14) skatinanti nepilnamečių seksualinę prievartą ir jų išnaudojimą, nepilnamečių lytinius santykius;
15) skatinanti lytinius santykius;
16) niekinanti šeimos vertybes, skatinanti kitokią, negu Lietuvos Respublikos Konstitucijoje ir CK įtvirtinta, santuokos sudarymo ir šeimos kūrimo sampratą;
17) kai vartojami nešvankūs posakiai, žodžiai ar nepadorūs gestai;
18) patarianti, kaip pasigaminti sprogmenų, narkotinių ar psichotropinių medžiagų ir kitų gyvybei ar sveikatai pavojingų dalykų, jų įsigyti ar juos naudoti;
19) skatinanti blogus mitybos, higienos ir fizinio pasyvumo įpročius;
20) demonstruojanti masinės hipnozės seansus, kurių poveikio objektas yra visuomenės informavimo priemonės auditorija;
21) kai pateikiami asmens duomenys, susiję su nepilnamečiu asmeniu.

Pagal Lietuvos Respublikos nepilnamečių apsaugos nuo neigiamo viešosios informacijos poveikio įstatymo 6 str., neigiamą poveikį nepilnamečio vystymuisi darančia ir draudžiama taip pat laikoma viešoji informacija (detalizuojant aukščiau minėtą (21) punktą), kuria:

1) siejant su nusikalstama veika ar kitais teisės pažeidimais, skelbiami nuo teisėsaugos institucijų ar teismo nesislapstančio įtariamojo padarius nusikalstamą veiką, kaltinamojo, nuteistojo ar nuo nusikalstamos veikos arba kitų teisės pažeidimų nukentėjusio nepilnamečio (aukos) asmens duomenys, pagal kuriuos galima nustatyti jo asmens tapatybę;
2) skelbiami susižalojusio ar mėginusio tai padaryti, nusižudžiusio ar mėginusio nusižudyti nepilnamečio asmens duomenys, pagal kuriuos galima nustatyti jo asmens tapatybę;
3) apie nepilnametį pateikiami duomenys žemina jo orumą ir (ar) pažeidžia jo interesus;
4) piktnaudžiaujant nepilnamečių pasitikėjimu ir nepatyrimu, neigiamų socialinių reiškinių kontekste pateikiamos jų nuomonės ir vertinimai;

5) neigiamų socialinių reiškinių kontekste rodomos nepilnamečių nuotraukos ar filmuota medžiaga apie juos, jeigu pagal tai galima nustatyti jų asmens tapatybę.

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 labai išsamiai neapibrėžia, kokio turinio informacijos skelbimas turėtų būti ribojamas ar draudžiamas. Nepakankamai apibrėžta lieka erotinio pobūdžio, baimę ar siaubą kelianti, taip pat alkoholio ar tabako gaminių vartojimą skatinanti ir kita informacija. Dėl tokio neapibrėžtumo gana dažnai kyla teisnių ginčų.

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 ar sveikatai, jo konstitucinėms teisėms) ir tarnybos paslapčių (politinių, ekonominių, karinių, teisėtvarkos, mokslo ir technikos duomenų, kurių platinimas ribojamas dėl valstybės bei jos institucijų interesų, ir siekiant apsaugoti žmogaus konstitucines teises) apsaugą. Pagal šio įstatymo 7 str., 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 minėtosios informacijos apsaugą ir užtikrinti, kad visi asmenys, susiję su neskelbtinos informacijos apsauga, turėtų atitinkamus leidimus su ja dirbti ar susipažinti.

Lietuvoje už minėtaisiais įstatymais nustatytos tvarkos pažeidimą (įskaitant ir šios tvarkos pažeidimą interneto aplinkoje) atsakomybę nustato Lietuvos Respublikos administracinių teisės pažeidimų kodeksas (toliau – ATPK), Baudžiamasis kodeksas (toliau – BK) ir CK.

ATPK 214 str. nustatyta 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 vaizdo filmų, radijo ir televizijos programų platinimo tvarkos pažeidimą. Tačiau šiuo atveju nieko nekalbama apie atsakomybę už tokio pat turinio informacijos platinimą internete. Į šios normos sritį realiai patenka tik internete platinami erotinio bei smurtinio pobūdžio kino ir vaizdo filmai.

ATPK 214^4 str. nustato atsakomybę už informacijos apie tabako gaminius ir alkoholinius gėrimus teikimo tvarkos pažeidimą, 214^6 straipsnis – už Respublikos Prezidento įžeidimą arba šmeižimą, naudojantis masinės informacijos priemonėmis, 214^8 straipsnis – už įstatymais uždraustos reklamos ir informacijos, įstatymais uždraustos ar neteisėtos veiklos reklamos ir informacijos apie šią veiklą arba prekių ar paslaugų, kurių gamyba ir pardavimas yra įstatymų uždrausti, reklamos skleidimas, naudojantis visuomenės informavimo priemonėmis.

BK 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;
4) mažamečio asmens tvirkinimo veiksmus;
5) tikrovės neatitinkančios informacijos apie kitą žmogų, galinčios paniekinti ar pažeminti tą asmenį arba pakirsti pasitikėjimą juo, skleidimą;
6) įžeidimą;
7) neteisėtą informacijos apie asmens privatų gyvenimą atskleidimą ar naudojimą;
8) nuteikinėjimą prieš bet kokios tautos, rasės, etninę, religinę ar kitokią žmonių grupę;
9) skatinimą vartoti narkotines ar psichotropines medžiagas;
10) pornografinio turinio produkcijos gaminimą, platinimą ar viešą demonstravimą. Atsakomybė už šių veikų vykdymą, atsižvelgiant į nusikaltimo ar nusižengimo pobūdį, svyruoja nuo baudos iki laisvės atėmimo.

4. Interneto turinio reguliavimo perspektyvos

Analizuojant esamas teisines interneto turinio reguliavimo priemones, akivaizdu, kad praktinis informacijos turinio reguliavimo priemonių taikymas ypač sudėtingas dėl reguliuotino turinio neapibrėžtumo ir subjektyvių kriterijų, kuriais remiantis išskiriamas žalingas ir nepageidaujamas interneto turinys. Aptartasis *Yahoo! Inc. v. La Ligue Contre le Racisme et l'Antisemitisme* atvejis rodo nevienareikšmį šių kriterijų vertinimą. Atkreiptinas dėmesys ir į tai, kad priverstinis ir visa apimantis interneto turinio reguliavimas neįmanomas nei teisiškai, nei techniškai, be to, yra sunkiai suderinamas su pamatinėmis demokratinėmis vertybėmis. Daugelyje valstybių interneto turinio reguliavimas iš esmės yra savanoriškas, pagrįstas savireguliacija ir įgyvendinamas techninėmis priemonėmis – specialiaisiais interneto turinio filtrais. Deja, tokios techninės priemonės – filtruojanti programinė įranga – nėra tobulos: atsižvelgiant į jų naudojimo kontekstą ir tikslus, reikalauja adaptacijų, atsijoja dalį pageidaujamo interneto turinio ir tuo pat metu neidentifikuoja dalies nepageidaujamojo.

Apskritai interneto turinio reguliavimas yra naujas dalykas ir jis ne visada nuoseklus. Šiuo metu Lietuvoje kaip vyriausybinio reguliavimo alternatyva menkai pripažįstamas savireguliavimas, arba jis išvis neveikia. Kita vertus, dauguma Lietuvos interneto paslaugų teikėjų naudoja individualius interneto turinio reguliavimo mechanizmus, veiksmingai reaguoja į pranešimus apie neteisėtą ir žalingą interneto turinį.

Vyrauja tendencija, kad tradicinėms visuomenės informavimo priemonėms taikomas normas mėginama pasitelkti ir internetui, o tai ne visada įmanoma. Kita vertus, reikia pripažinti, kad veiksmingos ir visaapimančios interneto turinio reguliavimo teisinės ar techninės priemonės šiuo metu dar nėra sukurtos.

Interneto turinio reguliavimas iš esmės remiasi techninėmis galimybėmis jį kontroliuoti. Šios techninės galimybės naudojamos filtruojant interneto srautą arba blokuojant tam tikrus jo išteklius. Esant decentralizuotai interneto infrastruktūrai, turimos technologijos neleidžia užtikrinti nei filtravimo, nei blokavimo, kai neteisėtas ar žalingas interneto turinys priklauso ne interneto tarpininko tinklui. Kitais žodžiais tariant, išties neįmanoma užblokuoti turinio ar išteklių, kurie yra už valstybės nacionalinės jurisdikcijos ribų (užsienyje). Be to, filtravimo ir blokavimo priemonės stabdo ir sunkina visą interneto infrastruktūrą, mažina jos greitaveiką ir patikimumą, o jų išlaidos yra perkeliamos paprastiems interneto vartotojams. Dar reikėtų pabrėžti, kad filtravimo ir blokavimo priemonės neišvengiamai užblokuoja dali pozityvios informacijos, kurios pateikimas yra pageidautinas

(pvz., pornografinės informacijos filtrai dažnai atmeta informaciją, susijusią su saugiais lytiniais santykiais, lytiniu būdu plintančių ligų ir nėštumo prevencija).

Interneto filtravimas ir blokavimas gali būti individualizuotas tik galiniuose įrenginiuose, t. y. paties vartotojo kompiuteryje. Jį įgyvendinant interneto tarpininkų lygmeniu, šios priemonės savaime būtų taikomos neapibrėžtam subjektų kiekiui – bet kuriam asmeniui, neatsižvelgiant į tai, ar jo veiksmai išvis galėtų būti susiję su reguliuojama informacija ar ištekliu. Taigi filtravimo ir blokavimo priemonės bus naudojamos bei sukels neigiamų padarinių asmenims, nuo kurių išvis nepriklauso reguliuojama informacija ir ištekliai. Tokia padėtis akivaizdžiai prieštarautų konstituciniam proporcingumo principui.

Be to, filtravimo ir blokavimo priemonės internete kelia klausimų dėl informacijos laisvės suvaržymo. Konstitucinė informacijos laisvė yra neatsiejama nuo konstitucinių įsitikinimų ir jų raiškos laisvės, yra jos sąlyga. Informacijos laisvė yra vienas iš atviros, teisingos ir darnios pilietinės visuomenės, demokratinės valstybės pagrindų, nes asmuo gali visavertiškai įgyvendinti daugelį savo konstitucinių teisių ir laisvių tik turėdamas laisvę nekliudomai ieškoti ar gauti informacijos ir ją skleisti.

ESTT 2011 m. bylose *Scarlet Extended* C-70/10 ir *Netlog* C-360/10 nagrinėjo, ar įpareigojimai interneto paslaugų teikėjams blokuoti ir filtruoti informaciją bei interneto išteklius yra suderinami su žmogaus teisėmis. Abiejose minėtosiose bylose ESTT nustatė labai griežtus reikalavimus, kada gali būti naudojamos blokavimo ir filtravimo priemonės. Šios priemonės laikytinos neproporcingomis ir neleistinomis, jeigu:

- filtruojama visa per interneto tinklą keliaujanti elektroninė komunikacija, įskaitant ir komunikacijos srautą, susijusį su *P2P* programomis;
- jeigu ji taikoma visiems vartotojams, neišskiriant tam tikrų grupių;
- jeigu filtravimas nustatytas kaip laikinoji apsaugos priemonė;
- jeigu interneto paslaugų teikėjai filtravimą turi atlikti tik savo sąskaita;
- jeigu jis yra neribojamas laiko atžvilgiu.

Lygiagrečiai su minėtąja ESTT praktika vis daugiau valstybių pripažįsta žmogaus teisę nevaržomai gauti informacijos internetu. Tarptautinės ir nevyriausybinės žmogaus teisių organizacijos pabrėžia vadinamąjį tinklo neutralumą, vadinasi, internetas turi būti skaidrus perduodamo turinio atžvilgiu ir negali tapti nacionalinių valstybių nacionalinės kontrolės įkaitu. Kaip jau minėta, tarptautiniu lygiu nesama bendro sutarimo dėl didelės

dalies interneto turinio teisinio vertinimo – tai, kas vienose valstybėse yra draudžiama ar nepageidaujama, kitose yra priimtina ir teisėta. Dėl šių priežasčių visos interneto turinio kontrolės priemonės turėtų būti vertinamos ypač atsargiai, kad būtų užtikrinamas visų subjektų žmogaus teisių ir laisvių, bendrųjų visuomenės interesų ir vertybių balansas.

Žinių įtvirtinimo klausimai

1. Kokius klausimus reglamentuoja interneto teisė?
2. Ar galime tradicines jurisdikcijos taisykles taikyti internetui?
3. Kuo pagrįsti siūlymai taikyti *sui generis* interneto teisę?
4. Kas yra interneto neutralumas (tinklo neutralumas)?
5. Kokios Briuselio ir Lugano konvencijų normos aktualios sprendžiant interneto jurisdikcijos klausimus?
6. Paaiškinkite kilmės šalies principą pagal ES direktyvą 2000/31/EB dėl elektroninės komercijos?
7. Kokios kilmės šalies principo išimtys nustatytos ES direktyvoje 2000/31/EB dėl elektroninės komercijos?
8. Kaip reglamentuojama interneto tarpininkų veikla?
9. Kodėl interneto tarpininkams nenustatoma pareiga tikrinti ir kontroliuoti jų tinklais perduodamos ir jų serveriuose laikomos informacijos turinio?
10. Kokios sąlygos keliamos interneto tarpininkams, kad jiems nereikėtų atsakyti už jų tinklais perduodamą ir jų serveriuose laikomą elektroninį turinį?
11. Kokios sąlygos taikytinos prieš nustatant draudimus ir įpareigojimus interneto tarpininkams?
12. Koks yra teisinis interneto domenų vardų statusas?
13. Kokie teisės aktai reglamentuoja domenų vardų išdavimą Lietuvoje?
14. Kaip reglamentuojamas interneto turinys?
15. Kokios interneto turinio kategorijos yra laikomos draudžiamomis, o kokios – ribojamomis?
16. Kokiais argumentais remiantis gali būti nustatoma žmogaus teisė nevaržomai gauti informacijos internetu?

/II/ *skyrius*

Teisinis elektroninių ryšių reguliavimas

/ 83–110 / *puslapiai*

1 skirsnis. Elektroninių ryšių samprata

Elektroninių ryšių koncepcijai svarbiausiais laikytini du elementai: tinklai ir paslaugos. *Elektroninių ryšių tinklas* pagal Lietuvos Respublikos elektroninių ryšių įstatymą apibrėžiamas kaip perdavimo sistemos ir (arba) komutavimo bei maršruto parinkimo įranga, kitos priemonės, įskaitant pasyviuosius tinklo elementus, leidžiančios perduoti signalus laidinėmis, radijo, optinėmis ar kitomis elektromagnetinėmis priemonėmis, įskaitant palydovinius tinklus, fiksuotuosius (kanalų ir paketų komutavimo, įskaitant internetą) ir judriuosius antžeminius tinklus, elektros perdavimo kabelines sistemas (kiek jos naudojamos signalams perduoti), tinklus, naudojamus radijo ir (arba) televizijos programoms transliuoti (retransliuoti), ir kabelinės televizijos bei mikrobangų daugiakanalės televizijos tinklus, neatsižvelgiant į perduodamos informacijos pobūdį. Tuo metu *elektroninių ryšių paslauga* pagal tą patį įstatymą apibrėžiama kaip paprastai už atlygį teikiama paslauga, kurią visiškai ar daugiausia sudaro signalų perdavimas elektroninių ryšių tinklais, įskaitant telekomunikacijų paslaugas ir perdavimo (siuntimo) paslaugas transliacijai (retransliacijai) naudojamais tinklais. Elektroninių ryšių paslaugos neapima elektroninių ryšių tinklais ar naudojant elektroninių ryšių paslaugas perduodamos informacijos turinio teikimo ar redakcinės turinio kontrolės paslaugų, tarp jų informacinės visuomenės paslaugų, kurių visiškai ar daugiausia nesudaro signalų perdavimas elektroninių ryšių tinklais.

Kaip labiausiai paplitusių elektroninių ryšių paslaugų pavyzdžius galima paminėti telefonijos ir interneto paslaugas. Dar labai populiarus duomenų perdavimas. Pastaruoju metu šios paslaugos konverguoja, tad galutiniam klientui ir (ar) vartotojui tampa svarbi prieiga prie elektroninių ryšių. Tokios prieigos svarbą rodo ir tai, kad pastaraisiais metais teisė į internetą vis dažniau įvardijama kaip viena svarbiausių žmogaus teisių. Autoriai P. De Hertas ir D. Kloza, atlikę tyrimą dėl teisės į internetą pripažinimo ir teisinio reguliavimo, priėjo prie išvados, kad argumentų už tokios teisės įvardijimą yra daugiau nei prieš.

Elektroniniai ryšiai laikomi vienu iš dinamiškiausių ir sparčiausiai besiplėtojančių sektorių. Minėtasis sektorius yra svarbus ne tik dėl savo ekonominio potencialo, bet ir dėl to, kad suteikia galimybę žmonėms bendrauti, t. y. atlieka tam tikrą socialinę funkciją. Pastaruoju metu didžiuliais tempais plinta vadinamosios *OTT* paslaugos (angl. *Over-the-top)* – tai internetu teikiamos garso, vaizdo ir kitos paslaugos, kai jų nekontroliuoja tradiciniai elektroninių ryšių operatoriai. Šios paslaugos kelia labai didelę konkurenciją tradicinėms elektroninių ryšių paslaugoms.

Labai svarbus yra elektroninių ryšių reguliavimo institutas. Visas šių ryšių reguliavimas grindžiamas efektyvios konkurencijos skatinimu bei vartotojams ir (ar) paslaugų gavėjams teikiama nauda.

2 skirsnis. Elektroninių ryšių kaitos ir teisinio reguliavimo raida

Šis skirsnis nėra skirtas visiems telekomunikacijų ir elektroninių ryšių raidos bei teisinio reguliavimo etapams aprašyti, tik siekiama suteikti daugiau aiškumo, kaip ir kodėl susiklostė dabartinė elektroninių ryšių bei su jais susijusio teisinio reguliavimo padėtis.

Iki 1980 m. viskas buvo gana paprasta. Tuo metu elektroninių ryšių sektorius buvo vadinamas telekomunikacijų sektoriumi ir buvo skirtas tam tikriems viešosios politikos tikslams pasiekti – užtikrinti universaliųjų paslaugų teikimą. Tam dažniausiai buvo naudojamas valstybės valdomas telekomunikacijų operatorius, įsteigtas tam tikroje valstybėje. Telekomunikacijų rinkos buvo nacionalinės, o viešai teikiamos paslaugos – gana ribotos (dažniausiai balso telefonijos paslaugos). To meto tradicinis sektorinis reguliavimas beveik neskyrė infrastruktūros, galinių įrenginių ir paslaugų. Taigi visa ši veikla buvo tradicinių monopolijų rankose. Kadangi monopolininko žinioje buvo ir infrastruktūra, vienintelė šių monopolinių paslaugų alternatyva – teikti paslaugas patiems, o tai galėjo daryti tik labai stambūs telekomunikacijų klientai ir už ypač dideles pinigų sumas. Iš esmės visi istoriniai operatoriai turėjo išimtinių teisių, ir toks modelis buvo grindžiamas vartotojų teisių apsauga nuo neigiamų natūralios monopolijos padarinių, todėl nemažai teisės normų (pvz., dėl konkurencijos ir kt.) nė nebuvo taikomos.

Vėliau prasidėjo telekomunikacijų sektoriaus transformacija. Keliama keletas versijų, kodėl tai įvyko. Viena iš jų – telekomunikacijų sektoriaus transformaciją paskatino perėjimas prie informacija paremtos ekonomikos, tai lėmė didelę plėtrą ir priklausymą nuo telekomunikacijos priemonių kaip tarpininkų, perduodant elektroninę informaciją. Todėl šiandien vietoj senųjų telekomunikacijų turime sudėtingą elektroninių ryšių ir interneto infrastruktūrą.

Elektroninių ryšių dinamika ir technologijų plėtra dar vadinamos konvergencijos procesais. Technologinės evoliucijos kontekste terminas „konvergencija“ reiškia, kad viena technologija apima visas turinio formas. Galiausiai ryškėja tendencija, kad skirtingų tipų tinklų atskirtis mažėja ir atsiranda vadinamoji viena didelė terpė (angl. *One Big Medium).*

Telekomunikacijų teisinio reguliavimo padėtis ėmė keistis, kai tam tikros valstybės (pirmoji buvo Jungtinė Karalystė) pradėjo telekomunikacijų demonopolizavimo procesą. Į tai reagavo Europos Komisija, kuri ėmėsi iniciatyvos atverti šio sektoriaus duris konkurencijos principais pagrįstai struktūrai ar struktūroms: 1987 m. Europos Komisija paskelbė žaliąjį dokumentą COM(87) 290 *final*, kuriame, be kitų priemonių, buvo pasiūlyta į telekomunikacijų rinkas įvesti konkurenciją, t. y. liberalizuoti atitinkamas telekomunikacijų rinkas.

Pirmosios Europos Komisijos direktyvos buvo susijusios su išimtinių teisių panaikinimu – tai direktyvos EEC 88/301 (dėl konkurencijos telekomunikacijų galinių įrenginių rinkoje), EEC 90/388 (dėl konkurencijos telekomunikacijų paslaugų rinkoje) bei EC 96/19 (dėl visiškos konkurencijos įgyvendinimo telekomunikacijų rinkose). Tačiau laikui bėgant ES lygmeniu buvo priimta vis daugiau teisės aktų, skirtų problemoms, kurių kilo rinkoms transformuojantis iš monopolinių į pagrįstas konkurencijos santykiais, spręsti.

3 skirsnis. ES elektroninių ryšių reguliavimo sistema

Per pirmąjį liberalizavimo etapą priimti ES teisės aktai vadinami senąja (arba 1998 m.) ES reguliavimo sistema. Juose daugiausia dėmesio buvo skiriama sektoriaus pertvarkai, tačiau šiems teisės aktams atlikus savo funkciją ir elektroninių ryšių rinkose įvykus didelių pokyčių reguliavimo sistema buvo gerokai pertvarkyta.

2002 m. ES buvo priimtas naujas elektroninių ryšių (telekomunikacijų direktyvų paketas). Naująją ES elektroninių ryšių (telekomunikacijų) veiklos reguliavimo sistemą sudarė šie teisės aktai:

- 2002 m. kovo 7 d. Europos Parlamento ir Tarybos direktyva 2002/21/EB dėl bendros elektroninių ryšių tinklų ir paslaugų reguliavimo sistemos (Bendroji direktyva);
- 2002 m. kovo 7 d. Europos Parlamento ir Tarybos direktyva 2002/20/EB dėl elektroninių ryšių tinklų ir paslaugų leidimo (Leidimo direktyva);
- 2002 m. kovo 7 d. Europos Parlamento ir Tarybos direktyva 2002/19/EB dėl elektroninių tinklų ir su jais susijusių priemonių sujungimo ir prieigos prie jų (Prieigos direktyva);
- 2002 m. kovo 7 d. Europos Parlamento ir Tarybos direktyva 2002/22/EB dėl universaliųjų paslaugų ir paslaugų gavėjų teisių, susijusių su elektroninių ryšių tinklais ir paslaugomis (Universaliųjų paslaugų direktyva);

– 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privataus gyvenimo apsaugos elektroninių ryšių sektoriuje (Privatumo ir elektroninių ryšių direktyva);
– 2002 m. rugsėjo 16 d. Komisijos direktyva 2002/77/EB dėl konkurencijos elektroninių ryšių tinklų ir paslaugų rinkose.
– Svarbiausi reguliavimo tikslai, iškelti 2002 m. ES elektroninių ryšių (telekomunikacijų) veiklos reguliavimo sistemai, buvo šie:
– skatinti atvirą ir konkurencingą Europos ryšių paslaugų rinką, siekiant užtikrinti, jog vartotojams ir verslui, atsižvelgiant į paslaugų gavėjų poreikius ir siūlant įvairių naujų paslaugų, būtų sąlygos sudaryti kuo geresnį kainos, kokybės ir pinigų vertės požiūriu sandorį, kad sudėtingoje ir konverguotoje rinkoje nebūtų iškraipoma konkurencija;
– užtikrinti, kad Europos piliečiai galėtų naudotis universaliosiomis (nustatytomis ES) ir informacinės visuomenės paslaugomis; apsaugoti vartotojų teises, kai sudaromi sandoriai su teikėjais, ypač suteikiant jiems paprastų ir nebrangių ginčų sprendimo procedūrų galimybę; užtikrinti kuo geresnę asmens duomenų ir privatumo apsaugą, nustatyti kuo aiškesnius tarifus ir sudaryti geresnes naudojimosi ryšių paslaugomis sąlygas; daugiau dėmesio skirti specifinių socialinių grupių (ypač neįgaliųjų ir vyresnio amžiaus asmenų) specialiesiems poreikiams;
– vienyti vidinę rinką konverguojančioje aplinkoje – panaikinti kliūtis teikti ryšių tinklus ir paslaugas Europoje taip, kad tomis pačiomis aplinkybėmis panašūs operatoriai būtų vertinami vienodai, neatsižvelgiant į tai, kur ES jie veiktų, ir užtikrinti efektyvų ribotų išteklių (ypač radijo spektro) valdymą, skatinti europinių tinklų steigimą ir plėtrą, vientisą europinių paslaugų tarpusavio sąveiką.

2002 m. ES elektroninių ryšių (telekomunikacijų) veiklos reguliavimo sistema buvo pagrįsta šiais penkiais svarbiausiais principais:

1) aiškiai nustatyti politiniai reguliavimo pagrindimo tikslai, skatinantys ekonominę plėtrą ir konkurencingumą (kartu ir darbo vietų steigimą) bei užtikrinantys visuomenės tikslų, nepasiekiamų rinkos jėgomis, įgyvendinimą;
2) minimalus būtinas reguliavimas – panaikinti galiojančios reguliavimo sistemos įpareigojimus, kurie nebūtini mechanizmams, leidžiantiems sumažinti tolesnį reguliavimą, kai tikslai gali būti pasiekti konkurencijos priemonėmis, kurti;

3) teisinis tikrumas kintant rinkai: reguliavimas turėtų būti stabilus, kad bendrovės neabejodamos galėtų priimti investicinius sprendimus, bet kartu ir lankstus – reikėtų atsižvelgti į rinkos plėtrą. Turi būti stiprinamos nacionalinės institucijos, kad būtų nepriklausomos ir efektyviai dirbtų – tinkamai taikytų pirmiau išdėstytą modelį ir laiku priimtų aiškius sprendimus;
4) technologinis neutralumas: reguliavimas negali nei skatinti naudoti kokią nors specifinę technologiją, nei tam trukdyti, tik užtikrinti, kad ta pati paslauga būtų vienodai reguliuojama, neatsižvelgiant į priemones, kuriomis ji teikiama. Pavyzdžiui, 1998 m. ES telekomunikacijų veiklos reguliavimo sistemoje nustatytos skirtingos paslaugų teikimo fiksuoto ir judriojo ryšio tinklais taisyklės. Lietuvos Respublikoje irgi priimtos skirtingos radijo dažnių skirstymo telekomunikacijų veiklai ir transliacijai taisyklės. Konvergencija suteikia galimybių tą pačią paslaugą teikti atskirais tinklais, taigi ta pati paslauga skirtingai reguliuojama. Dėl šių priežasčių siekiama, kad reguliavimas kuo mažiau priklausytų nuo technologijų, kuriomis naudojantis teikiamos paslaugos, nes kitoks reguliavimas greitai pasentų. Tačiau tai nereiškia, kad visa ryšių infrastruktūra turi būti vienodai reguliuojama – pvz., bevielių tinklų paslaugoms svarbios dažnių skyrimo ir naudojimo taisyklės, o laidinių tinklų paslaugoms taikomos teisės normos, reglamentuojančios tinklų tiesimą ir gatvių kasimą. Taigi paslaugų teikimas turėtų būti vienodai reguliuojamas ir nepriklausyti nuo to, kaip jos teikiamos. Pavyzdžiui, atliekant konkurencijos tyrimus, gali pasitaikyti atvejų, kai atskiri tinklai atitinkamai sudarys skirtingas rinkas ir reikės imtis specifinių tinklų ar technologinių produktų reguliavimo priemonių. Bet kuriuo atveju technologinio neutralumo principas negali būti taikomas siekiant bet kuriai rinkai nustatyti griežtesnes taisykles;
5) dėl reguliavimo gali būti susitariama pasauliniu, regioniniu ar nacionaliniu lygiu, bet jis taikomas (kiek praktiškai įmanoma) kuo arčiau reguliuojamos veiklos.

Palyginti su 1998 m. ES telekomunikacijų veiklos reguliavimo sistema, naujoji ES elektroninių ryšių (telekomunikacijų) veiklos reguliavimo sistema įvedė šias svarbiausias naujoves ir ekonomines investuotojų teises:

– nustatė vienodą ir technologiškai neutralų visos elektroninių ryšių, ne tik telekomunikacijų, veiklos reguliavimą. Naujoji sistema taikoma telekomunikacijų (fiksuotojo ir judriojo ryšio), palydoviniams, kabelinės televizijos ir antžeminiams transliavimo tinklams, prieigą prie paslaugų kontroliuojančioms priemonėms, pvz., taikomųjų

programų sąsajoms, šiais tinklais teikiamoms ryšio paslaugoms (telekomunikacijų ir kitoms) ir paslaugoms, susijusioms su autorizuota galimybe naudotis tinklais ir paslaugomis. Sąvoka „elektroniniai ryšiai“, be telekomunikacijų, apėmė ir technologinę informacijos turinio perdavimo dalį tinklais, skirtais transliacijai ir retransliacijai, – apimties požiūriu tai didžiausias naujosios reguliavimo sistemos skirtumas nuo 1998 metų. Minėtoji sistema netaikoma transliavimo ir informacinės visuomenės paslaugoms, teikiamoms per ryšių infrastruktūrą. Kadangi būtina atskirti perdavimo ir turinio reguliavimą, 2002 m. kovo 7 d. Europos Parlamento ir Tarybos direktyvoje 2002/21/EB dėl bendros elektroninių ryšių tinklų ir paslaugų reguliavimo sistemos (Bendroji direktyva) nurodoma, kad reguliavimo sistema neapima paslaugų, teikiamų elektroninių ryšių tinklais, pvz., turinio transliavimo, finansinių ir konkrečių informacinės visuomenės paslaugų, todėl neprieštarauja priemonėms, naudojamoms Bendrijos ar nacionaliniu lygiu, kiek tai neprieštarauja Bendrijos teisei, kad būtų skatinamas kultūrinis ir kalbinis skirtingumas bei užtikrinama žiniasklaidos pliuralizmo apsauga;

– įtvirtino technologinio neutralumo principą, iš esmės panaikindama judriojo ir fiksuotojo telefono ryšio tinklų bei paslaugų reguliavimo skirtumus, ir daugiau dėmesio skyrė dominuojančių (didelę įtaką rinkoje turinčių) bei tokios įtakos neturinčių operatorių skirtumams, taip pat užtikrino tinkamą, vienodą konverguotų telekomunikacijų, kompiuterių ir žiniasklaidos sričių reguliavimą. 2002 m. kovo 7 d. Europos Parlamento ir Tarybos direktyvoje 2002/21/EB dėl bendrosios elektroninių ryšių tinklų ir paslaugų reguliavimo sistemos (Bendroji direktyva) iš valstybių narių reikalaujama užtikrinti, kad nacionalinės reguliavimo institucijos ypač atsižvelgtų į technologiškai neutralaus reguliavimo būtinybę, t. y. tokia institucija neturėtų nei skatinti naudoti konkrečios technologijos, nei tam trukdyti, tačiau nedraudžiama proporcingai plėtoti tam tikras paslaugas, kai šitai yra pagrįsta: pvz., skaitmeninės televizijos – spektro naudojimo efektyvumą didinančios priemonės plėtrą;
– lengviau suteikia teisę verstis elektroninių ryšių (telekomunikacijų) veikla, panaikindama nereikalingus įėjimo į rinką trukdžius – individualių licencijų ir bendrųjų leidimų sistemą pakeisdama bendrųjų leidimų sistema (t. y. norminių teisės aktų, nustatančių bendrąsias vertimosi elektroninių ryšių veikla, nuostatomis, atsisakant išankstinių leidimų), tačiau palikdama telefono ryšio numerių ir radijo dažnių skyrimo sistemą;

– numatė lankstesnio reguliavimo galimybę, nustatydama mechanizmus, kurie leidžia mažinti reguliavimą, kai konkurencija rinkoje tampa efektyvesnė;
– iš esmės pakeitė efektyvios konkurencijos užtikrinimo doktriną, ankstesnę paprastesnę didelės įtakos rinkoje sampratą (kai valdomi 25 proc. atitinkamos rinkos) pakeisdama konkurencijos teisėje nustatyta dominavimo samprata;
– įtvirtino galimybę perkelti telefono ryšio numerius judriojo telefono ryšio tinkluose (1998 m. ES telekomunikacijų veiklos reguliavimo sistemoje tai nustatyta tik fiksuotojo telefono ryšiui).

Tačiau nuo 2002 m. praėjus keletui metų, buvo konstatuota, kad šioje dinamiškoje elektroninių ryšių rinkoje įvyko nemažai pokyčių, tad prireikė iš naujo įvertinti kai kuriuos reguliavimo aspektus. Dėl to 2009 m. lapkritį Ministrų taryba vienbalsiai patvirtino ES elektroninių ryšių reguliavimo reformos priemonių paketą, kurį 2007 m. pasiūlė Europos Komisija.

2009 m. lapkričio 25 d. buvo priimta Europos Parlamento ir Tarybos direktyva 2009/136/EB, iš dalies keičianti Direktyvą 2002/22/EB dėl universaliųjų paslaugų ir paslaugų gavėjų teisių, susijusių su elektroninių ryšių tinklais ir paslaugomis, ir Europos Parlamento, ir Tarybos direktyva 2009/140/EB, iš dalies keičianti Direktyvą 2002/21/EB dėl elektroninių ryšių tinklų ir paslaugų bendrosios reguliavimo sistemos, keičianti Direktyvą 2002/19/EB dėl elektroninių ryšių tinklų ir susijusių priemonių sujungimo ir prieigos prie jų ir Direktyvą 2002/20/EB dėl elektroninių ryšių tinklų ir paslaugų leidimo.

Toliau pateikiama apibendrinta informacija apie dešimt svarbiausių naujojo ES telekomunikacijų reguliavimo priemonių paketo pakeitimų:

1) **Europos vartotojų teisė per vieną darbo dieną pakeisti fiksuotojo arba mobiliojo ryšio operatorių, išlaikant senąjį telefono numerį, ir kitos sutarčių nuostatos**

Įgyvendinus naująjį paketą, elektroninių ryšių paslaugų teikėjams bus nustatyta pareiga per vieną darbo dieną savo telefono numerį perkelti kitam paslaugų teikėjui. Naujosios taisyklės dar papildomai numato, kad maksimalus pradinis sutarties su vartotoju terminas negalės būti ilgesnis nei dvidešimt keturi mėnesiai. Be to, operatoriai privalės vartotojams suteikti galimybę pasirašyti sutartis maksimaliam dvylikos mėnesių terminui.

2) **Išsamesnė informacija vartotojui**

Pagal naująsias taisykles, vartotojams turės būti suteikiama išsamesnės informacijos, kokias paslaugas jie užsisako, ir ypač pabrėžiama, ką jie gali ir ko negali daryti jomis naudodamiesi. Paslaugų teikėjai sutartyse su

vartotojais, be kitų klausimų, turės numatyti minimalius paslaugos kokybės parametrus ir kompensavimo mechanizmą, jeigu šių parametrų nebus laikomasi.

3) **Asmenų teisė gauti interneto paslaugas**

Pagal naująsias nuostatas dėl interneto laisvės, bet kokie paslaugos teikėjo veiksmai, darantys įtaką interneto paslaugų teikimo kokybei, turi atitikti žmogaus teises ir laisves, kaip numatyta Žmogaus teisių ir pagrindinių laisvių konvencijoje ir bendruosiuose ES teisės principuose. Šios priemonės atitinkamai turėtų būti taikomos ir demokratinei visuomenei. Be to, jos dar turi atitikti nekaltumo prezumpciją ir teisės į privatumą apsaugą. Kitaip tariant, remiantis naujosiomis nuostatomis, pažeidimo atveju interneto prieiga vartotojui gali būti užblokuota tik remiantis nustatyta procedūra, atitinkančia aukščiau nurodytus dokumentus ir principus.

4) **Naujos atviro ir dar neutralesnio tinklo (angl. *net neutrality)* garantijos**

Teigiama, kad nesant akivaizdžios naudos srauto valdymas gali neigiamai veikti paslaugos vartotojus, pvz., paslaugos teikėjas gali suprastinti paslaugos kokybę iki vartotojams nepriimtino lygio. Dėl to nacionalinės reguliavimo institucijos įgyja teisę elektroninių ryšių paslaugoms kelti minimalius kokybės reikalavimus. Sudarant sutartis pagal skaidrumo įpareigojimus, vartotojai dar papildomai turės būti informuojami apie naudojamas srauto valdymo technologijas ir jų įtaką paslaugų kokybei bei kitus apribojimus (pvz., galimą prisijungimo greitį).

5) **Vartotojų apsauga nuo neteisėtų duomenų pažeidimų ir brukalo (spamo)**

Manoma, kad svarbūs asmens duomenys (pvz., el. pašto adresas, banko sąskaitos numeris ir kt.) turi būti ypač gerai apsaugoti, ir operatoriai yra atsakingi už netinkamą tokios informacijos apdorojimą. Todėl naujosios nuostatos įveda privalomą informavimą apie asmens duomenų pažeidimus. Tai reiškia, kad elektroninių ryšių paslaugų teikėjai bus priversti institucijas ir vartotojus informuoti apie saugumo pažeidimus, darančius įtaką jų asmens duomenims.

6) **Geresnis ryšys su pagalbos tarnybomis numeriu 112**

Naujosiomis nuostatomis siekiama užtikrinti, kad vartotojams būtų suteikiama geresnė prieiga prie pagalbos paslaugų, keliant didesnius reikalavimus naujoms technologijoms, kuriomis teikiamos telefonijos paslaugos (pvz., *IP* telefonija), kartu įpareigojant paslaugų teikėjus atitinkamoms pagalbos institucijoms perduoti duomenis apie abonento buvimo vietą.

7) **Nacionaliniai reguliatoriai įgis daugiau nepriklausomybės**

Pagal naująsias taisykles, bus užtikrinama didesnė nacionalinių reguliavimo institucijų nepriklausomybė, kiek įmanoma pašalinant politinės įtakos galimybę ir panaikinant teisę savavališkai atleisti reguliavimo institucijos vadovą.

8) **Nauja Europos elektroninių ryšių agentūra**

2010 m. sukurta nauja Europos elektroninių ryšių agentūra BEREC (angl. *Body of European Regulators for Electronic Communications)*. Institucijai, be kitų įpareigojimų, bus priskirtos šios svarbiausios funkcijos:

- bendrosios pozicijos dėl nacionalinių reguliatorių bendradarbiavimo (pvz., keičiantis informacija) formavimas;
- rinkų tyrimo, analizės ir priemonių taikymo priežiūra;
- tarptautinių rinkų *(VoIP* technologijos pagrindu ir kitų) apibrėžimas;
- patarimai radijo dažnių suderinimo klausimais;
- sprendimo teisė administruojant numeraciją, patarimai dėl numerio portabilumo ir kt.

9) **Nauja Komisijos teisė dėl konkurencinių priemonių nustatymo elektroninių ryšių rinkoms**

Naujosios taisyklės suteiks Europos Komisijai teisę peržiūrėti nacionalinių reguliatorių pasiūlytas reguliavimo priemones (pvz., dėl prisijungimo prie *SMP* operatoriaus tinklo sąlygų arba dėl fiksuotojo ar mobiliojo ryšio operatorių skambučių baigimo kainų). Jeigu Europos Komisija, vertindama siūlomas reguliavimo priemones, įžvelgs bendrosios reguliavimo praktikos prieštaravimų ar kitų neatitikimų, iš nacionalinio reguliatoriaus galės pareikalauti pakeisti planuojamąsias priemones arba išvis jų atsisakyti. Naujosios taisyklės Europos Komisijai suteiks teisę imtis derinimo priemonių, kurios galės pasireikšti rekomendacijų ar privalomų sprendimų forma.

10) **Funkcinis atskyrimas**

Kilus konkurencijos problemų, nacionaliniams reguliatoriams suteikiama teisė taikyti funkcinio atskyrimo priemonę (kaip išimtinę priemonę, prižiūrint Europos Komisijai), kuri reiškia ūkio subjekto veiklos rūšių atskyrimą (atskiriant tinklus nuo paslaugų), jas išskiriant į atskirą verslo vienetą. Šis įpareigojimas turėtų būti taikomas tik tuo atveju, kai neveikia kiti įpareigojimai.

2009 m. direktyvų paketas į ES valstybių nacionalinę teisę turėjo būti perkeltas iki 2011 m. gegužės 25 d., t. y. per aštuoniolika mėnesių. Kai kurios valstybės vėlavo perkelti šių direktyvų nuostatas į nacionalinę teisę, tačiau 2012 m. liepą (praėjus metams nuo galutinio perkėlimo termino)

dauguma valstybių notifikavo, kad direktyvos visiškai perkeltos į nacionalinę teisę. Vis dėlto teigiama, kad dėl nacionalinių ypatybių direktyvos į nacionalinę teisę buvo perkeltos skirtingai.

Po 2009 m. reformos iki 2015 m., kiek tai susiję su teisiniu direktyvų reguliavimu, elektroninių ryšių reguliavimo srityje esminių pokyčių neįvyko. Tačiau ši sritis ypač dinamiška, todėl į joje kintančią padėtį reaguojama pasitelkiant įvairias rekomendacijas. Pavyzdžiui, 2013 m. rugsėjo 11 d. Europos Komisija priėmė rekomendaciją dėl nuoseklaus nediskriminavimo įpareigojimų ir sąnaudų apskaičiavimo metodikų, skirtų konkurencijai skatinti ir geresnei investicijų į plačiajuostį ryšį aplinkai sukurti, taikymo (2013/466/ES). Pagal rekomendaciją, viena didžiausių kliūčių, siekiant užtikrinti vienodas prieigos prie elektroninių ryšių tinklų sąlygas, – kainų ir su jomis nesusijusi diskriminacija (pvz., diskriminacija dėl paslaugų kokybės ir galimybės gauti informacijos, delsimo taktika, nepagrįsti reikalavimai ir strateginis svarbiausių produkto charakteristikų projektavimas) taikant lengvatinį režimą mažmeninėms įmonėms, pvz., didelę įtaką rinkoje turinčio vertikaliosios integracijos operatoriaus (DIR operatoriaus) mažmeninės prekybos padaliniui. Šiuo atžvilgiu labai sunku nustatyti su kainomis nesusijusio diskriminavimo atvejus ir su tokiu diskriminavimu susijusius klausimus spręsti taikant vien bendrąjį nediskriminavimo įpareigojimą. Todėl iš esmės svarbu užtikrinti vienodas prieigos sąlygas, griežtai taikant nediskriminavimo įpareigojimus ir imantis veiksmingų reikalavimų, stebėjimo ir užtikrinimo priemonių. Bene pagrindinis rekomendacijoje nustatytas įrankis – indėlio lygiavertiškumas (angl. *equivalence of inputs, EoI)*, kuris Europos Komisijos laikomas tinkamiausiu veiksmingos apsaugos nuo diskriminavimo būdu, nes norintys gauti prieigą subjektai su vertikaliosios integracijos DIR operatoriaus mažmeniniu verslo padaliniu galės konkuruoti naudodamiesi tuo pačiu reguliuojamųjų didmeninių produktų rinkiniu už tas pačias kainas ir taikydami tuos pačius sandorių procesus. Tiek teoriškai, tiek praktiškai nuomonės dėl *EoI* nesutampa.

2015 m. birželio 6 d. Europos Komisija patvirtino komunikatą COM(2015) 192 „Europos bendrosios skaitmeninės rinkos strategija“. Šis komunikatas daugiausia skirtas bendrosios skaitmeninės rinkos plėtrai ir tokiems klausimams kaip prieiga prie skaitmeninio turinio, geografinis blokavimas, tarpvalstybinės e. prekybos taisyklės spręsti. Be šių klausimų, komunikate užsimenama ir apie telekomunikacijų taisyklių koregavimą. Jame nurodoma, kad Komisija 2016 m. pateiks siūlymų dėl didelio užmojo telekomunikacijų reguliavimo sistemos pertvarkymo, sutelkdama dėmesį į šiuos dalykus: i) bendrajai rinkai būdingą nuoseklų santykį su spektro politika ir valdymu, ii) tikros bendrosios rinkos sąlygų sudarymą, sprendžiant

reguliavimo susiskaidymo problemą, kad galėtų būti sukurta masto ekonomija veiksmingai dirbantiems tinklų operatoriams ir paslaugų teikėjams bei užtikrinta efektyvi vartotojų apsauga, iii) vienodų sąlygų rinkos dalyviams užtikrinimą ir nuoseklų taisyklių taikymą, iv) investicijų į sparčiojo plačiajuosčio ryšio tinklus skatinimą (įskaitant Universaliųjų paslaugų direktyvos persvarstymą) ir v) efektyvesnę reguliavimo institucijų sistemą.

Vis dėlto viena iš svarbiausių 2015 m. priimtų iniciatyvų – naujasis 2015 m. lapkričio 25 d. Reglamentas (angl. *Telecom single market regulation (TSM)*, kurio visas pavadinimas: Europos Parlamento ir Tarybos reglamentas (ES) 2015/2120, kuriuo nustatomos priemonės, susijusios su atvira interneto prieiga, ir kuriuo iš dalies keičiami Direktyva 2002/22/EB dėl universaliųjų paslaugų ir paslaugų gavėjų teisių, susijusių su elektroninių ryšių tinklais ir paslaugomis, ir Reglamentas (ES) Nr. 531/2012 dėl tarptinklinio ryšio per viešuosius judriojo ryšio tinklus ES.

Šiuo reglamentu nustatomos bendrosios taisyklės, kad teikiant interneto prieigos paslaugas srauto atžvilgiu būtų užtikrintos vienodos ir nediskriminuojančios sąlygos bei kitos susijusios galutinių paslaugų gavėjų teisės. Minėtajame reglamente dar nustatomas naujasis ES lygiu reguliuojamų tarptinklinio ryšio paslaugų mažmeninių kainų nustatymo mechanizmas, siekiant panaikinti mažmeninėms tarptinklinio ryšio paslaugoms taikomus papildomus mokesčius, neiškraipant savosios ir lankomos šalies rinkų.

Naujuoju Reglamentu nustatytos taisyklės dėl tinklų neutralumo[14]. Juo detaliai reglamentuojama, kad „interneto prieigos paslaugų teikėjai teikdami interneto prieigos paslaugas visam srautui taiko vienodas sąlygas be diskriminavimo, apribojimų ar kišimosi, neatsižvelgiant į tai, kas yra siuntėjas ir gavėjas, koks yra prieinamas ar skleidžiamas turinys, kokios taikomosios programos ar paslaugos yra naudojamos ar teikiamos arba kokie galiniai įrenginiai yra naudojami“. Tačiau ši taisyklė nėra absoliuti, nes nesant tam tikro būtino ir pagrįsto srauto valdymo ar ribojimo internetu teikiamos paslaugos gali sutrikti. Todėl Reglamentas įveda ir tam tikrų išimčių, pvz., „neužkertamas kelias interneto prieigos paslaugų teikėjams diegti pagrįstas srauto valdymo priemones. Kad tokios priemonės būtų laikomos pagrįstomis, jos turi būti skaidrios, nediskriminacinės, proporcingos ir turi būti grindžiamos ne komerciniais sumetimais, o objektyviai skirtingais specifinėms srauto kategorijoms taikomais paslaugų techninės kokybės

[14] Pagrindinė taisyklė – interneto srautas turi būti traktuojamas vienodai. Ši taisyklė iš esmės taikytina siekiant užkirsti kelią internetu teikiamų paslaugų (kai tradiciniai operatoriai už tai negauna jokio užmokesčio) apribojimams. Tokios paslaugos gali būti susijusios su pokalbiais (pvz., *Skype)*, televizija (pvz., *Netflix)* ir kt.

reikalavimais. Tokiomis priemonėmis neturi būti stebimas konkretus turinys, ir jos neturi būti taikomos ilgiau, nei būtina.“

Be to, reglamentas įveda nuostatas dėl tarptinklinio ryšio paslaugų kainų. Tokių nuostatų tikslas – veiksmingai mažinti ir galutinai panaikinti tarptinklinio ryšio tarifus ES. Kartu nustatomas ir pereinamasis laikotarpis, kuris leis tarptinklinio ryšio paslaugas ES lygiu įtraukti į įvairiose vidaus rinkose siūlomus vidaus tarifų planus kaip neatskiriamą jų dalį. Nuo 2017 m. birželio vartotojai, keliaudami po ES, už pokalbius, *SMS* ir duomenis turės mokėti ne didesnę kainą nei savo valstybėje.

Šis reglamentas yra tiesiogiai taikomas. Jis įsigaliojo trečią dieną po to, kai buvo publikuotas ES oficialiame žurnale, t. y. nuo 2015 m. lapkričio 29 dienos.

Viena iš naujausių teisinio reguliavimo problemų – *OTT* operatoriai, kurie teikia paslaugas, naudodamiesi kitų operatorių sukurta ir palaikoma elektroninių ryšių infrastruktūra. Ypač stipri *OTT* operatorių konkurencija juntama telefonijos srityje. *Skype* ir kitos programos duoda naudos vartotojams, tačiau mažina tradicinių operatorių pajamas. Pavyzdžiui, galima bendrauti mobiliuoju telefonu, tačiau pokalbiai tokiomis programomis tradicinių operatorių yra neapskaitomi, vartotojas moka tik už duomenų kiekį (jeigu duomenys apskritai apmokestinami). Šis verslo modelis daro nemažą įtaką tradicinių operatorių veiklai – perskirsto atitinkamų rinkų dalis, todėl svarstoma, galbūt reikėtų reguliuoti ir pačius *OTT* „žaidėjus“. Vis dėlto naujausiose ES iniciatyvose *OTT* kol kas tiesiogiai neplanuojama to daryti.

4 skirsnis. Pagrindiniai ES elektroninių ryšių reguliavimo institutai

1. Teisė verstis elektroninių ryšių veikla

Leidimą verstis elektroninių ryšių veikla imta reguliuoti pradėjus sektoriaus demonopolizavimą. Iš pradžių ES valstybės narės visiškai savarankiškai reguliavo leidimo verstis elektroninių ryšių veikla klausimus, todėl ilgą laiką toks reguliavimas buvo skirtingas. Kai kuriose valstybėse buvo taikomos sudėtingos licencijavimo procedūros, kurios nesiderino su sektoriaus dinamiškumu. Diskusijos dėl paprastesnės licencijavimo sistemos įvedimo prasidėjo 1999 metais. 2002 m., priėmus direktyvų paketą, viena iš jų buvo 2002 m. kovo 7 d. Europos Parlamento ir Tarybos direktyva 2002/20/EB dėl elektroninių ryšių tinklų ir paslaugų leidimo (Leidimų direktyva).

Viena iš svarbiausių Leidimų direktyvoje įtvirtintų reguliavimo naujovių – ES valstybės narės įpareigotos leisti verstis elektroninių ryšių

veikla pagal bendruosius leidimus ir negali taikyti licencijavimo elektroninių ryšių veiklai. Į Leidimų direktyvą buvo įvesta sąvoka, „bendrasis leidimas“ – pagal šią direktyvą sukurta valstybių narių teisinė sistema, užtikrinanti teises teikti elektroninių ryšių tinklus ar paslaugas ir šiam sektoriui nustatanti specifinių įpareigojimų, kurie gali būti taikomi visiems arba tik tam tikro tipo elektroninių ryšių tinklams ir paslaugoms. Vadinasi, daugiausia, ko galima reikalauti iš elektroninių ryšių paslaugas ar tinklus pradedančio teikti ūkio subjekto – pateikti pranešimą atitinkamai institucijai.

Remiantis Leidimų direktyva, buvo numatyta: galima reikalauti, kad prieš pradėdama naudotis teisėmis pagal leidimą įmonė apie tai praneštų, tačiau negalima reikalauti, kad ji gautų atskirą nacionalinės reguliavimo institucijos sprendimą ar kokį nors kitą administracinį aktą. Šitaip buvo panaikinti bet kokie formalūs apribojimai pradėti verstis elektroninių ryšių veikla ir šios veiklos reguliavimas buvo atskirtas nuo elektroninių ryšių išteklių teikimo procedūrų.

2. Elektroninių ryšių reguliavimo institucijos

Gana svarbu apžvelgti ir elektroninių ryšių reguliavimo institucijų sistemą. Pagrindinė šios srities reguliavimo institucija ES – Nacionalinė reguliavimo institucija (angl. *National regulatory authority, NRA)*. Šios institucijos funkcijas Lietuvoje atlieka Lietuvos Respublikos ryšių reguliavimo tarnyba.

Gali kilti klausimas, kodėl reikalinga elektroninių ryšių reguliavimo institucija, kai atitinkama rinka yra demonopolizuojama? Elektroninių ryšių rinkai būtų galima taikyti *ex-post* reguliavimą ir pavesti konkurenciją prižiūrinčiai institucijai atlikti konkurencijos priežiūrą. Tačiau tokia priežiūra elektroninių ryšių rinkoje būtų gerokai pavėluota, nes *ex-post* reguliavimas taikomas padariniams. Todėl buvo nuspręsta taikyti *ex-ante* reguliavimą ir tai pavesti daryti savarankiškai elektroninių ryšių reguliavimo institucijai. Nurodoma, kad liberalizuojant elektroninių ryšių sektorių nė vienoje pasaulio šalyje dar nebuvo sukurta tokių konkurencingų elektroninių ryšių rinkų, kad joms tvarkyti užtektų bendrojo konkurencijos reguliavimo.

Nacionalinių elektroninių ryšių reguliavimo institucijų institutas reglamentuojamas 2002 m. kovo 7 d. Europos Parlamento ir Tarybos direktyvoje dėl elektroninių ryšių tinklų ir paslaugų bendrosios reguliavimo sistemos (Pagrindų direktyva). Pagal šios direktyvos 3 str. 1 d., valstybės narės užtikrina, kad visas užduotis, kurios šioje direktyvoje ir specifinėse direktyvose priskiriamos nacionalinėms reguliavimo institucijoms, vykdytų kompetentinga institucija.

Išskirtinos šios nacionalinių elektroninių ryšių reguliavimo institucijų savybės:

1) *nepriklausomumas* – valstybės narės garantuoja nacionalinių reguliavimo institucijų savarankiškumą užtikrindamos, kad jos teisiškai būtų atskirtos ir funkciškai nepriklausomos nuo visų organizacijų, teikiančių elektroninių ryšių tinklus, įrangą ir paslaugas. Valstybės narės, kurioms nuosavybės teise priklauso ar yra pavaldžios įmonės, teikiančios elektroninių ryšių tinklus ar paslaugas, užtikrina, kad reguliavimo funkcija būtų veiksmingai atskirta nuo veiklos, susijusios su nuosavybės teise ir valdymu;
2) *nešališkumas ir skaidrumas* – Valstybės narės užtikrina, kad nacionalinės reguliavimo institucijos nešališkai ir skaidriai vykdytų savo įgaliojimus;
3) *bendradarbiavimas* – nacionalinės reguliavimo institucijos ir nacionalinės konkurencijos institucijos viena kitai teikia informaciją, būtiną šios direktyvos ir specifinių direktyvų nuostatoms taikyti.

Aukščiau buvo aptartos nacionalinės elektroninių ryšių reguliavimo institucijos. Tačiau svarbu paminėti ir naują instituciją *BEREC* (angl. *Body of European Regulators of Electronic Communications)*, kuri buvo įkurta 2009 m., įvykdžius elektroninių ryšių reguliavimo reformą. BEREC buvo įkurta Reglamento Nr. 1211/2009 pagrindu ir pakeitė Europos reguliatorių grupę (angl. *European Regulators Group; ERG)*, kuri kaip patariamoji buvo įkurta 2002 m. prie Europos Komisijos.

BEREC savo veiklą pradėjo 2010 m., o visapusiškai ėmė funkcionuoti 2011 metais. Svarbiausia *BEREC* biuro, esančio Rygoje, veikla – teikti būtiną ekspertinę ir administracinę pagalbą ES valstybėms narėms ir institucijoms, taip pat sisteminti, skleisti bei rinkti informaciją apie naujausias įgyvendintas rinkos reguliavimo priemones, teisinio reglamentavimo pasikeitimus, elektroninių ryšių rinkų tendencijas iš visų dvidešimt septynių *BEREC* instituciją sudarančių ES nacionalinių elektroninių ryšių reguliavimo institucijų.

3. Didelės įtakos rinkoje koncepcija

Pagal didelės įtakos rinkoje koncepciją, įtvirtintą Pagrindų direktyvos 14 str. 2 d., manoma, kad įmonė daro didelę įtaką rinkai, jeigu jos vienos ar bendrai su kitomis įmonėmis padėtis prilygsta dominuojančiai, t. y. ji turi tokią ekonominę galią, kuri jai leidžia būti gana nepriklausomai nuo konkurentų, klientų ir galiausiai – vartotojų. Rinkos tyrimo ir didelės įtakos nustatymo gairėse (70 punkte) teigiama, kad didelės įtakos rinkoje

apibrėžimas buvo įtvirtintas ESTT bylose, aiškinančiose dominuojančios padėties nustatymą pagal EB steigimo sutarties 82 straipsnį.

Turinčiu didelę galią atitinkamoje elektroninių ryšių rinkoje ūkio subjektas tampa tada, kai nacionalinė elektroninių ryšių reguliavimo institucija jį pripažįsta darančiu didelę įtaką. Tvirtinama, kad elektroninių ryšių atveju didelė įtaka rinkoje nustatoma *ex-ante* (orientuota į ateitį), bet ne *ex-post* (orientuota į praeitį) tikslams.

Iš esmės didelės įtakos režimo algoritmą galima apibrėžti keturiais laipteliais:

1) Europos Komisija priima rekomendaciją, kuri pagal konkurencijos teisės principus apibrėžia atitinkamas elektroninių ryšių sektoriaus rinkas ir nustato charakteristikas, kurios pateisina *ex-ante* reguliavimą ir atitinkamus įpareigojimus;
2) pagal ES rinkų rekomendaciją ir Komisijos *SMP* gaires, nacionalinės elektroninių ryšių reguliavimo institucijos, atsižvelgdamos į nacionalinę padėtį, apibrėžia atitinkamas tam tikros geografinės teritorijos rinkas. Nacionalinė reguliavimo institucija gali nukrypti nuo Europos Komisijos rekomendacijų dėl rinkų ir apibrėžti kitą rinką;
3) nacionalinės reguliavimo institucijos analizuoja atitinkamas rinkas ir tiria, ar jose egzistuoja efektyvi konkurencija, kitaip tariant, aiškinasi, ar tam tikroje rinkoje veikia vienas ar daugiau *SMP* operatorių;
4) turint omenyje, kad atitinkama elektroninių ryšių rinka yra nekonkurencinga, *SMP* operatoriui taikomi įpareigojimai (pvz., prieigos, skaidrumo, kainų kontrolės ar kt.). Jeigu rinkoje nustatoma efektyvi konkurencija, nacionalinė reguliavimo institucija atitinkamai turi panaikinti patvirtintus įpareigojimus.

Minėtasis procesas vykdomas periodiškai, kad reguliavimo priemonės atitiktų tikrąją rinkos padėtį. Tokia procedūra bus atliekama iki to laiko, kol Europos Komisija nutars, kad *ex-ante* reguliavimas jau nebetikslingas.

Labai svarbu šiame kontekste paminėti Europos Komisijos rekomendaciją dėl elektroninių ryšių rinkų. Joje pateiktu reguliuotinų rinkų sąrašu rekomenduotina vadovautis nacionalinėms reguliavimo institucijoms, tiriant atitinkamas rinkas. Šiuo metu galioja antroji rekomendacijos versija, patvirtinta 2007 metais. Joje, palyginti su prieš tai galiojusiąja, gerokai sutrumpintas reguliuotinų mažmeninių rinkų sąrašas, o daugiausia dėmesio skiriama didmeninėms rinkoms. Remiantis šia rekomendacija, pateikiamas toks rekomenduotinų rinkų sąrašas:

Mažmeninis lygmuo

1. Prieiga, suteikiama klientams – gyventojams ir kitiems klientams, ne gyventojams, prie viešojo telefono tinklo fiksuotoje vietoje.

Didmeninis lygmuo

2. Iškvietos siuntimas viešuoju fiksuotojo telefono ryšio tinklu fiksuotoje vietoje.
3. Iškvietos gavimas atskiruose viešuosiuose telefono ryšio tinkluose fiksuotoje vietoje.
4. Didmeninė (fizinė) tinklo infrastruktūros prieiga (įskaitant bendrąją ar visiškai atsietą prieigą) fiksuotoje vietoje.
5. Didmeninė plačiajuostė prieiga.
6. Didmeniniai skirtųjų linijų baigiamieji segmentai, neatsižvelgiant į technologiją, naudojamą skirtiesiems ar specialiesiems pajėgumams teikti.
7. Balso iškvietų gavimas atskiruose mobiliojo ryšio tinkluose.

Paminėtina ir vadinamoji 7 str. procedūra, kuri priskiriama vienam iš pagrindinių reguliavimo instrumentų. Remiantis 2002/21/EC direktyvos 7 str., yra nustatytas konsultacijų ir notifikavimo mechanizmas, pagal kurį nacionalinės reguliavimo institucijos, siekdamos spręsti konkurencijos atitinkamose rinkose problemas, turi informuoti Europos Komisiją apie planuojamas naudoti priemones. Tokiu atveju Europos Komisija per mėnesį turi įvertinti minėtąsias priemones ir paskui arba jas patvirtinti, arba pateikti komentarų. Ji net gali reikalauti atsisakyti planuojamos priemonės.

4. Universaliosios paslaugos, paslaugų gavėjų ir vartotojų teisės

Universaliųjų paslaugų pradininke laikoma JAV. Europoje minėtųjų paslaugų institutas atsirado gerokai vėliau, kartu su telekomunikacijų sektoriaus liberalizavimu. Šis institutas ES plėtojosi nuo nacionalinio požiūrio iki savarankiškos universaliųjų paslaugų direktyvos.

Universaliųjų paslaugų koncepcijos esmė – tam tikro elektroninių ryšių paslaugų, atitinkančių minimalius reikalavimus, rinkinio teikimas visiems vartotojams (neatsižvelgiant į jų geografinę vietovę) už prieinamą kainą. Universaliosios paslaugos ES teisės požiūriu yra tarsi reguliuojanti „gelbėjimosi liemenė“, liberalizuotos rinkos sąlygomis visiems gyventojams garantuojanti prieigą prie minimaliai būtinų elektroninių ryšių paslaugų.

Pagal ES universaliųjų paslaugų direktyvą 2002/22/EB išskirtinos šios universaliosios paslaugos:

1) prieigos fiksuotoje vietoje teikimas;

2) informacijos apie abonentus teikimo paslaugos ir abonentų knygos;

3) taksofonų paslaugos;

4) specialios neįgaliems paslaugų gavėjams skirtos priemonės.

Iš aktualios teismų praktikos šioje srityje paminėtinas ESTT sprendimas byloje C-543/09 *Deutsche Telecom AG v. Bundesrepublik Deuchland*, priimtas 2011 m. gegužės 5 dieną. Prašymas nagrinėti bylą pateiktas dėl pareigos, kuri Telekomunikacijų įstatymu (vok. *Telekommunikationsgesetz*, toliau – *TKG)* numatyta telefono numerius abonentams skiriančioms įmonėms, suteikti kitoms įmonėms, teikiančioms viešai prieinamas informacijos apie abonentus teikimo ar abonentų knygos paslaugas, jos turimus duomenis apie trečiųjų įmonių abonentus. Vienas iš svarbiausių klausimų buvo: pirmuoju klausimu prašymą priimti prejudicinį sprendimą pateikęs teismas siekia išsiaiškinti, ar Universaliųjų paslaugų direktyvos 25 str. 2 d. reikia aiškinti taip, kad ji draudžia nacionalinės teisės aktus, kuriais įmonėms, skiriančioms telefono numerius galutiniams paslaugų gavėjams, nustatoma pareiga perduoti įmonėms, teikiančioms viešai prieinamas informacijos apie abonentus ir abonentų knygų paslaugas, turimus duomenis apie trečiųjų įmonių abonentus. ESTT, išnagrinėjęs visas aplinkybes, pranešė, kad Universaliųjų paslaugų direktyvos 25 str. 2 d. aiškintina kaip nedraudžianti nacionalinės teisės aktų, kuriais įmonėms, skiriančioms telefono numerius galutiniams paslaugų gavėjams, nustatoma pareiga perduoti įmonėms, teikiančioms viešai prieinamas informacijos apie abonentus ir abonentų knygų paslaugas, ne tik duomenis apie savo abonentus, bet ir jų turimus duomenis apie trečiųjų įmonių abonentus. Tokiu būdu ESTT atvėrė kelią įmonėms, teikiančioms viešai prieinamas informacijos apie abonentus paslaugas, iš didžiųjų duomenų valdytojų reikalauti ne tik duomenų apie savo abonentus, bet ir apie kitų operatorių klientus.

Dėl minėtojo universaliųjų paslaugų sąrašo šiandien manytina, kad kai kurios universaliųjų paslaugų instituto sritys prarado savo aktualumą. Kaip pavyzdį galima būtų pateikti taksofonų paslaugas, kuriomis dėl įvairių priežasčių atskirose ES valstybėse naudojamasi nevienodai. Tačiau reikėtų paminėti, kad gyventojų, kurie vis dar naudojasi taksofonais, procentas yra labai mažas. Todėl vargu ar reikia atitinkamus operatorius įpareigoti teikti taksofonų paslaugas, kuriomis beveik niekas nesinaudoja. Tokių universaliųjų paslaugų būtinybė tikrai abejotina. 2015 m. pabaigoje įpareigojimų teikti elektroninių ryšių paslaugas taksofonu jau buvo atsisakiusios devynios ES valstybės.

Kaip nurodyta Universaliųjų paslaugų direktyvos preambulės 1 punkte, „universaliųjų paslaugų“ sąvoka turėtų plėtotis ir atspindėti technologijos,

rinkos ir paslaugų gavėjų paklausos pokyčius. Deja, šioje srityje teisinis reguliavimas gerokai atsilieka nuo technologijų plėtros. Galbūt dar ankstoka atsisakyti universaliųjų paslaugų instituto, tačiau minėtųjų paslaugų sąrašą būtina kuo skubiau persvarstyti.

Aktualus ir universaliųjų elektroninių ryšių paslaugų teikimo finansavimo klausimas. Dažniausiai visa šių paslaugų teikimo našta tenka jas teikiantiems ūkio subjektams. Tik tuo atveju, jeigu nustatoma, kad tokia našta yra per didelė, apskaičiuojamos grynosios universaliųjų paslaugų teikimo sąnaudos, kurias dengia visi operatoriai. Šiame kontekste paminėtinas ESTT sprendimas byloje C-389/08 *Base NV ir kt. v. Ministerraad,* priimtas 2010 m. spalio 6 dieną. Šiuo sprendimu Teismas, be kita ko, informavo dėl pačios prievolės nepagrįstumo (būtent tuo atveju ir taikomas konpensavimas): nepagrįstai didele prievole, kurios buvimą prieš skirdama kokią nors kompensaciją turi pripažinti nacionalinė reguliavimo institucija, yra laikoma ta, kuri kiekvienai atitinkamai įmonei yra per didelė, kad ši pagal visus savo rodiklius (įrangos lygį, ekonominę ir finansinę padėtį bei užimamą rinkos dalį) galėtų ją įvykdyti. Be to, labai svarbus ir Teismo išaiškinimas dėl grynųjų sąnaudų įvertinimo: valstybės narės, laikydamosi iš Direktyvos 2002/22 išplaukiančių įsipareigojimų, negali pripažinti, jog universaliųjų paslaugų teikimas iš tiesų yra nepagrįstai didelė kompensuotina prievolė, tenkanti visoms įmonėms, kurios privalo teikti šias paslaugas, prieš tai neapskaičiavusios grynųjų sąnaudų ir neįvertinusios, ar šios sąnaudos minėtajai įmonei yra per didelė prievolė. Be to, jos negali priimti kompensavimo tvarkos, pagal kurią kompensacija nebūtų siejama su šiomis grynosiomis sąnaudomis.

5. Elektroninių ryšių išteklių valdymas

Pagrindiniai ištekliai, užtikrinantys elektroninių ryšių paslaugų teikimą, yra radijo dažniai (kanalai) ir telefono ryšio numeriai. Elektroninius išteklius valdo ir paskirsto nacionalinės reguliavimo institucijos.

Pagal Pagrindų direktyvą, nacionalinės reguliavimo institucijos kontroliuoja visus nacionalinius numeracijos išteklius ir nacionalinių numeracijos planų valdymą. Minėtosios institucijos nustato objektyvią, skaidrią ir nediskriminacinę nacionalinių numeracijos išteklių skyrimo tvarką bei užtikrina, kad numeracijos planai ir procedūros būtų vienodai taikomi visiems viešųjų elektroninių ryšių paslaugų teikėjams.

Labai svarbi išteklių koordinacija. Remdamosios Pagrindų direktyva, valstybės narės, siekdamos užtikrinti globalią paslaugų sąveiką (kai tai yra tikslinga), koordinuoja savo pozicijas tarptautinėse organizacijose ir foru-

muose, kuriuose priimami sprendimai su elektroninių ryšių tinklų ir paslaugų numeracija, pavadinimais bei adresais susijusiais klausimais.

Leidimų direktyva patikslina reikalavimus ir nustato, kad pagal ESTT jurisprudenciją bet kokie teisių, garantuojamų pagal EB steigimo sutarties 49 str., nacionaliniai apribojimai turėtų būti objektyviai pateisinami, proporcingi ir neviršyti to, kas būtinai reikalinga bendrųjų interesų tikslams, valstybių narių apibrėžtiems pagal EB teisę, pasiekti.

Pagal Leidimų direktyvos 5 str. 1 d., kai galima (ypač kai žalingųjų trikdžių tikimybė gana nedidelė), valstybės narės nereikalauja, kad radijo dažniams naudoti būtų suteikiamos individualios naudojimo teisės, tik tokių radijo dažnių naudojimo sąlygos įrašomos į bendrąjį leidimą.

Pagrindų direktyva, skiriant radijo dažnius (kanalus) ir ypatingą ekonominę vertę turinčius numerius, valstybėms narėms leidžia naudoti konkurencines ir palyginamąsias atrinkimo procedūras.

6. Naujosios kartos tinklai (angl. *NGN)* ir teisinis jų reguliavimas

Naujosios kartos tinklai (angl. *NGN, NGA)* susiję su optinių skaidulų naudojimu vietiniame prieigos tinkle. Atsižvelgiant į optikos naudojimą prieigos tinkle, sąlygiškai galima išskirti šias naujosios kartos tinklų grupes:

– *FTTH* (angl. *fiber to the home)*;
– *FTTB* (angl. *fiber to the building)*;
– *FTTN* (angl. *fiber to the node)*.

Viena iš svarbiausių 2020 m. Europos strategijos iniciatyvų – Europos skaitmeninė darbotvarkė (COM(2010)245 *final)* – nustato itin greito plačiajuosčio ryšio plėtros tikslus. Europos Komisijos rekomendacija dėl reguliuojamos prieigos prie naujosios kartos tinklų *(NGA* rekomendacija), priimta 2010 m. rugsėjį ir laikytina pagrindine priemone, skatinančia pasiekti atitinkamus tikslus.

Vienas iš svarbiausių *NGA* rekomendacijos tikslų – skatinti efektyvią elektroninių rinkų ryšių konkurenciją, naudojant esamą elektroninių ryšių infrastruktūrą ir kuriant naujus jos elementus. Dažnai tokią infrastruktūrą valdo didelę įtaką atitinkamose rinkose turintys operatoriai (dažniausiai buvusieji monopolininkai). Todėl pagal *NGA* rekomendaciją nacionalinės reguliavimo institucijos turi taikyti *ex-ante* įpareigojimus operatoriams, kurie atitinkamose rinkose turi didelę įtaką *(SMP)*. Taigi *NGA* rekomendacija nustato bendrąjį reguliavimo požiūrį, turėdama tikslą įgyvendinti prieigą prie naujosios kartos tinklų. Iš esmės *NGA* rekomendacija reglamentuoja tam tikras teisines priemones operatoriams, kurie turi didelę įtaką ketvirtojoje ir penktojoje (atitinkamai didmeninėje infrastruktūros prieigos ir didmeninėje plačiajuosčio ryšio prieigos) rinkose.

Pagal *NGA* rekomendaciją ir prieigos direktyvą, ketvirtojoje ir penktojoje rinkose *SMP* operatoriams gali būti taikomi tokie įpareigojimai:

- prieigos suteikimo;
- skaidrumo;
- nediskriminavimo;
- apskaitos atskyrimo;
- kainų kontrolės ir sąnaudų apskaitos.

Svarbiausias *NGA* rekomendacijos tikslas – spartinti bendrosios rinkos plėtrą didinant teisinį tikrumą ir skatinant investicijas, konkurenciją bei inovacijas plačiajuosčio ryšio paslaugų rinkoje, ypač pereinant prie naujosios kartos prieigos *(NKP)* tinklų. Detalesni *NGA* rekomendacijos tikslai yra tokie:

- prieigos reguliavimas turi skatinti konkurenciją mažmeninėse rinkose, kol šios rinkos taps konkurencingos;
- reguliavimas visoje ES turi būti nuoseklus;
- didesnė konkurencija ir nuoseklus reguliavimas turi lemti didesnius greičius, mažesnes kainas ir geresnį didelės spartos plačiajuosčio ryšio pasiūlymų prieinamumą.

Vis dėlto kyla abejonių, ar ši rekomendacija padės pasiekti numatytus tikslus: skatinti inovacijas, konkurenciją ir ypač investicijas į naujosios kartos prieigos *(NKP)* tinklus.

Reikėtų atkreipti dėmesį, kad Lietuva aiškiai išsiskiria *FTTH* plėtra ir yra įvardijama kaip valstybė, turinti vieną didžiausių *FTTH* skvarbų pasaulyje. Aiškių įrodymų, kad tokia situacija pasiekta dėl teisinio reguliavimo, nėra. Tikėtina, kad Lietuva pirmauja Europoje ir pasaulyje dėl didžiulių investicijų ir aktyvios konkurencijos atitinkamose elektroninių ryšių rinkose.

5 skirsnis. Elektroninių ryšių ES dereguliavimas ir jo tendencijos

ES norminių teisės aktų, reglamentuojančių *ex-ante* įpareigojimų nustatymą ir rinkos tyrimų atlikimą, nuostatos numato galimybę dereguliuoti atitinkamas elektroninių ryšių rinkas.

2002 m. kovo 7 d. Europos Parlamento ir Tarybos priimtoje Pagrindų direktyvos 2002/21/EB dėl elektroninių ryšių tinklų ir paslaugų bendrosios reguliavimo sistemos[15] 16 str. 3 dalyje numatyta, kad „Jei nacionalinė

[15] 2002-03-07 Europos Parlamento ir Tarybos priimta Pagrindų direktyva 2002/21/EB. Prieiga per internetą: <http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=DD:13:29:32002L0021:LT:PDF>.

reguliavimo institucija padaro išvadą, kad konkurencija rinkoje yra veiksminga, ji neskiria ir nepalieka galioti jokių šio straipsnio 2 dalyje minėtų specifinių įpareigojimų. Tais atvejais, kai įpareigojimai konkretiems sektoriams jau paskirti, nacionalinė reguliavimo institucija atitinkamos rinkos įmonėms tokius įpareigojimus panaikina. Apie tokį panaikinimą šalims, kurioms jis turi įtakos, pranešama iš anksto."

2009 m. lapkričio 25 d. priimtame Pagrindų direktyvos pakeitime 2009/140/EB[16] numatyta, kad:

- „5 d. Plėtojantis konkurencijai rinkose siekiama palaipsniui mažinti konkretiems sektoriams taikomas *ex ante* taisykles, o galiausiai siekiama, kad elektroninius ryšius reglamentuotų tik konkurencijos teisės nuostatos. Atsižvelgiant į tai, kad elektroninių ryšių rinkose pastaraisiais metais labai išaugo konkurencija, labai svarbu, kad *ex ante* reglamentuojančio pobūdžio įpareigojimai būtų nustatyti tik tais atvejais, kai nėra veiksmingos ir tvarios konkurencijos.
- 15 str. 1 d. Po viešųjų konsultacijų, įskaitant konsultacijas su nacionalinėmis reguliavimo institucijomis, bei atidžiai atsižvelgdama į EERRI nuomonę, Komisija, laikydamasi 22 straipsnio 2 dalyje nurodytos patariamosios procedūros, priima rekomendaciją dėl atitinkamų produktų ir paslaugų rinkų (toliau – rekomendacija). Rekomendacijoje bus nurodytos tos elektroninių ryšių sektoriaus produktų ir paslaugų rinkos, kurių charakteristikos pagrįstai leidžia joms taikyti specifinėse direktyvose nurodytus reglamentuojančio pobūdžio įpareigojimus, jų netaikant rinkoms, kurios konkrečiais atvejais gali būti apibrėžtos pagal konkurencijos teisę. Komisija rinkas apibrėžia pagal konkurencijos teisės principus.
- 16 str. 6 d. Pagal šio straipsnio 3 ir 4 dalis taikant priemones laikomasi 6 ir 7 straipsniuose nurodytos tvarkos. Nacionalinės reguliavimo institucijos atlieka atitinkamos rinkos tyrimą ir praneša apie atitinkamą planuojamą priemonę pagal 7 straipsnį: a) per trejus metus nuo ankstesnės su šia rinka susijusios priemonės patvirtinimo. Tačiau išimtiniais atvejais šis laikotarpis gali būti pratęstas ne daugiau negu trejais papildomais metais, jei nacionalinė reguliavimo institucija Komisijai praneša apie siūlomo pratęsimo priežastis, o Komisija per vieną mėnesį nuo pranešimo apie pratęsimą nepareiškia prieštaravimų; b) tų rinkų, apie kurias anksčiau nebuvo pranešta Komisijai, atveju – per dvejus metus po patikslintos rekomendacijos dėl atitinkamų rinkų priėmimo."

[16] 2009-11-25 direktyva Nr. 2009/140/EB. Prieiga per internetą: <http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0037:0069:lt:PDF>.

Remiantis Pagrindų direktyvos 15 str. 1 d., 2007 m. gruodžio 17 d. Europos Komisija priėmė rekomendaciją „Dėl elektroninių ryšių sektoriaus atitinkamų produktų ir paslaugų rinkų, kurioms gali būti taikomas *ex ante* reguliavimas pagal Europos Parlamento ir Tarybos direktyvą 2002/21/EB dėl elektroninių ryšių tinklų ir paslaugų bendrosios reguliavimo sistemos“ *(Pranešta dokumentu Nr. C(2007) 5406)* (2007/879/EB)[17], pakeitusią Europos Komisijos rekomendaciją 2003/311/EB, kurioje numatė, kad:

- 14 d. *Trijų kriterijų taikymas* (aut. didelės ir nuolatinės kliūtys patekti į rinką; jų taikymas rinkoms, kurių struktūra neleidžia per tam tikrą apibrėžtą laikotarpį atsirasti veiksmingai konkurencijai; vien taikant konkurencijos teisę nebus tinkamai išspręstas rinkos nepakankamumo klausimas) „turėtų apriboti rinkų, kurioms gali būti nustatomi *ex ante* reguliavimo įpareigojimai elektroninių ryšių sektoriuje, skaičių ir taip būtų prisidėta prie reglamentavimo sistemos tikslo laipsniškai sumažinti konkrečiam sektoriui taikomų *ex ante* taisyklių skaičių plėtojantis rinkoje konkurencijai. Šie kriterijai turėtų būti taikomi kaip suvestiniai, kad bent vieno iš jų neįvykdymas reikštų, jog rinka neturėtų būti įvardyta kaip tokia, kuriai galima taikyti *ex ante* reguliavimą.
- 18 d. Tai, kad šioje rekomendacijoje nurodytos tos produktų ir paslaugų rinkos, kuriose gali būti pagrįsta taikyti *ex ante* reguliavimą, nereiškia, kad reguliavimas visada pateisinamas, ar kad toms rinkoms bus skirti specialiose direktyvose nurodyti reguliavimo įpareigojimai. Visų pirma reguliavimas negali būti taikomas arba jo turi būti atsisakyta, jeigu ir be reguliavimo tose rinkose yra veiksminga konkurencija.“

Šioje rekomendacijoje Europos Komisija, taikydama visus tris minėtuosius suvestinius kriterijus, nustatė septynias (vietoj aštuoniolikos) rinkas ir 17 d. pabrėžė, kad tų rinkų, kurios nėra išvardytos rekomendacijoje, atveju nacionalinės reguliavimo institucijos, analizuodamos atitinkamą rinką, turėtų atsižvelgti į trijų kriterijų sąrašą ir įvertinti, ar pagal nacionalines aplinkybes rinkai vis dar gali būti taikomas *ex ante* reguliavimas.

2008 m. lapkričio 5 d. ELPA priežiūros institucijos rekomendacijoje „Dėl elektroninių ryšių sektoriaus atitinkamų produktų ir paslaugų rinkų, kurioms gali būti taikomas *ex ante* reguliavimas pagal EEE susitarimo XI priedo 5cl punkte nurodytą aktą *(Europos Parlamento ir Tarybos direktyva 2002/21/EB dėl elektroninių ryšių tinklų ir paslaugų bendrosios reguliavimo sistemos)*, priderintą prie to Susitarimo 1 protokolu ir sektorių

[17] 2007-12-17 EK rekomendacija Nr. 2007/879/EB. Prieiga per internetą: <http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:344:0065:0069:LT:PDF>.

adaptacijomis, pateiktomis to Susitarimo XI priede“ (2009/C 156/12)[18] buvo pakartota dauguma 2007 m. Europos Komisijos rekomendacijos nuostatų ir papildomai pabrėžta:

— 23 d. „Tai, kad šioje rekomendacijoje yra nurodytos tos produktų ir paslaugų rinkos, kuriose būtų pagrįsta taikyti *ex ante* reguliavimą, nereiškia, kad reguliavimas yra visuomet pateisinimas, arba kad toms rinkoms bus skirti specialiose direktyvose nurodyti reguliavimo įpareigojimai. Visų pirma reguliavimas negali būti taikomas arba jo turi būti atsisakyta, jeigu ir be reguliavimo tose rinkose yra veiksminga konkurencija, t. y. jei nė vienas operatorius neturi didelės įtakos rinkoje, remiantis Pagrindų direktyvos 14 straipsniu. Reguliavimo įpareigojimai turi būti tinkami ir pagrįsti nustatytos problemos pobūdžiu, proporcingi ir pateisinami atsižvelgiant į Pagrindų direktyvos nustatytus tikslus, visų pirma maksimaliai padidinti naudotojams teikiamą naudą, užtikrinti, kad konkurencija nebūtų iškreipta arba ribojama, skatinti veiksmingas investicijas į infrastruktūrą ir skatinti naujoves, taip pat veiksmingą radijo dažnių ir numeracijos išteklių naudojimą ir valdymą.“

Kol kas elektroninių rinkų dereguliavimas ES vyksta vangokai, nors pavienių jo atvejų jau pasitaiko. Būtent pastaruoju metu elektroninių ryšių operatorius vienijančios asociacijos akcentuoja dereguliavimo svarbą bei jo teigiamą įtaką investicijoms į elektroninių ryšių tinklus ir apskritai visai ES ekonomikai.

Viena iš pastarųjų metų dereguliavimo iniciatyvų visos ES mastu – aukščiau jau minėta ES rekomendacija dėl nediskriminavimo įpareigojimų Nr. 2013/466/ES. Šiuo dokumentu siekiama operatoriams, kurie pripažinti darantys didelę įtaką atitinkamoms rinkoms, sumažinti kainų kontrolės įpareigojimus arba išvis juos panaikinti, vietoj to įvedant naujų nediskriminavimo įpareigojimų (pvz., nustatant konkurentams prieigą prie dominuojančio operatoriaus sistemų ir pan.). Kaip jau minėta, ši rekomendacija, nors ir yra vienas iš svarbesnių mėginimų dereguliuoti (tik tiek, kiek tai susiję su atitinkamais įpareigojimais, o ne dereguliuoti apskritai) rinką, vertintina prieštaringai. Vis dėlto vietoj vienų įpareigojimų atsirastų kitų, dėl to minėtosios priemonės gali neturėti didelės įtakos konkurencijai.

[18] 2008-11-05 ELPA rekomendacija Nr. 2009/C 156/12. Prieiga per internetą: <http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:156:0018:0023:LT:PDF>.

6 skirsnis. Elektroninių ryšių reguliavimas Lietuvoje

Šiuo metu Lietuvoje yra įgyvendintas 2002 m. elektroninių ryšių direktyvų paketas, įskaitant ir 2009 m. direktyvų pakeitimus, be to, galioja 2004 m. priimtas Lietuvos Respublikos elektroninių ryšių įstatymas (su atitinkamais pakeitimais). Pastarieji esminiai pakeitimai padaryti 2011 metais. Priėmus 2009/136/EB ir 2009/140/EB direktyvas, įstatymų lygiu jos buvo perkeltos į Lietuvos nacionalinę teisės sistemą – Lietuvos Respublikos elektroninių ryšių įstatymą. Perkeliant 2009/136/EB ir 2009/140/EB direktyvų nuostatas, buvo padaryta šių pakeitimų:

- patikslintas viešųjų elektroninių ryšių paslaugų teikėjų ir galutinių paslaugų gavėjų teisių ir pareigų reglamentavimas, daugiau dėmesio skiriant galutinių paslaugų gavėjų teisėms ir interesams užtikrinti;
- pakeistas rinkos tyrimo procedūros reglamentavimas;
- Lietuvos Respublikos elektroninių ryšių įstatymas papildytas nauju funkcinio atskyrimo įpareigojimu didelę įtaką turinčiam ūkio subjektui ir galimybe vertikaliai integruotam subjektui savanoriškai atskirti viso prieigos prie tinklo turto ar didelės jo dalies valdymą;
- nustatyta operatoriaus, darančio didelę įtaką atitinkamai rinkai, pareiga kitiems ūkio subjektams suteikti prieigą prie konkrečių tinklo elementų ir (ar) priemonių, įskaitant prieigą prie pasyviųjų tinklo elementų, ir (ar) atsietą prieigą prie vietinės linijos, kad būtų sudarytos sąlygos pasirinkti išankstinį ir (arba) individualų viešųjų telefono ryšio paslaugų teikėją, ir (ar) pateikti siūlymą dėl didmeninės vietinės linijos skyrimo viešosioms telefono ryšio paslaugoms teikti, dar nustatoma pareiga suteikti prieigą prie susijusių paslaugų, įskaitant tapatybės, vietos ir būsenos nustatymo;
- patikslintos ir papildytos elektroninių ryšių infrastruktūros bendrą naudojimą ir apsaugą reglamentuojančios Lietuvos Respublikos elektroninių ryšių įstatymo nuostatos;
- įtvirtintos naujos nuostatos, skirtos elektroninių ryšių tinklų saugumui ir vientisumui užtikrinti, radijo dažniams (kanalams) perleisti;
- papildomai įtrauktas elektroninių ryšių tinklų neutralumo principas, t. y. galutiniams paslaugų gavėjams turi būti sudarytos sąlygos turėti prieigą prie savo pasirinktos informacijos ir ją platinti, naudoti savo pasirinktą programinę įrangą ir paslaugas.

Anot įstatymo projekto rengėjų, šios projekto nuostatos turėjo sudaryti nuoseklaus *ex ante* reguliavimo pagrindą, o tai savo ruožtu turėjo lemti geresnį konkurencijos elektroninių ryšių sektoriuje garantavimą. Be to,

projekto nuostatos turėjo užtikrinti geresnį elektroninių ryšių išteklių valdymą, jų naudojimą, spartesnį naujosios kartos tinklų diegimą.

Pagrindinė elektroninių ryšių veiklą Lietuvoje reguliuojanti institucija – Ryšių reguliavimo tarnyba (RRT). Ji yra finansuojama valstybės ir iš atskiro šios tarnybos biudžeto, kurį sudaro pajamos, gautos už teikiamas paslaugas ir atliekamus darbus. Jų objektus, dydžius ir mokėjimo tvarką nustato pati RRT, pagrįsdama savo sąnaudomis.

RRT tikslas – veiksminga konkurencija, efektyvus išteklių naudojimas ir paslaugų vartotojų teisių apsaugos užtikrinimas elektroninių ryšių srityje.

Ryšių reguliavimo tarnybos uždaviniai:

1) sudaryti veiksmingos konkurencijos sąlygas elektroninių ryšių (pirmiausia perduodant informacijos turinį elektroninių ryšių tinklais) rinkose ir užtikrinti, kad nebūtų diskriminuojami ūkio subjektai, teikiantys elektroninių ryšių tinklus ir (arba) elektroninių ryšių paslaugas, bei skatinti elektroninių ryšių infrastruktūros plėtrą;
2) užtikrinti elektroninių ryšių paslaugų gavėjų, įskaitant neįgaliuosius, senyvo amžiaus ir turinčiuosius specialiųjų socialinių poreikių (fizinius asmenis, dėl amžiaus, neįgalumo, socialinių problemų iš dalies ar visiškai neturinčius, neįgijusius arba praradusius gebėjimus ar galimybes savarankiškai rūpintis asmeniniu gyvenimu ir dalyvauti visuomenės gyvenime), teisių ir teisėtų interesų apsaugą, ypač užtikrinant paprastas ir nebrangias ginčų sprendimo procedūras bei skatinant viešųjų elektroninių ryšių paslaugų teikimo sąlygų ir tarifų skaidrumą, ir pagal kompetenciją užtikrinti galimybę naudotis universaliosiomis paslaugomis bei galimybę galutiniams paslaugų gavėjams turėti prieigą prie pasirinktos informacijos ir ją platinti teisės aktų nustatyta tvarka bei galimybę naudotis pasirinkta programine įranga ir paslaugomis;
3) skatinti efektyvias ilgalaikes investicijas, naujovių diegimą ir elektroninių ryšių plėtrą;
4) užtikrinti efektyvų elektroninių ryšių išteklių naudojimą ir pakankamą nacionalinių telefono ryšio numerių, reikalingų viešosioms elektroninių ryšių paslaugoms teikti, kiekį, o numeracijos planai ir procedūros būtų taikomi tokiu būdu, kuris užtikrintų vienodas visų viešųjų elektroninių ryšių paslaugų teikėjų galimybes ir ypač tai, kad ūkio subjektai, kuriems skirti nacionalinių telefono ryšio numerių ištekliai, nediskriminuotų kitų elektroninių ryšių paslaugų teikėjų, kiek tai susiję su numeracijos sekomis, naudojamomis jų paslaugoms pasiekti;

5) pagal savo kompetenciją reguliuoti, kad Lietuvoje naudojama aparatūra ir įrenginiai atitiktų galiojančius privalomuosius Lietuvos Respublikos reikalavimus, užtikrinti aparatūros ir įrenginių elektromagnetinį suderinamumą;
6) pagal kompetenciją skatinti ES vidaus rinkos plėtrą ir suderintą elektroninių ryšių reguliavimą visos ES mastu;
7) bendradarbiauti su kompetentingomis institucijomis ir su Valstybine duomenų apsaugos inspekcija, kad būtų užtikrinta žmogaus privataus gyvenimo neliečiamumo teisė, kiek tai susiję su asmens duomenų tvarkymu;
8) užtikrinti, kad operatoriai ir elektroninių ryšių paslaugų teikėjai vykdytų įpareigojimus, kurie gali būti nustatyti valstybės gynybos, nacionalinio saugumo ir viešosios tvarkos palaikymo interesais bei susiklosčius ypatingoms aplinkybėms;
9) garantuoti, kad viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjai naudotų tinkamas technines ir organizacines priemones savo teikiamų viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų saugumui ir vientisumui užtikrinti.

Šiandien reguliavimo našta Lietuvoje veikiantiems operatoriams, ypač turintiems didelę įtaką atitinkamose rinkose, išlieka gana didelė.

Pabrėžtina, kad dėl elektroninių ryšių dereguliavimo Lietuvoje Elektroninių ryšių įstatymas nustato Tarnybai teisę atlikti rinkos tyrimą, kurio vienas iš tikslų – užtikrinti veiksmingą konkurenciją elektroninių ryšių srityje ir nustatyti, pakeisti ir (ar) panaikinti nustatytus įpareigojimus didelę įtaką atitinkamose rinkose turintiems ūkio subjektams. Šio įstatymo 17 str. 7 d. nustatytais atvejais, sąlygomis ir tvarka Tarnybai numatyta teisė panaikinti didelę įtaką atitinkamoje rinkoje turėjusiems ūkio subjektams skirtus įpareigojimus, jeigu tokie buvo nustatyti:

„7. Jeigu atlikus atitinkamos rinkos tyrimą nustatoma, kad jos charakteristikos negali pateisinti įpareigojimų, nurodytų šiame straipsnyje, taikymo ir (arba) joje nėra didelę įtaką turinčių ūkio subjektų, Ryšių reguliavimo tarnyba šio Įstatymo nustatyta tvarka ir sąlygomis nenustato šiame straipsnyje nurodytų įpareigojimų ūkio subjektams ir (ar) panaikina didelę įtaką atitinkamoje rinkoje turėjusiems ūkio subjektams nustatytus įpareigojimus, jei tokie buvo nustatyti. Panaikindama įpareigojimus, Ryšių reguliavimo tarnyba turi teisę motyvuotu sprendimu nustatyti jų vykdymo pabaigos terminą, ne ilgesnį kaip 28 dienos nuo atitinkamos šio Įstatymo 16 straipsnio 19 dalyje nurodytos informacijos paskelbimo Ryšių reguliavimo tarnybos interneto svetainėje.“

Lietuvos Respublikos elektroninių ryšių įstatymo 16 str. 4 d. numato Tarnybos teisę atlikti rinkos tyrimą suinteresuotų ūkio subjektų prašymu.

Tarnybos direktoriaus 2004 m. rugsėjo 17 d. įsakymu Nr. 1V-297 patvirtintos Rinkos tyrimo taisyklės numato, kad Tarnyba, vertindama, ar atitinkamos rinkos charakteristikos gali pateisinti įpareigojimų, nurodytų Lietuvos Respublikos elektroninių ryšių įstatymo 17 str., taikymą, įvertina:

„16.1. kliūtis, kurios trukdo pradėti veikti atitinkamoje rinkoje ir (ar) vystytis konkurencijai joje;

16.2. ar rinka pasižymi tokiomis charakteristikomis, kurios lemia veiksmingos konkurencijos atsiradimo tendenciją be poreikio taikyti įpareigojimus, nurodytus Įstatymo 17 straipsnyje;

16.3. bendrosios konkurencijos teisės pakankamumą sumažinti ar pašalinti kliūtis, kurios trukdo pradėti veikti rinkoje ir (ar) vystytis konkurencijai joje, ir (ar) įtvirtinti veiksmingą konkurenciją atitinkamoje rinkoje, netaikant Įstatymo 17 straipsnyje nurodytų įpareigojimų."

Aktuali informacija apie reguliuojamas rinkas ir didelę įtaką jose turinčius ūkio subjektus bei nustatytus įpareigojimus skelbiama RRT tinklalapyje[19].

Lietuvoje, kaip ir visoje ES, vyrauja tendencija dereguliuoti kai kurias mažmenines (paliekant įpareigojimus didmeninėse) rinkas, taip siekiama įgyvendinti vieną iš svarbiausių efektyvios konkurencijos užtikrinimo tikslų – suteikti prieigą prie atitinkamų paslaugų ir infrastruktūros.

Žinių įtvirtinimo klausimai

1. Kaip apibrėžiami elektroniniai ryšiai?
2. Kokie yra pagrindiniai elektroninių ryšių teisinio reguliavimo raidos etapai?
3. Kokios direktyvos sudaro ES elektroninių ryšių teisinio reguliavimo sistemą?
4. Kokie yra svarbiausi ES elektroninių ryšių teisinio reguliavimo tikslai?
5. Kokie yra svarbiausi ES elektroninių ryšių teisinio reguliavimo sistemos principai?
6. Kokie yra pagrindiniai ES elektroninių ryšių teisinio reguliavimo institutai?
7. Kokias žinote elektroninius ryšius reguliuojančias institucijas?

[19] <http://www.rrt.lt/lt/verslui/konkurencijos-prieziura/didele-itaka-turintys-hn5f.html>.

/III/ *skyrius*

Elektroninė komercija ir jos teisinis reguliavimas

/ 111–161 / *puslapiai*

1 skirsnis. Elektroninės komercijos samprata ir ypatumai

1. Teisiniai elektroninės komercijos aspektai

1.1. Elektroninės komercijos samprata ir ypatumai

Pasaulyje nėra nusistovėjusio visuotinai priimtino elektroninės komercijos apibrėžimo. Net ES 2000 m. birželio 8 d. priimta Elektroninės komercijos direktyva jo nepateikia.

Elektroninę komerciją galima būtų apibrėžti kaip prekybą prekėmis ar paslaugomis, kai sandoriai sudaromi ar vykdomi taikant elektronines priemones.

Pasitelkus elektroninę prekybą, gali būti teikiamos paslaugos ir prekiaujama dviejų rūšių produktais:

1) materialiaisiais (šių produktų neįmanoma persiųsti e. erdve. Tai – tradicinės prekės, kuriomis buvo prekiaujama iki atsirandant informacinėms technologijoms ir kurios negali būti arba nėra išreikštos skaitmenine forma);
2) skaitmeniniais (pasitelkus informacines technologijas, šie produktai gali būti išreiškiami skaitmenine forma ir siunčiami e. erdve).

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

1) tiesioginis (skaitmeniniai produktai persiunčiami tiesioginiu darbo režimu arba naudojant kitas elektronines priemones);
2) netiesioginis (materialieji produktai užsakomi elektroninėmis priemonėmis, tačiau pristatomi tradiciškai).

Pagrindiniai elektroninės komercijos modeliai pagal subjektus, dalyvaujančius komerciniuose sandoriuose, kurie vykdomi e. erdvėje, yra šie:

- verslas verslui *(B2B* – didmeninė prekyba). Elektronine komercija užsiimančioje bendrovėje, kurios adresas: *www.amazon.com*, kitos įmonės irgi gali plėtoti savo elektroninį verslą. Knygų leidyklos tokia galimybe naudojasi pristatydamos savo produkciją didelei svetainės vartotojų rinkai ir galimiems savo klientams. Norėdamos naudotis šia paslauga ir plėtoti savo mažmeninės prekybos verslą, įmonės su bendrove „Amazon“ sudaro paslaugų teikimo sandorius;
- verslas vartotojui *(B2C* – mažmeninė prekyba). Šis verslo modelis apima sandorius, sudaromus tarp verslo subjektų bei vartotojų ir (ar) klientų (pvz., elektroninė bankininkystė, kelionių paslaugos ir pan.);

- vartotojas vartotojui *(C2C)*. Šis verslo modelis apima sandorius, sudaromus tarp dviejų vartotojų – vienas iš jų parduoda, o kitas perka. Tokie vartotojai dažniausiai naudojasi pagalbinėmis svetainėmis, tokiomis kaip *eBay*, kurios užtikrina jų tarpusavio bendravimą. Internete esantys aukcionai galėtų būti pateikiami kaip klasikinis šio modelio pavyzdys, tačiau svarbu, kad abu (ir pirkėjas, ir pardavėjas) registruotųsi svetainėje, kurioje vykdomas toks aukcionas. Pardavėjas moka tam tikrą mokestį, kad galėtų pardavinėti savo prekę, o pirkėjas be jokio mokesčio siūlo savo kainą;
- vartotojas verslui (*C2B*). Panašus modelis, kaip ir *B2C*, tačiau šiuo atveju vartotojas tampa pardavėju. Specialiai tam pritaikytose svetainėse (pvz., *www.monster.com*) vartotojai savo prekes ar paslaugas siūlo įmonėms – jie pateikia savo pasiūlymų, o susidomėjusi organizacija gali tiesiogiai susisiekti su vartotoju-pardavėju.

Literatūroje dar išskiriama ir kitų elektroninės komercijos modelių: valstybės institucija valstybės institucijai *(G2G)*; valstybės institucija vartotojui *(G2C)*; valstybės institucija verslui *(G2B)*; verslas valstybės institucijai *(B2G)*; vartotojas valstybės institucijai *(C2G)*.

Kai elektroninei komercijai taikomos pažangios informacinės technologijos, atsiranda naujų galimybių reklamuoti prekes, pristatyti jas į kitas valstybes ar teikti paslaugas jų piliečiams, vykdyti atsiskaitymus tarp sandorio šalių ar pereiti į kitas verslo stadijas. Be to, šios technologijos stipriai veikė įmonių valdymą bei prekių ir pinigų srautų kontrolę. Norint suprasti, kokios naujovės turi įtakos tradicinei tarptautinei komercijai, reikia išsiaiškinti, kas jai būdinga ir kuo ji skiriasi nuo tradicinės prekybos. Palyginti su gerai žinomais tradiciniais tarptautinio verslo modeliais, ne visi elektroninės komercijos požymiai daro išskirtinę įtaką jos teisiniam reguliavimui. Remiantis D. A. Hardesty, būtų galima išskirti tokias svarbiausias elektroninės komercijos savybes:

Pasaulinė prekyba. Kaip rodo istorija, geografinės valstybių sienos tapdavo nemenka kliūtimi parduoti prekes jų teritorijoje. Naujos elektroninės komercijos galimybės leidžia bendrovėms lanksčiau vykdyti verslą ne tik nacionalinės valstybės teritorijoje, bet ir visame pasaulyje. Labiausiai tai veikia smulkųjį ir vidutinį verslą, nes suteikia galimybę pradėti tarptautinę prekybą, net ir neturint didesnių lėšų. Tokia galimybė pirmiausia priklauso nuo visą pasaulį vienijančio interneto tinklo.

Sudarant prekybos sandorius, lokalinių tinklų naudojimas informacinių technologijų požiūriu irgi įmanomas, nors pasitaiko kur kas rečiau. Kuriami ir tarptautiniu mastu veikiantys uždarieji tinklai, tačiau jie

dažniausiai naudojami konkretiems iš anksto numatytiems tikslams pasiekti, neįtraukiant galimybės sudaryti prekybos sandorių.

Technologiniai pokyčiai lėmė pasauliniu mastu vykdomos prekybos prieinamumą smulkiosioms ir vidutinėms bendrovėms. Naujumas pasireiškia tuo, kad elektroninės komercijos pardavėjai gali ne tik prekiauti visame pasaulyje, bet ir patys tuo metu būti savo valstybėje. Smulkiosioms ar vidutinėms įmonėms, norinčioms pradėti elektroninį verslą, nereikia didelių lėšų savo prekes ar paslaugas pasiūlyti viso pasaulio rinkai. Priešingai nei tradicinės prekybos atveju, elektroninį verslą pradedantis subjektas pats sprendžia, kokiu mastu apriboti rinką, kurioje bus vykdoma prekybos veikla. Svetainės kalbos pasirinkimas (svetainė, turinti tik lietuvių kalbos versiją, nebus tinkama pasaulinei prekybai), atsiskaitymo priemonių taikymas (pardavėjas gali rinktis tokias atsiskaitymo priemones, kurių negalės naudoti tam tikrų teritorijų subjektai), prekių pristatymo būdo galutiniam vartotojui pasirinkimas (gali numatyti prekių pristatymą tik vienos valstybės teritorijoje arba naudotis tarptautinių siuntų gabenimo bendrovių paslaugomis ir neriboti verslo gabendamas prekes po visą pasaulį) ar svetainės adreso užregistravimas bei kitos didelių investicijų nereikalaujančios priemonės gali lemti, kokiai rinkos daliai yra skiriamos prekės ar paslaugos.

Anonimiškumas. Daugelis pirkėjų ir pardavėjų, dalyvaujančių internetu sudaromuose sandoriuose, vienas kito niekada nemato. Dauguma elektroninę prekybą vykdančių svetainių negauna vartotojo asmenį identifikuojančių duomenų. Naudojami informacijos persiuntimo protokolai leidžia lengvai nustatyti kompiuterinės sistemos *IP* adresą, tačiau tai nesuteikia informacijos apie vartotoją, kuris ta kompiuterine sistema naudojasi. Atsiskaitymų pranešimuose pardavėjai gauna patvirtinimą dėl finansinės operacijos legalumo, tačiau tik bankas ar kita tarpinė finansinė institucija gali matyti tikruosius už prekes ar paslaugas atsiskaitančio asmens duomenis. Prekės pristatymo adresas, kurį mato pardavėjas, dar nereiškia, kad tai yra tikrasis pirkėjo adresas. Reikėtų atkreipti dėmesį, kad dažniausiai net nebūtina identifikuoti pirkėjo, tačiau tam tikrais tarptautinės prekybos atvejais (ypač mokestinės sistemos atžvilgiu) pardavėjas apie pirkėją turėtų gauti atitinkamos informacijos.

Skaitmeniniai produktai. Ne visi produktai gali būti išreikšti skaitmenine forma. Dažniausiai tokia forma parduodama programinė įranga, muzikos įrašai, knygos, vaizdo kūriniai. Bendrovėms, pardavinėjančioms tokias prekes, visiškai nereikalingi kai kurie prekybinės veiklos etapai. Pardavėjams nebereikia pirkti žaliavų ir gaminti prekių. Be to, tą pačią prekę gali atsisiųsti daugelis pirkėjų, o bendrovei nereikia rūpintis padidinti tokios

prekės kiekio. Naudodamiesi programine įranga, pirkėjai iš vienintelio duomenų bazėje esančio pardavėjo gali atsisiųsti produkto kopijų, negaišdami tam laiko ir neatlikdami papildomų komandų. Tokie informacinių technologijų pranašumai, be abejo, palengvina verslą prekiautojams, tačiau valstybės institucijoms tampa vis sunkiau kontroliuoti prekių srautus. Padaugėja galimybių nuslėpti tikrąjį parduotų prekių kiekį, be to, nėra bendro skaitmeninę formą turinčių prekių vertinimo. Vienur jos priskiriamos paslaugoms, kitur – prekėms.

Nuotoliniu būdu valdoma bendrovė. Elektroninę prekybą vykdančios bendrovės daugelį operacijų, turinčių įtakos prekybinei veiklai, gali atlikti nuotoliniu būdu. Labiausiai tai lemia programinės įrangos teikiamos galimybės. Ji padeda pardavėjui nuspręsti, kurias prekes parduoti, kokias išimti iš apyvartos, nustatyti norimą kainą, pateikti reklamą, atsiskaityti su pirkėju už įsigytas prekes ar suteiktas paslaugas ir persiųsti prekes į pirkėjo kompiuterinę sistemą. Taip nuotoliniu būdu bus valdoma visa įmonė. Teisinio ginčo atveju apribojama galimybė operatyviai išnagrinėti tokį atvejį, nes visas įmonės personalas yra kitoje šalyje. Ypač tai aktualu toms valstybėms, su kuriomis nėra glaudaus teisinio bendradarbiavimo. Atsižvelgiant į tai, kad elektroninė prekyba išskirtinai palanki smulkiajam ir vidutiniam verslui, daugelis ginčų gali nepadaryti didelės žalos, dėl to tarptautinis ginčų sprendimas dažnai gali būti tiesiog per brangus.

Nematerialumas. Parduodamos skaitmeninės prekės, interneto svetainė, kurioje bendraujama su pirkėju, ar programinė įranga, naudojama prekybos operacijoms atlikti, neturi jokios materialiosios išraiškos. Todėl kartais būna sunku apibrėžti, kokios valstybės jurisdikcijai priklauso vienas ar kitas objektas. Jų neapčiuopiamumas pasunkina, o kartais ir apskritai neleidžia tradiciniu geografiniu požiūriu nustatyti jų buvimo vietos. Net ir teismo priimti sprendimai gali nebūti tinkamai įgyvendinti be kitos valstybės pagalbos, jeigu nebus materialiojo turto, dėl kurio būtų galima įvykdyti sprendimą.

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

1.2. Elektroninės sutartys ir elektroninės komercijos teisinio reguliavimo modelis

Elektroninės komercijos teisinio reglamentavimo iniciatyvos

ES elektroninės komercijos teisės ribos sparčiai plečiasi. Nors įstatymų leidybos mašina įprastai yra gana lėta, didelis informacinių technologijų plėtros tempas reikalauja ir atitinkamos teisinės bazės sukūrimo.

Santykius, susijusius su elektronine prekyba, reglamentuojančios direktyvos orientuotos dviem kryptimis: rinkos ir individo. Vartotojo apsaugai būdinga stipri orientacija į individą. Šias vartotojo apsaugos nuostatas galima rasti Vartotojų apsaugos, susijusios su nuotolinės prekybos sutartimis (toliau – Nuotolinės prekybos direktyva), Elektroninės komercijos, Asmens duomenų apsaugos ir kitose direktyvose.

Interneto kompiuteriniam tinklui išaugus į pasaulinės komunikacijos aplinką, verslo įmonės, siekdamos panaudoti interneto potencialą, pradėjo ieškoti naujų, šiai aplinkai tinkančių, verslo formų.

Viena iš tokių verslo formų – sutarčių sudarymas, naudojant kompiuterines priemones ir kompiuterinį tinklą. Ši verslo kryptis suteikia keletą pranašumų:

1) išlaidų mažinimas;
2) sutarčiai sudaryti skirto laiko taupymas;
3) produkcijos pateikimas naujoms rinkoms;
4) tarptautinių sutarčių sudarymo galimybės;
5) galimybė teikti paslaugas (sudaryti sutartis) 365 dienas per metus ir 24 val. per parą.

Plėtojantis naujajam sutarčių sudarymo būdui, atsiranda jų teisinio reglamentavimo poreikis. Įstatymo normų, reguliuojančių įprastai sudarytas sutartis, dažnai nepakanka, jos neretai trukdo verslo santykių kompiuteriniuose tinkluose plėtrai.

Su šiomis elektroninio dokumento reglamentavimo ir 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 šiuos procesus pradėjo reguliuoti Jungtinių Tautų tarptautinės prekybos teisės komisija (toliau – *UNCITRAL)*. Šios dvi organizacijos lygiagrečiai atliko reglamentavimo darbą, koncentruodamos veiklą į elektroninės informacijos naudojimo įteisinimą, įrodomojo statuso elektroninei informacijai suteikimą ir teisinio reglamentavimo suvienodinimą atskirose valstybėse, kuris leistų sėkmingai plėtotis elektroninei prekybai.

Elektroninės komercijos įstatymo modelis pagal *UNCITRAL*

UNCITRAL 1998 m. spalį patvirtino Elektroninės komercijos įstatymo modelį (toliau – Modelis). Jo tikslas – suvienodinti valstybių narių teisnę bazę formuojant bendrą požiūrį į elektroninę prekybą, įteisinti elektroninę sutarties sudarymo formą ir prilyginti ją rašytinei.

Rengdama Elektroninės komercijos įstatymo modelį, Komisija siekė, kad valstybėms jis taptų efektyviu teisinės bazės modernizavimo įrankiu ir pateiktų svarbiausią informaciją bei gaires, kuriomis turėtų vadovautis įstatymų, susijusių su elektroninės informacijos naudojimu verslui, kūrėjai. Todėl, rengiant šį Modelį, savo įstatymus kuriančioms valstybėms buvo siekiama pateikti reikalingas gaires, o ne apskritai reglamentuoti elektroninę komerciją. Dėl šios priežasties daugelis nuostatų Modelio tekste nebuvo apibrėžtos, o tik pateiktos kaip paaiškinimai aiškinamajame rašte, kuriame teikiami ne tik Modelio teisinių normų paaiškinimai, bet ir nurodoma, kodėl viena ar kita nuostata yra įtraukta į šį dokumentą.

Šiuolaikinių komunikacijų, tokių kaip *EDI*, elektroninis paštas ir pan., naudojimas prekybiniams santykiams plečiasi, tai lemia greita viešųjų tarptautinių informacinių tinklų plėtra, leidžianti vis daugiau vartotojų naudotis informacija. Tuo pat metu, pasitelkus šiuolaikines technologijas, kuriama, siunčiama ir saugoma informacija susiduria su teisinės vertės kliūtimi, kurią sukuria teisės normos, priimtos gerokai anksčiau, nei atsirado minėtosios technologijos. Modelis pateikia būdą, kaip panaikinti tokias teisines kliūtis ir įteisinti elektroninį informacijos apdorojimą. Didžiausios teisinės kliūtys, su kuriomis susiduria nacionalinės valstybių teisės sistemos, yra šios: rašytinė forma, dokumento parašas, dokumento originalas ir pan.

Rašytinė forma. Modelyje elektroninis pranešimas apibrėžiamas kaip informacijos vienetas, sukurtas, atsiųstas, atsakytas ar saugomas elektroniniu, optiniu ar panašiu būdu, įskaitant *EDI*, elektroninį paštą, telegrafą, teleksą ar telekopijavimą. Be to, numatyta, kad valstybėje, kurios teisinė sistema reikalauja rašytinio informacijos pateikimo, šią formą atitinka elektroninis pranešimas. Įvesdama „elektroninio pranešimo“ sąvoką, *UNCITRAL* laikosi funkcinio ekvivalento požiūrio. Remiantis šiuo požiūriu, elektroninis pranešimas neturėtų idealiai atkartoti rašytinio dokumento rekvizitų ir atitikti rašytiniam dokumentui keliamų formalių reikalavimų. Elektroninis pranešimas turėtų tiesiog atlikti rašytinio dokumento funkcijas: pvz., patikimai pateikti dokumente užfiksuotą informaciją ir gana ilgą laiką nesikeisti, be to, turėtų būti galimybė jį kopijuoti, kad kiekviena sutarties šalis turėtų kopiją, dokumentas privalo būti patvirtintas parašu, leidžiančiu patikimai identifikuoti jį sukūrusį bei informaciją jame patvirtinusį asmenį ir pan. Tokie funkciniai reikalavimai keltini ir elektroniniam pranešimui, tačiau juos įgyvendinti galima visiškai kitais, naujomis technologijomis grindžiamais metodais.

Modelyje koncentruojamasi ne į visas įmanomas rašytinės formos funkcijas, kaip svarbiausios išskiriamos tos, kurios yra susijusios su įrodomąja galia, ir teigiama, kad elektroninis pranešimas atitinka rašytinei formai

keliamus reikalavimus, kai informacija jame yra prieinama ir gana ilgą laiką išlieka nepakitusi. Šiuo atveju žodį „pasiekiamą“ reikėtų suprasti kaip galimybę perskaityti informaciją ir ją interpretuoti, be to, programinė įranga, skirta informacijai perskaityti, turėtų būti įprasta ir lengvai įsigyjama.

Dokumento parašas. Kalbant apie popierinio dokumento parašą, Modelis išskiria tokias jo funkcijas:

1) identifikuoja pasirašiusįjį asmenį;
2) užtikrina, kad šis asmuo būtų įtrauktas į pasirašymo procesą;
3) susieja asmenį su pasirašyto dokumento tekstu.

Dar reikėtų pabrėžti, kad šalyse tradiciškai egzistuoja ir papildomų procedūrų, lygiagrečiai su dokumento parašu ar atskirai nuo jo atliekančių išvardytąsias funkcijas. Tai galėtų būti antspaudavimo ir perforavimo (perdūrimo) ar kitokios procedūros. Modelio kūrėjai visas šias procedūras supranta kaip pasirašymą ir įvardija jas vienu pavadinimu. Elektroninio pranešimo parašo atliekamos funkcijos turėtų būti tokios pačios, todėl Modelio 7 str. ir formuluojami du parašui taikomi kriterijai:

1) pasirašymo metodas turi identifikuoti pasirašiusįjį asmenį;
2) garantuoja asmens pasirašytos informacijos patvirtinimą.

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

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

Reglamentuojant elektroninės sutarties sudarymą, modelis įteisina ofertos ir akcepto elektroninę formą. Vadinasi, naudojantis elektroniniais pranešimais sudaryta sutartis vien dėl šios priežasties negali būti pripažįstama negaliojančia, tačiau gali būti pripažinta negaliojančia dėl kitų teisės aktuose numatytų priežasčių (pvz., Lietuvoje negalioja tik dėl akių sudarytas sandoris, neketinant sukelti kokių nors teisinių padarinių).

Nustatomi apsaugos mechanizmai, draudžiantys sudaryti sutartį tokiu būdu, kai tarpusavyje komunikuoja tik informacinės sistemos ir nereikalaujama žmogaus įsikišimo – įtvirtinama laisva šalių valia, asmeniui suteikiama galimybė spręsti, ar sudaryti sutartį ir prisiimti atsakomybę, ar ne.

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 rengiant *UNCITRAL* elektroninės komercijos įstatymo modelį. Šia direktyva buvo siekiama apsaugoti vartotojo interesus sudarant sutartis tokiais būdais, kai sutarties šalys viena kitos nemato ir betarpiškai nebendrauja vienoje vietoje. Tokios apsaugos tikslas pagrįstas faktu, kad vartotojas, sudarydamas nuotolinės prekybos sutartį, lieka nežinioje, nes prieš sudarydamas sutartį negali apžiūrėti prekės ir įvertinti jos kokybės. Tiek prekės, tiek paslaugos gali būti prastesnės kokybės nei vartotojas tikėjosi, pardavėjas gali turėti prastą reputaciją ar sukčiauti. Vartotojas, įsigijęs nekokybišką prekę, paprastai patenka į nepalankią poziciją pardavėjo atžvilgiu, todėl jo apsaugai skirtina daugiau dėmesio. Direktyva pabrėžia, kad, be joje nustatytųjų, valstybės vartotojui dar gali savarankiškai suteikti papildomų garantijų.

Direktyva kaip nuotolinės prekybos sutartį apibrėžia ne tik tą, kuri sudaryta elektroniniu būdu. Nuotolinės prekybos sutartis apima bet kokią prekių ar paslaugų teikimo sutartį, sudarytą pagal paslaugos teikėjo pasiūlytą mechanizmą, naudojant išimtinai tik nuotolinę komunikaciją. Nuotolinės prekybos sutartimi ji pripažįstama būtent dėl sudarymo būdo, tai gali būti ne tik elektroninis telekomunikavimas naudojant kompiuterinį tinklą, bet ir komunikacija paštu, telefonu ir pan. Ar, remiantis šia direktyva, nuotolinės prekybos sutartimi galima pripažinti sutartį, sudarytą nuotoliniu būdu, tačiau tik po to, kai buvo pristatytos prekės, ir klientas galėjo jas apžiūrėti bei įvertinti? Analizuojant šią situaciją, reikėtų atkreipti dėmesį į nuostatą: „naudojant sutarties sudarymui išimtinai tik nuotolinį komunikavimo būdą“ – jeigu sutartis buvo sudaryta nuotoliniu būdu, išankstinis tiesioginis prekės apžiūrėjimas laikytinas įtakos sutarties sudarymo formai nedarančia aplinkybe. Nuotolinės prekybos sutarties sudarymo būdas direktyvoje suprantamas kaip nereikalaujantis vienalaikio fizinio abiejų sutarties šalių dalyvavimo sutarties sudarymo metu.

Direktyva reikalauja, kad dar prieš sudarant nuotolinės prekybos sutartį pardavėjas vartotojui pateiktų savo duomenis, prekės charakteristiką, prekių ir paslaugų kainas bei teisę atšaukti sutartį. Šiuo atveju pateikimą reikėtų suprasti kaip galimybės vartotojui suteikimą prieš sudarant sutartį

perskaityti ir įvertinti pateiktą informaciją. Netinkamai pateikta informacija bus tuo atveju, jeigu visi reikalingi duomenys bus išsiųsti paštu ir pasieks vartotoją tik tada, kai jis jau bus sudaręs sutartį elektroniniu paštu.

Sudarant nuotolinės prekybos sutartį telefonu ar internetu, informacija yra neilgalaikė, neužtikrinama patikima jos apsauga. Direktyva nurodo, kad vartotojas, sudaręs nuotolinės prekybos sutartį, turi gauti sudarytos sutarties patvirtinimą ilgalaike jam prieinama forma, ne vėliau kaip pristatant prekes. Nėra priežasties manyti, kad patvirtinimas elektroniniu paštu nėra pateikiamas ilgalaike forma, nes žinutę galima išspausdinti ir taip ją išsaugoti.

Remiantis Direktyva, civilinių teisinių santykių srityje kaip viena iš vartotojo teisių gynimo garantijų atsiranda naujovė – sutarties atšaukimo teisė, kuri leidžia vartotojui per septynias dienas atšaukti sudarytą sutartį ir nevykdyti prisiimtų įsipareigojimų bei nemokėti netesybų ar baudų, o tik – prekės grąžinimo mokesčius, jeigu ši buvo atsiųsta.

CK 6.367 str. nustato, kad vartotojas turi teisę atsisakyti pirkimo–pardavimo sutarties, sudarytos naudojant ryšio priemones, ir apie tai privalo raštu pranešti pardavėjui per septynias darbo dienas nuo:

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

Direktyvoje numatomi atvejai, kai sutarties atšaukti negalima:

1) kai, esant vartotojo sutikimui, paslaugos pradedamos teikti dar nesibaigus septynių darbo dienų terminui;
2) kai prekių kainos yra greitai kintančios, priklauso nuo rinkos, kurios pardavėjas nekontroliuoja, pokyčių;
3) kai prekės buvo pagamintos pagal specialiai pirkėjo pateiktą specifikaciją ar pagal savo paskirtį yra pritaikytos konkrečiam asmeniui;
4) kai dėl tam tikrų savybių prekių neįmanoma grąžinti, nes jos yra greitai gendančios ar jų galiojimo terminas gana trumpas;
5) kai yra praplėštos garso ar vaizdo įrašų ir kompiuterinių programų pakuotės;
6) kai parduodami laikraščiai, žurnalai ar kiti periodiniai leidiniai;
7) kai platinami loterijos bilietai.

Svarbiausias klausimas šiuo atveju galėtų kilti dėl „prekių, kurių kainos yra greitai kintančios priklausomai nuo rinkos“. Ši išimtis yra taikoma rinkai, kuri yra labai nepastovi, ir vartotojas, protingai naudodamasis sutarties atšaukimo teise (pvz., užsienio valiutos rinka), gali iš to gauti pelno. Nors iš pirmo žvilgsnio šią išimtį būtų galima pritaikyti daugeliui prekių ar paslaugų, minėtoji direktyvos citata turėtų būti suprantama kiek siauriau.

Teisė atšaukti sutartį prarandama tik tuo atveju, kai įtariama, kad vartotojas iš tiesų atsisakė sutarties dėl vėlesnio prekės kainos sumažėjimo.

Nors direktyva nustato sutarties atšaukimo teisę, ji nereguliuoja išankstinio atsiskaitymo už prekę. Vartotojas, norėdamas atšaukti sutartį, kai pinigai jau sumokėti, patenka į keblią padėtį. Jam kartais lieka tik pasikliauti gera pardavėjo valia. Valstybės narės šią problemą sprendžia įvairiai. Portugalijoje vartotojai neprivalo mokėti už prekes iš anksto, Olandijoje pardavėjas neturi teisės reikalauti didesnio kaip 50 proc. išankstinio atsiskaitymo. Kitas metodas, padedantis išvengti išankstinio mokėjimo problemos, – vartotojo sąskaitoje įšaldyti atitinkamą pinigų sumą, kol baigsis sutarties atšaukimo terminas.

Sudarant nuotolinės prekybos sutartį, Direktyva draudžia tam tikrus komunikavimo būdus. Draudžiama sudaryti sutartis tarp automatinių fakso ar skambinimo mašinų, jeigu abi sutarties šalys iš anksto dėl to nesitarė.

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, susijusius su komerciniais pranešimais, sutartimis, įsiskolinimais, licencijavimu ir tam tikrų reikalavimų įgyvendinimu. Atsižvelgdama į minėtuosius dalykus, Europos Komisija ėmėsi veiksmų visus šiuos visuomeninius santykius reglamentuoti vienu norminiu aktu ir priimė Elektroninės komercijos direktyvą. Minėtoji Direktyva pradėta rengti 1997 m. nuo Europos Komisijos elektroninės komercijos komunikato. Ši iniciatyva buvo intensyviai palaikoma Europos Parlamento. Direktyva siekiama palengvinti laisvą keitimąsi informacinėmis paslaugomis tarp valstybių narių pagal kilmės šalies įstatymus.

Siekis suvienodinti valstybių narių teisinę bazę elektroninių sutarčių klausimais matomas direktyvos 9 str., kuris teigia, jog ES valstybės narės privalo sukurti teisinę bazę, kuri leistų sudaryti elektronines sutartis ir užtikrintų, kad įstatymų, reguliuojančių sutartinius teisinius santykius, reikalavimai nestabdytų elektroninių sutarčių naudojimo ir elektroninės sutarties vykdymo metu sukurti teisiniai santykiai neprarastų savo galios vien dėl to, kad buvo sukurti sudarant elektroninę sutartį. Iš šio straipsnio ir pačios direktyvos esmės matyti, kad Europos Komisija pritaria *UNCITRAL* elektroninės komercijos įstatymo modelio idėjai ir elektroninę sutartį prilygina rašytinei.

Nuo 2006 m. liepos 1 d. įsigaliojo 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 visapusiškai įgyvendino Elektroninės komercijos direktyvos nuostatas.

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

1) informacijos apie paslaugą ir jos teikėją atskleidimo reikalavimus;
2) kai kuriuos sutarčių, sudaromų elektronine forma, aspektus;
3) informacinės visuomenės paslaugų teikėjų (tarpininkų) atsakomybės klausimus.

Informacinės visuomenės paslauga

Šiame įstatyme, kaip ir direktyvoje, tačiau skirtingai nei *UNCITRAL* elektroninės komercijos įstatymo modelyje, įvedama nauja sąvoka „informacinės visuomenės paslaugos". Informacinės visuomenės paslaugomis yra 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 ar kliento informacijos saugojimą, kiek tai yra susiję su ekonomine veikla), tačiau ir kai kurias kitas susijusias paslaugas, iš jų ir prieigą prie elektroninio turinio (tarpininkavimo). Komerciniai pranešimai, naudojant elektroninį paštą, irgi pripažįstami informacinės visuomenės paslauga, išskyrus atvejus, kai asmenys šį telekomunikacijos būdą naudoja verslo ar profesiniams tikslams. Sutarčių tarp individualių asmenų sudarymas elektroniniu paštu dar nelaikomas informacinės visuomenės paslauga. Nustatomas ir papildomas informacinės visuomenės paslaugos kriterijus, t. y. paslaugos, turinčios konkretų adresatą. Paslaugos, teikiamos tiesioginiu darbo režimu, bet ne konkrečiam vartotojui (televizijos ar radijo transliacijos), nėra informacinės visuomenės paslaugos. Informacinės visuomenės paslaugomis nepripažįstami ir darbiniai santykiai tarp darbdavio ir darbuotojo, bei paslaugos, kurios iš esmės negali būti kokybiškai teikiamos per atstumą, pvz., auditas, medicinos pagalba, kai reikia tiesioginės kliento apžiūros, ir pan.

Įstatymas netaikomas mokesčių, rinkliavų, kitų įmokų į valstybės ar savivaldybių biudžetus ir jų administravimo srityse, nereguliuoja asmens duomenų tvarkymo ir privatumo klausimų, notarų ir analogiškoms veiklos rūšims bei paslaugoms, susijusioms su teisminiu atstovavimu, azartinių lošimų ir loterijų veikla.

Pagrindiniai Informacinės visuomenės paslaugų įstatyme deklaruojami informacinės visuomenės paslaugų reglamentavimo principai yra šie: 1) elektroninės formos nediskriminavimo principas, kuris 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; 2) technologinio neutralumo principas reiškia, kad teisės normos turi būti taikomos atsižvelgiant į tikslus, kurių siekiama atitinkamomis teisės normomis, ir stengiantis (kiek tai pagrįsta), kad vien tik dėl jų taikymo nebūtų skatinamas arba diskriminuojamas konkrečių technologijų naudojimas, be to, teisės normos būtų taikomos kiek tik įmanoma neatsižvelgiant į technologijas, kurios naudojamos informacinės visuomenės paslaugoms teikti.

Informacijos pateikimas elektroninėje komercijoje

Daugelio šalių įstatymuose ir ES elektroninės komercijos direktyvoje 2000/31/EB yra nustatytos teisinės normos, kurios reguliuoja informacijos teikimą prieš sudarant sutartį, jos sudarymo metu ir po sutarties sudarymo. Lietuvoje šios normos įtvirtintos CK 6.366 str. ir nustatytos Informacinės visuomenės paslaugų įstatyme.

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

1) paslaugos teikėjo pavadinimą;
2) kontaktus (paslaugų teikėjo fizinį adresą ir informaciją, kuri palengvintų greito kontakto su pardavėju ir (ar) paslaugos teikėju užmezgimą (el. pašto adresas, telefono numeris, telefakso numeris ir pan.);
3) nurodyti valstybės registrą, į kurį jis įrašytas, ir jo registracijos numerį ar analogišką identifikavimo priemonę, jeigu jis užsiregistravęs įmonių ar panašiame viešajame registre;
4) pridėtinės vertės mokesčio (toliau – PVM) mokėtojo kodą (jeigu jis yra PVM mokėtojas);
5) atitinkamos licencijuojamos veiklos priežiūros institucijos rekvizitus, jeigu norint verstis šia veikla būtina gauti įstatymų nustatyta tvarka išduotą licenciją (leidimą);
6) profesinį vardą (pvz., mediko ar 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, jeigu paslaugos teikėjas yra reglamentuojamos profesijos atstovas.

Elektroninės komercijos subjektai, be kitų dalykų, vartotojui turi suteikti aiškios informacijos apie:

1) svarbias produkto ar paslaugos ypatybes;
2) visus galimus pasiūlymo apribojimus, išlygas ir pan.;
3) pasirinktų prekių ir paslaugų kainas (kainos sudėtines dalis būtina aiškiai įvardyti bei įskaičiuotį į galutinę sumą ir tai turi būti atlikta ne vėliau kaip užsakymo metu, paprastai perkeliant prekes į prekių krepšelį ir pan., o ne už jas atsiskaitant);
4) periodą, per kurį galioja specialus pasiūlymas ar specialios kainos;
5) visas svarbias sutarties sąlygas ir terminus (ypač pristatymo, apmokėjimo sąlygas ir terminus ar nuolatinio paslaugų teikimo sąlygas);
6) specifines sąlygas, jeigu jas būtina įvykdyti norint naudotis konkrečiu produktu ar paslauga;
7) visas įmanomas garantines paslaugas ir terminus;
8) pranešimo apie sutarties nutraukimą terminus, kai sudaroma neterminuota arba ilgesnė nei vienų metų sutartis.

Pagal CK 6.366 str. 6 d., iki elektroninės sutarties sudarymo, o kai daiktai tiekiami ne pardavėjo įgaliotojo asmens – iki jų pateikimo, vartotojas raštu turi gauti informacijos apie:

1) siūlomą daiktą (pavadinimas, svarbiausios savybės);
2) pardavėją (nurodant, kur ir kam vartotojas gali pateikti bet kokį skundą);
3) vartotojo teisės atsisakyti vykdyti sutartį tvarką;
4) mokėjimo, pristatymo ar atlikimo tvarką, pardavėjo teikiamas daikto priežiūros paslaugas ir garantijas (jeigu tokios teikiamos);
5) sutarties nutraukimo sąlygas, jeigu sutartis neterminuota arba ilgesnė nei vieni metai.

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

Pabrėžtina, kad informacija turi būti pateikiama vartotojui suprantama kalba, dažniausiai – valstybine. Komercinė informacija turi būti aiškiai atpažįstama, iš jos turėtų būti įmanoma nustatyti fizinio ar juridinio asmens, kurio vardu teikiama komercinė informacija, tapatybę. Iš komercinės informacijos srauto turi būti aiškiai išskiriami reklaminiai pasiūlymai

(nuolaidos, priemokos ar dovanos), o sąlygos, kurias reikia įvykdyti, norint gauti šias nuolaidas, priemokas ar dovanas, turi būti lengvai prieinamos ir aiškiai (nedviprasmiškai) pateiktos. Be to, turėtų būti aiškiai atpažįstami reklaminiai konkursai arba žaidimai, o sąlygos, kurias reikia įvykdyti norint juose dalyvauti, turi būti lengvai prieinamos ir aiškiai (nedviprasmiškai) pateiktos, pvz., netoleruotina, kad svarbi informacijos dalis būtų skelbiama atskiruose tinklalapiuose, kurių vartotojui reikėtų specialiai ieškoti, arba smulkiu neišsiskiriančiu šriftu.

Teisinis elektroninės sutarties pripažinimas Lietuvoje

Nors ir esama įvairios užsienio valstybių praktikos, elektronine forma ir (ar) priemonėmis sudaromos elektroninės sutartys Lietuvoje nėra aiškiai reglamentuotos kaip specifinė sutarčių rūšis ar forma. Šioms sutartims, kaip ir sudaromoms rašytine forma, iš esmės taikomi bendrieji CK nustatyti reikalavimai, tačiau keliama ir papildomų sąlygų. Elektroninėmis priemonėmis neleidžiama sudaryti sutarčių, kurioms įstatymais nustatyta notarinė forma ir privalomoji teisinė registracija. Apskritai paminėtina, kad Informacinės visuomenės paslaugų įstatymo IV skyriuje vartojama sąvoka „sutartis, sudaroma elektroninėmis priemonėmis“ gali būti interpretuojama dvejopai:

- kaip sutartis, kurios sąlygos šalims pateikiamos elektronine forma, o šalys savo valią irgi išreiškia elektroniniu būdu;
- 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 savo valią išreiškia ne elektronine forma.

Sistemiškai analizuojant Informacinės visuomenės paslaugų įstatymo ir CK nuostatas manytina, kad „sutartimi, sudaroma elektroninėmis priemonėmis“ laikytina tik pirmoji aukščiau identifikuota sutarčių kategorija. Deja, ši reguliavimo dviprasmybė leidžia netaikyti elektroninėms sutartims nustatytų taisyklių antros, aukščiau identifikuotos, kategorijos, tokiu būdu informacinės visuomenės paslaugų teikėjas gali išvengti papildomų pareigų vartotojams. Būtent tokią praktiką Lietuvoje šiuo metu taiko finansinių paslaugų teikėjai, kai rašytinėse sutartyse su vartotojais pateikiama blanketinių nuorodų į elektroninius išteklius ir taip suteikiama galimybė paslaugos teikėjui iš esmės vienašališkai, neinformuojant vartotojo, pakeisti sutarties sąlygas ir pan. Tokiu būdu paslaugų teikėjai diskriminuoja vartotojus, kurie tiesiogine prasme sudaro sutartis elektroninėmis priemonėmis. Apskritai pabrėžtina, kad paslaugų teikėjai (ypač profesionalūs paslaugų teikėjai – verslininkai) vengia sudaryti vien tik elektronines sutartis, o elektroninį informacijos ir užsakymų keitimąsi tarp šalių siekia

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 reglamentuotos. CK 1.73 str. 2 d. rašytinės formos dokumentui prilygina šalių pasirašytus dokumentus, perduotus telegrafinio, faksimilinio ryšio ar kitokiais galiniais telekomunikacijų įrenginiais, jeigu yra užtikrinama teksto apsauga ir galima identifikuoti parašą. CK 1.76 str. 2 d. 2. nustato, kad jeigu sandoris buvo sudarytas naudojant galinius telekomunikacijų įrenginius, visais atvejais privalo būti užtektinai duomenų sandorio šalims nustatyti.

Elektroninės sutarties sudarymas

Informacinės visuomenės paslaugų įstatyme yra nustatyta papildomų reikalavimų dėl informacijos, susijusios su elektroninės sutarties sudarymu, užsakymo pateikimu, pasiūlymu sudaryti sutartį (ofertą) ir pateikto pasiūlymo sudaryti sutartį priėmimu (akceptu). Įstatymo 9 str. informacinės visuomenės paslaugos teikėjus įpareigoja paslaugos gavėjui pateikti sutarčių sąlygas (taip pat ir standartines) tokiu būdu, kuris leistų jam šią informaciją išsaugoti ir vėliau ja naudotis. Įstatymo 10 str. nustato, kad gautas elektroninis užsakymas turi būti nedelsiant patvirtintas paslaugos teikėjo elektroninėmis priemonėmis. Vienas iš tokių tinkamų užsakymo gavimo patvirtinimo būdų yra užsakytos informacinės visuomenės paslaugos teikimas elektroninėmis priemonėmis (pvz., prieigos prie elektroninės duomenų bazės ar 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 paslaugos gavėjui turi suteikti tinkamas, veiksmingas ir prieinamas techninės priemones, leidžiančias pastarajam prieš pateikiant užsakymą nustatyti ir ištaisyti įvesties klaidas. Šie reikalavimai yra privalomi, kai viena iš sutarties šalių yra vartotojas, išskyrus tą atvejį, kai užsakymas pateikiamas ir tvirtinamas tik keičiantis elektroninio pašto arba analogiškais individualiais pranešimais. Ši išimtis yra pateisinama, nes pats elektroninio pašto ar individualaus pranešimo formatas nustato, kad atitinkama informacija būtų asmeniškai atsiųsta užsakovui (vartotojui) ir išsaugota jo kompiuteryje ar elektroninio pašto bylose.

Kaip jau minėta, specialios taisyklės nustatytos ir pasiūlymui sudaryti elektroninę sutartį (ofertai) ir pateikto pasiūlymo sudaryti sutartį priėmimui (akceptui). Įstatymo 11 str. visų pirma nustato prezumpciją, kad šalis išsiuntė siūlymą sudaryti sutartį (ofertą) ir (ar) pateiktą pasiūlymą sudaryti sutartį priėmė (akceptą), jeigu juos išsiuntė pati šalis, jos atstovas arba

informacinė sistema, kuri šalies ar jos vardu suprogramuota veikti automatiškai. Ši norma turi ypatingą reikšmę, nes pripažįstama, kad šalis gali išreikšti savo valią iš anksto suprogramuodama informacinę sistemą priimti siūlymus, atitinkančius tam tikras sąlygas. Siūlymas sudaryti sutartį (oferta) ir (ar) pateikto pasiūlymo sudaryti sutartį priėmimas (akceptas) laikomi išsiųsti, kai šalis ar jos atstovas, kurie juos išsiuntė, nebegali jų pasiekti ir kontroliuoti, t. y. neįmanoma jų vienašališkai atšaukti ar paneigti. Savo ruožtu siūlymas sudaryti sutartį (oferta) ir (ar) pateikto siūlymo sudaryti sutartį priėmimas (akceptas) laikomi gauti, kai šalis, kuriai jie skirti, gali juos pasiekti, t. y. gali juos įvertinti ir priimti sprendimą. Įstatymu nustatytas ir elektroninių sandorių jurisdikciją apibrėžiantis principas, teigiant, kad siūlymas sudaryti sutartį (oferta) ir (ar) pateikto pasiūlymo sudaryti sutartį priėmimas (akceptas) laikomi išsiųsti ir (ar) gauti pasiūlymą sudaryti sutartį pateikusios šalies (oferento) ir (ar) pasiūlymą sudaryti sutartį priėmusios šalies (akceptanto) gyvenamojoje arba verslo vietoje.

Tarpininkų vaidmuo sudarant elektroninius sandorius

Direktyva apriboja informacinės visuomenės paslaugų teikėjo finansinę atsakomybę dėl interneto svetainėje skelbiamos informacijos turinio. Tai ypač svarbu telekomunikacijų paslaugas teikiančioms organizacijoms, kurios prižiūri informacijos paslaugų infrastruktūrą ir interneto svetainių savininkams teikia informacijos perdavimo ryšio tinklo ar prieigos prie šio tinklo suteikimo paslaugas.

Paslaugos teikėjai yra atleidžiami nuo finansinės atsakomybės, kai jie paprasčiausiai laikinai saugo ar laiko informaciją. Sąvoka „laikymas“ suprantama kaip tarpinis informacijos saugojimas, siekiant paspartinti jos siuntimą. Pavyzdžiui, jeigu pilietis X Jungtinėms Amerikos Valstijoms priklausantį puslapį pasiekia iš Voriko (Didžioji Britanija) universiteto, šio universiteto serveris paprastai saugo visą informaciją, kurią pilietis X pasiekia, kad galėtų laikinai ja naudotis. Tai paprastai trunka apie valandą. Jeigu pilietis X vėl nori prieiti prie informacijos dar nepraėjus valandai, informacinėse sistemoje išlikę duomenys gerokai sutrumpins laiką, skirtą tai informacijai pasiekti. Esama tam tikrų šios bendrosios informacijos laikymo paslaugos teikimo išimčių. Pati svarbiausia iš jų – teikėjas nesiima skubiai blokuoti priėjimo prie informacijos, gavęs žinių, kad kompetentinga valstybės institucija įpareigojo tai padaryti.

Direktyva numato panašią nuostatą, skirtą vadovauti. Su tipiška vadovavimo situacija susiduriama tada, kai bendrovė, tokia kaip *VirginNet* (Didžioji Britanija), savo interneto svetainę išnuomoja kitam subjektui. Tada asmuo gali laisvai skelbti informaciją internete, nors *e.VirginNet* ir yra interneto svetainės šeimininkė, ji nesistengia kontroliuoti, kokio

pobūdžio informacija joje yra pateikiama. Tokiu atveju vadovavimo paslaugos teikėjai yra atleidžiami nuo finansinės atsakomybės už informaciją, saugomą paslaugos gavėjo prašymu:

1) teikėjas neturi faktinių žinių apie neteisėtą veiklą arba informaciją ir reikalavimų atlyginti žalą atveju nežino apie faktus ar aplinkybes, rodančias, kad verčiamasi neteisėta veikla arba teikiama neteisėta informacija;
2) teikėjas, gavęs tokių žinių arba apie tai sužinojęs, nedelsdamas panaikina šią informaciją arba atima galimybę ją pasiekti.

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

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

Direktyva apima plačią šių priemonių taikymo ir vykdymo nuostatų skalę. Komisija ir valstybės narės skatina kodeksų taikymą Bendrijos lygiu. Nuostatos sukurtos tam, kad padrąsintų su šiuo reikalu susijusias šalis siųsti savo nacionalinių kodeksų projektus Komisijai, kad ši galėtų juos įvertinti pagal jų suderinamumą su Bendrijos teisės aktais. Tačiau kol kas neaišku, ar elgesio kodeksai Bendrijoje pasitvirtins kaip gana veiksmingas ir pastovus teikėjų kontrolės įrankis. Direktyva šių kodeksų nesusieja į kokią nors įpareigojančią teisinę schemą. Tyrimai rodo, kad didelių labai skirtingų rinkų, sudarytų iš mažų segmentų, griežtas bendrasis reglamentavimas gali būti neefektyvus, o elektroninės rinkos dalis yra puikus to pavyzdys.

Toliau skatindama Bendrijos elgesio kodeksų plėtojimą, direktyva nustato, kad efektyvus neteisminių ginčų sistemos sureguliavimas privalo būti reglamentuotas valstybės įstatymais. Direktyva įpareigoja šalis, vadovaujantis Komisijos rekomendacija „Dėl įstatymų, taikytinų dėl neteismi-

nių vartotojų ginčų sureguliavimo“, 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 ypač vertingas sudarant nedidelės vertės sutartis, kai viena šalis yra gerokai už kitą galingesnė. Tokiais atvejais daug brangaus laiko atimančio teismo proceso perspektyva gali įbauginti tuos, kurie turi ribotus išteklius, ir visa tai gali užkirsti kelią išspręsti ginčą. Direktyvos reikalavimas dėl efektyvaus neteisminio mechanizmo prieinamumo yra pozityvus dalykas, ypač iš vartotojų (pirmiausia turint omenyje fizinius asmenis) požiūrio taško.

Teisinė elektroninio parašo galia

Elektroninio parašo direktyva (1999/93/EC) nustatė teisinius e. parašo ir tam tikrų sertifikavimo paslaugų reikalavimus. Nuo 2014 m. liepos 23 d. buvo priimtas Europos Parlamento ir Tarybos reglamentas (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje. Šis reglamentas panaikino ankstesniąją direktyvą.

Direktyva buvo vienas pirmųjų informacinės visuomenės reglamentavimo žingsnių, o jos ašimis buvo tapę:

- juridinis e. parašo pripažinimas;
- e. parašo naudojimo taisyklių nustatymas;
- sertifikavimo paslaugų teikimo įteisinimas ir reglamentavimas.

Be e. parašo, naujuoju reglamentu dar buvo apibrėžta ir elektroninių spaudo, laiko žymos, dokumentų, registruoto pristatymo paslaugų ir interneto svetainių tapatumo nustatymo teisinė sertifikavimo paslaugų schema.

Vadovaujantis funkcinio ekvivalentiškumo ir elektroninės formos nediskriminavimo principais, reglamente buvo įtvirtintas teisinis visų minėtųjų elementų pripažinimas. Tiek teisinė galia, tiek tinkamumas vykstant teismo procesui juos naudoti kaip įrodymą negali būti ginčijami vien tik dėl to, kad šie yra sukurti ar pateikti elektronine forma. Elektroninis parašas prilyginamas rašytiniam. Be to, naujasis reglamentas aiškiai nurodo, kad vienoje ES valstybėje narėje išduotas kvalifikuotas e. parašas, kuris patvirtintas kvalifikuotu sertifikatu, turi būti pripažįstamas ir visose kitose ES valstybėse.

Reglamente neužsimenama apie dokumento pasirašymo vietos nustatymą, nors tai gana svarbu sutarčių teisei. Šį aspektą mini Elektroninės komercijos direktyva, ji teigia, kad nustatant pasirašymo vietą reikėtų remtis bendrosiomis tarptautinės privatinės teisės nustatytomis taisyklėmis.

Kaip jau buvo minėta, reglamentas e. parašą apibrėžia kaip vieną iš įrodinėjimo priemonių. Jis suteikia galimybę jį pateikti teismui kaip įrodymą. Tai dar nereiškia, kad e. parašo nebuvo galima pateikti teismui kaip įrodymo dar iki priimant šį dokumentą ar ankstesniąją direktyvą, tačiau, atsižvelgiant į atskirų ES valstybių procesinės teisės ypatumus, e. parašo naudojimas buvo problemiškas dėl dviejų aspektų:

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

Šios dvi problemos atskirų valstybių narių teisėje pasireiškia skirtingai, tai priklauso nuo šalyse egzistuojančių įrodymų sistemų:

1) laisvo įrodymų pateikimo sistemos (Danija, Švedija) leidžia pateikti teismui visus įmanomus įrodymus. Teisėjas laisvas vertinti įrodymų tinkamumą. Esant tokiai įrodinėjimo sistemai, e. parašas gali tapti įrodymu ir be papildomos reglamentacijos. Tačiau šiuo atveju egzistuoja įrodymų vertingumo hierarchija. Jų vertė yra skirtinga, todėl, esant prieštaringų įrodymų, kyla problema, kuris iš jų pagal įrodymų hierarchiją yra vertingesnis;
2) teisinė įrodymų pateikimo sistema (Vokietija, Ispanija, Portugalija) griežtai nustato įrodymų, kurie yra priimtini teisme, reikalavimus. Teismas priima ne visus įrodymus, o tik tuos, kurie atitinka procesinių normų reikalavimus. Be to, yra reglamentuojama ir įrodymų hierarchija. Esant tokioms sistemoms, popieriniai dokumentai dažniausiai vertinami kaip turintieji didesnę vertę nei žodžiai ar kitokie įrodymai. Tokios sistemos e. parašą gali pripažinti kaip netinkamą įrodymą arba jo vieta įrodymų hierarchijoje yra labai nereikšminga;
3) mišrios sistemos (Prancūzija, Belgija, Liuksemburgas) turi abiejų įrodymų sistemų požymių. Šioje sistemoje e. parašo įrodomoji vertė yra skirtinga.

Būtent įrodinėjimo sistemų įvairovė paskatino į šias sritis įvesti ES reguliavimą, nes įrodinėjimo ir skirtingo įrodymų vertinimo problema galėjo sukelti rimtų elektroninės komercijos ir informacinių technologijų plėtros kliūčių. Nevienodas e. parašo kaip įrodymo vertinimas galėjo smarkiai trukdyti prekėms ir paslaugoms laisvai judėti ES vidaus rinkoje.

Reglamentas nepateikia laisvo įrodymų vertinimo taisyklių, kurias savo nacionaliniais norminiais aktais nustato pačios valstybės narės, todėl šiuo atveju dar svarbesnis tampa eksperto vaidmuo. Tačiau reglamente jau atsisakyta neaiškumą kėlusios sąvokos „pakankamas elektroninio parašo patikimumas“ ir įvesta nauja – „pažangus elektroninis parašas“. Šis parašas turi atitikti šiuos reikalavimus:

- turi būti vienareikšmiškai susietas su pasirašančiuoju asmeniu;
- pagal jį galima nustatyti pasirašančiojo asmens tapatybę;
- sukurtas naudojant e. parašo kūrimo duomenis, kuriuos tik pats pasirašantysis asmuo gali labai patikimai naudoti;
- susietas su juo pasirašytais duomenimis taip, kad bet koks tų duomenų pakeitimas būtų matomas.

Sertifikavimo paslaugų reglamentavimas

Reglamente Nr. 910/2014 irgi kalbama ir apie trečiąjį asmenį, kurio funkcija – užtikrinti e. parašo galiojimą. Pasirašant e. parašu, gali kilti abejonių dėl sutarties partnerio sąžiningumo. Šalys viena kitos nemato ir negali patikrinti tapatybės, todėl reikalingas trečiasis asmuo, kuris garantuotų, kad e. parašas yra būtent to asmens, o ne kito. Toks garantas yra trečiojo asmens – kvalifikuoto patikimumo užtikrinimo paslaugų teikėjo – išduodamas dokumentas (sertifikatas), garantuojantis, kad sertifikato turėtojas yra būtent tas asmuo, kuriuo jis prisistato komunikavimo dalyviams.

Kalbant apie sertifikavimo paslaugas, galima rasti panašumų su notaro atliekamomis rašytinių dokumentų patvirtinimo funkcijomis. Notaro patvirtintas dokumentas turi didesnę juridinę vertę nei paprastas rašytinis. Dėl šios priežasties kai kurios notarų kontoros ES valstybėse pareiškė pageidavimų užsiimti ir sertifikavimo veikla, nes, jų manymu, tai yra toks pat patvirtinimas, kaip ir rašytinio dokumento atveju.

Be to, minėtasis Reglamentas nustato kvalifikuotų e. parašų sertifikatams keliamus reikalavimus. Papildomų privalomų reikalavimų, nei numatyta šiame reglamente, negali būti keliama. Visi tokie papildomi specifiniai kvalifikuoto e. parašo sertifikato reikalavimai gali egzistuoti, tačiau jie nebus privalomi ir neturės jokio poveikio kvalifikuotų e. parašų sąveikumui ir pripažinimui.

Reglamente yra numatyti kvalifikuotiems patikimumo užtikrinimo paslaugų teikėjams keliami reikalavimai. Nustatytas laisvas patikimumo užtikrinimo paslaugų teikimo principas. Valstybės narės neturi riboti, licencijuoti ar kaip nors kitaip stabdyti kvalifikuotų patikimumo užtikrinimo paslaugų teikėjų kūrimosi ir veiklos, neturi būti išduodami išankstiniai leidimai ar keliamos kliūtys užsienio bendrovėms valstybės teritorijoje teikti minėtąsias paslaugas.

Kiekvienai valstybei narei palikta teisė savarankiškai kontroliuoti kvalifikuotų patikimumo užtikrinimo paslaugų teikėjų veiklą. Nacionalinės teisės normos taikomos tiems kvalifikuotų patikimumo užtikrinimo paslaugų teikėjams, kurie veikia (teikia paslaugas) atitinkamos valstybės teritorijoje.

Kontrolės pagrindu tampa Reglamento 24 str. nustatyti kvalifikuotų patikimumo užtikrinimo paslaugų teikėjui keliami reikalavimai ir 1995 m. Europos Komisijos direktyvos dėl fizinių asmenų asmeninių duomenų apsaugos nuostatos, nurodančios, jog asmeninių duomenų rinkimas pateisinamas tik tuo atveju, kai juos rinkti būtina, siekiant kokybiškai teikti paslaugas, ir gali būti atliekamas tik gavus asmens, kurio duomenys renkami, sutikimą.

Reguliuojant kvalifikuotų paslaugų teikimo patikimumo užtikrinimą ir saugant asmens privatų gyvenimą, numatytas draudimas neleisti sertifikato naudotojui vietoj tikrosios pavardės suteikti slapyvardžio. Reglamentas iš principo leidžia naudotis slapyvardžiu, tačiau šiuo atveju kvalifikuotų patikimumo užtikrinimo paslaugų teikėjas turi turėti tikruosius asmens duomenis ir juos pateikti nacionalinės ar ES teisės numatytais atvejais.

Tačiau bene stipriausias saugiklis, reguliuojant sertifikavimo veiklą, yra kvalifikuotų patikimumo užtikrinimo paslaugų teikėjo atsakomybės prezumpcija. Jeigu tretiesiems asmenims pagal sertifikavimo sutartį padaroma žalos, sertifikate nurodant neteisingą informaciją, sustabdant ar atšaukiant sertifikatą, ar jo neregistruojant, tokiu atveju atsako kvalifikuotų patikimumo užtikrinimo paslaugų teikėjas. Šis principas yra palankus tretiesiems asmenims, kurie ginčo atveju turės įrodinėti tik žalą, atsiradusią dėl neteisėtos veikos, bei priežastinį žalos ir sertifikavimo sutarties ryšį. Kvalifikuotų patikimumo užtikrinimo paslaugų teikėjas, paneigdamas savo kaltę, turės įrodyti, kad žala atsirado ne dėl jo kaltės, o dėl trečiojo asmens aplaidumo (neprotingai ar turėdamas piktybiškų tikslų naudojo sertifikatą, nepasinaudojo *on-line* pateiktu atšauktų sertifikatų sąrašu, viršijo leistinas sadorių sumas), papildomai sertifikavimo paslaugų teikėjas dar gali paminėti *force majoure* aplinkybes.

Alternatyvūs vartotojų elektroninių ginčų sprendimai

Vis didesnis interneto erdvės naudojimas skatina dėl elektroninės prekybos santykių kylančius ginčus. Šiems ginčams būdinga tai, kad dažniausiai jie yra globalaus pobūdžio ir nedidelės vertės. Tokiems ginčams spręsti kol kas buvo naudojami tradiciniai ginčų sprendimo būdai. Tačiau minėtieji būdai šiuo metu neatitinka vartotojų poreikių. Tad skatintini alternatyvūs ginčų su vartotojais sprendimo elektroninės prekybos srityje mechanizmai. Elektroninės komercijos direktyvos 17 str. nurodoma, kad nacionalinė teisė neturi kliudyti atsirasti neteisminėms ginčų sprendimo procedūroms.

Vis daugiau verslo sandorių perkeliama į e. erdvę. Kartu keičiasi ir žmonių bendravimas sudarant tokius sandorius. Ginčams interneto erdvėje spręsti pasitelkiamos informacinės technologijos. Tačiau reikėtų pabrėžti,

kad tos pačios technologijos sėkmingai naudojamos ir sprendžiant tradicinius ginčus.

Autoriai dažniausia išskiria tris pagrindines ginčų sprendimo internete technologijas:

1) visiškai automatizuoti ginčų sprendimo mechanizmai e. erdvėje. Tokio tipo svetainėse ginčų šalys pateikia savo skundus, kuriems išspręsti nustatomas fiksuotas terminas. Sistema elektroniniu paštu informuoja kitą šalį apie pasiūlytą ginčo sprendimo variantą ir suteikia prisijungimo prie interneto svetainės duomenis. Šalis gali sutikti arba nesutikti dalyvauti sprendžiant ginčą tokiu būdu. Jeigu šalis sutinka, ji prisijungia prie svetainės ir pateikia savo reikalavimus. Programinė įranga automatiškai sulygina abiejų šalių reikalavimus ir elektroniniu paštu išsiunčia pranešimą, kurios pozicijos sutampa ir kurios skiriasi. Skirtingos sistemos numato nevienodą ciklų skaičių, kai šalys gali pateikti savo reikalavimus. Kai kurios sistemos nuo pat pradžių prašo pateikti visus reikalavimus kiekvienam ciklui atskirai. Galimas variantas, kai ciklų skaičius neribojamas, tačiau nustatytas laikas, per kurį šalys privalo baigti ginčą;
2) tarpininkavimas e. erdvėje naudojant specialią programinę įrangą ir dalyvaujant neutraliai trečiajai šaliai. Šioje sistemoje tarpininkas bendrauja su kiekviena šalimi tiek internetu, tiek tradiciškai ir padeda joms pareikšti savo ginčo sprendimo reikalavimus. Kai kuriose sistemose tarpininkai turi išeiti specialius 30 val. mokymo kursus. Kiekviena šalis pateikia bent po keletą reikalavimų. Paskui šalys išsirenka, jų manymu, tinkamiausius viena kitos pasiūlymus ir programinė įranga kartu su tarpininku suderina jų interesus, kad abi šalys gautų daugiausia naudos;
3) tradicinis tarpininkavimas naudojant internetą. Tokios svetainės yra įsteigtos bendrovių tarpininkių arba pačių elektroninės komercijos įmonių. Tai tradicinis tarpininkavimas arba bendravimas su vartotojais, tačiau pirmenybė teikiama komunikavimui, grindžiamam informacinėmis technologijomis.

Internetu teikiamos ir kitos paslaugos, kurios nėra tiesioginis ginčų sprendimo internetu atitikmuo, tačiau iš dalies prisideda priimant galutinį sprendimą: įvertinimas ir rekomendacijos (trečiųjų šalių pateikta nuomonė dėl nagrinėjamojo ginčo esmės), diskusijų nutraukimas (proceso, kurį šalys buvo paskubomis inicijavusios, nutraukimas, nors ginčo priežastis yra paprasčiausias nesusipratimas ar techninis nesklandumas), vidinis skundų valdymas (standartinis skundas kartais gali būti nukreiptas į elektronine

prekyba užsiimančio pardavėjo tokio pobūdžio skundų sprendimo sistemą), pagalba sprendžiant ginčus (pradedamas nagrinėti ginčas gali būti nukreipiamas į kitas sistemas, pvz., pasitikėjimo ženklus teikiančių subjektų svetaines) ir kitos paslaugos (teisinė konsultacija, informacijos apie verslo praktiką pateikimas ir ginčų sprendimas, vartotojų atsiliepimų paskelbimas ir kt.). Visi šie metodai, palyginti su tradiciniais, suteikia galimybę juos pritaikyti kiekvienos ginčo šalies poreikiams. Ginčų sprendimo internete pranašumai lemia didėjantį jų populiarumą, ypač tarp elektroninės prekybos subjektų:

- Lėšų taupymas – tai vienas iš pranašumų, kurį suteikia ginčų sprendimo internetu metodas. Ši sistema ypač palanki toms ginčo šalims, kurios dėl ginčo sprendimo negali keliauti didelių atstumų, taip pat sandoriams, kurių vertė nėra didelė, ir tradicinis ginčų sprendimas tiesiog būtų finansiškai nenaudingas. Naudojantis šiuo metodu, šalims neprivalu išleisti daug pinigų advokatams. Nereikalingi tarptautiniai skambučiai.
- Laiko taupymas. Šalys be jokio išankstinio pasirengimo gali pradėti teikti savo siūlymus dėl susitikimo laiko ir vietos. Nebūtina skirti laiko susitikimams derinti.
- Šalių anonimiškumas. Šalims vienai kitos nematant ir neturint jokio tiesioginio ryšio, yra mažesnė tikimybė, kad tarp jų gali kilti koks nors ginčas dėl asmeninės, rasinės, lytinės, amžiaus ar kitokios antipatijos.
- Patogumas derėtis. Naudojantis interneto technologijomis, priešingai nei tradiciniu būdu, šalys neprivalo tuo pat metu būti prisijungusios prie sistemos. Be to, taupomas laikas, nes tarpininkai gali visą dėmesį skirti vienai šaliai ir neversti laukti kitos. Bendravimas elektroniniu paštu iš dalies apsaugo šalis ir nuo impulsyvių pareiškimų viena kitos atžvilgiu.
- Išvengiama keblių jurisdikcijos problemų. Sistema labiau pritaikyta ieškoti kompromiso, o ne taikyti nuobaudą, todėl šalims nėra aktualios imperatyviosios valstybių nuostatos. Svarbiausias motyvas – didžiausia abipusė nauda. Tarpininkų (tiek programinės įrangos, tiek žmonių) tikslas – rasti ne teisės aktą, kuris buvo pažeistas, o priemonę ir (ar) sprendimą, kuris būtų priimtinas abiem šalims.

Išskiriami ir šie papildomi alternatyvių ginčų sprendimo mechanizmų pranašumai: nepriklausomumas, skaidrumas ir prieinamumas vartotojams.

Didžiausias ginčų sprendimo internetu paradoksas – šalys viena su kita niekada nesusitinka. Jos nežino viena kitos silpnybių ir trūkumų. Vykstant

tradiciniams ginčams, buvo įprasta tiesiogiai bendraujant su kita šalimi ieškoti kompromiso. Naujasis mechanizmas jokiu būdu negali būti veidrodinis tradicinių ginčų atspindys. Toks skirtumas, be abejo, sudaro šalims ir tam tikrų kliūčių, dėl kurių pati sistema ne visada yra priimtina:

- Apribota ginčų sritis. Visiškai automatizuoti ginčų sprendimo mechanizmai gali būti efektyvūs tik sprendžiant finansinius klausimus. Dažnai šalys jau iki tol turi būti sutarusios, kas ir kiek kaltas dėl jų ginčų. Sistemai turi būti pateikiami pradiniai duomenys, kad ji galėtų tinkamai įvertinti derinamus finansinius klausimus.
- Nepriimtina bendravimo aplinka. Šių sistemų nenaudos žmonės, kuriems bendravimas kompiuteriu dėl įvairių priežasčių yra nepriimtinas. Šis trūkumas gali pasireikšti dažniausiai tada, kai šalys sudaro tradicinius sandorius.
- Dideli mokesčiai. Nors jau buvo minėta, kad naujasis ginčų sprendimo mechanizmas leidžia taupyti lėšas, vis dėlto kai kurios esamos sistemos išlieka pernelyg brangios smulkesniems sandoriams. Ne visos bendrovės pateikia įkainius, tačiau kai kurių mokestis siekia net iki 500 ir daugiau eurų.
- Konfidencialumas. Šios sistemos kelia šalims rūpesčių dėl jų pateikiamos informacijos konfidencialumo. Šalis nėra garantuota, kad jos pateiktas rašytinis dokumentas nebus išplatintas ar kaip nors kitaip panaudotas.

Be to, pabrėžiama, kad alternatyvūs ginčų sprendimo mechanizmai dažnai neužtikrina tinkamo kokybiško teisingumo, stinga vartotojų pasitikėjimo tokiais ginčų sprendimo mechanizmais.

Viena pirmųjų iniciatyvų Europoje – Dublino ir Namiūro universitetų projektas *ECODIR*, kurį 2001 m. spalį finansavo Europos Komisija. Įgyvendinant šį projektą sukurta internetines paslaugas teikianti sistema buvo orientuota į internete sudarytus „verslas vartotojui“ sandorius. Paslaugos dalyviams teikiamos nemokamai. Sistema yra suskirstyta į tris etapus:

- Derybos. Šiuo etapu šalys, naudodamosi sistemos teikiamomis komunikavimo galimybėmis, pačios mėgina rasti joms priimtiną sprendimą.
- Tarpininkavimas. Šis etapas prasideda, kai šalys bendram kompromisui rasti pasitelkia tarpininko pagalbą.
- Rekomendacijos. Tarpininkas pateikia rekomendacijas vienai iš šalių, jeigu šios neranda bendro sutarimo.

Nuo pirmųjų Europos Komisijos finansuotų projektų praėjo daugiau kaip dešimt metų, kai ES priėmė du svarbius šią sritį reglamentuojančius teisės aktus. 2013 m. gegužės 21 d. buvo patvirtinta Europos Parlamento ir Tarybos direktyva Nr. 2013/11ES dėl alternatyvaus vartotojų ginčų sprendimo, kuria iš dalies keičiami Reglamentas (EB) Nr. 2006/2004 ir Direktyva 2009/22/EB (Direktyva dėl vartotojų AGS) bei 2013 m. gegužės 21 d. buvo patvirtintas Europos Parlamento ir Tarybos reglamentas (ES) Nr. 524/2013 dėl elektroninio vartotojų ginčų sprendimo, kuriuo iš dalies keičiami Reglamentas (EB) Nr. 2006/2004 ir Direktyva 2009/22/EB (Reglamentas dėl vartotojų EGS).

Šiais dokumentais yra reglamentuotas ginčų sprendimas verslas-vartotojui sudarant pirkimo–pardavimo ar paslaugų teikimo sandorius. Šiuose teisės aktuose vartotojas apibrėžiamas kaip fizinis asmuo, kuris veikia siekdamas su savo verslu, amatu ar profesija nesusijusių tikslų.

Alternatyvaus ginčų sprendimo subjektai privalo valstybės institucijoms pateikti reikiamos informacijos ir turi būti įtraukti į sąrašą, kuris būtų prieinamas visiems ES vartotojams. Bendras alternatyvaus ginčų sprendimo subjektų reglamentavimas turi sudaryti palankias sąlygas vartotojams jų paslaugomis naudotis visoje ES teritorijoje. Valstybių institucijos yra įpareigotos, kad minėtieji subjektai būtų nepriklausomi ir nešališki, o juose dirbantys asmenys turėtų būtinų ekspertinių žinių.

Šiems ginčams spręsti Europos Komisija sukuria elektroninio vartotojų ginčų sprendimo platformą, kuri būtų patogi naudoti, užtikrintų vartotojų privatumą ir būtų visiems prieinama. Reglamentas Nr. 524/2013 nustato reikalavimus dėl skundo pateikimo, ginčo sprendimo, asmens duomenų tvarkymo, vartotojams teikiamos informacijos.

Apibendrinant reikėtų pasakyti, kad sudarant šiuolaikinius verslo sandorius alternatyvūs ginčų sprendimo mechanizmai duos daugiau naudos nuotoliniu būdų sudaromiems sandoriams ir ypač turintiems nedidelę vertę. Pastarųjų metų ES priimti sprendimai tik dar kartą patvirtina, kad elektroninei prekybai reikia ieškoti alternatyvių būdų ir pateikti adaptuotų premonių, kurios tik dar labiau skatintų tokios formos prekybą.

1.3. Elektroninės komercijos apmokestinimas

Elektroninės komercijos sampratos apmokestinimo kontekste

Siekiant pateikti tinkamą elektroninės komercijos sąvoką, kuri atspindėtų apmokestinimo ypatybes, svarbu atsižvelgti į tiesioginių ir netiesioginių mokesčių specifiką. Nagrinėdami netiesioginius mokesčius, matysime, kad kai kurie sandoriai buvo įmanomi dar iki kompiuterinių sistemų ir jų tinklų išplėtojimo. Naudojantis faksimilėmis ir teleksais, buvo galima pateikti

užsakymus nuotoliniu būdu. Tačiau pirkėjui pristatyti prekes buvo įmanoma tik materialiąja jų forma.

Tokie prekybos sandoriai egzistavo jau gana ilgą laiką. Tam tikslui buvo priimti atitinkami teisės aktai, reglamentuojantys specifines minėtųjų sandorių sritis. ES buvo priimta Nuotolinės prekybos direktyva. Panašios nuostatos buvo įtvirtintos ir kitų valstybių teisės aktuose. Palyginti su elektroninės komercijos ypatybėmis, šių sandorių specifika buvo ta, kad parduodamos prekės materialiąja forma turėjo būti gabenamos tik per valstybių sienas. Taip buvo galima užtikrinti prekių judėjimo srautų kontrolę ir atitinkamą jų apmokestinimą.

Tik išsiplėtojus informacinėms technologijoms, tapo įmanoma perkelti prekes į e. erdvę. Tokia galimybė atsirado tada, kai minėtosiomis priemonėmis kai kurias prekes buvo galima išreikšti skaitmenine forma (nematerialiąją išraišką turinčiais produktais). Pagrindinės tokios prekės būtų šios: knygos, žurnalai, muzikos ir vaizdo įrašai, kompiuteriniai žaidimai, programinė įranga ir kt.

Jeigu kompiuterinėmis sistemomis ir telekomunikaciniais tinklais bus vykdomos visos verslo operacijos – išskyrus paskutiniąją (prekės pristatymą pirkėjui), tada pažangias informacines technologijas (kompiuterines sistemas ir internetą) galėsime prilyginti faksimilėms ar teleksams. O tokių sandorių teisinis reglamentavimas yra užtikrintas iki šiol nuotolinius komercinius sandorius reglamentuojančiomis teisės normomis.

Kalbant apie prekybą e. erdvėje ir šių sandorių apmokestinimo netiesioginiais mokesčiais galimybes, reikėtų pabrėžti, kad prekės, perkeltos į e. erdvę, visiškai išvengia tradicinei prekybai būdingų kontrolės punktų. Todėl, norint analizuoti elektroninės komercijos apmokestinimą netiesioginiais mokesčiais, pirmiausia reikėtų suformuluoti elektroninės komercijos apibrėžimą, kuris atspindėtų būtent naujų sąlygų palaikant tradicinius mokestinius santykius atsiradimą.

Viena iš elektroninės komercijos specifinių ypatybių – galimybė perkelti prekes į e. erdvę. Tačiau ne visos prieš tai minėtuosiuose elektroninės komercijos apibrėžimuose pateiktos technologijos gali atlikti šią funkciją. Tik kompiuterinės sistemos kartu su programine įranga gali atitinkamas prekes paversti skaitmenine jų forma. Jokios kitos technologijos tokios galimybės neturi.

Kita elektroninės komercijos specifika susijusi su tuo, kad kompiuterinės sistemos kartu su globaliu telekomunikacijų tinklu leidžia nematerialiąją išraišką turinčias prekes elektroniniu būdu persiųsti pirkėjui. Tai paskutinė ir svarbiausia verslo operacija, kurios buvimas elektroninei komercijai suteikia naujų savybių.

Atsižvelgiant į minėtuosius argumentus, elektroninės komercijos apmokestinimui netiesioginiais mokesčiais taikoma ši elektroninės komercijos samprata – tai e. erdvėje vykstanti prekyba prekėmis ar paslaugomis tarp mokestiniuose santykiuose dalyvaujančių subjektų, kai įvykdomos visos verslo operacijos – pradedant prekių ar paslaugų reklamavimu (pateikimu) ir baigiant jų pristatymu galutiniam vartotojui.

Pateiktoje sąvokoje nesiekiama nurodyti konkrečių technologijų, kurios naudojamos elektroninei komercijai. Kaip jau minėta, e. erdvė gali būti sukurta tik pasitelkus kompiuterines sistemas ir tinklus, jokios kitos technologijos to padaryti negali. Be to, sąvokoje nėra sukonkretinta, kad prekės turi būti išreikštos skaitmenine forma. Tačiau bet kokia prekyba e. erdvėje įmanoma tik tada, kai prekės yra parduodamos skaitmeniniu pavidalu. Tačiau pirkėjas, norėdamas gauti tam tikrų elektroninių paslaugų ar prekių, nebūtinai turi naudotis kompiuterine įranga. Mobiliaisiais telefonais jau dabar galima parsisiųsti logotipų, žaidimų ar melodijų ir atsiskaityti už suteiktas paslaugas. Ši „elektroninės komercijos“ sąvoka kol kas geriausiai atspindi elektroninės prekybos apmokestinimo netiesioginiais mokesčiais pateiktas mokestinių santykių naujoves ir jų teisinį reglamentavimą.

Elektroninės komercijos apmokestinimas tiesioginiais mokesčiais išryškina visiškai kitas ypatybes, kurias svarbu tinkamai teisiškai reglamentuoti. Šiuo atveju didesnės įtakos neturės tai, kokia forma prekė pristatoma į užsienio valstybę. Norėdamos tinkamai pritaikyti tiesioginių mokesčių teisines normas, valstybių institucijos neturėtų kontroliuoti prekės judėjimo. Svarbiausia aplinkybė, lemianti tinkamą tiesioginių mokesčių pritaikymą elektroninei komercijai – nustatyti, kaip valstybėje yra atstovaujama užsienio bendrovei. Todėl, skirtingai nei taikant netiesioginius mokesčius, prekės galutiniam vartotojui gali būti pristatomos tiek materialiąja, tiek ir nematerialiąja forma.

Apibendrinus aukščiau pateiktas elektroninės komercijos sampratas, taikomas apmokestinant tiesioginiais ir netiesioginiais mokesčiais, galime išryškinti pagrindinį skirtumą, kuris priklauso nuo to, kokia mokesčių sistema yra taikoma. Prekių pristatymą materialiąja forma galima analizuoti tik nagrinėjant elektroninės komercijos apmokestinimą tiesioginiais mokesčiais. Tuo metu nagrinėjami tik netiesioginiai mokesčiai už e. erdve pristatomas prekes.

Elektroninės komercijos prekių ir paslaugų apmokestinimas

Nors dauguma autorių, kalbėdami apie elektroninę komerciją, vartoja terminą „prekės“, nėra bendros nuomonės, kaip konkrečiai jas pristatyti – kaip prekes ar kaip paslaugas. Tradicinės komercijos atveju tokia dilema

neiškildavo, nes buvo gana paprasta atskirti prekes nuo paslaugų. Pagrindinis kriterijus, kuriuo buvo vadovaujamasi, – materialioji prekių išraiška. Elektroninės komercijos atveju, kai prekės pristatomos e. erdvėje, remtis šiuo kriterijumi neįmanoma. Pagal Lietuvos Respublikos PVM įstatymo 3 str. nuostatas, prekių tiekimas ir paslaugų teikimas yra laikomi PVM objektu, todėl šis klausimas ypač aktualus dėl PVM, siekiant tiksliai identifikuoti jo objektą.

Elektroninės komercijos sandoriai, tokie kaip programinės įrangos ar knygų, muzikos, filmų ar kitokių garso ar vaizdo kūrinių pirkimas ir 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 pagrindinės elektroninei komercijai priskiriamos prekės, kurias galima paversti virtualiosiomis, yra knygos, žurnalai, laikraščiai, programinė įranga, filmai, muzika ar nuotraukos. Norint tinkamai taikyti PVM nuostatas, svarbu nustatyti, kokiai kategorijai priskirtinos virtualios prekės – prekių ar paslaugų.

Direktyvoje „Dėl pridėtinės vertės mokesčio“ pareikšta nuomonė, pagal kurią virtualios prekės dėl savo nematerialumo yra priskiriamos paslaugų kategorijai. Remiantis šia direktyva ir 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 priskirtinos elektroniniu būdu teikiamoms paslaugoms. Šiai nuomonei pritarė ir Pasaulio prekybos organizacija (toliau – PPO). Tokia pat išvada buvo padaryta ir per 1998 m. Otavoje vykusią EBPO ministrų konferenciją.

2003 m. sausio 8 d. Europos Komisija patvirtino Pridėtinės vertės mokesčio komiteto dėl elektroniniu būdu teikiamų paslaugų pasiūlytas gaires. Toks paslaugų apibūdinimas ir pateiktas sąrašas yra gana reikšmingas norint pritaikyti tinkamą apmokestinimo būdą, nes ES direktyvoje „Dėl pridėtinės vertės mokesčio“ nėra konkretizuota, kokios paslaugos laikomos teikiamomis 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 turėtų labiausiai priklausyti nuo informacinių technologijų (paslauga automatizuota, reikia minimalaus žmogaus įsikišimo, be informacinių technologijų ji išvis negalėtų būti teikiama).

Apibrėždami elektroninės komercijos sąvoką, jau minėjome, jog nagrinėjant netiesioginį apmokestinimą svarbu pabrėžti, kad tais atvejais, kai sandorio šalys bendrauja virtualioje erdvėje, tačiau pati prekė pristatoma ar 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 ir elektroniniu būdu, ir tradiciškai teikiamoms paslaugoms. Tai priklausys nuo informacinių technologijų vaidmens teikiant šias paslaugas. Pavyzdžiui, nuotolinis mokymas bus pripažįstamas elektroniniu būdu teikiama paslauga, jeigu ji bus visiškai automatizuota, teikiama internetu ir nereikės žmogaus įsikišimo. Tačiau jeigu internetas bus naudojamas kaip studento ir dėstytojo bendravimo priemonė (reikiama mokomoji medžiaga bus siunčiama elektroniu paštu ir pan.), tai jau nebus priskiriama elektroniniu būdu teikiamai paslaugai. Tokios pat taisyklės taikomos ir finansinėms ar teisinėms konsultacijoms.

Pagal šiuos kriterijus, Europos Komisijos gairėse pateikiamas ir konkretus elektroniniu būdu teikiamų paslaugų sąrašas: internetinių svetainių ir nuotolinis programų darbo palaikymas, duomenų saugojimas, programinės įrangos ir teminių kompiuterinių sistemų – darbalaukių (angl. *desktop themes)* parsisiuntimas, knygų ir skaitmeninio formato leidinių, elektroninių žurnalų bei laikraščių prenumerata ir (ar) abonentinis mokestis, e. erdvėje teikiama teisinė bei finansinė informacija (pvz., duomenys apie vertybinių popierių rinką), reklamai skirtos vietos internete suteikimas, mokamų paieškos sistemų naudojimas, muzikos kūrinių, vaizdo filmų, elektroninių žaidimų parsisiuntimas tiek į kompiuterius, tiek ir į mobiliuosius telefonus, žaidimas e. erdvėje, nuotolinis mokymas, įskaitant virtualias mokymo klases, ir kt.

Be abejo, šis sąrašas nėra išsamus. Sudaryti tokio išsamaus sąrašo net nebūtų įmanoma, nes sparti informacinių technologijų plėtra suteikia vis daugiau galimybių įtraukti naujų paslaugų, kurios galėtų būti teikiamos elektroniniu būdu. Be to, šiose gairėse buvo pateiktas sąrašas paslaugų, kurios nėra pripažįstamos teikiamomis elektroniniu būdu:

Lietuvos PVM įstatymas nepateikia elektroniniu būdu teikiamų paslaugų apibrėžimo, tačiau 13 str. 14 d. 8 p. sudarytas pagrindinių paslaugų, kurios priskirtinos prie teikiamų elektroniniu būdu, sąrašas: „...interneto puslapių kūrimas ir jų priežiūra, kompiuterinių programų tiekimas, jų

atnaujinimas ir priežiūra, prieigos prie duomenų bazių teisės suteikimas, muzikos kūrinių, filmų, žaidimų tiekimas, 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 virtualių prekių priskyrimo prekių ar paslaugų kategorijai koncepcija teigia, kad virtualios prekės turi būti vertinamos ne kaip paslaugos, o kaip prekės. Tokio požiūrio laikosi JAV ir Japonija, kurios nesieja prekių su materialiąja jų išraiška. Pasaulinė informacinių technologijų ir paslaugų sąjunga (toliau – *WITSA*) dėl vartojimo mokesčio virtualias prekes 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, buvo pareikšta ir priešinga nuomonė. Tuo atveju, kai viena iš sandorio šalių kitai šaliai užsako sukurti turtą (elektroninės komercijos srityje šiuo turtu galime laikyti programinės įrangos sukūrimą ir pan.) ir pirmoji sandorio šalis valdo šį turtą nuo jo sukūrimo momento, tada tokio turto pristatymas pirmajai sandorio šaliai bus vertinamas kaip paslaugos teikimas. Tuo atveju, kai toks turtas pagal užsakymą bus sukurtas ne vienai sandorio šaliai, o parduodamas daugeliui vartotojų (pabrėžtina, kad dažniausiai būtent tokiu būdu vyksta automatizuotas pardavimas internetu), jis turėtų būti vertinamas ne kaip paslaugos teikimas, o kaip prekės pristatymas.

Kaip matyti iš aukščiau pateiktų argumentų, požiūris į virtualias prekes turi įtakos pridėtinės vertės mokesčiui. Akivaizdžiausiai tai matoma nagrinėjant kai kurioms prekėms taikomus mažesnius mokesčių tarifus. Standartiniai ar mažesni mokesčių tarifai taikomi ir prekėms, tiekiamoms elektroniniu būdu ar fiziškai, pvz., knyga, parduota popierine forma ar parsisiųsta iš interneto kaip tekstinis failas, lemia skirtingų mokesčių tarifų nustatymą prekėms, kurių turinys toks pat, tačiau skiriasi jų išraiškos ir pristatymo forma.

PVM įstatymo 19 str. 3 d. 2 ir 4 p. nustato vieną iš prekių, kurioms taikomas lengvatinis devynių procentų PVM tarifas, rūšių: „knygoms ir neperiodiniams informaciniams leidiniams (įskaitant vadovėlius, pratybų sąsiuvinius, enciklopedijas, žodynus, žinynus, informacines brošiūras, nuotraukų ir reprodukcijų albumus, vaikiškas knygeles su paveikslėliais, piešimo ir spalvinimo knygeles, spausdintas ar rankraštines natas, žemėlapius, schemas ir brėžinius, tačiau išskyrus kalendorius, užrašų knygeles ir kitus panašaus pobūdžio spaudinius); laikraščiams, žurnalams ir kitiems periodiniams leidiniams, išskyrus erotinio ir (ar) smurtinio pobūdžio arba

profesinės etikos nesilaikančius 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 elektroninei komercijai, nes jos gali būti išreikštos skaitmenine forma ir pristatytos e. erdvėje. Tačiau tokios virtualios prekės, skirtingai nei tradicinėje komercijoje, bus vertinamos kaip elektroniniu būdu teikiama paslauga ir joms taikomas standartinis dvidešimt vieno procento PVM tarifas. Panašūs lengvatiniai PVM tarifai šioms prekėms nustatomi ir kitose ES valstybėse.

Nuostata dėl tokio skirtingo prekių vertinimo, atsižvelgiant ne į jų turinį, o į išraiškos formą bei pristatymo būdą, galėtų būti laikoma principo dėl vienodo vertinimo pažeidimu. Šiuo atveju, neatsižvelgiant į minėtosios prekės išraišką (skaitmeninė ar popierinė forma), savo turiniu ji bus visiškai identiška. Pozicijai, kad pagal savo turinį identiškoms prekėms būtų taikomi skirtingi PVM tarifai, nepritaria ir *WITSA*. Jos teigimu, mokesčių srityje yra remtina tokia valstybės politika, kai neatsižvelgiant į prekių pristatymo būdą taikomi atitinkamai vienodi PVM tarifai. Tokiu atveju nebus pažeidžiamas neutralumo principas.

Be to, reikėtų pabrėžti, kad toks prekės įsigijimas turi būti susijęs su jos parsisiuntimu ir išsaugojimu galutinio vartotojo (pirkėjo) kompiuterinės sistemos kietajame diske. Be abejo, interneto teikiama galimybė, prisijungus prie svetainių, naudotis jose esančiais atitinkamais produktais (pvz., enciklopedijomis, žodynais ir kt.), nesant galimybės jų parsisiųsti ir išsaugoti savo kompiuterinės sistemos kietajame diske, turėtų būti priskiriama paslaugai.

Virtualias prekes, kaip ir daugumą kitų, galime saugoti, sunaikinti, kopijuoti ar perduoti kitiems asmenims ir pan. Turbūt sunkiai galime įsivaizduoti paslaugą, kurią įmanoma išsaugoti ar sunaikinti. Tokio pobūdžio operacijos būdingos tik prekėms.

Svarbiausias argumentas, kuriuo remiantis virtualios prekės pateikiamos kaip paslaugos, yra jų nematerialioji išraiška. Tačiau reikėtų paminėti, kad virtualių prekių dėl vartojimo mokesčio priskyrimas prekių kategorijai nebūtų išimtis ES (ir Lietuvos) kontekste. Netgi tradicinės komercijos srityje pasitaiko atvejų, kai prekėms priskiriami ir kai kurie materialiosios išraiškos neturintys objektai. Minėtosios PVM įstatymo nuostatos tokiais objektais jau dabar laiko elektros energiją, dujas ir šilumą. Taigi, valstybės nuožiūra, kai kurioms prekėms yra suteikiama išimčių (jeigu pagrindine nuostata laikysime tai, kad prekės turi būti materialiosios formos). Todėl autorių, ginančių dabartiniuose teisės aktuose įtvirtintas nuostatas, svarbiausio argumento nebuvo besąlygiškai laikomasi dar iki atsirandant elektroninei komercijai.

Pirmųjų naujojo požiūrio požymių jau matyti ir kai kurioms valstybėms priimant sprendimus. Prancūzija ir Liuksemburgas skaitmeninėms e. erdve parsiunčiamoms knygoms pritaikė lengvatinį PVM tarifą (Prancūzija – penki su puse procento, Liuksemburgas – trys procentai). ES lengvatinis PVM tarifas gali būti taikomas tik popierinėms knygoms. Elektroniniu būdu parsisiųstos knygos prilyginamos šiuo būdu teikiamoms paslaugoms ir joms turi būti taikomas standartinis PVM tarifas. Toks minėtųjų valstybių sprendimas sukėlė Europos Komisijos susidomėjimą, nes šių valstybių pardavėjams, palyginti su kitomis valstybėmis, bendrojoje ES rinkoje sudaromos palankesnės konkurencijos sąlygos. Tai ypač aktualu turint omenyje, kad e. erdvėje nėra skirtumo, iš kurios šalies pardavėjo bus perkama ir parsisiunčiama elektroninė knyga.

2015 m. kovo 5 d. Prancūzijai ir Liuksemburgui buvo priimtas nepalankus sprendimas ir pripažinta, kad šios valstybės neįvykdė savo įsipareigojimų dėl bendrosios PVM sistemos.

Bito mokestis

Daugiausia diskusijų ir išsamiausių mokslinių tyrimų sulaukė 1994 m. pirmą kartą A. Cordellos ir T. Ide'o iškelta idėja dėl naujo, išskirtinai elektroninei komercijai taikytino, mokesčio. Šiai idėjai pritarė ir ją išplėtojo profesorius L. Soete'as.

Svarbiausias bito mokesčio šalininkų argumentas – daugumą paslaugų įmanoma teikti e. erdvėje, o kai kurias prekes (pvz., knygas, muzikos įrašus, programinę įrangą, filmus ir kt.) galima išreikšti skaitmenine forma ir taip pat persiųsti elektroniniu būdu. Tradicinės prekybos atveju tiekiant prekes buvo privaloma kirsti valstybių sienas. Tokiu būdu jų importo ir eksporto srautai buvo lengvai kontroliuojami. Elektroninėje erdvėje valstybių sienos išnyksta. Per gana trumpą laiką skaitmeninė prekė internetu gali būti persiųsta iš vienos pasaulio vietos į kitą. Taigi iki šiol, kertant valstybių sienas, egzistavusi tarpinė kontrolės grandis e. erdvėje tampa neįmanoma.

Siūlymai įvesti naują mokestį elektroninei komercijai remiasi prielaida, jog informacinės technologijos ateityje netaps tokios sudėtingos, kad nebūtų įmanoma kontroliuoti informacijos srautų. Bus galima nustatyti, kuri informacija priskiriama elektroninės komercijos sandoriams ir kokiais srautais paprasčiausiai keičiamasi informacija internetu.

Pagrindinis vartojimo mokestis ES šalyse – PVM. Šis mokestis priklauso netiesioginiams mokesčiams ir priskiriamas ES kompetencijai. PVM sistema buvo sukurta ir daug kartų tobulinta dar iki atsirandant elektroninei komercijai. L. Soete'as teigia, kad PVM yra pritaikytas komercijai, kur prekės turi materialiąją išraišką, be to, įmanoma kontroliuoti jų

judėjimo srautus ir sužinoti pristatymo vietą. Tačiau ši sistema nėra tinkama e. erdvėje vykdomai prekybai.

Naujojo mokesčio šalininkai teigia, kad iki šiol taikomą PVM sistemą galima pakeisti duomenų perdavimo pagrindu (apskaičiuojant siunčiamos informacijos kiekį) paremta mokesčių sistema, kuri būtų taikoma tik virtualioms (e. erdvėje teikiamoms) prekėms ir paslaugoms. Tokiu atveju naujasis mokestis būtų proporcingas informacinėmis technologijomis perduodamos informacijos kiekiui.

A. Cordella pasiūlė 0,000001 cento[20] už vieną bitą mokesčio dydį (tai sudarytų vieną centą už vieną megabitą informacijos). 1995 m. duomenimis, *Hewlett-Packard* bendrovė per metus turėtų sumokėti 4,8 mln. JAV dolerių už 480 terabitų persiųstos informacijos.

Autoriai pateikia ir papildomų argumentų, kuriais remiantis būtų priimtinas bito mokestis:

1) papildomos pajamos, gautos dėl bito mokesčio, padėtų valstybėms užtikrinti socialinę darbuotojų apsaugą, įsteigtų naujų darbo vietų, 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 kopijų, kurios yra visiškai identiškos originalui, ir be didesnių išlaidų persiųsti jas daugeliui asmenų arba sudaryti sąlygas, kad šios kopijos būtų visiems prieinamos e. erdvėje, įskaitant ne tik naudojimąsi jomis, bet ir parsisiuntimą į kompiuterinės sistemos kietąjį diską;
3) bito mokestis turėtų teigiamos įtakos gerinant darbuotojų, turinčių priėjimą prie interneto, darbo kokybę. Tai apribotų jų lankymąsi interneto svetainėse, kurios nėra susijusios su jų atliekamu darbu. Darbdaviams tai leistų efektyviau naudotis elektroninėmis komunikacijomis;
4) viena iš didesnių problemų – internete labai sparčiai daugėja informacijos, priskiriamos „informacijos šiukšlėms“. Naujasis mokestis iš dalies apribotų nereikalingos informacijos plitimą ir apsaugotų internetą nuo perkrovimo.

Anot B. J. ter Weelo, didžiausios kliūtys, kurios neleidžia sėkmingai taikyti naujojo, tik elektroninei komercijai skirto, mokesčio yra šios:

1) mokestis yra paremtas tik informacijos persiuntimu, jis ekonomiškai visiškai nesusijęs su prekės verte;

[20] Autorius naudojo JAV valiutą.

2) neegzistuoja jokių mokesčių, kurie būtų taikomi kitais metodais siunčiamai informacijai (pvz., telefaksu);
3) šis mokestis varžytų žodžio laisvę, privačius vartotojus pastatytų į keblią padėtį, prilygindamas juos verslininkams, ir nė nebūtų atsižvelgiama į skirtumus, esančius tarp šių subjektų;
4) mokestis varžytų, o ne skatintų naudotis internetu. Toks padarinys atsirastų dėl ekonominio neveiksmingumo. Neefektyvios elektroninės komercijos plėtros tikimybė padidėtų dėl keleto priežasčių: naudojant archyvavimo programas, būtų dirbtinai mažinamas siunčiamos informacijos kiekis; kitas ekonominis nukrypimas – bendrovės steigs vidinius komunikacijos tinklus ir taip sieks išvengti mokesčių;
5) bito mokestis gali riboti žmonių naudojimąsi internetu keičiantis informacija. Siekiant išvengti šio mokesčio, dalis informacijos vėl bus siunčiama naudojant popierines ar kitokias laikmenas. Tai turės neigiamų padarinių aplinkai (pvz., padidės medienos naudojimas popieriaus gamybai);
6) šį mokestį bus sunku taikyti praktiškai. Naudojantis informacinių technologijų teikiamomis galimybėmis, bus siekiama nuslėpti siunčiamų bitų skaičių;
7) jeigu šis mokestis nebus taikomas visame pasaulyje, gali būti iškraipoma konkurencija, t. y. sandorių sudarinėjimas iš e. erdvės gali persikelti į tą jurisdikciją, kur nėra bito mokesčio.

Siūloma naujojo mokesčio sistema šiuo metu praktiškai nėra taikoma nė vienoje valstybėje. Dar 1998 m. Europos Komisijos padarytame pranešime EBPO ir Pasaulinei prekybos organizacijai buvo pabrėžta, kad elektroninės komercijos atsiradimas ir siekis kiek galima efektyviau ją apmokestinti neturėtų būti paremtas naujojo mokesčio įvedimu. Tų pačių metų birželį šį principą patvirtino ir *ECOFIN* Taryba. 1998 m. JAV priėmė teisės aktą, kuriame įtvirtino nuostatą, kad elektroninė komercija negali būti apmokestinama naujaisiais mokesčiais. Žaliojoje knygoje, skirtoje Pietų Afrikos Respublikai, pabrėžiama, kad šiuo metu nėra būtinybės įvesti naujų mokesčių, skirtų elektroninei komercijai apmokestinti.

Norint efektyviai apmokestinti naująją komercijos formą, pakaktų padaryti dabartinių teisės aktų pakeitimų. Tokios pat pozicijos laikosi ir Didžioji Britanija. Portugalija, savo teisės aktuose įtvirtindama panašias nuostatas, siekia skatinti elektroninę komerciją, remiantis laisvosios rinkos taisyklėmis, ir apriboti valstybės galimybę piktnaudžiauti nustatant teisines taisykles, kai šios nebūtinos siekiant efektyviai apmokestinti elektroninę komerciją.

Elektroninių paslaugų apmokestinimas pridėtinės vertės mokesčiu

PVM kritika dėl neefektyvumo elektroninėje komercijoje iš esmės rėmėsi tuo, kad neįmanoma identifikuoti antrosios sandorio šalies (pirkėjo). Informacinės technologijos leidžia nustatyti tik kompiuterinės sistemos *IP*, bet jokiu būdu ne subjektą, kuris juo naudojasi.

ES priimta Šeštoji direktyva „Dėl pridėtinės vertės mokesčio“ atsižvelgė į elektroninės komercijos plėtrą ir įtvirtino teisines nuostatas, kurios turėtų sureguliuoti elektroninių paslaugų apmokestinimą PVM. Kaip jau minėjome, remiantis šia direktyva, bet kokios skaitmeninės prekės, parduodamos e. 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 str. 1 ir 2 d. įtvirtina bendrą taisyklę dėl paslaugų teikimo vietos. Tokia paslauga laikoma suteikta Lietuvoje, jeigu: „paslauga apmokestinamajam asmeniui, kuris sandorį sudaro veikdamas kaip toks, yra suteikta šalies teritorijoje, jeigu šis asmuo yra įsikūręs šalies teritorijoje, t. y. jeigu jo buveinė (jeigu tai ne fizinis asmuo) arba nuolatinė gyvenamoji vieta (jeigu tai fizinis asmuo) yra Lietuvos Respublikoje... ir paslauga asmeniui, kuris nėra apmokestinamasis asmuo, 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“.

Minėtojo straipsnio 14 d. numatyta, kaip turi būti nustatoma elektroniniu būdu teikiamų paslaugų vieta, kai užsienio apmokestinamasis asmuo jas teikia Lietuvos Respublikos apmokestinamiesiems asmenims: „jeigu šioje dalyje išvardytas paslaugas ne šalies teritorijoje įsikūręs paslaugų teikėjas ar 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 str. 14 d. 8 p. minimos elektroniniu būdu teikiamos paslaugos, kurioms taikoma aukščiau pateikta teisinė norma. Remiantis PVM įstatymo 95 str. 2 d., prievolė apskaičiuoti PVM ir sumokėti į biudžetą tenka paslaugų pirkėjui.

„Paslaugų pirkėjas, jeigu jis yra apmokestinamasis asmuo, kaip jis suprantamas šio Įstatymo 13 straipsnyje, privalo apskaičiuoti ir sumokėti į biudžetą PVM už jam šalies teritorijoje užsienio asmens, neįsikūrusio

šalies teritorijoje, teikiamas paslaugas, nurodytas šio Įstatymo 13 straipsnio 2 dalies 1 punkte."

Esant šioms teisinėms nuostatoms, elektroninių paslaugų teikėjai negali registruotis ES valstybėje narėje, kur yra taikomas mažiausias PVM tarifas. Tai aktualu, nes bendrovėms elektroniniu būdu ypač lengva perkelti savo verslą į kitas valstybes. Be to, dauguma elektroninių paslaugų teikiama būtent apmokestinamiesiems asmenims. Remiantis J. Owenso skaičiavimais, jos sudaro apie 80 proc. visų elektroniniu būdu teikiamų paslaugų. Jeigu elektroninėms paslaugoms būtų taikoma bendra taisyklė, labai tikėtina, kad bendrovės, norėdamos mokėti mažesnį PVM, savo verslo buveines perkeltų į mažiausią PVM tarifą taikančias ES valstybes nares.

Nustatant paslaugų teikimo vietą, didelę įtaką turi ir tai, kam yra teikiamos tokio pobūdžio paslaugos – apmokestinamajam asmeniui ar ne. Pagrindiniai elektroninės komercijos modeliai yra „verslas verslui" (angl. *business to business)* ir „verslas vartotojui" (angl. *business to consumer)*. Atsižvelgiant į atsirandančius mokestinius santykius ir jų teisinį 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.

Taikant elektroninės komercijos „verslas verslui" modelį, nėra sudėtinga nustatyti pirkėją. Identifikuojant visada galima pasinaudoti duomenų bazėmis, kuriose skelbiami visi juridiniai asmenys, įsiregistravę PVM mokėtojais. Valstybinės mokesčių inspekcijos prie Lietuvos Respublikos finansų ministerijos viršininko 2004 m. kovo 25 d. įsakymu Nr. VA-39 buvo patvirtintos ES valstybių narių pridėtinės vertės mokesčio mokėtojų identifikacinių duomenų tikrinimo taisyklės.

Atsižvelgiant į elektroninės komercijos specifiką, buvo priimta papildomų teisinių nuostatų, skirtų tik šiai komercijos formai. Nuo 2003 m. liepos 1 d. ES ir nuo 2004 m. gegužės 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 naudotis elektroninių paslaugų teikėjai, esantys JAV, Japonijoje, Rusijoje, Australijoje ir kt.

PVM įstatymo 2 str. 37 d. užsienio apmokestinamąjį asmenį apibrėžia kaip:

„...bet kokio pobūdžio ekonominę veiklą vykdantis:

1) užsienio valstybės juridinis asmuo ar 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".

Be to, asmuo, atitinkantis šį apibrėžimą, kurioje nors valstybėje narėje neturi būti įsiregistravęs kaip PVM mokėtojas ir negali turėti padalinio ar buveinės ES teritorijoje.

Tokia registravimosi prievolė, taikoma užsienio valstybėje esančiam neapmokestinamajam asmeniui, kelia sunkumų šiam registruojantis kiekvienoje ES valstybėje narėje. Vykdant elektroninę prekybą ekonomiškai išsivysčiusiose valstybėse, kurių piliečių kompiuterinio raštingumo lygis gana aukštas, 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 rinktis, kurioje ES valstybėje narėje jis nori registruotis PVM mokėtoju. Pasirinkęs vieną iš ES valstybių, jis galės nebesiregistruoti kitose (taip pat ir Lietuvoje) (PVM įstatymo 71 str. 11 d.).

„Už Europos Bendrijų teritorijos ribų įsikūręs apmokestinamasis asmuo ar 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 Bendrijos teritorijos ribų įsikūręs apmokestinamasis asmuo stengsis registruotis toje ES valstybėje narėje, kur PVM tarifas yra mažiausias. Šiuo metu ES standartiniai PVM tarifai svyruoja nuo septyniolikos iki dvidešimt septynių procentų.

Apmokestinamiesiems asmenims, įsikūrusiems Už ES teritorijos ribų ir elektroniniu būdu teikiantiems paslaugas, palankiausios šalys PVM požiūriu būtų Liuksemburgas ir Malta. Dauguma paslaugų teikėjų, be abejo, būtų suinteresuoti registruotis PVM mokėtojais būtent tose valstybėse ir taikyti nuo septyniolikos iki aštuoniolikos procentų PVM tarifą. Siekiant išvengti tokių sukčiavimo atvejų, specialioje schemoje buvo įtvirtinta

taisyklė, jog užsienio šalies apmokestinamieji asmenys, užsiregistravę vienoje iš ES valstybių narių, privalo taikyti tą PVM tarifą, kuris numatytas pirkėjo šalyje. Jeigu Rusijos apmokestinamasis asmuo elektroniniu būdu teikia paslaugas Švedijos neapmokestinamajam asmeniui, o pats yra įsiregistravęs Lietuvos valstybėje, jis privalo taikyti ne 21 proc., o 25 proc. PVM tarifą. Tokiu atveju paslaugos teikėjas per Lietuvos valstybę įsipareigos vykdyti savo mokestines prievoles visose ES valstybėse, į kurias jis elektroninėmis priemonėmis teikia savo 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. Minėtosios institucijos interneto svetainėje *(www.vmi.lt)* sukurta speciali aplikacija, kuria naudodamasis paslaugų teikėjas gali registruotis PVM mokėtoju. Šioje svetainėje, pildydamas registracijos formą, subjektas nurodo: savo pavadinimą, nuolatinės buveinės adresą ir valstybę, elektroninio pašto ir interneto svetainės, kuria naudodamasis vykdo elektroninę prekybą, adresą, mokesčio mokėtojo numerį (jeigu turi), kontaktinį asmenį, telefono numerį, datą, nuo kurios jis nori pradėti (ar jau pradėjo) taikyti specialią apmokestinimo PVM schemą. Be to, paslaugų teikėjas turi patvirtinti, kad jis nėra įregistruotas PVM mokėtoju kurioje nors kitoje ES valstybėje narėje. Jeigu asmuo atitinka visus jam keliamus reikalavimus, jis įregistruojamas PVM mokėtoju, o Valstybinė mokesčių inspekcija apie tai informuoja atitinkamas kitų ES valstybių 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 PVM mokėtoju turi registruotis įprastine tvarka. Tai jis turės daryti kiekvienoje ES valstybėje narėje, kurioje teikia tokio pobūdžio paslaugas.

Teikdamas PVM deklaraciją elektroniniu būdu, paslaugų teikėjas turi nurodyti, į kokias ES valstybes nares buvo teikiamos paslaugos, koks taikytinas PVM tarifas ar tarifai, kiekvienai ES valstybei mokėtiną PVM ir bendrą mokėtiną PVM sumą.

Nors, palyginti su bendra elektroninės komercijos apimtimi, tokie sandoriai sudaro tik 10–20 proc., esant būtent šiai stadijai ir sunkiausia identifikuoti pirkėją. Remdamasis specialia elektroniniu būdu teikiamų paslaugų apmokestinimo schema, paslaugų teikėjas turi identifikuoti neapmokestinamuosius asmenis. Tokiais asmenimis gali būti tiek fiziniai, tiek juridiniai asmenys. Autoriai sutaria, kad juridinių asmenų, vykdančių elektroninę

prekybą, identifikavimas nekelia didesnių problemų. Tačiau paslaugų teikėjui uždėta našta identifikuoti fizinį asmenį nėra taip lengvai pakeliama. Netgi naudojantis pažangiomis informacinėmis technologijomis, neįmanoma tiksliai nustatyti fizinio asmens. Vadovaudamasis šiuo metu galiojančiomis teisinėmis nuostatomis, ES ir Lietuvos pardavėjas turi pasikliauti ta informacija, kurią pateikia fizinis asmuo. Be abejo, fizinis asmuo gali pateikti klaidingą informaciją, kaip savo gyvenamąją vietą nurodydamas kitą valstybę. Tokiu atveju paslaugos teikėjas taikytų tos valstybės, kurią nurodė klientas, PVM tarifą. Tačiau neturėtų būti šitaip sukčiaujama, nes fiziniai asmenys nėra suinteresuoti nurodyti neteisingus duomenis. Kad ir kokios ES valstybės pirkėju prisistatytų fizinis asmuo, už suteiktas paslaugas jis vis tiek turėtų mokėti tokią pat sumą. Šiuo atveju suinteresuota šalimi galėtų būti tik paslaugų teikėjas, nes jis turėtų galimybę taikyti mažesnius PVM tarifus. Tačiau esant automatizuotam paslaugų teikimo procesui, jis negali daryti įtakos fiziniam asmeniui, kai šis pateikia duomenis, ar kaip nors kitaip keisti informacijos turinio.

Teisinis nuolatinės buveinės 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, siekdama išvengti dvigubo apmokestinimo, pradeda vykdyti ūkinę-komercinę veiklą. Šiuo pagrindu pasirašomos dvišalės ar net daugiašalės[21] sutartys, vienai ar kitai sutarties šaliai suteikiančios apmokestinimo teisę.

Nuolatinės buveinės koncepcija buvo suformuluota remiantis Vokietijos nacionalinės teisės nuostatomis. Manoma, kad pirmą kartą nuolatinės buveinės institutas tarptautinėse mokesčių sutartyse buvo paminėtas XIX a. pabaigoje. Tai buvo tarp Vokietijos ir žemyninės Europos valstybių pasirašytos dvišalės sutartys. Nuo 1928 iki 1946 m. Tautų Lyga pristatė tris mokesčių sutarties projektus, kuriuose buvo pateiktos trys skirtingos nuolatinės buveinės koncepcijos. 1943 m. Meksikos projekte buvo pateiktas

[21] 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. Pirmą kartą ji buvo pasirašyta 1983 m. kovą ir įsigaliojo tų pačių metų gruodį. Naujoji versija buvo pasirašyta 1987 m. vasarį ir įsigaliojo 1987 m. gruodį. 1989 m. rugsėjį pasirašyta trečioji sutarties versija, kuri įsigaliojo 1989 m. gruodį. Paskutinioji 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 (turinčia savarankišką teisę pasirašyti sutartį), Suomija, Islandija, Norvegija ir Švedija.

nuolatinės buveinės apibrėžimas, kuris visiškai atspindėjo pajamų šaltinio principu paremto 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. EBPO patvirtino pirmąją rekomendaciją dėl dvigubo apmokestinimo išvengimo, 1958 m. EBPO 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. kartu su komentaru patvirtino naująjį variantą. 1963 m. ir 1977 m. EBPO modelinės konvencijos tapo modeliais 1980 m. Jungtinių Tautų modelinei konvencijai ir dar reikšmingesnės buvo sudarant 1981 m. JAV modelinę sutartį.

Vėliau, ypač sparčiai plėtojantis technologijoms, įvyko esminių pasikeitimų dėl sandorių sudarymo tarp skirtingų valstybių. EBPO nagrinėjo pataisas ir jas priimdavo dėl Modelinės konvencijos ir jos komentarų. Be to, ši konvencija išplito ir už EBPO narių ribų. Minėtoji organizacija nusprendė, kad Modelinės konvencijos pakeitimai galėtų duoti naudos, jeigu būtų įtrauktos valstybės, kurios nėra EBPO narės, kitos tarptautinės organizacijos ar suinteresuoti dalyviai. 1992 m. buvo pateikta „laisvų – lapų“ Modelinė konvencija, kuri, skirtingai nei 1963 m. ar 1977 m., nebuvo galutinė versija, o tik pirmasis žingsnis darant pakeitimus. 1997 m. buvo išleistas antrasis tomas, kuriame buvo pateiktos valstybių, nesančių EBPO narėmis, pozicijos. Apibendrintas EBPO modelinės konvencijos variantas buvo paskelbtas 2010 m., paskui, atsižvelgiant į elektroninės komercijos ypatybes ir kilusius praktinius sunkumus pritaikyti nuolatinės buveinės institutą, buvo atlikta 5 str. komentaro pataisų. 2014 m. išleistas paskutinis konvencijos variantas.

Iki XX a. pabaigos nuolatinės buveinės samprata išliko beveik nepakitusi. Pagrindinė idėja, kuria remiasi ši koncepcija – kiekvienas asmuo, gaunantis naudos iš tam tikros visuomenės, privalo jai mokėti mokesčius. Teisinis nuolatinės buveinės institutas nusako būtinus kriterijus, kuriais remiantis komercinės-ūkinės veiklos ryšys su tam tikra valstybe yra laikomas pakankamu, kad atsirastų reikalavimas toje valstybėje mokėti mokesčius.

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. Mokesčių mokėtojų apmokestinimas pajamų šaltinio valstybėje

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 (angl. *residence-based taxation)*, arba pajamų šaltinio valstybei (angl. *source-based taxation)*. Remiantis EBPO dvigubo apmokestinimo išvengimo sutarties modeliu ir jos ekspertų pastabomis, sudaryta daugelis tarptautinių sutarčių dėl dvigubo apmokestinimo išvengimo. Lietuvos Respublika nėra EBPO narė, tačiau visos sutartys dėl dvigubo apmokestinimo išvengimo remiasi minėtąja EBPO Modeline konvencija. Šia konvencija, atsižvelgiant į gautas pajamas, nustatomos dvi taisyklės, kuriomis siekiama išvengti dvigubo apmokestinimo. Pagal pirmąją taisyklę išimtinė teisė apmokestinti yra suteikiama buveinės valstybei. Remiantis antrąja – šaltinio valstybė turi visišką arba dalinę teisę apmokestinti pajamas, tada buveinės valstybė, siekdama išvengti dvigubo apmokestinimo, privalo ją atleisti nuo mokesčių.

Elektroninės komercijos išplitimas stipriai paveikė tradicinę tarptautinę apmokestinimo koncepciją, paremtą pajamų šaltinio valstybei suteikta apmokestinimo teise. Iš esmės pajamų šaltinis yra priskiriamas tai vietai, kurioje tiesiogiai vykdoma ūkinė-komercinė veikla. Elektroninės komercijos atveju dėl pirkėjų anonimiškumo ir galimybės realiuoju laiku sudaryti sandorį su bet kuria e. erdvėje prekiaujančia bendrove, neatsižvelgiant į geografinius atstumus ir skirtingas valstybių jurisdikcijas, nustatyti vietą, kur vykdoma ekonominė veikla, tampa labai sunku, o kai kuriais atvejais net neįmanoma.

Apibendrinant galima teigti, kad apmokestinimas, grindžiamas pajamų šaltinio principu, remiasi idėja, jog valstybė turi teisę apmokestinti bendrovės pajamas, kurios gaunamos iš tos valstybės subjektų, bendrovei tiesiogiai vykdant ūkinę-komercinę veiklą. Apmokestinimas, grindžiamas buveinės vietos principu, remiasi koncepcija, jog valstybė turi teisę apmokestinti bendrovės pajamas, jeigu tarp tos valstybės ir užsienio bendrovės yra glaudus ryšys.

Taigi nuolatinės buveinės institutas įkurtas daug anksčiau, nei atsirado elektroninė komercija, todėl dauguma tarptautinių sutarčių dėl dvigubo apmokestinimo išvengimo nenurodo, kad nuolatinės buveinės sąvoka apima ir serverį, kuriuo bendrovė vykdo ūkinę-komercinę veiklą. Vienintelis bendrovę su užsienio valstybe siejantis ryšys gali būti prie interneto prijungtas serveris ir jame esanti interneto svetainė. Bendrovėms, norinčioms pardavinėti savo prekes užsienyje, nebūtina toje valstybėje turėti atskirų patalpų. Dėl tokio bendrovės atstovavimo kitoje šalyje kyla problemų

nustatant nuolatinę buveinę. Todėl būtina suteikti serveriui teisinį statusą toje valstybėje, į kurią bendrovė, siekdama vykdyti ūkinę-komercinę veiklą, jį perkelia. Be to, turėtų būti apibrėžiami kriterijai, kuriais remiantis serverį ar interneto svetainę būtų galima vertinti kaip nuolatinę buveinę.

1999 m. apie devyniolika Pietų Afrikos Respublikos (toliau – PAR) institucijų analizavo įvairius elektroninės komercijos aspektus ir esančios teisinės bazės efektyvumą reglamentuojant nuolatinės buveinės institutą. PAR ryšių departamentas buvo įgaliotas pateikti elektroninės komercijos plėtros strategiją. Šie darbai buvo atliekami remiantis 1996 m. *Katz* komisijos pateiktomis ataskaitomis. PAR iki šiol taikytas pajamų šaltinio principas ir egzistavusi teisinė sistema nenumatė jokių specifinių teisės normų, skirtų elektroninei komercijai apmokestinti. B. du Plessiso nuomone, pateikta elektroninės komercijos plėtros strategija ir galiojančios teisės 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 dėl elektroninės komercijos apmokestinimo, remiantis iki šiol PAR taikytu pajamų šaltinio principu.

Atsižvelgiant į naujas elektroninės komercijos teikiamas tarptautinės prekybos galimybes, per siauras nuolatinės buveinės traktavimas būtų palankus įmonėms, norinčioms mokėti mokesčius rezidavimo valstybėje. Kita vertus, per platus nuolatinės buveinės koncepcijos suvokimas gali būti nepalankus ekonomiškai išsivysčiusių šalių įmonėms, siekiančioms išplėsti savo ūkinę-komercinę veiklą į kitas šalis.

Pagrindinius šaltinius, keliančius diskusijų dėl nuolatinės buveinės instituto ir apmokestinimo jurisdikcijos nustatymo, galima būtų suskirstyti į keturias rūšis:

1) plačios EBPO 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 – iki šiol egzistavusios teisės normos dėl nuolatinės buveinės vertinimo ir toliau gali būti sėkmingai taikomos elektroninei komercijai. Vėliau buvo išplėstas šių normų interpretavimas, 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 ūkinės-komercinės veiklos vietos interpretavimui, t. y. minėtąją vietą galima apibūdinti tik kaip fizinį objektą. Tačiau kaip alternatyvą pirmajai nuomonei galima būtų pateikti Australijos pasirinktą poziciją. Šis požiūris sietinas su lankstesniu ūkinės-komercinės veiklos vietos interpretavimu, pagal kurį net ir fizinės išraiškos neturintis objektas galėtų būti minėtosios veiklos vieta. Tokiu atveju interneto svetainė irgi galėtų būti vertinama kaip nuolatinė buveinė. Portugalija ir Ispanija taip pat pareiškė poziciją, kad norint pateikti objektą kaip nuolatinę buveinę jam nebūtina fizinė išraiška.

Trečiosios pozicijos šiuo klausimu laikosi Airija ir Didžioji Britanija. Jų manymu, serveris neturėtų būti vertinamas kaip nuolatinė buveinė. Didžiosios Britanijos vyriausybė ne tik paneigė galimybę pripažinti serverį kaip nuolatinę buveinę, bet ir argumentavo, kodėl negalima ieškoti panašumų tarp smulkių prekių automatų, 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 kiekvieną savaitę keistų savo prekybos vietą, greitai prarastų klientus. Dėl serverio pirkėjui nėra jokio skirtumo, nes, naudodamasis internetu, jis iš bet kurios vietos gali prie jo prisijungti.

Didžiosios Britanijos vyriausybės nuomone, veikla, iš kurios bendrovė gauna pelno, yra priskirtina tai vietai, kur yra bendrovės įstaiga, arba vieta, kur atliekami svarbiausi tyrimai.

Airijos nuomone, serverį pripažinus nuolatine buveine, gali taip nutikti, kad minėtoji šalis praras galimybę apmokestinti bendrovių pajamas, jeigu šios savo ūkinę-komercinę veiklą iš jos perkels į kitą valstybę. Labiausiai tai nulemtų mažesni kitose valstybėse mokami mokesčiai. Be to, didelę įtaką turėtų ir maži kaštai, reikalingi bendrovei, norinčiai pradėti verslą kitose šalyse.

Kiek kitokią poziciją šiuo klausimu yra pasirinkusi Indija. Iki elektroninei komercijai pasiekiant dabartinę apimtį, Indijoje vyravo nuostata, kad subjektas, norintis turėti nuolatinę buveinę, nebūtinai turi reziduoti toje valstybėje. Pelnas būdavo apmokestinamas net ir tuo atveju, kai bendrovė neturėdavo toje šalyje fiziškai išreikštos buveinės. Kompetentingos Indijos institucijos tvirtina, kad bendrovės, teikiančios elektronines paslaugas ir esančios už šalies ribų, Indijoje turi nuolatinę virtualią buveinę. Tokiu atveju mokestis, gaunamas iš šios šalies vartotojų, yra bendrovės pelnas ir jis toje šalyje turėtų būti apmokestinamas. Deja, sąvoka „nuolatinė virtuali

buveinė“ nėra tiksliai apibrėžta ir norint ją nustatyti didelių sunkumų kyla ir pačiai valstybei, ir elektroninės komercijos sandorių šalims.

Reikėtų pabrėžti, kad toks požiūris visiškai atitinka svarbiausią apmokestinimo, paremto pajamų šaltinio principu, nuostatą – bendrovė, gaunanti pelno iš Indijos piliečių, šiai šaliai privalo mokėti mokesčius. Tačiau elektroninei komercijai dar būdinga ir tai, kad nėra galimybių identifikuoti visų bendrovės klientų ir nustatyti pelno dalies, gaunamos 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 puikiai parodo valstybės reakciją į naujai susiklosčiusią komercinę padėtį. Valstybė siekia neprarasti pagrindo apmokestinti užsienio bendrovių, kurios nereziduoja toje šalyje, tačiau turi galimybę elektroniniu būdu prekiauti jos rinkoje.

Interneto paslaugų teikėjas ir priklausomo agento statusas

Bendrovės savo veiklą kitoje valstybėje dažnai vykdo naudodamosi fizinių ar 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. Elektroninės komercijos atveju tokio agento statusą daugiausia turi interneto paslaugų teikėjai (toliau – IPT), iš kurių įmonės, vykdydamos savo veiklą užsienio šalyje, dažnai nuomojasi serverius. Tačiau, norint turėti nuolatinę buveinę kitoje šalyje ir naudotis agento paslaugomis, šis turi būti priklausomas nuo įmonės, kuriai teikia paslaugas. Šiuo atveju netaikomas nuolatinės ūkinės-komercinės veiklos vietos reikalavimas.

Remdamiesi teisės normomis, kurios iki šiol reglamentavo agento kaip nuo bendrovės priklausomo subjekto statusą, galime išskirti šiuos minėtajam agentui keliamus reikalavimus:

- turi būti valstybės teritorijoje (asmuo gali būti tiek fizinis, tiek 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 pabrėžti, kad ne visos įmonės gali naudotis IPT teikiamomis paslaugomis. Stambiosios bendrovės, vykdydamos elektroninę prekybą, dažniausiai naudojasi ne vienu, o keliais serveriais, išdėstytais skirtingose pasaulio šalyse, taip pat ir įmonės patentuota programine ar technine įranga, kuriomis gali efektyviau valdyti duomenų srautus. IPT personalas nėra specializuotas atlikti tokias komercines operacijas. Šių specialistų veikla pirmiausia nukreipta į techninės bazės užtikrinimą, kad serveris galėtų tinkamai funkcionuoti. Be to, bendrovės kitiems subjektams nepatiki patentuotos programinės ar techninės įrangos. Tokiais atvejais įmonės dažniausiai pačios nuosavybės teise valdo serverius, esančius užsienio valstybėse, o bendrovės personalas užtikrina techninės įrangos funkcionavimą ir net komercinių sandorių sudarymą.

Tačiau dauguma bendrovių naudojasi IPT paslaugomis. Labiausiai paplitę elektroninės komercijos modeliai, kai užsienio bendrovės nuomoja serverį arba tam tikrą jo atminties dalį, kur įkelia savo interneto svetainę, o IPT užtikrina šios įrangos funkcionavimą. Šiuo atveju IPT veiksmai atitinka EBPO Modelinės konvencijos 5 str. 4 d. numatytus pagalbinius veiksmus. Užsienio bendrovės interneto paslaugų teikėjams dažniausiai nesuteikia įgaliojimų sudaryti sandorių su pirkėjais. Tačiau reikėtų atkreipti dėmesį, kad ir pati bendrovė tiesiogiai šių sandorių nesudarinėja. Šiuos veiksmus savarankiškai atlieka automatizuota programinė įranga. Tačiau didžiausią įtaką įrangos egzistavimui, jos atliekamų operacijų apimčiai ir savarankiškumui daro bendrovės priimami sprendimai.

Vykdydami savo veiklą, IPT paslaugas gali teikti ne vienai, bet kelioms užsienio bendrovėms. Dažnai kelios įmonės iš karto į vieną serverį įkelia savo interneto svetaines, kurių priežiūra rūpinasi tas pats interneto paslaugų teikėjas. Tvarkydamas įvairių bendrovių interneto svetaines, esančias jų serveryje, IPT plėtoja savo verslą ir nesiekia naudos užsienio bendrovei. Be to, jis veikia savo interesais ir yra visiškai nepriklausomas nuo užsienio bendrovės.

Interneto paslaugų teikėjas neatitinka šių reikalavimų ir neturi jokių įgaliojimų, susijusių su sandorių sudarymu, taigi jis nevykdo priklausomo agento funkcijų ir gali būti vertinamas tik kaip nepriklausomas agentas.

Tačiau EBPO neatmeta galimybės, kad esant tam tikroms aplinkybėms IPT gali būti pateikiamas kaip priklausomas agentas. Šiuo atveju, remiantis aukščiau nurodytais priklausomam agentui keliamais reikalavimais, IPT turi veikti užsienio bendrovės vardu ir jos naudai, turėti įgaliojimą sudaryti sandorius bei priklausyti nuo užsienio bendrovės.

Kai kurie autoriai šalia tradicinio agento suvokimo (tai gali būti fizinis arba juridinis asmuo) svarsto galimybę šiai kategorijai priskirti ir

elektroninei komercijai naudojamą programinę įrangą. Rezervuojant kelionės bilietus, tokia programinė įranga gali pateikti kainų sąrašus, parinkti tinkamą laiką ir maršrutą, palyginti turimą ir kliento pateiktą informaciją ar, remdamasi pateiktais duomenimis, rasti tinkamiausią sprendimo variantą bei sudaryti sandorį. Kad ir kiek daug funkcijų galėtų atlikti programinė įranga, jos funkcionavimui užtikrinti visada bus reikalinga išorinio subjekto pagalba.

Galima rasti ryšį tarp programinės įrangos vykdomų operacijų ir tradicinių agentų atliekamų veiksmų apribojimo, pirmasis užtikrinamas techninėmis, o antrasis – teisinėmis priemonėmis (pasirašant sutartis). Taigi, sudarant sandorį, fizinis arba juridinis asmuo dalyvauja kaip vienas iš sandorio šalių, turi tam tikras teises, prisiima atitinkamas pareigas ir jam gali būti taikomas teisinės atsakomybės institutas. Tuo metu programinė įranga negali būti teisinių santykių subjektas. Ji gali būti vertinama tik kaip bendrovei nuosavybės teise priklausantis turtas.

Nors programinės įrangos atliekamų veiksmų diapazonas yra gana platus ir klientas gali iki pat galo sudaryti sandorį, programinės įrangos nesavarankiškumas ir teisinio statuso nebuvimas neleidžia jos vertinti kaip priklausomo agento, kuris užsienio šalyje sukurtų nuolatinės buveinės institutą. Tuo metu IPT elektroninės komercijos srityje neįgyja išskirtinių savybių, dėl kurių jo atžvilgiu nebūtų galima taikyti tradicinių teisės normų, nekeičiant iki šiol egzistavusio jų interpretavimo.

Nuolatinė buveinė ir personalas

2010 m. EBPO Modelinės konvencijos 5 str. papildomame komentare, kuriame atsižvelgiama į elektroninės komercijos įtaką tarptautiniams mokestiniams santykiams, įtvirtinta nuostata, susijusi su užsienio bendrovės personalo buvimu valstybėje, kurioje serveris yra kaip nuolatinė buveinė. Tradicinės komercijos atveju būtų sunku įsivaizduoti fiksuotą verslo vietą, kuriai nereikalingas joks žmogaus įsikišimas. Elektroninėje komercijoje automatizuoti procesai leidžia atlikti visas komercines operacijas be personalo veiksmų. Todėl papildydama komentarą EBPO patvirtino, kad personalo buvimas ar jo atliekami veiksmai nėra privalomi, jog serverį būtų galima vertinti kaip nuolatinę buveinę. Tačiau panaši nuostata buvo sukurta dar iki atsirandant elektroninei komercijai. Dažniausiai ji buvo taikoma lošimo ir smulkių prekių automatams. Tačiau reikia paminėti, kad ir kiti įrenginiai galėtų būti priskiriami tai įrangos kategorijai, kuri leistų toje šalyje atsirasti nuolatinės buveinės institutui. Viena iš tokių bylų buvo nagrinėjama Vokietijoje. Šioje byloje buvo priimtas sprendimas, kad užsienio bendrovė minėtojoje šalyje turi nuolatinę buveinę, per kurią driekiasi tos bendrovės

naftotiekis, nors jis ir yra reguliuojamas Olandijoje esančio kompiuterio. Be to, Olandijoje veikianti bendrovė niekada nesamdė priklausomo agento iš Vokietijos, kurios teismo priimtas sprendimas neatspindi visų EBPO narių požiūrio. Olandijoje galiojo teisinės nuostatos, pagal kurias naftotiekis nebūtų priskiriamas nuolatinei buveinei.

Po EBPO Modelinės konvencijos komentarų, susijusių su elektronine komercija, pakeitimų ši nuostata išliko nepakitusi. Tačiau jos taikymo galimybės buvo išplėstos – šiems automatiniams mechanizmams ir (ar) įrenginiams buvo priskirtas ir serveris.

Norint užtikrinti automatinių įrenginių funkcionavimą, neišvengiamai reikalingas ir personalas. Tačiau savo komentaruose EBPO yra nustačiusi, kad norint automatinius įrenginius vertinti kaip nuolatinę buveinę personalo veikla gali būti apribota tik vykdant tam tikras operacijas: įrenginių surinkimą, montažo darbus, jų eksploatavimą, remontą ir kt. Ši personalo veikla apsiriboja tik techninės įrangos priežiūra ir yra 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 vertinamas kaip nuolatinė buveinė, išskyrus atvejus, kai toje šalyje dirba ir asmenys. Šis požiūris prieštarauja EBPO pateiktai nuostatai, kad nuolatinė buveinė gali egzistuoti ir tuo atveju, jeigu bendrovės verslas kitoje valstybėje vykdomas tik pasitelkus automatinę įrangą. R. Portner nuomone, tarp lošimo bei smulkių prekių automatų ir serverio yra reikšmingas skirtumas, todėl jų lyginti negalima. Serveriui, priešingai nei kitiems įrenginiams, reikalinga programinė įranga, kuri galėtų užtikrinti vykdomas operacijas. Be to, R. Portner teigia, kad norint pripažinti serverį kaip nuolatinę buveinę yra keliama tam tikrų su personalu susijusių reikalavimų. Šalia esantis personalas turi atlikti ne tik pagalbinius, įrangos techninę priežiūrą užtikrinančius, bet ir kitus darbus, kurie turėtų įtakos bendrovės vykdomam verslui.

Panašios nuomonės laikosi ir C. Dunahoo kartu su kitais „Pricewaterhouse Coopers“ nariais. Jų manymu, bet kurios valstybės jurisdikcijoje nuolatinė buveinė gali egzistuoti tik tada, kai toje valstybėje esantys darbuotojai ar bendrovei priklausantys agentai vykdo veiklą, kurios užtenka, kad buveinė būtų pripažinta kaip nuolatinė. Šių agentų ar personalo atliekami veiksmai turi daryti įtaką bendrovės vykdomam verslui, o ne apsiriboti vien tik šalutiniais darbais.

R. Portner ir C. Dunahoo oponentai teigia, kad minėtųjų nuostatų taikymas galėtų būti išplėstas ir tikti serveriui, kuris tam tikrais atvejais

funkcionuoja kaip ir smulkių prekių automatas. Ši analogija ypač išryškėja, kai prekiaujama virtualiomis prekėmis arba paslaugos teikiamos e. erdvėje. Tada serveris, kaip ir kiti minėtieji įrenginiai, paskirstys šias prekes pirkėjams.

Tačiau šis skirtumas nėra reikšmingas ir neturi jokios įtakos personalo dėl vieno ar kito įrenginio atliekamiems veiksmams. Pagrindinis šių įrenginių skirtumas turėtų būti siejamas su kitomis EBPO pateiktomis rekomendacinėmis nuostatomis. Nuolatinė buveinė gali egzistuoti tik tada, kai užsienio bendrovė pati ar jos priklausomas agentas valdo serverį. Kaip jau minėjome, užsienio bendrovės, vykdydamos elektroninę prekybą, dažnai nuomojasi tik dalį serverio atminties, todėl, remiantis EBPO, R. Portner ir C. Dunahoo argumentais, tas pats serveris iš karto galėtų būti nuolatinė kelių bendrovių buveinė. Vienintelis elektroninės komercijos objektas, kuris nuosavybės teise visada priklausys užsienio bendrovei, yra interneto svetainė. Todėl personalo įtaką tikslinga nagrinėti ne atsižvelgiant į serverį, o į interneto svetainę.

Dėl užsienio bendrovės personalo ir nuolatinės buveinės instituto elektroninės komercijos srityje santykio išsiskiria dvi skirtingos autorių nuomonės. Vieni iš jų (R. Portner, C. Dunahoo, L. Hinnekenas, M. Geurtsas) teigia, kad personalo buvimas yra privaloma sąlyga, norint pripažinti serverį kaip nuolatinę buveinę. Šiuo atveju nėra akcentuojamas serverio ir interneto svetainės klausimas, nes daugelis mokslininkų personalo atliekamus veiksmus ir jų įtaką komerciniams procesams sieja su serverio veikla. Tačiau reikėtų pabrėžti, kad tie patys veiksmai turi glaudesnį ryšį su interneto svetaine. Bendrovės teikiamų paslaugų reklamavimas, prekių užsakymas, atsiskaitymas e. erdvėje, automatizuotas prekių pristatymas ir jų pavertimas skaitmenine forma yra atliekamas naudojantis programine įranga. Serveris, kaip mechanizmas arba įrenginys, užtikrina tik aplinką, kurioje programinė įranga gali vykdyti minėtuosius procesus. Todėl, susiejus aukščiau minėtų autorių teiginius su pozicija, kad ne serveris, o interneto svetainė turėtų būti pripažistama kaip nuolatinė buveinė, galima teigti, kad viena pozicija bendrovės personalo klausimu yra tokia: norint, kad interneto svetainė būtų pripažįstama kaip nuolatinė buveinė užsienio šalyje, šioje turėtų būti ir tos bendrovės personalas.

Kitos nuomonės atstovai (EBPO darbo grupės nariai) teigia, kad serveris, neatsižvelgiant į tai, ar toje šalyje yra bendrovės personalas, gali sukurti nuolatinę buveinę. Tokia pat nuomonė buvo įtvirtinta ir Vokietijos teisminėje praktikoje: „nėra būtini darbuotojai ar žmogaus atliekami veiksmai, kad serverį būtų galima traktuoti kaip nuolatinę buveinę“.

Tradicinės komercijos atveju būtų sunku įsivaizduoti užsienio bendrovės veiklą kitoje šalyje be joje esančio personalo. Tačiau iki šiol egzistavusios nuolatinės buveinės institutą reglamentuojančios teisės normos daugelyje valstybių nenumatė imperatyvių teisės normų, reikalaujančių personalo buvimo. Šis klausimas tampa dar aktualesnis elektroninei komercijai. Visos komercinės operacijos, kurios vyksta e. erdvėje, gali būti programuojamos nuotoliniu būdu. Be to, užsienio bendrovės personalas gali būti savoje valstybėje ir, naudodamasis elektroninės komercijos teikiamomis galimybėmis, nustatyti prekių ar paslaugų kainas, skaitmenine forma pateikti naujų prekių, parinkti skirtingus virtualių prekių pristatymo formatus ir atlikti kitas funkcijas. Asmenys, vykdantys šias operacijas, gali būti ne tik savo šalyje (kur įsteigta bendrovė) ar net trečiojoje valstybėje, bet ir vienas operacijas atlikti vienoje šalyje, o kitas – kitoje. Norinčiam atlikti tokius veiksmus asmeniui pakanka turėti nešiojamąjį kompiuterį, reikiamą programinę įrangą ir leidimą atlikti numatytas operacijas. Šiuo atveju leidimas suprantamas ne tik teisiniu, bet ir technologiniu požiūriu (pvz., slaptažodžių turėjimas). Toks personalo ir kartu atliekamų veiksmų mobilumas yra labai naudingas bendrovėms: leidžia lanksčiau reaguoti į rinkos pokyčius ir operatyviai priimti sprendimus.

Dėl elektroninės komercijos mobilumo negalima sutikti su autorių nuomone, kad serveris kaip nuolatinė buveinė gali būti pripažįstamas tik tada, kai toje šalyje yra ir užsienio bendrovės personalas. Toks požiūris sietinas su serverio mobilumo problema. Siekiant ją išspręsti, pasitelkiamas bendrovės personalas, kuris leistų lengviau užtikrinti stacionarumo kriterijaus įgyvendinimą. Tačiau abu minėtieji objektai – tiek serveris, tiek personalas – elektroninės komercijos srityje pasižymi dideliu mobilumu ir tai daro labai sudėtingą, o kartais ir neįmanomą, teisės normų taikymą įvairiems elektroninės komercijos modeliams. Todėl tik interneto svetainės kaip nuolatinės buveinės vertinimas leidžia pastarąją lengviau identifikuoti. Tokiu būdu skatinama elektroninės komercijos plėtra, netaikant bendrovėms tradicinės komercijos apribojimų, visiškai nepriimtinų elektroninei komercijai, būtent – personalo buvimo šalyje, kur yra nuolatinė buveinė, ar serverio privalomo stacionarumo.

Žinių įtvirtinimo klausimai

1. Kuo skiriasi elektroninės komercijos suvokimas siaurąja ir plačiąja prasmėmis?
2. Raskite internete tiesioginės ir netiesioginės elektroninės komercijos pavyzdžių?

3. Ar gali elektroninis dokumentas būti „originalus“?
4. Kokie teisiniai įpareigojimai dėl kitų subjektų skelbiamos informacijos taikomi interneto paslaugų teikėjams?
5. Ar teisiškai pripažįstamas elektroniniu parašu pasirašytas dokumentas?
6. Kuo skiriasi elektroninės komercijos suvokimas tiesioginių ir netiesioginių mokesčių kontekste?
7. Kam skirta ir kaip funkcionuoja elektroninei komercijai taikoma naujoji pridėtinės vertės apmokestinimo schema?
8. Kokių pranašumų ir trūkumų turi bito mokestis?
9. Kas elektronine komercija besiverčiančiai bendrovei gali atstoti nuolatinę buveinę užsienio valstybėje?
10. Ar gali interneto paslaugų teikėjas tapti priklausomu agentu?
11. Ar elektronine komercija besiverčiančiai bendrovei būtinas personalas užsienio valstybėje, kad joje atsirastų nuolatinės buveinės institutas?

/IV/ *skyrius*

Elektroniniai įrodymai[22]

[22] Kalbant apie elektroninius įrodymus, dėl ribotos darbo apimties šiame skyriuje bus analizuojami tik civilinio ir administracinio procesų elektroniniai duomenys.

1 skirsnis. Elektroninių įrodymų samprata

Paskutiniaisiais XX a. dešimtmečiais į mūsų kasdienį ir dalykinį gyvenimą pradėjo skverbtis technologinės naujovės, kurias šiandien apibendrintai įprasta vadinti informacinėmis ir elektroninių ryšių technologijomis. Informacinių technologijų plėtra atvėrė iš esmės naujas globalaus bendravimo ir sąveikos galimybes – sukurta pasaulio komunikacijos erdvė be įprastų laiko ir atstumo suvaržymų. Naujosios technologijos turėjo įtakos ir naujo tipo komercinių santykių – elektroninės komercijos – raidai ir naujoms galimybėms verslo įmonėms rinkti, sugoti, perduoti ir analizuoti didelius duomenų, gaunamų apie savo klientus ir iš jų, kiekius. Sparti informacinių technologijų plėtra lėmė, kad vis daugiau informacijos buvo kuriama ir saugoma e. erdvėje. JAV atliktų tyrimų duomenimis, internete yra sukuriama ir saugoma daugiau kaip 92 proc. visos pasaulyje naujai atsirandančios informacijos. Šie pokyčiai paveikė ir teisės kaip socialinio mokslo raidą. Nuo aštuntojo XX a. dešimtmečio elektroninės teisinės informacijos ir informacinių technologijų reglamentavimo problematiką imta skirti kaip savarankišką teisės sritį, o teismų sektoriuje Vakarų Europoje bei JAV, vėliau ir kitose šalyse, pradėtos taikyti informacinių ir elektroninių ryšių technologijų naujovės.

Dėl didesnio poreikio užtikrinti vykstančių procedūrų patikimumą, kokybę ir skaidrumą, nusistovėjusių gilių tradicijų ir intensyvaus teisinio reguliavimo teismo procesui ir jo administravimui būdingas konservatyvumas. Teisei ir teismams yra įprastas didesnis ar mažesnis atsilikimas nuo aplinkinio gyvenimo. Todėl paprastai teismuose į technologinę pažangą žiūrima nepatikliai. Daugiau nei prieš šimtmetį JAV teismai nebuvo linkę priimti fotografijų kaip įrodymų, argumentuodami, kad dėl fotografo įgūdžių stokos, netinkamų medžiagų ar įrangos, dėl sąmoningos ir talentingos manipuliacijos fotografija gali būti ne tik netiksli, bet ir pavojingai klaidinanti. 1934 m. JAV Naujojo Džersio Aukščiausiasis Teismas nagrinėtoje byloje *State v Simon* atsisakė kaip įrodymą priimti fonografu įrašytą pokalbį. Tokio pat likimo iš pradžių sulaukė ir kino juostos, kurias JAV teismai, atsisakydami priimti kaip įrodymus bylose, įvardydavo kaip suteikiančias dideles galimybes būti suklastotoms, padirbtoms arba iškraipytoms.

Pasaulyje daugėjant elektroniniu būdu sukurtos informacijos, teismams neišvengiamai teko prisitaikyti prie kintančios aplinkos ir priimti bei vertinti šalių į bylą pateikiamus elektroninius duomenis, kurie ilgainiui tapo įprastine įrodinėjimo priemone teismų nagrinėjamose bylose.

Lietuvos Respublikos civilinio proceso kodekso (toliau – CPK) 177 str. 1 d. įrodymus civilinėje byloje apibrėžia kaip bet kokius faktinius

duomenis, kuriais remdamasis teismas įstatymų nustatyta tvarka konstatuoja, kad yra aplinkybių, pagrindžiančių šalių reikalavimus ir atsikirtimus, ir kitokių aplinkybių, turinčių reikšmės bylai teisingai išspręsti, arba jų išvis nėra. Lietuvos Respublikos administracinių bylų teisenos įstatymo (toliau – ABTĮ) 57 str. 1 d. nustato, kad administracinėje byloje kaip įrodymai yra visi faktiniai duomenys, priimti bylą nagrinėjančio teismo, ir kuriais remdamasis teismas įstatymų nustatyta tvarka konstatuoja, kad esama aplinkybių, pagrindžiančių proceso šalių reikalavimus bei atsikirtimus, ir kitokių aplinkybių, turinčių reikšmės bylai teisingai išspręsti, arba jų išvis nėra. ABTĮ 57 str. 2 d. elektroninius įrodymus išskiria kaip atskirą įrodymų rūšį, tačiau jų apibrėžimo nepateikia. CPK 175[1] str. 7 d. nustato, kad elektroniniai duomenys teismui pateikiami teisingumo ministro nustatyta tvarka ir forma, o jų įrodomoji galia yra tokia pat, kaip ir kitų įrodymų. Tačiau elektroninių duomenų apibrėžimas nei CPK, nei Lietuvos Respublikos teisingumo ministro 2012 m. gruodžio 13 d. įsakymu Nr. 1R-332 patvirtintame Procesinių dokumentų pateikimo teismui ir jų įteikimo asmenims elektroninių ryšių priemonėmis tvarkos apraše (toliau – Aprašas) nėra pateiktas.

Jungtinių tautų tarptautinės prekybos teisės komisijos (toliau – *UNCITRAL)* 1996 m. parengto Elektroninės komercijos pavyzdinio įstatymo 2 str. (a) p. nurodoma, kad duomenų pranešimas reiškia informaciją, sukurtą, išsiųstą, gautą ar saugomą elektroninėmis, optinėmis ar panašiomis priemonėmis, įskaitant (bet neapsiribojant) elektroninių duomenų apsikeitimą (EDI), elektroninį paštą, telegramas, teleksą ar telekopijas. Nors išvardydamas minėtąsias priemones Elektroninės komercijos pavyzdinis įstatymas iš esmės mini informacijai siųsti ir jai gauti naudojamas priemones, pati sąvoka apima ir kompiuteriu sukurtus duomenis, kurie nėra skirti perduoti, o sąvokos tikslas – iš esmės apimti bet kokius duomenis, kurie yra sukurti, saugomi ar perduodami nepopierine forma (tai pabrėžiama ir šio įstatymo priėmimo vadovo 30 ir 31 paragrafuose). Terminas „panašios priemonės“ reiškia priemones, atliekančias ekvivalentišką funkciją – taip užtikrinama, kad ši sąvoka ilgainiui nepasentų.

Kanados Bendrojo elektroninių įrodymų akto 1 str. b) p. elektroninius duomenis apibrėžia kaip duomenis, kurie yra įrašyti ar išsaugoti bet kokioje kompiuterinės sistemos laikmenoje ar kompiuterinės sistemos arba kito panašaus įrenginio, kurie gali būti perskaityti arba suprasti asmens ar kompiuterinės sistemos ar kito panašaus įrenginio. Jais laikomi šių duomenų spaudiniai, pateiktis ir išvediniai. Duomenys iš esmės gali būti fiksuojami bet kokioje laikmenoje, elektroninė jų forma nuo kitų skiriasi tik tuo, kad yra saugoma ar sukurta pasitelkus kompiuterines sistemas ar panašius

prietaisus. Šiuo atveju akte daromas skirtumas tarp informacijos perdavimo būdų. Jeigu, tarkime, informacija buvo persiųsta elektroniniu paštu arba perduota kompaktiniame diske, ji bus laikoma elektronine. Tačiau jeigu informacija persiųsta teleksu ar fakso aparatu (išskyrus kompiuterinius faksus) ji nebus laikoma elektronine, nes nebuvo jokio faktinio įrašymo į skaitmeninę laikmeną. Be to, elektronine informacija nebūtų laikomas ir telefoninis pokalbis, nes jis ne įrašomas, o tik perduodamas kompiuteriu ar panašiu įrenginiu. Tačiau balso pašto žinutė jau būtų prilyginta elektroninei informacijai, nes ji yra įrašoma į kompiuterį arba jame išsaugoma.

Elektroninių duomenų apibrėžimas yra pateiktas Lietuvos Respublikos elektroninio parašo įstatymo 2 str. 2 p., kuris nustato, kad elektroniniais duomenimis laikomi visi duomenys, kurie tvarkomi informacinių technologijų priemonėmis. Duomenų tvarkymas – visos su jais atliekamos operacijos: rinkimas, užrašymas, klasifikavimas, grupavimas, kaupimas, saugojimas, keitimas, kopijavimas, sujungimas, atskleidimas, teikimas, naudojimas, naikinimas. Lietuvos Respublikos elektroninio parašo įstatyme įtvirtintas platus elektroninių duomenų apibrėžimas yra vertintinas teigiamai, nes įstatymų leidėjo pasirinktos formuluotės greičiausiai nereikės keisti ar papildyti ir toliau plėtojantis informacinėms technologijoms, be to, po kurio laiko ji neturėtų prarasti savo aktualumo. Pavyzdžiui, jau minėtojo Kanados Bendrojo elektroninių įrodymų akto 1 str. b) p. įtvirtintas elektroninių duomenų apibrėžimas teisės doktrinoje yra kritikuojamas dėl savo neišsamumo, nelankstumo ir siaurumo.

Teisės doktrinoje nurodoma, kad informacija yra pripažįstama elektronine tik tuo atveju, jeigu ji egzistuoja laikmenoje, kuri gali būti perskaityta tik kompiuterio, įskaitant elektroninius laiškus, interneto tinklalapius, teksto apdorojimo programas (pvz., *Microsoft Word)*, garso ir vaizdo rinkmenas, nuotraukas, duomenų bazes, skaičiuokles ir visa kita, kas yra saugoma duomenų apdorojimo įrenginyje. Į šią daugialypę terpę patenka tarnybinės stotys, darbalaukiai, nešiojamieji kompiuteriai, mobilieji telefonai, kietieji diskai, atminties kortelės, Mp3 grotuvai ir delninukai. Šis sąrašas nėra baigtinis. Dar 2000 m. JAV Kanzaso apygardos teismas nagrinėtoje byloje *Kleiner v Burns* konstatavo, kad kompiuterizuotai ir kitai elektroniniu būdu įrašomai informacijai priskiriama: balso pranešimai ir failai (angl. *voice mail messages and files)*, atsarginiai balso pašto failai (angl. *backup voice mail files)*, elektroniniai pranešimai ir failai (angl. *e-mail messages and files)*, atsarginiai elektroninių pranešimų failai (angl. *backup e-mail files)*, sunaikintų elektroninių pranešimų failai (angl. *deleted e-mails)*, duomenų failai (angl. *data files)*, programiniai failai (angl. *program files),* atsarginiai ir archyviniai įrašai (angl. *backup and archival tapes)*, laikini failai (angl.

temporary files), sistemos istorijos failai (angl. *system history files)*, interneto puslapio informacija, išsaugota tekstiniu, grafiniu ar garso formatu (angl. *web site information stored in textual, graphical or audio format)*, interneto puslapio sisteminių įrašų bylos (angl. *web site log files)*, spartinimui saugomi failai (angl. *cache files)*, slapukai (angl. *cookies)*, tačiau vien jais neapsiribojama, dar apimama ir kita elektroniniu būdu įrašyta informacija.

Ko gero, vienas autoritetingiausių elektroninių įrodymų teisinį reguliavimą tyrinėjančių mokslininkų S. Masonas elektroninius įrodymus įvardija kaip atskirą įrodymų rūšį ir siūlo vartoti gana platų elektroninių įrodymų apibrėžimą *(Mason*, 2008). Pasak jo, elektroniniai įrodymai: duomenys (apimantys analoginių įrenginių išvestį arba skaitmeninio formato duomenis), kurie yra valdomi, laikomi ar perduodami bet kokiu dirbtiniu įrenginiu, kompiuteriu arba kompiuterių sistema arba siunčiami komunikacijos sistema, ir kurie turi galimybę padaryti šalių faktinius teiginius daugiau ar mažiau tikėtinus, negu jie tokie būtų nesant įrodymų.

Lietuvos teisės doktrinoje yra mokslininkų *(Stankevič*, 2012), manančių, kad elektroninių įrodymų kaip atskiros įrodinėjimo priemonės išskyrimas nėra nei pagrįstas, nei būtinas, nei tikslingas, o pats „elektroninio įrodymo“ terminas, nors ir plačiai paplitęs, nėra sėkmingas *(Stankevič*, 2012). Tokia pozicija iš esmės grindžiama tuo, kad skirtumai tarp analoginės ir skaitmeninės informacijos saugojimo formų teismo procese negalėtų būti tokie svarbūs, kad reikėtų keisti civilinio proceso įstatymus. Tarp Kinijos Liaudies Respublikos teisininkų irgi vyksta debatai dėl elektroninių įrodymų priskyrimo kuriai nors rūšiai. Vieni siūlo elektroninius įrodymus priskirti garso ir vaizdo duomenims, nes, pasak jų, elektroninių įrodymų turinys kompiuteriniame įrenginyje vis vien turėtų atsispindėti grafiko, skaitmenų, laiško ar emblemos pavidalu. Kiti laikosi pozicijos, kad elektroniniai įrodymai yra rašytinių įrodymų rūšis. Be to, yra teisininkų, kurie palaiko elektroninių įrodymų kaip atskiros rūšies išskyrimą. Galiausiai šalininkų sulaukė ir pozicija, kad elektroniniai įrodymai yra tik būdas pateikti įrodymų ir kitos jų rūšys gali būti demonstruojamos elektroniniu formatu (pvz., elektroninis dokumentas, elektroninė sutartis, elektroniniai užrašai ir pan.).

Dėl aiškumo reikėtų pabrėžti, kad informacijos teorijoje yra išskiriami du informacijos tipai – analoginė (ištisinė) ir skaitmeninė (diskretinė). Analoginė laikmena paprastai yra suprantama kaip materialioji medžiaga, kurioje fiksuojama norima perduoti informacija, sudaranti dokumento turinį. Analoginėje aplinkoje informacija yra neatsiejama nuo laikmenos (pvz., popierinių dokumentų turinys niekaip negali būti nuo jų atskirtas, nebent sunaikinant patį dokumentą). Skaitmeninėje aplinkoje sukurtų dokumentų turinys yra atskiriamas nuo laikmenos, kurioje jie buvo sudaryti.

Tradicinių dokumentų turinys fiksuojamas laikmenoje (popieriuje, fotojuostoje ir pan.), naudojant simbolių (raidžių, skaičių ir pan.) reikšmes, kurias žmogus gali perskaityti ir suprasti iš karto, nenaudodamas jokių papildomų priemonių. Tokiu būdu užtikrinama, kad dokumentą gali perskaityti visi, kurie tik atpažįsta simbolius. Elektroniniu būdu sukurtos informacijos turinys laikmenoje koduojamas (informacija įrašoma 0 ir 1 sekomis, t. y. skaitmeninama), todėl ji negali būti perskaitoma ar atpažįstama tiesiogiai, nenaudojant specialių priemonių. Kiekvieną kartą naudojant elektroninę informaciją, koduota informacija transformuojama iš savo pirminės – dvejetainės formos – į žmogui atpažįstamą ir suprantamą. Toks informacijos fiksavimo būdas lemia jos priklausomumą nuo informacinių technologijų priemonių (techninės ir programinės įrangos), kuriomis dokumentas yra sudaromas, naudojamas ir saugomas visu elektroninės informacijos gyvavimo metu, o tradicinėje aplinkoje sukurtas dokumentas nuo jo sudarymo momento tampa visiškai nepriklausomas nuo priemonių, kuriomis buvo sudarytas. Tradicinių dokumentų forma (šriftas, spausdinimo būdas, kalba, spalvos, specialūs ženklai, anspaudai ir t. t.) yra vartotojo tiesiogiai atpažįstama ir suprantama. Tuo metu visa elektroniniu būdu sukurtos informacijos forma vartotojui paprastai yra nežinoma. Elektroninės informacijos sudarytojo sukurtas žmogaus atpažįstamas ir suprantamas vaizdas, matomas kompiuterio ekrane, yra tik dalis elektroniniu būdu sudarytos informacijos struktūros, kurią žmogus gali suvokti. Didesnė dalis elektroninės informacijos formos elementų vartotojo nėra matomi, jie priklauso nuo techninės ir programinės įrangos, kurią naudojant informacija buvo sukurta, savybių. Kiekvieną kartą transformuojant elektroninę informaciją (pvz., į vartotojui atpažįstamą ir suprantamą vaizdą), elektroniniu būdu sukurtos informacijos forma kinta.

Užsienio teisės doktrinoje yra išskiriami šeši pagrindiniai elektroniniu būdu sukurtos informacijos ir rašytinių dokumentų skirtumai:

1) apimtis ir dauginimo galimybė. Elektroniniu būdu sukuriamos informacijos kiekis yra didesnis nei rašytinių dokumentų, ji sukuriama ir kopijuojama greičiau nei rašytiniai dokumentai;
2) išlaikomumas. Atsikratyti elektroniniu būdu sukurtos informacijos yra sudėtingiau nei rašytinės. Sunaikintas rašytinis dokumentas yra praktiškai nebeatkuriamas. Tuo metu, kalbant apie elektroninius duomenis, terminas „sunaikintas“ nereiškia negrįžtamo praradimo. Ištrinta iš kompiuterio rinkmena nėra visiškai sunaikinama, ji gali būti atkurta;
3) dinaminis, kintantis turinys. Elektroniniu būdu sukurtos informacijos turinys yra dinaminis ir sukurtas periodiškai keistis, kartais

net be žmonių įsikišimo. Vien pats prisijungimo prie tokios informacijos veiksmas gali pakeisti tokios informacijos turinį. Pvz., elektroninių dokumentų perkėlimo iš vienų laikmenų į kitas (pvz., kopijuojant juos į naujesnes laikmenas ar keičiant programinę įrangą) metu pakeičiama dalis formos elementų, nors dokumento turinys ir jo loginė forma, kurią atpažįsta ir supranta vartotojas, gali likti visiškai nepakitusi;

4) metaduomenys. Kontekstinė informacija atspindi aplinką, kurioje rašytinis dokumentas buvo sudarytas, jo sudarymo metu atliktus veiksmus, procedūras, kurių privaloma laikytis sudarant dokumentą, ir asmenis, dalyvavusius sudarant dokumentą. Kontekstinės informacijos sudedamosios dalys yra šios: dokumento sudarytojas, adresatas, antraštė (pavadinimas), sudarymo vieta, data, registracijos įrašai, įrašai apie dokumento autorių ar jį sudariusį asmenį, jų parašai, specialūs administracines ir teisines procedūras fiksuojantys įrašai – dokumento tvirtinimo, derinimo, dokumento perdavimo, gavimo žymos ir t. t. Dokumente fiksuojamos kontekstinės informacijos kiekį, formą, išdėstymo struktūrą ir pan. lemia jo administracinės ir teisinės aplinkos nustatyti reikalavimai bei taisyklės, kuriomis remiantis dokumente fiksuota kontekstinė informacija atpažįstama ir atskiriama nuo jo turinio. Tradiciniuose dokumentuose kontekstinė informacija paprastai yra pateikiama pačiame dokumente. Elektroniniu būdu sukurtos informacijos atveju šią funkciją atlieka metaduomenys, kurie apibrėžiami kaip duomenys apie duomenis (duomenys apie dokumento ar rinkmenos sudarymo aplinką ir dokumento ar rinkmenos struktūrą) ir yra būtini dokumentui ir rinkmenai suprasti ir naudoti. Metaduomenys fiksuojami atskirai nuo dokumento ar rinkmenos turinio, dalis jų yra sukuriami automatiškai kompiuterio programinės įrangos ir loginiais ryšiais susiejami su dokumentu ar rinkmena;

5) priklausomumas nuo aplinkos ir nusidėvėjimas. Elektroniniu būdu sukurta informacija gali tapti nesuprantama, kai yra atskiriama nuo savo aplinkos. Pvz., į duomenų bazę įdėta informacija gali tapti neįskaitoma, jeigu yra pašalinama iš struktūros, kurioje ji buvo sukurta. Slaptažodžiai, kriptografinės technikos ir kiti saugumo įrankiai irgi gali riboti vartotojo galimybę prieiti prie elektroniniu būdu sukurtos informacijos. Dėl techninės ir programinės įrangos senėjimo ir trumpalaikiškumo, elektroniniu būdu sukurta informacija po tam tikro laiko gali būti nebeatkuriama arba jos atkūrimas pareikalauti neproporcingai didelių sąnaudų;

6) sklaida ir tinkamumas paieškai. Elektroniniu būdu sukurta informacija, skirtingai nuo rašytinių dokumentų, gali būti išskirstyta į daugybę saugojimo vietų: išorinius kietuosius diskus, nešiojamuosius kompiuterius, atminties korteles, *CD* ir *DVD* laikmenas ir pan. Todėl elektroniniu būdu sukurtos informacijos kilmė nustatoma kur kas sudėtingiau, tačiau naudojant automatinius metodus tokios informacijos paieška vykdoma daug paprasčiau ir greičiau.

Įvertinus teisinį reguliavimą ir teisės doktriną galima teigti, kad teisės doktrinoje yra susiformavusi vyraujanti pozicija dėl elektroninių įrodymų kaip atskiros įrodymų rūšies išskyrimo, ir elektroniniai įrodymai negali būti prilyginami nei rašytiniams, nei kokiai nors kitai įrodymų rūšiai.

2 skirsnis. Elektroninių įrodymų svarba vykstant teismo procesui

Elektroninėms informacijos apdorojimo priemonėms vis labiau skverbiantis į kasdienę veiklą, internetas ir daugialypė terpė plėtojasi neįtikimais tempais. 2005 m. elektroniniu būdu saugomos informacijos kiekis pasauliniu mastu sudarė 130 eksabaitų[23], o 2011 m. – jau 1800 eksabaitų, t. y. toks kiekis duomenų yra pakankamas norint visiškai užpildyti 57,5 mlrd. 32 gigabaitų talpos *Apple iPad* planšetinius kompiuterius. Komunikacija naudojant elektronines priemones tapo įprasta vien dėl to, kad, palyginti su popierine, turi nenuginčijamų pranašumų:

1) duomenys sukuriami (sugeneruojami) ir apdorojami bei išsiunčiami toje pačioje aplinkoje (e. erdvėje) ir tomis pačiomis priemonėmis;
2) duomenys gali būti siunčiami iš vienos pasaulio vietos į kitą nepaisant atstumų ir beveik nepatiriant laiko sąnaudų. Tyrimais yra nustatyta, kad iš šimtą darbuotojų turinčios bendrovės per metus vidutiniškai išsiunčiama apie 1 200 000 el. laiškų;
3) elektroninių duomenų dauginimas ir kopijavimas yra palyginti nebrangus ir greitas procesas. Pavyzdžiui, į vieną gigabaitą telpa 64 782 *Microsoft Word* formato puslapių;
4) elektroniniai duomenys nereikalauja daug vietos saugoti ir archyvuoti. Skirtingai nei rašytiniai dokumentai, jie gali būti saugomi didesne apimtimi, įvairiose vietose ir juos saugoti yra kur kas paprasčiau (pvz., kietuosiuose diskuose, atminties kortelėse, nešiojamuosiuose kompiuteriuose, mobiliuosiuose telefonuose, „debesyse“ ir t. t.). Todėl natūralu, kad pasaulyje itin sparčiai daugėjant

[23] Vienas eksabaitas yra lygus milijardui gigabaitų.

elektroniniu būdu sukurtos informacijos (daugelyje pasaulio šalių daugiau kaip 90 proc. visų duomenų yra sukuriama, saugoma ir perduodama elektroniniu formatu), atitinkamai daugėja ir neabejotinai daugės ginčų teismuose, kur faktines aplinkybes bylos šalys įrodinėja ir įrodinės remdamosi būtent elektroniniu būdu sukurta informacija.

Jau dabar vykstant ginčui teisme, tam tikras faktines aplinkybes kai kuriais atvejais galima įrodyti tik elektroniniais duomenimis. Sprendžiant tokius ginčus teismuose, elektroniniai duomenys dažniausiai yra vienintelė arba svarbiausia tokių bylų įrodymų rūšis ir pagrindas. Kaip pavyzdžius (tai jokiu būdu nėra baigtinis sąrašas) galima nurodyti bylas, susijusias su:

1) judriojo telefono ryšio operatorių teikiamomis viešosiomis judriojo telefono paslaugomis. Minėtojo ryšio operatorius abonentui suteiktų paslaugų realumą ir kainų už jas pagrįstumą įrodinėja remdamasis automatizuotos sistemos, kuri analizuoja atitinkamo abonento *(SIM* kortelės) atliekamus telekomunikacijų įvykius (skambučius, *SMS*, duomenų perdavimą ir kt.), suteikiamos paslaugos kiekius (skambučio trukmę, perduotą duomenų kiekį ir pan.) ir priskiria sutarto dydžio kainą kiekvienam telekomunikacijų įvykiui, duomenimis (žr. pvz., Vilniaus apygardos teismo 2012 m. rugpjūčio 14 d. nutartį, priimtą civilinėje byloje *E. M. v. UAB „Omnitel“*, bylos Nr. 2A-1885-656/2012);
2) saugos tarnybos prievolės tinkamai reaguoti į iškvietimą tinkamu įvykdymu. Tokiose bylose teismas privalo vertinti saugos tarnybos centrinio stebėjimo pulto pagrindinio serverio duomenis (žr. pvz., Vilniaus apygardos teismo 2010 m. gegužės 12 d. sprendimą, priimtą civilinėje byloje *UADB Ergo Lietuva v. UAB G4S Lietuva*, bylos Nr. 2A-426-492/2010);
3) CK 2.22 str. įtvirtintos asmens teisės į atvaizdą ir LR CK 2.23 str. įtvirtintos asmens teisės į privatų gyvenimą ir jo slaptumą pažeidimais tais atvejais, kai informacija apie asmenį yra paskelbiama tik e. erdvėje, pvz., interneto tinklalapyje, socialiniuose tinkluose ar persiunčiama el. paštu tretiesiems asmenims, (žr. pvz., Šiaulių apygardos teismo 2013 m. kovo 28 d. nutartį, priimtą civilinėje byloje *R. P v. V. M*, bylos Nr. 2A-120-124 /2013);
4) teisių į intelektinę nuosavybę e. erdvėje pažeidimais[24].

[24] Plačiau apie tai skaitykite vadovėlio VI skyriuje.

3 skirsnis. Elektroninių įrodymų pateikimas teismui

Teisės doktrinoje įrodymų pateikimas teismui yra apibrėžiamas kaip faktinis įrodymų perdavimas teismui. Teisę pateikti įrodymus turi visi byloje dalyvaujantys asmenys (LR CPK 42 str., LR ABTĮ 53 str.). Bylos šalys savo turimus įrodymus byloje paprastai pateikia kartu su teismui pateikiamais procesiniais dokumentais: ieškiniu, atsiliepimu į ieškinį, priešiniu ieškiniu, rašytiniais paaiškinimais civilinėje byloje, skundu (prašymu), atsiliepimu į skundą (prašymą) administracinėje byloje (LR CPK 42 str., 135 str. 2 d., 142 str., LR ABTĮ 23 str. 2 d. 7 p., 72 str.).

LR CPK 114 str. 1 d. nustato, kad dalyvaujantis byloje asmuo, kuris procesinio dokumento turinį pagrindžia rašytiniais įrodymais, prideda jų originalus arba kopijas (skaitmenines kopijas), patvirtintas teismo, notaro (ar kito atlikti notarinius veiksmus įgalioto asmens), byloje dalyvaujančio advokato ar dokumentą išdavusio (gavusio) asmens. LR CPK 198 str. 2 d. nustato, kad rašytiniai įrodymai pateikiami šio LR CPK 114 str. nustatytos formos. Prieš įstatymų leidėjui pakeičiant LR CPK 198 str.[25], jame buvo nustatyta, kad dokumento rašytinei formai prilyginami dalyvaujančių byloje asmenų pasirašyti dokumentai, įstatymų ir kitų teisės aktų nustatyta tvarka perduoti telekomunikacijų galiniais įrenginiais. Teisės doktrinoje komentuojant LR CPK 198 str. buvo paaiškinta, kad rašytiniu įrodymu pripažintini ir elektroninio pašto pranešimai, jeigu juose esanti informacija gali būti pateikta vėlesniam naudojimui ir yra žinių apie nagrinėjamai bylai reikšmingas aplinkybes. Teisės doktrinoje elektroniniai įrodymai irgi buvo analizuojami prilyginant juos rašytiniams, įskaitant (bet neapsiribojant) elektroninių įrodymų pateikimo teismui klausimą. Todėl bylos šalys elektroninius įrodymus (pvz., susirašinėjimą el. paštu, nuotraukas, interneto tinklalapių išrašus ir t. t.) dažniausiai pateikdavo teismui išspausdintus popieriniu formatu. Nuo 2011 m. spalio 1 d. įsigaliojusio LR CPK 177 str. 2 d. atvėrė nebaigtinį įrodinėjimo priemonių sąrašą, todėl įrodinėjimas priemonėmis, kuriose užfiksuoti elektroniniai duomenys, įstatymo lygiu teisėtu ir leistinu pripažįstamas jau nuo 2011 m. spalio 1 dienos.

Teismų praktikos analizė patvirtina, kad bylos šalys, teikdamos teismui procesinius dokumentus raštu, dažnai prie šių dokumentų pridedamus ir teismui teikiamus elektroninius įrodymus *(SMS* žinutes, programos *Skype* pokalbių išklotines, el. laiškus, socialiniuose tinkluose ar interneto tinklapiuose skelbiamą informaciją) užfiksuoja naudodamosi antstolio pagalba šiam konstatuojant faktines aplinkybes. Faktinių aplinkybių

[25] Lietuvos Respublikos civilinio proceso kodekso pakeitimo ir papildymo įstatymas. Valstybės žinios, 2011, Nr. 85-4126.

konstatavimas – tai smulkus antstolio objektyviai matomų ir (ar) nustatomų faktinių aplinkybių aprašymas faktinių aplinkybių konstatavimo protokole. Konstatuojamos faktinės aplinkybės papildomai gali būti fiksuojamos vaizdo ar garso įrašymo priemonėmis. Tokie garso ar vaizdo įrašai laikomi sudedamąja faktinių aplinkybių konstatavimo protokolo dalimi (LR CPK 635 str. 1 d.). Vadinasi, surašydamas faktinių aplinkybių konstatavimo protokolą antstolis gali užfiksuoti bet kokius objektyviai matomus arba girdimus įrodymus: el. laiškų, asmenų susirašinėjimo internetinių pokalbių programomis bei informacijos, paskelbtos interneto tinklalapyje ar socialiniuose tinkluose ir atvaizduotos kompiuterio ar kito įrenginio ekrane, turinį. LR CPK 635 str. 4 d. nustato, kad antstolio surašytas faktinių aplinkybių konstatavimo protokolas laikomas oficialiu rašytiniu įrodymu ir turi didesnę įrodomąją galią.

Teismų įstatymo 37^1 str. 3 d. nustato, kad proceso dalyviai turi teisę visus procesinius dokumentus ir su teismo procesu susijusią informaciją teismams teikti elektroninės formos, teisingumo ministro nustatyta tvarka naudodami elektroninių ryšių priemones. Asmenys, teikiantys procesinius dokumentus elektroninių ryšių priemonėmis, turi juos pasirašyti saugiu e. parašu arba savo asmens tapatybę patvirtinti kitais būdais (per elektroninės bankininkystės sistemas ir pan.), arba užsiregistruoti teismų informacinėje sistemoje. LR CPK 175^1 str. iš esmės numatytos analogiškos nuostatos. Su teismo proceso bylomis susiję elektroniniai duomenys teismuose yra tvarkomi, įtraukiami į apskaitą ir saugomi naudojant informacines ir elektroninių ryšių technologijas Teisėjų tarybos nustatyta tvarka, suderinta su Lietuvos vyriausiuoju archyvaru. Bylos dėl teismo įsakymo išdavimo ir kitos Teisėjų tarybos nustatytos bylos bei su teismo procesu susijusi informacija gali būti tvarkomos vien elektronine forma. Elektroninėje byloje saugomos proceso metu sudarytų ar gautų rašytinių procesinių dokumentų skaitmeninės kopijos, išskyrus dokumentus, kurių dėl teisės aktų nustatytų reikalavimų negalima skaitmeninti, ir sudaryti ar pateikti elektroniniai procesiniai dokumentai. Rašytiniai procesiniai dokumentai turi būti skaitmeninti ir jų skaitmeninės kopijos perkeltos į elektroninę bylą ne vėliau kaip per tris darbo dienas nuo jų gavimo teisme. Skaitmeninėje kopijoje turi būti nurodytas dokumento skaitmeninimo laikas, dokumentą skaitmeninęs asmuo ir ji turi būti patvirtinta dokumentą skaitmeninusio asmens saugiu elektroniniu parašu. Kai dėl šioje dalyje nurodytų priežasčių rašytinių dokumentų negalima skaitmeninti, teismas priima motyvuotą nutartį saugoti dokumentus tik rašytinės formos ir tai nurodoma elektroninėje byloje (Teismų įstatymo 37^1 str. 6 d.). LR ABTĮ 24 str. 1 d. nustato, kad kai skundas (prašymas) paduodamas elektroninių ryšių priemonėmis, prie

jo turi būti pridedamos ir priedų skaitmeninės kopijos. Elektroninės formos skundai (prašymai) ir prie jų pridedamų priedų skaitmeninės kopijos pateikiami teisingumo ministro nustatyta tvarka.

Procesiniai dokumentai elektroninių ryšių priemonėmis teismui pateikiami naudojantis Lietuvos teismų informacinės sistemos (toliau – *LITEKO)* Viešųjų elektroninių paslaugų posistemiu (toliau – *VEP* posistemis). Asmuo prie *LITEKO VEP* posistemio paskyros gali prisijungti interneto svetainėse *www.teismai.lt* ir *www.epaslaugos.lt,* pasirinkęs Lietuvos teismų elektroninių paslaugų portalo nuorodą. Jungdamasis prie *LITEKO VEP* posistemio paskyros, asmuo privalo patvirtinti savo tapatybę. Jis tai gali padaryti naudodamasis Viešojo administravimo institucijų informacinių sistemų interoperabilumo sistemos teikiamomis priemonėmis arba teismo suteiktais asmenį identifikuojančiais prisijungimo duomenimis. Pastaruoju atveju pirmą kartą jungiantis prie *LITEKO VEP* posistemio, prisijungimo duomenis suteikia teismas, kuriame yra ar gali būti iškelta administracinė byla, arba byla nagrinėjama civilinio proceso tvarka, kurioje asmuo yra proceso dalyvis. Suteiktais prisijungimo duomenimis asmuo gali naudotis neribotą laiką. Fizinis asmuo, prisijungęs prie *LITEKO VEP* posistemio, atitinkamoje paskyroje veikia savo vardu arba kaip kito fizinio ar juridinio asmens atstovas. Kai asmuo teikia procesinius dokumentus, susijusius su konkrečios iškeltos bylos nagrinėjimu, prisijungęs prie *LITEKO VEP* posistemio paskyros jis iš sąrašo pasirenka konkrečią bylą, kurioje teikiami procesiniai dokumentai (tais atvejais, kai asmuo yra proceso dalyvis), arba nurodo bylos, į kurią teikiami procesiniai dokumentai, identifikacinius duomenis (jeigu asmuo nėra proceso dalyvis). Procesiniai dokumentai teismui gali būti pateikiami pildant *LITEKO VEP* posistemyje esančias procesinių dokumentų formas (šablonus) arba į ją gali būti įkeliami jau parengti procesiniai tokių formatų, kuriuos palaiko sistema, dokumentai. *LITEKO VEP* posistemis neleidžia asmeniui pateikti procesinių dokumentų teismui, jeigu nepateikti duomenys, kurie sistemoje nurodyti kaip privalomi. Jeigu procesiniai dokumentai teikiami pildant procesinių dokumentų formas (šablonus), šie duomenys vėliau įvedami automatiškai. Apie tai informuojamas dokumentus teikiantis asmuo ir nurodoma, kokių duomenų trūksta. Procesiniai dokumentai pateikiami teismui, kai dokumentus teikiantis asmuo *LITEKO VEP* posistemyje patvirtina konkrečių dokumentų siuntimą ir nurodo, kad žyminis mokestis sumokėtas, arba patvirtina konkrečių dokumentų siuntimą ir nurodo, kad žyminis mokestis nėra mokamas. Dokumentus teikiančiam asmeniui patvirtinus procesinių dokumentų siuntimą, *LITEKO VEP* posistemyje automatiškai fiksuojamas jų pateikimo teismui momentas. *LITEKO VEP*

posistemyje teismui pateikti procesiniai dokumentai automatiškai gaunami teismo *LITEKO* paskyroje.

Vykdant elektroninių paslaugų teisingumo procesą, informacinės sistemos naudotojo vadove nurodyta, kad į *LITEKO VEP* posistemį teikiamų procesinių dokumentų ir jų priedų bendras rinkmenos dydis negali viršyti 200 MB[26], o elektroniniu būdu teikiant procesinius dokumentus teismui kaip priedus galima pridėti:

1) tekstinių dokumentų formatus: *doc, docx, odt, rtf, txt, adoc*;
2) skaičiuoklių formatus: *xls, xlsx, ods*;
3) pateikčių formatus: *ppt, pptx, ppsx, odp*;
4) vektorinės grafikos vaizdų ir teksto formatus: *pdf, aplication/pdf*;
5) taškinės grafikos vaizdų formatus: *tif, tiff, jpg, jpeg, jfif, png, gif, bmp*;
6) vaizdo formatus: *avi, mpg, 3gp, 3g2, asf, asx, swx, swf, flv, vob, wmv, mov, rm*;
7) garso formatus: *wav, aif, mp3, mid, wma, flac, aac*.

Diskutuotina, ar tokia leidžiamų įkelti duomenų apimtis yra pakankama. Yra bylų, į kurias proceso šalys kaip įrodymus ketina teikti nemažai nuotraukų, skenuotų dokumentų ir (ar) vaizdo įrašų, kurių bendras dydis atitinkamai viršija maksimalią leistiną duomenų pateikimo teismui ribą. Manytina, kad atsižvelgiant į teismuose nagrinėjamų bylų pobūdį, į bylas pateikiamų įrodymų kiekį, teismui galimų pateikti elektroninių duomenų formatus ir teismų naudojamos elektroninių ryšių tinklų infrastruktūros pralaidumą, spartą bei turimų duomenų talpyklų apimtis tokia duomenų apimtis kol kas nėra laikytina racionalia ir pakankama. Be jokios abejonės, aukščiau minėtoji naujovė neužkerta kelio proceso šalims toliau teikti teismui elektroninius duomenis (pvz., el. laiškus, spausdintus interneto tinklalapius, informaciją iš socialinių tinklų ir pan.) popieriniu formatu arba *CD, DVD, USB* ar kituose duomenų saugojimo įrenginiuose, kurie yra nuskaitomi kompiuterio, tačiau reikėtų pabrėžti, kad procesinius dokumentus ir jų priedus pateikiant teismui tik elektroninių ryšių priemonėmis, remiantis CPK 80 str. 7 d., yra mokama tik 75 proc. už atitinkamą procesinį dokumentą mokėtinos žyminio mokesčio sumos, bet ne mažiau kaip dešimt litų.

Norėtųsi atkreipti dėmesį, kad tam tikrų elektroninių duomenų pateikimas teismui vis tiek išlieka problemiškas. Pvz., Autorių teisių ir gretutinių

[26] 2015 m. lapkričio 23 d. duomenimis, inicijuojant elektroninę civilinę bylą per *LITEKO VEP* posistemį Lietuvos teismų elektroninių paslaugų portale nurodoma, kad teismui teikiamų procesinių dokumentų ir jų priedų rinkmenos bendras dydis negali viršyti 40 megabaitų.

teisių įstatymo 2 str. 7 d. apibrėžia duomenų bazę kaip susistemintą ar metodiškai sutvarkytą kūrinių, duomenų arba kitokios medžiagos rinkinį, kuriuo galima individualiai naudotis elektroniniu ar kitu būdu, išskyrus kompiuterių programas, naudojamas tokių duomenų bazėms kurti ar valdyti. Manytina, kad duomenų bazės negalėtų būti priskirtos prie daiktinių įrodymų, nes įrodinėjimo prasme svarbiausi yra ne serveriai, kuriuose laikoma duomenų bazių informacija, bet jų turinys. Išspausdinta duomenų bazėse esanti informacija prarastų savo prasmę ir iki galo neatspindėtų tokios duomenų bazės turinio. Tuo metu antstolio paslaugos techninėmis priemonėmis fiksuojant duomenų bazės turinį (pvz., darant vaizdo įrašą) neišvengiamai reikštų bylos šaliai itin padidėjusias bylinėjimosi išlaidas. Vokietijos civilinio proceso kodekso 371 str. numatoma, kad netgi tokie elektroniniai duomenys kaip elektroniniai laiškai yra vertinami kaip apžiūros objektas. Todėl manytina, kad tais atvejais, kai nėra galimybės pateikti teismui tam tikrų elektroninių duomenų, užfiksuotų kokia nors forma taip, kad nagrinėjant bylą teisme galėtų kilti abejonių dėl tokių duomenų patikimumo, šalys, remdamosios CPK 210 str., galėtų prašyti teismo leisti pasinaudoti elektroninių duomenų apžiūros galimybe.

4 skirsnis. Elektroninių įrodymų sąsajumas

LR CPK 180 str. nustato, kad teismas priima nagrinėti tik tuos įrodymus, kurie patvirtina arba paneigia reikšmės bylai turinčias aplinkybes. Įrodymai konkrečioje byloje yra ne bet kokia informacija, o tik informacija apie aplinkybes, kurios yra įrodinėjimo dalykas. Šis reikalavimas yra vadinamas įrodymų sąsajumo taisykle. Įrodymų sąsajumas reiškia įrodymų turinio loginį ryšį su konkrečios bylos įrodinėjimo dalyku, t. y. informacija (faktiniai duomenys), sudaranti įrodymų turinį, turi patvirtinti arba paneigti aplinkybes, kurios yra reikšmingos konkrečiai civilinei bylai. Įrodymų sąsajumo taisyklę turi taikyti ne tik teismas, bet ir byloje dalyvaujantys asmenys. Teismas, per įrodinėjimo procesą vykdydamas savo pareigas, tikrina, ar įrodymus teikiantys asmenys vadovavosi LR CPK 180 str., nustatančio sąsajumo taisyklę, nuostatomis (žr. pvz., Lietuvos Aukščiausiojo Teismo 2012 m. balandžio 4 d. nutartį, priimtą civilinėje byloje *UAB „Vindeva“ v. UAB „Vilpra“*, bylos Nr. 3K-3-146/2012). Preliminariai įrodymų sąsajumas nustatomas jau rengiantis nagrinėti bylą. Įrodymus, neturinčius ryšio su įrodinėjimo dalyku, ir pakartotinai pateiktus įrodymus, kurie jau anksčiau buvo pateikti ir priimti, teismas atsisako priimti. Tokiais atvejais teismas priima rašytinę arba žodinę motyvuotą nutartį (CPK 181 str. 1 d., 290 str. 1–4 d.). Ar šalių prašomi pateikti ir prašomi išreikalauti įrodymai

yra susiję su įrodinėjimo dalyku, galutinai vertina ir sprendžia bylą nagrinėjantis teismas. Tam tikri reikšmingi faktai byloje nustatomi, ištyrus ir įvertinus įrodymus, kurių pagrindu susiformuoja teismo įsitikinimas, kad tam tikros aplinkybės, susijusios su ginčo dalyku, egzistuoja arba neegzistuoja. Šalių į bylą teikiamus įrodymus teismas dažniausiai prideda prie bylos ir juos įvertina priimdamas teismo sprendimą, išskyrus atvejus, kai šalių teikiami įrodymai yra akivaizdžiai nesusiję su nagrinėjamąja byla.

Lietuvos vyriausiasis administracinis teismas savo praktikoje yra ne kartą pabrėžęs, kad įrodinėjimo procesui reikšmingi tik tie įrodymai, kurie yra susiję su nagrinėjamąja byla. Tokia sąsaja nustatoma atsižvelgiant į administracinės bylos ribas, kurias nustato pareiškėjo suformuluoti reikalavimai. Sąsajumo taisyklių turi paisyti tiek teismas, tiek ir byloje dalyvaujantys asmenys. Pavyzdžiui, reikšdami prašymus priimti įrodymus ar juos išreikalauti, asmenys privalo nurodyti, kokias reikšmingas aplinkybes tie įrodymai gali patvirtinti arba paneigti. Įrodymus, neturinčius ryšio su byla, atsisakoma priimti, o kai jie yra byloje, teismas gali jų nevertinti ir pripažinti, kad tam tikri bylos dokumentai nelaikytini įrodymais.

Tiek Lietuvoje, tiek kitose valstybėse (Kanadoje, Australijoje, Indijoje, JAV, Šveicarijoje, Latvijoje, Vengrijoje ir kt.) įrodymų sąsajumo taisyklė yra taikoma visoms be išimties įrodymų rūšims. Elektroniniai įrodymai nėra išimtis, todėl kiekviena šalis, teikdama įrodymus teismui, privalo pagrįsti šių įrodymų sąsają su įrodinėjimo dalyku, t. y. motyvuotai pagrįsti, kad jos į bylą teikiami elektroniniai duomenys (el. pašto laiškai, *Skype* programos pokalbių išklotinė, socialiniame tinkle paskelbtos nuotraukos ir t. t.) yra susiję su įrodinėjimo dalyku konkrečioje byloje, pvz., įrodo kitos proceso šalies neištikimybės santuokoje, įmonės komercinės paslapties atskleidimo faktą ir t. t.

5 skirsnis. Elektroninių įrodymų vertinimas

Įrodymų vertinimas yra baigiamasis etapas, kurio metu teismas, remdamasis bylos nagrinėjimo metu ištirtais įrodymais ir vadovaudamasis savo vidiniu įsitikinimu, pateikia išvadas dėl konkrečių įrodymų leistinumo, sąsajumo, jų įrodomosios vertės, ryšio su kitais įrodymais, taip pat – ar konkrečiais įrodymais grindžiamos faktinės aplinkybės yra nustatytos ar nenustatytos. ABTĮ įtvirtina laisvo įrodymų vertinimo principą, reiškiantį, kad jokie įrodymai teismui neturi iš anksto nustatytos galios, o įrodymus teismas, vadovaudamasis įstatymu ir teisingumo bei protingumo kriterijais, vertina pagal savo vidinį įsitikinimą, pagrįstą visapusiškai išsamiu bylos aplinkybių išnagrinėjimu. CPK 185 str. irgi įtvirtina laisvo įrodymų

vertinimo principą, kuris reiškia, kad galutinai ir privalomai įrodymus vertina teismas pagal savo vidinį įsitikinimą, pagrįstą visapusišku ir objektyviu aplinkybių, kurios buvo įrodinėjamos proceso metu, išnagrinėjimu. Vertinant kiekvieno įrodymo įrodomąją reikšmę, nurodytinas jo ryšys su įrodinėjimo dalyku, nustatytina, ar įrodymas yra leistinas ir patikimas, ar nėra klastojimo požymių, ar tinkamai buvo paskirstytos įrodinėjimo pareigos, ar nepaneigtos pagal įstatymus nustatytos prezumpcijos, ar yra prejudicinių faktų. Vertindamas įrodymų visumą, teismas turi įsitikinti, kad pakanka duomenų išvadai, jog tam tikri faktai egzistavo arba neegzistavo, ir nėra esminių prieštaravimų, paneigiančių tokias išvadas.

Atsižvelgiant į elektroninių duomenų specifiką, kai kuriose užsienio valstybėse elektroninių įrodymų vertinimas yra reglamentuotas teisiniu lygiu (pvz., Kanada, Filipinai, Vokietija) arba reguliuojamas atitinkamų standartų. Didžiosios Britanijos standartų institucija yra priėmusi šiuos standartus: „Dėl elektroniniu būdu laikomos informacijos teisinio priimtinumo bei įrodomojo svorio“, „Dėl elektroninių pranešimų teisinio priimtinumo ir įrodomojo svorio“, „Dėl elektroninės tapatybės susiejimo su dokumentais teisinio priimtinumo ir įrodomojo svorio“. Kanados visuotinių standartų valdyba yra priėmusi šiuos standartus: „Elektroniniai įrašai kaip dokumentiniai įrodymai“, CAN-CGSB 72.34 (2005), „Mikrofilmai ir elektroniniai atvaizdai kaip dokumentiniai įrodymai“, CAN-CGSB-72.11-93. Tarptautinė standartizacijos asociacija (ISO) irgi yra priėmusi standartą „Dokumentų valdymas-Elektroniniu būdu saugoma informacija-Rekomendacijos dėl patikimumo ir tikrumo“ ISO/TR 15801:2009. Be jokios abejonės, tokie standartai suteikia teisinio aiškumo verslo subjektams organizuojant savo veiklą ir tvarkant elektroninius duomenis bei kartu padeda teismui tinkamai įvertinti jam elektronine forma pateiktus įrodymus.

Lietuvoje elektroninių įrodymų vertinimo klausimo kol kas nereguliuoja nei įstatymai, nei atitinkami standartai, todėl šiuo atveju reikėtų vertinti tarptautinį ir užsienio valstybių teisinį reguliavimą, doktriną ir teismų praktiką. *UNCITRAL* elektroninės komercijos pavyzdinio įstatymo 9 str. 1 d. (a) p. nustato, kad elektroninio duomenų pranešimo įrodomoji galia negali būti sumenkinta dėl to, kad jis nėra originalios formos, jeigu tai yra geriausias įrodymas, kokį iš jį pateikiančio asmens protingai galima tikėtis gauti. Minėtojo įstatymo 9 str. 2 d. nustatyti kaip įrodymo elektronine forma pateikiamos informacijos priemonės vertinimo kriterijai:

1) būdo, kuriuo duomenų pranešimas buvo sukurtas, saugotas ar persiųstas, patikimumas;
2) informacijos integralumo (vientisumo, nepakeičiamumo) išlaikymo būdo patikimumas;

3) būdas, kuriuo nurodomas duomenų pranešimo kūrėjas;

4) bet kuris kitas tinkamas faktorius.

Kanados Bendrojo elektroninių įrodymų akto 3 str. nustato, kad asmuo, siekiantis teismui pateikti elektroninius duomenis, turi pareigą įrodyti jų autentiškumą, pateikdamas įrodymų, kad elektroniniai duomenys yra tai, ką asmuo tvirtina esant. Minėtojo akto 4 str. nustato geriausio įrodymo taisyklę (angl. *best evidence rule)*. Ši taisyklė paprastai reiškia, jog tiriant tam tikro įrodymo turinį (teismas reikalauja įrodymo originalo) jos bus laikomasi, jeigu teismui bus pateikti įrodymai apie elektroninių duomenų sistemos, kurioje arba kurią pasitelkus duomenys buvo įrašyti ar saugoti, vientisumą. Akto 5 str. įtvirtina vientisumo prezumpciją. Nesant įrodymų, kurie leistų daryti priešingą išvadą, elektroninių duomenų sistemos vientisumas yra preziumuojamas, jeigu kompiuterių sistema ar kitas panašus įrenginys visada tinkamai funkcionavo, o jeigu tinkamai nefunkcionavo, tai faktas, kad ji nepaveikė elektroninių duomenų vientisumo, ir neegzistuoja jokių kitų pagrįstų priežasčių abejoti elektroninių įrodymų sistemos vientisumu. Akto 5 str. nustato, kad nesant įrodymų, kurie leistų daryti priešingą išvadą, elektroninių duomenų sistemos vientisumas irgi yra preziumuojamas, jeigu elektroniniai duomenys buvo įrašyti ar išsaugoti proceso šalies, tačiau ne tos, kuri siekia tokius elektroninius duomenis pateikti teismui, arba elektroniniai duomenys buvo įrašyti ar išsaugoti trečiųjų asmenų, kurie nėra proceso šalys, komercinėje veikloje (pvz., bankai, interneto paslaugų teikėjai, telefono ryšio operatoriai ir pan.). Akto 7 str. nustato, kad elektroninių duomenų sistemos vientisumą šalys gali įrodinėti rašytiniais parodymais prisiekusios ir pasirašiusios (angl. *affidavit)*.

Filipinų Aukščiausiojo Teismo elektroninių įrodymų vertinimo taisyklių 3 str. 2 d. nustato, kad elektroninis dokumentas yra leistinas kaip įrodymas, jeigu jis atitinka visas įrodymų leistinumo taisykles, kurios nustatytos teismo taisyklėse ir susijusiuose teisės aktuose bei jo autentiškumas yra patvirtintas taisyklių nustatyta tvarka. Taisyklių 2 str. 1 d. h) p. nustato, kad jų taikymo tikslams sąvoka „elektroninis dokumentas“ gali būti vartojama kaip sąvokos „elektroninis duomenų pranešimas“ sinonimas. Taisyklių 7 str. 1 d. pateiktas detalus sąrašas kriterijų, į kuriuos būtina atsižvelgti vertinant elektroninių duomenų įrodomąją vertę:

1) būdo ar metodo, kuriuo duomenys buvo surinkti, saugoti ar perduoti, patikimumą, įskaitant (bet neapsiribojant) duomenų įvedimo ar ištrynimo procedūras, įvairius testus ir patikrinimus, skirtus duomenų patikimumui ir tikslumui patvirtinti;

2) būdų, kuriais identifikuojamas dokumentą patvirtinęs asmuo (teksto autorius), patikimumą;

3) informacinių sistemų, kuriose elektroniniai duomenys buvo sugeneruoti ir saugomi, vientisumą, įskaitant (bet neapsiribojant) techninę ir programinę įrangą, kompiuterių programas ir šių klaidas;
4) liudytojo ar asmens, kuris naudojosi komunikacijos ir informacijos sistema, išprusimo lygį;
5) informacijos, kuria remiantis buvo sukurti elektroniniai duomenys, tipą ir kokybę;
6) kitus veiksnius, kurie, teismo nuomone, galėjo turėti įtakos elektroninių duomenų vientisumui ir tikslumui.

Taisyklių 7 str. 2 d. nustato, kad tuo atveju, kai kyla ginčas dėl informacinės ar komunikacinės sistemos vientisumo, kurioje elektroninis dokumentas ar elektroninių duomenų žinutė yra įrašyta ar saugoma, teismas, be kita ko, dar turi atsižvelgti ir į šiuos veiksnius:

1) ar informacinės ir komunikacinės sistemos arba kitas panašus įrenginys funkcionavo tokiu būdu, kuris nepaveikė sukurto elektroninio dokumento vientisumo ir neegzistuoja jokios kitos pagrįstos priežasties abejoti informacinės ar komunikacinės sistemos vientisumu;
2) ar elektroninis dokumentas buvo įrašytas ar saugomas tos proceso šalies, kuri ketina jį panaudoti savo naudai;
3) ar elektroninis dokumentas buvo sukurtas ar saugomas įprastu būdu normalioje komercinėje veikloje tų asmenų, kurie nėra teismo proceso šalys ir kuriems negalėjo daryti įtakos asmenys, dalyvaujantys byloje kaip šalys.

JAV teismų praktikoje (žr. pvz., JAV Merilando apygardos teismo 2007 m. gegužės 4 d. sprendimą byloje *Lorraine v. Markel American Insurance Company* 241 F.R.D. 534) yra suformuluotos Elektroninių duomenų vertinimo taisyklės. Kai elektroniniai duomenys yra teikiami kaip įrodymai, teismas privalo vertinti:

1) ar elektroniniai duomenys yra susiję su nagrinėjamąja byla (įrodymų sąsajumo taisyklė);
2) jeigu elektroniniai duomenys susiję su nagrinėjamąja byla, ar jie yra autentiški;
3) ar elektroniniams duomenims taikoma gandų (angl. *hearsay rule)*[27] taisyklė, jeigu taip, ar šiai taisyklei numatoma tam tikrų išimčių pagal atitinkamas Federalinių įrodymų taisyklių nuostatas;

[27] JAV liudytojo parodymai apie aplinkybes, kurių jis pats nematė ir negirdėjo, tik sužinojo iš kitų, yra vertinami kaip gandai.

4) ar elektroniniai duomenys, kurie teikiami kaip įrodymas, yra pateikiami originalios formos, ar tai yra kopija pagal geriausio įrodymo taisyklę, jeigu nė viena iš šių sąlygų nėra tenkinama, ar egzistuoja leistinumo reikalavimus atitinkantys išvestiniai įrodymai, galintys patvirtinti elektroninių duomenų turinį;
5) ar įrodomoji elektroninių duomenų vertė iš esmės pranoksta neteisingo išankstinio nusistatymo grėsmę pagal atitinkamas Federalinių įrodymų taisyklių nuostatas.

1. Elektroninių įrodymų leistinumas

Jeigu įrodymų sąsajumas yra įrodymų turinio dalykas, tai leistinumas paprastai reiškia reikalavimus, keliamus įrodymų formai. Antra, įrodymai turi būti surinkti, pateikti, ištirti ir įvertinti laikantis įstatymo nustatytos tvarkos. Trečia, įrodinėjant tam tikras konkrečios bylos aplinkybes būtina naudoti įstatymų tiesiogiai nurodytas įrodinėjimo priemones.

Teisės doktrinoje pripažįstama, kad elektroninių duomenų autentiškumas yra bene svarbiausia problema vertinant elektroninių duomenų leistinumą. Duomenų autentiškumas apibrėžiamas kaip įrodymas teismui, kad:

1) duomenų turinys, kuriuo remiasi proceso šalis, išliko nepakitęs nuo to momento, kai jis buvo sukurtas, iki tokių duomenų pateikimo teismui kaip įrodymo;
2) užfiksuota informacija yra atsiradusi iš jos pirminio šaltinio ir nesvarbu, ar tas šaltinis yra žmogus, ar įrenginys;
3) techniniai ir organizaciniai duomenys patvirtina faktą, kad duomenų vientisumas yra patikimas, todėl ir duomenys laikomi patikimais.

Elektroninių duomenų autentiškumo įrodinėjimas priklauso nuo jų rūšies. Atsižvelgiant į žmogaus dalyvavimą, išskiriamos kelios elektroninių duomenų rūšys:

1) elektroniniai duomenys, kurie patvirtina tam tikro įvykio ar fakto buvimą ir kuriems sukurti būtinas aktyvus asmens (ar kelių) dalyvavimas (pvz., elektroniniai laiškai, pokalbių programų žinutės, teksto redagavimo programomis sukurti dokumentai). Šiuo atveju įrodinėjimo prasme gali būti itin svarbu nustatyti, ar duomenų turinys patikimai atspindi asmens išreikštas mintis;
2) elektroniniai duomenys, kurie patvirtina tam tikrą faktą ar įvykį, tačiau generuojami automatiškai, ir tiesioginis žmogaus dalyvavimas kuriant (generuojant) šiuos duomenis nėra būtinas (pvz., interneto paslaugų teikėjo *web* serverių sisteminiai įrašai, telefono

ryšio operatorių duomenys, ATM (angl. *activity transaction model)* finansinės operacijos). Įrodinėjimo prasme svarbiausias uždavinys proceso šalims būtų pateikti teismui patikimų įrodymų, kad kompiuterio programa, kuri sugeneravo įrašus, atitinkamu laikotarpiu funkcionavo be sutrikimų;

3) tam tikrą faktą ar įvykį patvirtinantys elektroniniai duomenys, kuriems sukurti būtinas tiek tiesioginis žmogaus dalyvavimas, tiek kompiuterio programos atliktos operacijos, pvz., elektroninė finansų skaičiuoklė, į kurią asmuo suveda duomenis, o skaičiavimus atlieka kompiuteris. Įrodinėjimo prasme svarbu ir tai, kas tokiu atveju yra turinio autorius (asmuo ar kompiuteris) ir kokia turinio dalis yra sukurta žmogaus, o kokia – kompiuterio.

Paprastai elektroninių duomenų autentiškumas įrodinėjamas liudytojų parodymais, trečiųjų asmenų pateiktais duomenimis (pvz., interneto paslaugų teikėjo įrašai, telefono ryšio operatorių duomenys), specialisto išvada ar ekspertizės duomenimis. Elektroninių duomenų autentiškumui įrodyti plačiai naudojamasi kriptografinėmis technikomis. Būtent jomis yra paremtas elektroninio parašo naudojimas[28]. Elektroninio parašo įstatymo 8 str. 1 d. nustato, kad saugus elektroninis parašas, sukurtas saugia parašo formavimo įranga ir patvirtintas galiojančiu kvalifikuotu sertifikatu, elektroniniams duomenims turi tokią pat teisinę galią kaip ir rašytinius dokumentus patvirtinantis parašas ir yra leistinas kaip įrodinėjimo priemonė teisme. Vadinasi, teismas preziumuos, kad elektroniniai dokumentai, pasirašyti saugiu elektroniniu parašu, yra autentiški. Iš esmės analogiškos nuostatos dėl elektroninių dokumentų autentiškumo yra įtvirtintos ir Vokietijos civilinio proceso teisėje bei Filipinų Aukščiausiojo Teismo elektroninių įrodymų vertinimo taisyklėse. Tačiau teismų praktikos analizė rodo, kad teismai kartais nepagrįstai suabsoliutina elektroninio parašo naudojimą kaip vienintelę elektroninių duomenų autentiškumo patvirtinimo priemonę. Lietuvos apeliacinis teismas 2011 m. spalio 10 d. nutartyje, priimtoje civilinėje byloje *UAB „Furnitūra marketingas" v. UAB DHL Lietuva*, bylos Nr. 2A-435/2011, konstatavo, kad Elektroninio parašo įstatymo 8 str. 1 d. išdėstytas teisinis reglamentavimas apibrėžia ne tik patį elektroninį parašą, bet ir įtvirtina taisyklę, pagal kurią tik elektroniniu parašu patvirtinti elektroniniai duomenys gali būti laikomi leistinais įrodymais teisme. Pasak teismo, tik esant elektroniniam parašui galima objektyviai įvertinti, kad elektroninio laiško siuntėjo ir gavėjo duomenys atitinka tikrovę ir kad šio laiško turinys bei kiti duomenys irgi atitinka tikrovę, t. y. nėra prielaidų

[28] Plačiau apie tai žr. vadovėlio V skyrių.

abejonėms, kad elektroninio laiško turinys gali būti pakeistas. Ši teismo pozicija pagrįstai kritikuojama teisės doktrinoje, nurodant, kad teismas netaikė Elektroninio parašo įstatymo 8 str. 2 d. įtvirtinto kitų elektroninio parašo formų nediskriminavimo reikalavimo ir įstatymo 8 str. prezumpciją visiškai be pagrindo pritaikė kaip įsakmų reikalavimą visais atvejais reikalauti kvalifikuoto elektroninio parašo. Tokia teismo pozicija prieštarauja užsienio teisės doktrinai ir teismų praktikai, nes, kaip minėta, kriptografinė technika yra tik vienas iš elektroninių duomenų autentiškumo įrodymo būdų. Norėtųsi pabrėžti, kad Lietuvos apeliacinis teismas 2013 m. gegužės 27 d. nutartyje, priimtoje civilinėje byloje *UAB „Lintera" v. L.G. ir BUAB Prof-T*, bylos Nr. 2A-379/2013, atmesdamas apelianto argumentus dėl netinkamo elektroninių laiškų vertinimo ir vertindamas šių laiškų autentiškumą, apsiribojo argumentu, kad pats apeliantas neginčijo, jog elektroninis susirašinėjimas vyko iš jo elektroninio pašto, todėl pagrįstai sprendė, kad itin menkai tikėtina, jog nevienkartinį susirašinėjimą iš apelianto elektroninio pašto būtų vykdę nežinomi asmenys.

Tuo atveju, jeigu proceso šalis negalės pagrįsti elektroninių duomenų autentiškumo, teismas tokio įrodymo apskritai nepripažins leistinu ir jo nevertins. Pvz., Kauno miesto apylinkės teismas 2012 m. lapkričio 19 d. sprendime, priimtame civilinėje byloje *UAB „Sergel" v G. M.*, bylos Nr. 2-11525-877/2012, konstatavo, kad iš nežinomo kompiuterio ekrano išspausdinto vaizdo nelaiko leistinu bylos įrodymu.

Be to, svarbu pabrėžti, kad vertindamas elektroninių įrodymų autentiškumą praktikoje teismas remiasi byloje surinktų įrodymų visuma ir vadovaujasi logikos dėsniais. Pavyzdžiui, vienoje civilinėje byloje pirmosios instancijos teismas atsisakė remtis atsakovės, kuri buvo saugos tarnyba, pateiktais skaitmeninėje laikmenoje (CD) užfiksuotais centrinio stebėjimo pulto pagrindinio serverio duomenimis ir sprendime nurodė, kad bylos nagrinėjimo metu nebuvo kategoriškai paneigta techninė galimybė keisti užfiksuotus centrinio stebėjimo pulto pagrindinio serverio duomenis. Apeliacine tvarka nagrinėdamas bylą Vilniaus apygardos teismas nesutiko su tokiu įrodymų vertinimu ir 2010 m. gegužės 12 d. sprendime, priimtame civilinėje byloje *UADB Ergo Lietuva v. UAB G4S Lietuva*, bylos Nr. 2A-426-492/2010, nurodė, kad galimybė keisti užfiksuotus serverio duomenis yra tik prielaida ir ja grįsti teismo sprendimo argumentų negalima. Teismas pabrėžė, kad Lietuvos teismo ekspertizės centras vienareikšmio atsakymo dėl galimybės manipuliuoti serveryje užfiksuotais originaliais duomenimis nepateikė ir pasiūlė teismui kreiptis į programinės įrangos gamintoją ar jo įgaliotąjį atstovą Lietuvoje. Tuo metu per teismo posėdį apklaustas ekspertas negalėjo atsakyti, ar yra galimybė keisti

užfiksuotus duomenis, o ieškovas byloje atsisakė atlikti skaitmeninės informacijos ekspertizę. Pasak teismo, ieškovas, iškėlęs argumentą, kad atsakovės įrodymas suklastotas (pakeisti serverio duomenys), turėjo pateikti tokį argumentą patvirtinančių įrodymų. Priešingu atveju, kaip konstatavo apeliacinės instancijos teismas, nėra kliūčių teismo išvadas grįsti atsakovo pateiktais užfiksuotais centrinio stebėjimo pulto pagrindinio serverio duomenimis, juo labiau kad šiuos duomenis patvirtina liudytojo parodymai.

Teismai reaguoja į technologijų įtaką asmenų tarpusavio bendravimui ir ją vertina. Apeliacine tvarka nagrinėdamas bylą dėl teisės į atvaizdą pažeidimo ir neturtinės žalos atlyginimo Vilniaus apygardos teismas 2014 m. kovo 21 d. nutartyje, priimtoje civilinėje byloje *J. Ž. v. O. K,* bylos Nr. 2A-1006-340/2014, konstatavo, kad tai, jog socialinio tinklo „Facebook" svetainėje sukurto profilio autorius turi galimybę nuotraukas ar kitą informaciją rodyti (skleisti) neribotam žmonių arba apibrėžtam draugų kiekiui ar kitiems autoriaus nurodytiems asmenims, yra laikytina visiems žinoma aplinkybe, kuri nereikalauja papildomo įrodymo.

Dar norėtųsi atkreipti dėmesį į LAT 2015 m. lapkričio 20 d. nutartį, priimtą civilinėje byloje *B. L. v. VĮ Biržų ligoninė*, bylos Nr. 3K-3-603-701/2015, kurioje kasacinis teismas išaiškino, kad bylą nagrinėjančiam teismui nėra draudžiama pradinę informaciją apie specialiųjų žinių reikalaujančias teisinių santykių sritis, tarp jų – ir medicinos, rinkti naudojantis įvairiais šaltiniais, specialiąja literatūra, taigi – ir internetu. Vis dėlto, pasak kasacinio teismo, tokie šaltiniai negali pakeisti specialiųjų žinių turinčių asmenų (ekspertų) išvadų, kurios yra viena iš įrodinėjimo priemonių, ir teismas negali paneigti eksperto išvados, remdamasis vien interneto šaltiniu.

Kritiškai vertintina tokia teismų praktika, kai teismas apskritai neanalizuoja bylai pateiktų elektroninių duomenų ir jų nevertina. Kauno apygardos teismas 2011 m. lapkričio 24 d. nutartyje, priimtoje civilinėje byloje *M. M v. UAB „Vykom"*, bylos Nr. 2A-2130-555/2011, apskritai nevertino apelianto argumentų, kuriais šis kėlė klausimą dėl *Skype* programos pokalbių išklotinių turinio tapatumo, perkėlus pokalbių turinį į *Microsoft Excel* programą, kurioje duomenys galbūt galėjo būti redaguojami. Teismas nevertino fakto, kad duomenų perkėlimą atliko atsakovo darbuotojas, kuris nėra informacinių technologijų specialistas, ir visiškai nevertino aplinkybės, kad *Skype* programos pokalbių išklotinių turinys kompiuterio ekrane nebuvo konstatuotas antstolio, o buvo perkeltas *Microsoft Excel* programa, kuria įmanoma redaguoti duomenis.

Elektroninių duomenų rinkimas yra glaudžiai susijęs su asmens teise į privatumą[29]. Elektroninių ryšių įstatymo 61 str. 1 d. nustatyta, kad be faktinių elektroninių ryšių paslaugų naudotojų sutikimo draudžiama klausytis, įrašyti, kaupti ar kitu būdu perimti pranešimų turinį ir srauto duomenis ar su jais susipažinti, išskyrus atvejus, kai tai galima teisėtai daryti pagal šio įstatymo 66 ir 77 str.; be faktinių elektroninių ryšių paslaugų naudotojų sutikimo draudžiama atskleisti elektroninių ryšių tinklais perduodamų pranešimų turinį ir (ar) susijusius srauto duomenis arba sudaryti sąlygas sužinoti tokią informaciją ir (ar) susijusius srauto duomenis, išskyrus įstatymo nustatytus atvejus. Elektroninių ryšių įstatymo 3 str. 21 p. yra pateikta „faktinio elektroninių ryšių paslaugų naudotojo“ sąvoka – tai fizinis asmuo, asmeniniams ar verslo tikslams naudojantis viešąsias elektroninių ryšių paslaugas; šis asmuo nebūtinai turi būti šių paslaugų abonentas. Vilniaus apygardos teismas, apeliacine tvarka nagrinėdamas civilinę bylą, kurioje, be kita ko, buvo kilęs ginčas ir dėl to, ar darbdavys, kuris nėra viešąsias elektroninių ryšių paslaugas teikiantis subjektas, teisėtai padarė savo darbuotojos *Skype* programos išrašą ir iš kompiuterio atminties nukopijavo duomenis apie interneto svetainių adresus, savo 2012 m. gruodžio 28 d. nutartyje, priimtoje civilinėje byloje *R. J. v UAB „Baltic Transport Group“*, bylos Nr. 2A-3217-781/2012, konstatavo, kad sisteminė Elektroninių ryšių įstatymo analizė leidžia daryti išvadą, kad fizinis asmuo (šiuo atveju darbuotojas) visais atvejais, net ir turint pagrįstą įtarimą, jog atliekami neteisėti ir neleistini veiksmai, turėtų būti iš anksto informuojamas apie jo naudojamų prietaisų ir programų išklotinių patikrinimą. Teismas sprendė, kad nenustatęs darbo priemonių naudojimosi tvarkos apribojimų (lokalinių teisės aktų), iš jų ir dėl draudimo *Skype* programa naudotis asmeniniams tikslams, ir neįspėjęs, kad susirašinėjimas ar lankymasis interneto tinklalapiuose bus tikrinamas, bei slapta nurašęs kompiuterio atmintyje esančius programos *Skype* ir lankytų internetinių svetainių adresų duomenis, darbdavys pažeidė ieškovės privatumą, todėl pripažino neleistinais ir nevertino atsakovo pateiktų įrodymų *(Skype* programos išrašų ir duomenų iš kompiuterinės atminties apie interneto svetainių adresus). Tokiai teismo pozicijai iš esmės pritariama ir teisės doktrinoje[30].

[29] Plačiau apie tai žr. vadovėlio VII skyrių.

[30] Plačiau apie tai žr. vadovėlio VII skyrių.

2. Elektroninių įrodymų įrodomoji galia

Pagal įrodomąją galią įrodymai skirstomi į dvi rūšis: turintieji didesnę įrodomąją galią, arba *prima facie*, ir turintieji įprastą įrodomąją galią. CPK 175[1] str. 7 d. nustato, kad elektroninių duomenų įrodomoji galia yra tokia pat kaip ir kitų įrodymų. ABTĮ 57 str. 2 d. elektroninius įrodymus išskiria kaip atskirą įrodymų rūšį, tačiau nuostatų, kuriose būtų apibrėžta elektroninių įrodymų įrodomoji galia, ABTĮ nėra. Manytina, kad remiantis ABTĮ 4 str. 6 d. vertinant elektroninių įrodymų įrodomąją galią administraciniam procesui turėtų būti vadovaujamasi CPK 175[1] str. 7 d.

Jokie įrodymai teismui neturi iš anksto nustatytos galios, išskyrus oficialiuosius rašytinius (lot. *prima facie)*, kuriais patvirtintos aplinkybės laikomos visiškai įrodytomis, iki jos nebus paneigtos įstatymų nustatyta tvarka (CPK 197 str. 2 d.). Didesnė įrodomoji galia suteikiama dokumentams, išduotiems valstybės ar savivaldybės institucijų arba patvirtintiems kitų valstybės įgaliotųjų asmenų, neviršijant jiems nustatytos kompetencijos ir laikantis tam tikriems dokumentams keliamų formos reikalavimų. Oficialiųjų rašytinių įrodymų įrodomoji galia įstatymais gali būti suteikta ir kitiems dokumentams. Pagal LAT praktiką rašytinis įrodymas gali būti teismo pripažintas oficialiuoju tik esant tokioms sąlygoms: 1) jis turi būti išduotas valstybės ar savivaldybės institucijos ar kitų įstatyme išvardytų subjektų; 2) įstatyme nurodyti subjektai, išduodami oficialų dokumentą, neviršijo savo kompetencijos; 3) dokumentas atitinka teisės aktų nustatytus jo formos ir turinio reikalavimus; 4) jame pateikta informacija yra pakankama nustatyti įrodinėjimo dalyką sudarančias aplinkybes (pvz., žr. LAT 2011 m. gegužės 27 d. nutartį, priimtą civilinėje byloje *Lietuvos autorių teisių gynimo asociacijos agentūra v. UAB „Konto“*, bylos Nr. 3K-3-260/2011). Oficialiais rašytiniais įrodymais yra laikomi ir kitų valstybės įgaliotųjų asmenų išduoti dokumentai. Pavyzdžiui, notaro patvirtinti dokumentai yra oficialūs (viešieji), nes Notariato įstatymo 26 str. 2 d. nustatyta, kad notarine tvarka patvirtintuose dokumentuose nurodomi faktai yra nustatyti ir neįrodinėjami, kol šie dokumentai (ar jų dalys) nustatyta tvarka nėra pripažinti negaliojančiais. Prie šios rūšies įrodymų priskirtini ir civilinės būklės aktų, įvairių valstybės registrų (juridinių asmenų, nekilnojamojo turto, turto areštų, hipotekos, testamentų, vedybų ir t. t.) įrašai. Šiuo metu asmuo gali internetu užsisakyti ir gauti minėtuosius įrašus, be to, daugelis valstybės ir savivaldybės institucijų irgi išduoda nebe popierinius, o elektroninius dokumentus.

Įvertinus esamą teisinį reguliavimą kyla klausimas, ar teisme *prima facie* galią turėtų valstybės ar savivaldybės institucijos išduotas elektroninis

dokumentas ir valstybės registrų elektroniniai įrašai. Dokumentų ir archyvų įstatymo 2 str. 5 d. dokumentą apibrėžia kaip Lietuvos Respublikoje ar užsienio valstybėje įsteigto juridinio asmens, kitos organizacijos ar jų padalinio ar fizinio asmens veiklos proceso metu užfiksuotą informaciją, nepaisant jos pateikimo būdo, formos ir laikmenos. Minėtojo įstatymo 2 str. 11 d. apibrėžia elektroninį dokumentą kaip juridinio ar fizinio asmens norminių teisės aktų nustatyta tvarka informacinių technologijų priemonėmis sudarytą, patvirtintą ar gautą dokumentą, pasirašytą teisinę galią turinčiu elektroniniu parašu. Oficialus dokumentas – tai valstybės ar savivaldybės institucijos, įstaigos ar įmonės, valstybės įgaliotojo asmens, vykdančio teisės norminių aktų nustatytus įgaliojimus, sudarytas, patvirtintas ar gautas dokumentas, įtrauktas į apskaitą. Lietuvos Respublikos informacinės visuomenės paslaugų įstatymo 3 str. 2 d. nustato, kad informacijos teisinė galia negali būti paneigta ar apribota vien tik tuo pagrindu, kad ši informacija yra sukurta, išsiųsta, gauta ar išsaugota elektroninėmis priemonėmis. Vokietijos civilinio proceso teisėje tinkamai valstybės institucijos išduotų elektroninių dokumentų įrodomoji vertė yra prilyginama valstybės institucijos išduotų rašytinių dokumentų įrodomajai vertei (Vokietijos civilinio proceso kodekso 371 str. 2 p.). Todėl įvertinus esamą teisinį reguliavimą būtų galima teigti, kad tinkamai valstybės institucijos išduoti elektroniniai dokumentai ir valstybės registrų elektroniniai įrašai yra prilygintini oficialiems rašytiniams įrodymams ir teisme turėtų būti vertinami kaip turintieji didesnę įrodomąją galią.

Žinių įtvirtinimo klausimai

1. Kuo elektroniniu būdu sukurta informacija skiriasi nuo rašytinės?
2. Kuo elektroniniai įrodymai svarbūs teismo procesui?
3. Kokius reikalavimus turi atitikti elektroninis įrodymas, kad juo būtų galima remtis nagrinėjant bylą teisme?
4. Į ką turėtų atkreipti dėmesį bylą nagrinėjantis teismas ir bylos šalys, vertindamos bylai pateiktus elektroninius įrodymus?
5. Kokia yra elektroninių įrodymų įrodomoji galia?

/V/ *skyrius*

Technologinės elektroninių dokumentų ir elektroninių sutarčių apsaugos priemonės

/ 189–233 / *puslapiai*

1 skirsnis. Elektroninio dokumento samprata ir ypatumai

Sėkmingas elektroninio verslo plėtojimas beveik neįmanomas be elektroninių sutarčių. Tarptautiniu lygiu verslą vykdantiems asmenims tai yra dar svarbiau, nes elektronines sutartis galima operatyviau ir gerokai pigiau pasirašyti bei perduoti internetu nei paprastu paštu ar tiesiogiai vykstant į užsienio šalį pas partnerius ar klientus. Be to, elektroninėms sutartims saugoti reikia daug mažiau vietos, informacijai koreguoti jos pasiekiamos kur kas greičiau ir patogiau. Tačiau problemų kyla dėl informacijos patikimumo, svarbiausias klausimas – kaip užtikrinti, kad informaciją pateikė konkretus asmuo, ir elektroninės sutarties turinys, keliaudamas nuo siuntėjo iki gavėjo, nebuvo pakeistas? Būtent šiam tikslui ir buvo sukurtas elektroninis parašas, kuris garantuoja pasirašytų elektroninių duomenų autentiškumą ir įgalina patikrinti pasirašiusiojo asmens tapatybę. Jis sudaro prielaidas asmenims patikimiau, greičiau ir patogiau bendrauti su įvairiomis institucijomis, padeda greičiau plėtoti verslą, suteikia didesnį finansinių operacijų saugumą, pagerina įvairių organizacijų veiklą. E. parašo diegimui įtakos turi ne vien finansiniai ištekliai ar technologiniai sprendimai, bet ir esamas teisinis reguliavimas bei visuomenės informuotumo lygis. Lietuvai dalyvaujant bendroje ES šalių narių rinkos sąjungoje, e. parašo plėtra e. versle įgyja ne tik vidaus, bet ir išorės ekonominės rinkos svarbą. Todėl akivaizdu, kad inovacijų naudojimas irgi tampa labai svarbiu faktoriumi keliose pagrindinėse techninių ir socialinių mokslų srityse: informatikoje, ekonomikoje, vadyboje ir ypač teisėje. Reikėtų atkreipti dėmesį, kad informacinių technologijų plėtra, kompleksiškai paliečianti ir susiejanti aukščiau įvardytas skirtingas mokslų sritis, pabrėžia ne tik mokslo naujumo, bet ir tarpdisciplinišKumo svarbą.

Sparti informacinių technologijų plėtra sugebėjo padaryti perversmą pasaulio ekonomikoje. Rinkų transformacija ir naujų sukūrimas, kitokių metodų įsigyti prekes ir paslaugas ar pasiekti informaciją atsiradimas, nacionalinių sienų išnykimas – tai tik keli pranašumai, kuriuos suteikė informacinių technologijų plėtra. Tuo pat metu iškilo daugybė teisinių klausimų dėl elektroninių technologijų naudojimo sudarant komercinius sandorius. Dėl šios priežasties greta tradicinių sutarčių atsirado ir elektroninės. Tai sukėlė daug diskusijų ne tik tarp teisės teoretikų, bet ir praktikų. Atsirado būtinybė jas išanalizuoti, išskirti svarbiausias ypatybes ir palyginti su tradicinėmis sutartimis. Analogiškai kilo klausimas, ar tokie sandoriai neprieštarauja tradicinės sutarčių teisės principams *(Dontoglou,* 2002).

Elektroninės sutartys šiandien yra tapusios neatskiriama šiuolaikinio gyvenimo dalimi, jos įsigali visose visuomeninių santykių srityse. Esant

išplėtotoms informacinėms ir telekomunikacinėms technologijoms, jas galima labai greitai ir daug ekonomiškiau perduoti bet kur esantiems vartotojams. Be to, elektroninėms sutartims saugoti reikia daug mažiau vietos, o joms apdoroti – mažesnių sąnaudų, informacija pasiekiama kur kas greičiau ir patogiau. Vienas iš pagrindinių elektroninių dokumentų skirtumų nuo tradicinių yra tas, kad jis yra sukurtas, laikomas, naudojamas ir saugomas skaitmeniniu formatu *(Petravičiūtė*, 2006). Be to, svarbu pabrėžti, kad informacijos fiksavimo ir simbolių naudojimo būdas[31], turinio ir laikmenos santykis[32], fizinė (išorinė) ir loginė (vidinė) dokumento struktūra[33] skiriasi nuo popierinių dokumentų.

Taigi toks dokumentas e. erdvėje egzistuoja nepriklausomai nuo jo sudarymo formos ir materialaus objekto, kuriame tas dokumentas sudaromas. Tačiau atsižvelgiant į tai, kad materiali forma greitai keičiasi ir tobulėja (turima omenyje elektroninės laikmenos), ji netenka tos prasmės, kurią turi paprastas dokumentas, taigi elektroninio dokumento samprata remiasi tuo, kad intelektualiu požiūriu toks dokumentas vertinamas kaip atskiras objektas, o svarbiausias jo požymis – fiksuotas informacijos turinys.

Pabrėžtina, kad elektroninės sutartys kaip specifinė sutarčių rūšis ar forma Lietuvoje nėra aiškiai reglamentuotos. Teisiniu pagrindu galėtume laikyti CK 6.192 str. 2 d., kur numatyta, kad „kai pagal įstatymus ar šalių susitarimą sutartis turi būti paprastos rašytinės formos, ji gali būti sudaroma tiek surašant vieną šalių pasirašomą dokumentą, tiek ir apsikeičiant raštais, telegramomis, telefonogramomis, telefakso pranešimais ar kitokiais telekomunikacijų galiniais įrenginiais perduodama informacija, jeigu yra užtikrinta teksto apsauga ir galima identifikuoti jį siuntusios šalies parašą“. Ilgą laiką teisės doktrinoje vyko diskusijos dėl šios teisės normos taikymo internetu sudaromoms sutartims. M. Civilka *(Civilka*, 2004) teigė, kad iš šios nuostatos neaišku, ar jos formuluotė apima ir internetu sudaromus

[31] Elektroninių dokumentų turinys magnetinėje ar optinėje laikmenoje yra fiksuojamas taikant binarinį informacijos fiksavimo būdą, kur visa fiksuojama informacija yra koduojama, todėl ji negali būti perskaitoma ar atpažįstama tiesiogiai, nenaudojant specialių priemonių. Kad žmogus galėtų perskaityti ir suprasti informaciją, ji turi būti transformuojama iš savo pirminės – binarinės – formos į žmogui suprantamą. Nagrinėjamoje koncepcijoje išskiriamos dvi elektroninio dokumento formos: pirmoji, binarinė, atpažįstama ir perskaitoma techninių priemonių, ir antroji – žmogaus atpažįstama ir perskaitoma.

[32] Elektroninių dokumentų turinys fiksuojamas laikmenoje, kuri netampa fiziškai neatskiriama dokumento dalimi. Elektroninio dokumento turinys gali būti perkeltas iš vienų priemonių į kitas, pvz., iš kietojo disko į kompaktinį, iš senesnės programinės įrangos į naujesnę ir pan.

[33] Elektroninio dokumento fizinė forma paprastai vartotojui yra nežinoma. Loginė forma suprantama kaip dokumento vidinė struktūra ir jo ryšiai su kitais susijusiais objektais, kuriuos sukūrė vartotojas ir kurie gali būti atpažinti ir suprasti žmogaus.

sandorius. Padėtį iš esmės pakeitė LR elektroninių ryšių įstatymas (Valstybės žinios, 2004, Nr. 69-2382), kuris buvo priimtas vietoj jau nebegaliojančio LR telekomunikacijų įstatymo. Šio įstatymo 3 str. 58 d. nurodo, kad telekomunikacijų galinis įrenginys – „tai leidžiantis palaikyti ryšį įrenginys ar jo atitinkama dalis, skirti tiesiogiai ar netiesiogiai bet kokiomis priemonėmis būti prijungti prie viešųjų telekomunikacijų tinklų (t. y., tinklų, visiškai ar iš dalies skirtų viešosioms telekomunikacijų paslaugoms teikti)". Tokiu būdu įstatymų leidėjas jau nebediferencijuoja elektroninių sutarčių pagal prisijungti prie interneto naudotas informacines technologijas ir išplečia „telekomunikacijų galinių įrenginių" sąvoką. Todėl klausimas dėl CK 6.192 str. 2 d. taikymo internetu sudaromoms pirkimo–pardavimo sutartims neturėtų kilti. LR informacinės visuomenės paslaugų įstatymo (Valstybės žinios, 2006, Nr. 65-2380) 4 skyriuje yra minima sąvoka „sutarčių sudarymas elektroninėmis priemonėmis". M. Kiškis *(Katuoka, Kiškis, Pranevičius ir kt.*, 2006) teigia, kad šiame įstatyme vartojama sąvoka gali būti suprantama dvejopai:

- „kaip sutartis, kurios sąlygos pateikiamos šalims elektronine forma ir šalys išreiškia savo valią elektronine forma;
- kaip sutartis (žodinė, rašytinė ir 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 ne elektronine forma."
- M. Kiškio *(Katuoka, Kiškis, Pranevičius ir kt.*, 2006) nuomone, sistemiškai analizuojant LR informacinės visuomenės paslaugų įstatymo ir CK nuostatas, „sutartimi, sudaroma elektroninėmis priemonėmis" laikytina tik pirmoji sutarčių kategorija. Manytina, kad su tokia nuomone reikėtų sutikti, todėl kalbėdami apie elektronines sutartis omenyje turime tas sutartis, kai šalims sąlygos pateikiamos elektronine forma ir tokia pat forma šalys išreiškia savo valią.

Apskritai teisės doktrinoje elektroninė sutartis yra suprantama ir plačiąja, ir siaurąja prasme. „*Elektroninės sutartys plačiąja prasme* apibrėžtinos kaip apimančios dvišalius sandorius, sudarytus ir (ar) vykdomus elektroninėmis, optinėmis ar panašiomis priemonėmis, tiek atviruose, globaliuose kompiuteriniuose tinkluose (pvz., internete), tiek ir privačiuose, vidiniuose tinkluose (intranete), įskaitant, bet neapsiribojant, EDI, elektroninį paštą, telegramą, teleksą ar telekopiją, tiek ir programinės įrangos licencijavimo sutartis" *(Civilka, Lamanauskas, Osinaitė ir kt.,* 2004). Tuo metu *elektroninės sutartys siaurąja prasme* apibrėžtinos kaip sutartys, sudaromos atviruose tinkluose, tokiuose kaip internetas *(Civilka, Lamanauskas, Osinaitė ir kt.,* 2004).

Elektroninėje erdvėje sudaromas civilines sutartis galime sugrupuoti į dvi dideles kategorijas:

1) „internetu sudaromos arba internetinės sutartys;
2) kitos elektroninės sutartys – sudaromos EDI ir kitų ar panašių priemonių pagalba." *(Civilka, Lamanauskas, Osinaitė ir kt.*, 2004).

Internetu sudaromas sutartis savo ruožtu galima skirstyti į tokias stambias kategorijas:

1) „*chat and video contracts*[34] – jie suteikia galimybę komunikuoti sinchroniškai ir interaktyviai ir todėl gali būti *mutatis mutandis* reguliuojami tų pačių taisyklių, kaip ir telefoninės sutartys (dėl informacinių paslaugų teikimo telefonu);
2) elektroninio pašto sutartys – elektroninis paštas reikalauja techninio trečiųjų šalių – serverių – įsikišimo, kurie šalims suteikia tiek elektroninio pašto sąskaitas ir adresus, tiek saugo jų elektroninio pašto pranešimus, kol šie yra persiunčiami į šalių kompiuterius. Mes galime įsivaizduoti „grynas" elektroninio pašto sutartis (pasiūlymas, akceptas ir akcepto gavimo patvirtinimas vyksta elektroniniu paštu), taip pat ir mišrius (pasiūlymas tinklalapyje, akceptas elektroniniu paštu). Nėra daug problemų dėl šių elektroninių sutarčių rūšių – joms gali būti labai lengvai pritaikytos laiškams taikomos taisyklės, be to, tai dažniausiai C2C (angl. *consumer to consumer)* sutartys;
3) *WWW* sutartys – tai visos elektroninės komercijos esmė. Šios sutartys sudaromos pasitelkiant populiariausią interneto paslaugą – *World Wide Web (WWW)*, kuri įgalina sandorių sudarymą atviruose tinkluose, eliminuojant ir elektroninio pašto sistemos būtinybę." *(Civilka, Lamanauskas, Osinaitė ir kt.,* 2004).

Pabrėžtina, kad sudarant internetines pirkimo–pardavimo *WWW* ir elektroninio pašto sutartis dalyvauja ne tik sutarties, bet ir trečiosios šalys, pvz., autentifikuotos šalys (sertifikatų teikėjai) ar finansinės grupės, kurios administruoja elektroninius atsiskaitymus. Be to, būtent tokių sutarčių kontekste akivaizdžią reikšmę įgyja e. parašo ir su juo susijusios laiko žymos klausimai.

2001 m. gruodį paskelbtas elektroninių sutarčių konvencijos projektas, kuriuo nepažeidžiant sutarties laisvės ir šalies autonomiškumo principų siekiama numatyti teisines priemones, padėsiančias įgyti daugiau pasitikėjimo virtualiomis sutartimis. Pabrėžtina, kad jau tada bendros teisinės

[34] Angl. pokalbių kambarių ir vaizdo sutartys.

bazės, reglamentuojančios elektronines sutartis, nebuvimas yra įvardijamas kaip vienas iš veiksnių, trukdančių tarptautiniu mastu plėtoti elektroninę komerciją ir verslą.

CK 1.73 str. nurodo, kokie sandoriai turi būti sudaromi rašytine forma, be to, sandoriai ir sutartys gali būti sudaromi naudojant galinius telekomunikacijų įrenginius (iš esmės – elektronines ryšio priemones). Šio straipsnio 2 dalis nustato, kad „rašytinės formos dokumentui prilyginami šalių pasirašyti dokumentai, perduoti telegrafinio, faksimilinio ryšio ar kitokiais telekomunikacijų galiniais įrenginiais[35], jeigu yra užtikrinta teksto apsauga ir galima identifikuoti parašą.“ Taigi CK iš esmės formuluoja du reikalavimus, keliamus sutartims, sudarytoms elektroninėmis priemonėmis, kad šios būtų pripažintos kaip ir sudarytosios paprasta rašytine forma:

1) sutarties tekstas turi būti apsaugotas;
2) sutarties parašas turi būti identifikuojamas, t. y. nustatoma, kas yra sutartį pasirašęs asmuo.

Tokie reikalavimai pagrįsti principiniais civilinės teisės reikalavimais – sudarantys sutartis asmenys (sutarties šalys) turi būti aiškiai ir vienareikšmiškai identifikuojami, o sudarytos sutarties tekstas turi būti apsaugomas nuo pakeitimų, kad vėliau kilus nesutarimų juo būtų galima remtis kaip įrodymu.

Taigi elektroninis dokumentas – rašytinis dokumentas, išreikštas elektronine forma. Jis laikomas ekvivalentišku rašytiniam, kai neatsižvelgiant į taikomas technologijas yra užtikrinamas dokumentui būtinų funkcijų atlikimas.

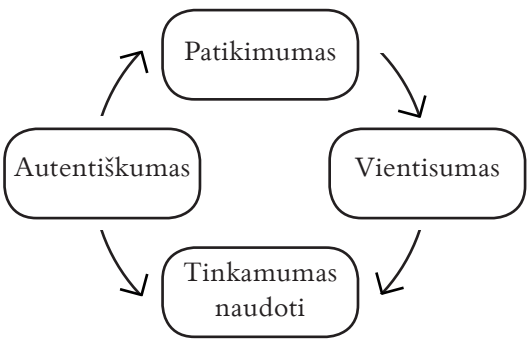
Su rašytinės formos dokumentais ir sutartimis, sudaromomis elektroniniu būdu, susiję šie reikalavimai:

- dokumentas turi būti „pasirašytas“. Rašytinės formos sandorius turi pasirašyti juos sudarę asmenys. Jeigu fizinis asmuo dėl fizinių trūkumų, ligos ar kitokių priežasčių negali pats pasirašyti, jo pavedimu sandorį už jį gali pasirašyti kitas asmuo. Jeigu sandoris buvo sudarytas naudojant galinius telekomunikacijų įrenginius, visais atvejais privalo būti pakankamai duomenų sandorio šalims nustatyti.
- dokumentas turi būti „originalus“. Jeigu įstatymas reikalauja, kad dokumentas būtų pateiktas originaliu formatu, jį atitinka elektroninis duomenų pranešimas, kuriame užtikrinama, kad informacija nebuvo pakeista nuo to laiko, kai elektroninių duomenų pranešimas buvo baigtas sudaryti pirmą kartą ir išsiųstas, iki tol, kol jį gavo

[35] Galiniai įrenginiai – telekomunikacijų paslaugų gavėjų įrenginiai, skirti prisijungti prie atitinkamo telekomunikacijų tinklo galinių taškų.

adresatas (*UNCITRAL*, 2001). Kaip jau minėjome, dokumento „originalumo“ reikalavimas įtvirtintas CK 1.73 str. 2 d., kuriame reikalaujama teksto apsaugos užtikrinimo, kad sandoris būtų laikomas sudarytu rašytine forma.

Naudojantis elektroniniais dokumentais kyla klausimas ir dėl jų nepatikimumo. Dokumentas turi liudyti atliktą veiksmą, taigi jo struktūra ir sudėtinių dalių ryšiai turi išlikti nepakitę. Atsižvelgiant į šį reikalavimą, elektroninių dokumentų būtinomis savybėmis, leidžiančiomis elektroninį dokumentą identifikuoti kaip lygiavertį tradiciniam rašytiniam, yra laikoma autentiškumas, patikimumas, vientisumas ir tinkamumas naudoti (žr. 2 pav.).



2 pav. Elektroninių dokumentų savybės (Petravičiūtė, 2006)

Remiantis Lietuvos Respublikos dokumentų ir archyvų įstatymo 2 str. 5 d. ir 11 d., galima teigti, kad elektroninis dokumentas turi tokią pačią teisinę galią, kaip ir tradicinis popierinis dokumentas (Valstybės žinios, 1995). Vadinasi, elektroninis dokumentas gali būti pateikiamas kaip įrodymas vienam ar kitam faktui pagrįsti. Todėl labai svarbu užtikrinti dokumento autentiškumą. Šis teisės aktuose ir mokslinėse publikacijose apibrėžiamas gana panašiai. Pavyzdžiui, pagal *ISO* (angl. *International Organization for Standardization)* standartą autentišku yra laikomas toks dokumentas, „kuris gali būti įrodytas, kad yra tai, kuo manoma jį esant, yra sukurtas ar išsiųstas asmens, kuris manoma jį esant sukūrus“ . Tam, kad būtų užtikrintas dokumentų autentiškumas, reikalinga įdiegti sistemos kontrolę, kuri fiksuotų elektroninio dokumento apyvartą. Autentiškumas vertinamas kaip užtikrinimas, kad dokumentas „nebūtų piktavališkai ar netyčia pakeistas ir turėtų būtinus atributus dokumento autoriui nustatyti“ *(Davidavičienė, Gatautis, Paliulis, Petrauskas*, 2009). Tarptautinė archyvų taryba akcentuoja, kad dokumentų autentifikavimo procesui labai svarbus organizacijos vaidmuo (angl. *Authenticity of electronic records)*, išreiškiamas dėmesiu,

diegiant dokumentų valdymo sistemas. *ISO* standarte teigiama, kad elektroninių dokumentų autentiškumą patvirtina teisinę galią turintis e. parašas. Elektroninio dokumento organizavimo sistemoje svarbiausia e. parašo funkcija – duomenų kodavimas, naudojant šifravimo sistemas ir e. parašą. Tai leidžia atlikti šias funkcijas *(Davidavičienė, Gatautis, Paliulis, Petrauskas*, 2009):

- užtikrinti reikiamą konfidencialumą ir sumažinti nesankcionuotos prieigos prie duomenų galimybę;
- užtikrinti dokumento autentiškumą ir duomenų vientisumą;
- užtikrinti dokumento autoriaus identifikaciją*;*
- užtikrinti efektyvų duomenų kodavimą perduodant duomenis.

Dokumento patikimumas pagal *ISO* standartą siejamas su jo turinio patikimumu. Dokumentai turi būti sukuriami vykdomos veiklos ar įvykio, su kuriuo jis susijęs, metu, asmenų, kurie turi atitinkamų žinių apie vykstantį veiksmą.

Kita dokumento savybė – vientisumas, ji yra tiesiogiai proporcinga autentiškumui. Vientisumas reiškia, kad dokumentas yra užbaigtas ir nekeičiamas. Tokie dokumentai turi būti apsaugoti nuo bet kokių korekcijų, išskyrus atvejus, kai nustatoma, kokių parengto dokumento papildymų ar pakeitimų dar gali būti atliekama ir kas įgaliotas juos atlikti.

Elektroninių dokumentų savybių analizę užbaigia jų tinkamumas naudoti. Teisės aktai kaip tinkamą naudoti apibūdina tokį dokumentą, „kurį galima nustatyti, surasti, pateikti ir suprasti visu dokumento gyvavimo ciklo metu“ *(ISO)*. Kadangi dokumentai kuriami ne tik vykdant konkrečią veiklą, bet ir vėliau, jie turi išsaugoti visas sąsajas su veikla, iš kurios kilo pats dokumentas.

Išanalizavus elektroninių dokumentų savybes, darytina išvada, kad svarbiausia elektroninio dokumento savybė yra autentiškumas, apimantis turinio nekeičiamumą, ir autoriaus bei laiko, kada buvo sukurtas dokumentas, identifikaciją.

Autentiškumą patvirtina teisinę galią turintis e. parašas. Naudojant saugius e. parašus, elektroninis dokumentas, siunčiamas kompiuterių tinklu, yra užkoduojamas tokiu būdu, kad neįmanoma jo dekoduoti, o mėginant pakeisti pranešimo turinį ar patį parašą pranešimo tekstas virsta nesuprantamų simbolių virtine *(Davidavičienė, Gatautis, Paliulis, Petrauskas*, 2009).

2 skirsnis. Elektroninio parašo kūrimo principai ir diegimo problematika

Visi rašytiniai sandoriai patvirtinami asmenų parašais. Pasirašytas popierinis dokumentas turi didžiulę reikšmę įtvirtinant žmonių tarpusavio pasitikėjimą ir garantuojant teisinių santykių stabilumą. Atsiradus elektroninėms duomenų perdavimo priemonėms, internetas ir elektroninis paštas tapo vienu svarbiausių informacinės visuomenės atributų (IT teisė). Kiekvienas dokumentas, kad būtų juridiškai galiojantis, privalo turėti jo tikrumą užtikrinančius rekvizitus. Būtent tokią galimybę e. erdvėje suteikia e. parašas *(Garuckas, Kaziliūnas*, 2008).

Svarbiausia priežastis, paskatinusi elektroninius dokumentus pasirašinėti e. parašu, – pasirašytų, gautų ir išsiųstų duomenų saugumo užtikrinimas *(Civilka, Lamanauskas, Nosinaitė ir kt.* 2004). E. parašas leidžia pasirašyti elektroninius laiškus ir taip užtikrinti gavėją, kad šis gavo laišką būtent iš nurodytojo asmens, be to, e. parašas suteikia galimybę užšifruoti duomenis (dokumentą, laišką, paveikslėlį, vaizdo įrašą ir kt.) taip, kad jį iššifruoti gali tik tas, kam skirtas laiškas, taigi duomenys nebus pakeisti. Įdomus faktas – šiandien nėra užfiksuota e. parašo klastojimo atvejų, beje, to negalime pasakyti apie paprastą parašą.

Greita technologijų plėtra ir interneto paplitimas visame pasaulyje reikalauja plėtoti atvirą požiūrį į elektroninių duomenų autentiškumo patvirtinimo technologijas ir paslaugas.

Pripažįstant elektroninių dokumentų juridines teises tarptautiniu mastu, didelę įtaką darė 1996 m. Elektroninės prekybos įstatymas *UNICITRAL*, 1995 m. Jutos elektroninio parašo įstatymas JAV, 1997 m. Vokietijos elektroninio parašo įstatymas. Žinoma, negalima nepaminėti, kad ES elektroninio dokumento forma buvo prilyginta rašytiniam dokumentui 1999/93/EB elektroninio parašo ir 2000/31/EB elektroninės prekybos direktyvose.

Tarptautinės standartų organizacijos *(ISO)* koncepcijoje e. parašas apibrėžiamas taip: „Duomenų siuntėjo atliekama vieneto kriptografinė transformacija, leidžianti duomenų adresatui atpažinti duomenų siuntėją bei užtikrinti duomenų vientisumą ir apsaugą nuo nesankcionuoto priėjimo“. Europos Parlamento ir Tarybos e. parašo direktyvoje nustatyta, kad e. parašas – tam tikra elektronine forma pateikiami duomenys, kurie yra prijungti (įterpti) prie kitų elektroninių duomenų ar logiškai su jais susieti ir gali būti naudojami kaip autentifikavimo priemonė *(Directive* 2000/31/EC). Paprastai tariant, e. parašas naudojamas juo pasirašantiems asmenims identifikuoti ir duomenų autentiškumui užtikrinti, jis atitinka tikrą konkretaus asmens parašą, jo tapatybės dokumentą ir turi teisinę galią *(Kunigėlis*, 2011).

Saugus elektroninis parašas turi atitikti šiuos reikalavimus (Valstybės žinios, 2000):

1) yra vienareikšmiškai susietas su pasirašančiuoju asmeniu;
2) leidžia identifikuoti pasirašantįjį asmenį;
3) yra sukurtas priemonėmis, kurias pasirašantis asmuo gali tvarkyti tik savo valia;
4) yra susijęs su pasirašytais duomenimis taip, kad bet koks šių duomenų pakeitimas yra matomas.

Saugiam e. parašui keliami reikalavimai siejami su CK įtvirtintais teksto apsaugos ir pasirašiusiojo asmens identifikavimo reikalavimais, tik šie reikalavimai dar papildomai detalizuojami užtikrinant, kad tik pasirašantysis asmuo galėtų pasirašyti elektroninę informaciją ir jokia trečioji šalis vietoj jo tokių veiksmų negalėtų atlikti. Iš esmės Elektroninio parašo įstatymo 1, 2, ir 3 str. reikalavimai yra CK antrojo reikalavimo – parašo identifikuojamumo ir pasirašiusiojo asmens nustatymo – detalizavimas, o 4 reikalavimas perfrazuoja ir visiškai atitinka CK nurodomą sutarties teksto apsaugos reikalavimą, todėl įgyvendinus Elektroninio parašo įstatymo reikalavimus yra įgyvendinami ir CK reikalavimai bei e. parašu patvirtinti įrodymai atitinka Civilinio proceso kodekso nuostatas, kad teismui turi būti pateikiami byloje dalyvaujančių asmenų pasirašyti dokumentai (Valstybės žinios, 2000), nes ir paprasto, ir e. parašo paskirtis bei atliekama funkcija yra analogiškos – patvirtinti teksto vientisumą ir identifikuoti pasirašantįjį. Iš esmės elektroninis dokumentas yra toks pat, kaip ir rašytinis, tik išreikštas elektronine forma, ir turi tokią pat vertę tais atvejais, kai atitinka jam keliamus reikalavimus (pvz., išskyrus dokumentus, kuriems reikia notaro patvirtinimo).

Dokumentai e. parašu pasirašomi naudojant e. parašo formavimo duomenis, (žinoma, tam reikalinga speciali parašo formavimo įranga), o patikrinami – juos atitinkančiais e. parašo tikrinimo duomenimis (naudojama parašo tikrinimo įranga). Elektroninio parašo įstatymas įtvirtina technologinio neutralumo principą, kuris reiškia, kad jis taikomas elektroninių duomenų pasirašymui reglamentuoti, ir nesvarbu, kokia technologija naudojama. Parašo formavimo ir tikrinimo – kompiuterių techninė ir (ar) programinė – įranga yra gana brangi, todėl tai gali tapti nemenka vartotojų grupės plėtros kliūtimi. Kaip alternatyva Lietuvoje galima naudotis elektroninių dokumentų pasirašymo sistema tinklalapyje *www.eparasas.lt*, per kurį, pasitelkus bankų elektronines sistemas, suteikiama galimybė pasirašyti dokumentus. Žinoma, prieš tai kaip e. parašas kiekvienam klientui yra suteikiamas slaptažodis (kodas) ir garantuojama, kad toks pat kodas nebus

skirtas kam nors kitam. PIN kodas ir slaptažodžių kortelė ar generatorius (juos žino tik gaunantysis ir įsipareigoja niekam neatskleisti, o jį praradęs nedelsdamas pranešti bankui) suteikiama klientui atvykus į banką ir pasirašius elektroninės bankininkystės sutartį, todėl bankas tiesiogiai gauna asmens duomenis, pagal kuriuos vėliau identifikuoja prisijungusįjį, taip užtikrindamas vienasmenišką sandorio susiejimą su konkrečiu asmeniu. Elektroninių dokumentų pasirašymo metu visi sistemos apdoroti duomenys ir jų surašymo tvarka susiejami su e. parašu. Po šios procedūros bet koks pasirašytų duomenų keitimas daro įtaką e. parašui, todėl adresatas (parašą tikrinantis asmuo) pastebės, kad pasirašyti duomenys buvo keičiami, nes e. parašas tiesiog nebegalios. Taigi toks pasirašymo būdas atitinka visus keturis saugiam e. parašui keliamus reikalavimus, juo labiau kad dėl tokio pasirašymo būdo iš anksto sutaria pačios šalys, atsižvelgdamos į Elektroninio parašo įstatymo nuorodą, jog e. parašas negali būti laikomas negaliojančiu dėl to, kad:

1) yra elektroninis;
2) nėra patvirtintas kvalifikuotu sertifikatu;
3) nėra patvirtintas akredituoto sertifikavimo paslaugų teikėjo išduotu kvalifikuotu sertifikatu;
4) nėra sukurtas saugia parašo formavimo įranga.

Kvalifikuotu sertifikatu patvirtintas e. parašas yra patikimesnis, saugesnis dėl už jį laiduojančio trečiojo asmens – sertifikavimo paslaugų teikėjo, atitinkančio Vyriausybės ar jos įgaliotos institucijos (Informacinės visuomenės plėtros komiteto prie Lietuvos Respublikos Vyriausybės) nustatytus reikalavimus. UAB Skaitmeninio sertifikavimo centras – pirmoji Lietuvoje tokias paslaugas teikianti įmonė.

Kaip jau minėta, pasirašyti e. parašu gali ne kiekvienas, nes tam, kad e. parašas turėtų tokį pat statusą kaip ir rašytas ranka, reikalinga gauti kvalifikuotą elektroninio parašo sertifikatą, jo laikmeną ir e. parašo formavimo bei tikrinimo programinę įrangą. Sertifikatas – tai elektroninio pavidalo liudijimas, kuris patvirtina, kad viešasis ir jį atitinkantis privatusis šifravimo raktai priklauso sertifikate nurodytam asmeniui. Sertifikatas suteikia galimybę prieiti prie reikalingos informacijos arba įrodyti savo tapatybę internete, kaip ir pasas ar vairuotojo pažymėjimas realiame gyvenime *(Musteikis, Paulavičius, Rakalovič*, 2008). Sertifikatą sudaro šie elementai: savininko viešasis raktas ir vardas, viešojo rakto galiojimo terminas, sertifikatą teikiančios bendrovės pavadinimas ir sertifikatą teikiančios organizacijos skaitmeninis parašas *(Garuckas, Kaziliūnas*, 2008). Sertifikatas identifikuoja žmogų, garantuoja jo teisėtą ir saugią veiklą e. erdvėje. Elektroninio

parašo infrastruktūrai būtina patikima sertifikavimo institucija. Be to, naudojant skaitmeninį sertifikatą yra galimybė patikrinti vartotojo teises į konkretų raktą – tai užkerta kelią neteisėtai naudoti asmeninį raktą. Taigi skaitmeniniai sertifikatai dėl specialaus šifravimo suteikia visišką saugumą ir garantuoja visų elektroninių veiksmų dalyvių tapatybę.

Elektroniniam parašui sukurti naudojama raktų (specialių kodų) pora, vienas iš jų vadinamas privačiuoju, kitas – viešuoju raktu. Privatusis raktas yra slaptas ir turi būti saugomas kompiuteryje arba nešiojamas kartu su savimi. Viešasis raktas skirtas tiems, kam adresuojamas laiškas ar dokumentas, kurį galima perduoti savo adresatams elektroniniu paštu arba paskelbti internete. Privatusis ir viešasis raktai sudaro porą, todėl turint tik viešą raktą negalima sužinoti privataus rakto kodo. Būtent tai, kad jie gali funkcionuoti tik tada, kai naudojami kartu, užtikrina saugumą ir suteikia galimybę patikimai identifikuoti elektroninius veiksmus atliekančius asmenis. Skaitmeninio rakto technologija leidžia ne tik pasirašyti dokumentus, bet ir užšifruoti juos taip, kad niekas, išskyrus nurodytąjį gavėją, negalėtų perskaityti *(Garuckas, Kaziliūnas*, 2008). Taigi elektroninių sutarčių autentiškumą patvirtina teisinę galią turintis e. parašas *(ISO)*. Svarbiausia e. parašo funkcija elektroninio dokumento organizavimo sistemoje – duomenų kodavimas. Tai leidžia atlikti šias funkcijas *(Davidavičienė, Gatautis, Paliulis, Petrauskas,* 2009):

- užtikrinti reikiamą konfidencialumą ir sumažinti nesankcionuotos prieigos prie duomenų galimybę;
- užtikrinti dokumento autentiškumą ir duomenų vientisumą;
- užtikrinti dokumento sudarytojo identifikaciją;
- užtikrinti efektyvų duomenų kodavimą perduodant duomenis.

Autentiškumą įgyvendina teisinę galią turintis e. parašas.

E. parašo naudojimas svarbus ir naudingas sudarant sandorius, kuriems įstatymas nustato rašytinę formą. „Elektroninis parašas nėra būtina sąlyga užtikrinti per atstumą sudaromų sandorių galiojimą, tačiau sudarant sutartis elektroninėmis priemonėmis, pvz., pateikiant užsakymą internetu, niekas nėra apsaugotas, kad kas nors į užsakymo formą neįrašys svetimų duomenų. Pati sukčiavimo nustatymo problematika yra baudžiamosios teisės dalykas, tačiau pareiga atlyginti žalą dažnai atsiranda informacinių sistemų valdytojams (pvz., dėl naudojimosi internetine bankininkyste) ir draudikams pagal civilinės teisės normas. Bankai tam naudoja specialias kodavimo programas, kurios sumažina žalos atsiradimo riziką dėl neteisėtų klientų ar kitų asmenų veiksmų, bet tokios priemonės nėra lygiavertės pasirašytiems raštams, o sprendžiant ginčus paprastai reikalaujama pasirašytų dokumentų“ *(Vaitkevičienė*, 2005).

Konkrečios valstybės nacionaliniai įstatymai nustato teisinę naudojamo e. parašo galią. Tai tik viena iš kliūčių, su kuriomis susiduriama norint nustatyti tapatybę naudojant elektroninės atpažinties priemones ar siekiant pasinaudoti viešosiomis paslaugomis tarpvalstybinio naudojimo kontekste. Kliūtis siekiama panaikinti Europos Parlamento ir Tarybos reglamentu Nr. 910/2014 „Dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje“, kuriuo panaikinama Direktyva 1999/93/EB „Dėl Bendrijos elektroninių parašų reguliavimo sistemos“. Šiuo reglamentu yra įtvirtinamos aiškios taisyklės dėl e. parašų teisinės galios, kvalifikuoto e. parašo galia prilyginama rašytiniam, o kvalifikuotas e. parašas, patvirtintas vienoje valstybėje narėje išduotu kvalifikuotu sertifikatu, pripažįstamas ir kitose narėse. Dėl šio reikalavimo valstybėse narėse tampa paprasčiau naudotis viešosiomis elektroninėmis paslaugomis. Siekiant palengvinti tarpvalstybinį įvairių paslaugų teikimą vidaus rinkoje ir suteikti įmonėms galimybę vykdyti veiklą tarpvalstybiniu mastu, Europos Parlamento ir Tarybos reglamente Nr. 910/2014 „Dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje“ apibrėžiamas elektroninių parašų, elektroninių spaudų arba elektroninių laiko žymų kūrimas, patikrinimas ir patvirtinimas, elektroninio registruoto pristatymo paslaugos ir su tomis paslaugomis susiję sertifikatai arba interneto svetainių tapatumo nustatymo sertifikatų kūrimas, patikrinimas ir patvirtinimas, arba elektroninių parašų, spaudų ar su tomis paslaugomis susijusių sertifikatų ilgalaikis išsaugojimas.

Atsižvelgiant į šį Europos Parlamento ir Tarybos 2014 m. liepos 23 d. reglamentą išleistas Lietuvos Respublikos vidaus reikalų ministro 2014 m. gruodžio 1 d. Nr. 1V-820 įsakymas „Dėl nacionalinės elektroninės atpažinties informacinės sistemos nuostatų patvirtinimo“, kuris reglamentuoja Nacionalinės elektroninės atpažinties informacinės sistemos (toliau – NETAIS) steigimą, jos tikslą, uždavinius, funkcijas, organizacinę, informacinę ir funkcinę struktūras, NETAIS duomenų teikimą, naudojimą ir saugą, jos finansavimą, modernizavimą ir likvidavimą. Visos Europos Parlamento ir Tarybos reglamento nuostatos Lietuvoje turėtų įsigalioti nuo 2016 m. antrojo ketvirčio.

3 skirsnis. Laiko žymos sąsaja su elektroniniu parašu, jos kūrimo principai ir diegimo problematika

Pereinant prie visavertės elektroninės komercijos ir elektroninės bankininkystės, spartėjant duomenų perdavimo ir jų tvarkymo inovatyviosioms technologijoms, ypač svarbi tampa laiko žyma. 2000 m. liepos 11 d. priimtame

Elektroninio parašo įstatyme numatyta, kad laiko žymą kaip priedą gali nustatyti elektroninio parašo sertifikatą teikianti organizacija. Elektroninės laiko žymos paskirtis – ne tik informacinė, nurodanti dokumento sukūrimo ar sandorio sudarymo laiką, bet ir teisinė, patvirtinanti sandorio pirmumo teisę. Tam, kad laiko žyma turėtų teisinę galią, ją suteikiančių organizacijų įranga turi būti susieta (sinchronizuota) su Nacionaliniu metrologijos institutu, kurio atominiai laikrodžiai susiję su koordinuotojo pasaulinio laiko skale.

Deja, šiuo metu nėra bendros tarptautiniu mastu pripažintos technologijos, skirtos elektroninei laiko žymai formuoti. Tačiau visos laiko žymos formavimo ir perdavimo technologijos suderintos su tarptautiniu standartu X.509, reglamentuojančiu skaitmeninio parašo sertifikato formatą.

Pasirašančiųjų asmenų sertifikatuose yra sertifikato galiojimo pradžios ir pabaigos terminai. Tačiau sertifikatas dėl įvairių priežasčių gali būti atšauktas anksčiau. Pavyzdžiui, asmeniui, pametusiam kortelę su privačiuoju raktu, būtina nedelsiant kreiptis į CA dėl sertifikato atšaukimo (galiojimo nutraukimo anksčiau, nei sertifikate nurodytas pabaigos terminas). Galioja tik tokie e. parašai, kuriuos asmenys sukūrė jų sertifikatų galiojimo laikotarpiu. Pasibaigus sertifikatų galiojimo terminui (pvz., jau archyve esantiems elektroniniams dokumentams), būtina turėti galimybę patikrinti, ar asmenys šiuos dokumentus pasirašė atitinkamų sertifikatų galiojimo laikotarpiu. Todėl į e. parašus gali būti įterpiamos (dedamos) laiko žymos. Tai turėtų būti padaroma kaip galima greičiau, vos tik pasirašius dokumentą. Tam, kad tikrintojas galėtų įsitikinti, jog e. parašas buvo sukurtas pasirašiusiojo asmens sertifikato galiojimo laikotarpiu, reikalinga e. parašo laiko žyma ir sertifikato duomenys. Informacija apie atšauktus sertifikatus saugoma *CA* atšauktų sertifikatų sąraše *(CRL)*. Elektroniniam parašui laiko žyma turi būti dedama pasirašiusiojo asmens sertifikato galiojimo laikotarpiu. Priešingu atveju e. parašo laiko žyma neturės prasmės. Laiko žymas kuria (deda) patikimos trečiosios šalys – laiko žymų tarnybos *(TSA – Time Stamping Authorities)*. Asmenys, norintys gauti elektroninių duomenų laiko žymą, į *TSA* turi nusiųsti užklausą ir šių elektroninių duomenų santrauką. Laiko žyma yra įrodymas, kad elektroniniai duomenys (pvz., skaitmeninis parašas) jau egzistavo iki žymoje užfiksuoto laiko.

Taigi laiko žyma yra paslauga, ir ja naudojantis galima nurodyti elektroninių dokumentų ir (ar) elektroninių parašų tikslią datą bei laiką. Laiko žyma internete yra skaitmeninis pašto datos žymėjimo ekvivalentas.

Laikas, kai buvo pasirašytas dokumentas, nėra susietas su sistemos laiku (darbo vietos ar serverio), jį nurodo patikimas trečiasis asmuo. Laiko žymos dažniausiai prireikia, kai dedami elektroniniai parašai, naudojantis privačiais skaitmeniniais sertifikatais.

Laiko žymos paslauga gali būti skirta:

- verslo klientams;
- viešajam administravimui;
- individualiems klientams.

Laiko žyma gali būti naudojama:

- elektroninės formos sutartims, bankams, draudimo įmonėms ar kt.;
- elektroniniams dokumentams, kad šie išsaugotų savo, kaip įrodymų, vertę;
- pareiškimams ir prašymams, elektronine forma nusiųstiems viešojo administravimo įstaigoms;
- vidiniams elektroniniams dokumentams, siekiant juos apsaugoti nuo klastojimo ir žymėjimo atgaline data;
- sistemos žurnalams, siekiant apsaugoti juos nuo klastojimo;
- elektronine forma gavėjams nusiųstoms elektroninėms sąskaitoms;
- asmeniniame kompiuteryje saugomiems elektroniniams dokumentams, siekiant juos apsaugoti nuo klastojimo ir žymėjimo atgaline data;
- kompiuterinėms programoms, siekiant apsaugoti jas nuo klastojimo ir virusų.

Laiko žymos kaip paslaugos naudojimo pranašumai:

- datos patikimumas;
- garantija, kad dokumentai buvo sukurti ir (ar) sudaryti nurodytu laiku;
- garantuojamas elektroninių dokumentų autentiškumas;
- saugi prekyba internetu.

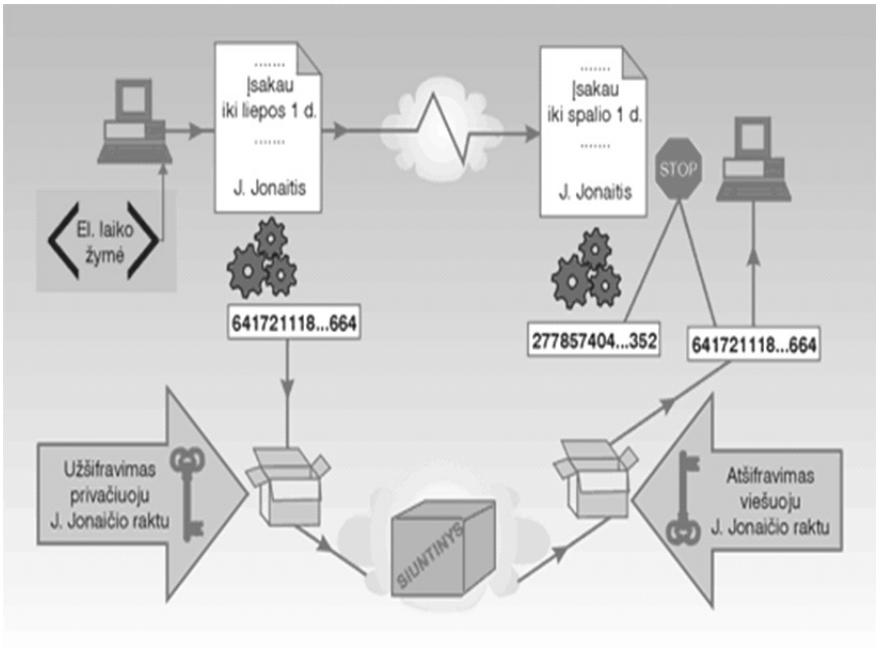
Išskiriamos tokios laiko žymos formos:

- standartinė laiko žyma;
- sertifikuota laiko žyma.

Paprasčiausia laiko žyma – failo įrašymo į kompiuterio atmintį laikas. Tačiau šis laikas susietas tik su kompiuterio vidiniu laikrodžiu ir neturi nieko bendra su koordinuotuoju pasauliniu laiku. Sinchronizuojant kompiuterio laikrodį su Nacionalinio metrologijos instituto laikrodžiu (pvz., naudojant *NTP* technologiją), ši laiko žyma įgyja sietį su koordinuotuoju pasauliniu laiku, tačiau dar netampa tikrąja laiko žyma, turinčia teisinę galią. Tikroji laiko žyma turi būti suformuojama ir perduodama taip, kad niekas negalėtų jos pakeisti. Tai galima padaryti tik naudojant informacijos perdavimo saugumo technologijas. Vienas iš būdų elektroninei laiko žymai suteikti teisinę galią – ją susieti su skaitmeniniu parašu, identifikuojančiu dokumento sudarytoją.

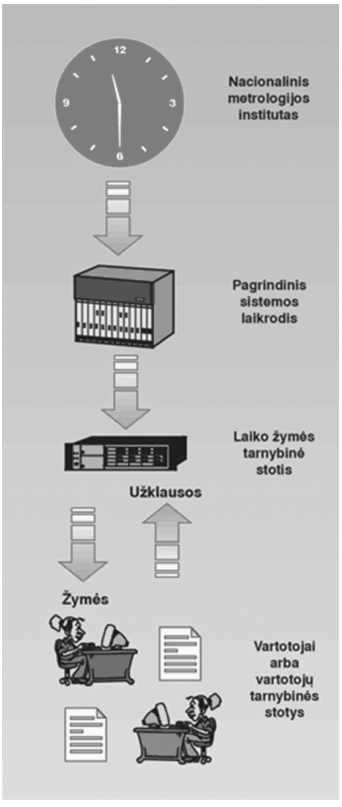
Paanalizuokime, kaip veikia vienas iš galimų skaitmeninio parašo „mechanizmų“. Skaitmeninio parašo veikimą, kurio schema pavaizduota 3 pav., galima suskirstyti į keletą grandžių:

1) naudodamas specialią programą (vadinamąją *hash* funkciją), siuntėjas iš savo dokumento sugeneruoja skaitmeninę duomenų santrauką. Šiai santraukai būdinga tai, kad visų, net mažiausių skirtumų turinčių, dokumentų santraukos būna skirtingos, ir iš jokios santraukos neįmanoma atkurti pradinio teksto. Jos reikalingos tam, kad nereikėtų šifruoti viso pradinio dokumento, nes šifravimas asimetriniu būdu, ypač naudojant ilgus šifravimo raktus, užima gana daug laiko;
2) siuntėjas, naudodamas savo asmeninį raktą, minėtąją santrauką šifruoja kartu su papildomais rekvizitais (laiko žyma ir pan.);
3) gavėjas, naudodamasis ta pačia specialiąja programa *(hash* funkcija), sugeneruoja atsiųstojo dokumento santrauką;
4) gavėjas, naudodamasis siuntėjo viešuoju raktu, iššifruoja siuntėjo atsiųstą šifruotą santrumpą;
5) gavėjas, palyginęs savo sugeneruotą santrauką su iššifruotąja, įsitikina gautojo dokumento ir nurodytosios laiko žymos tikrumu.



3 pav. Elektroninio parašo veikimo schema
Šaltinis: < *http://www.elpasas.lt/gp/savokos.htm*>.

Kaip matome, elektroninė laiko žyma padaroma siuntėjo kompiuteryje arba tarnybinėje stotyje, generuojančioje skaitmeninį parašą. Kaip jau buvo minėta, nėra bendros technologijos elektroninei laiko žymai formuoti ir perduoti. Gana nuoseklų ir išbaigtą šios problemos sprendimo variantą pasiūlė JAV bendrovė *DATUM*, ji pateikė elektroninės laiko žymos generavimo ir perdavimo sistemą, pavadintą „Patikimu laiku“ (angl. *Trusted Time)*. Minėtoji sistema, kurios schema pavaizduota 3 pav., tenkina visus elektroninės laiko žymos generavimo ir perdavimo reikalavimus. Pirma, elektroninės laiko žymos šaltinis yra Nacionalinis metrologijos institutas, antra, visi laiko žymos perdavimai tarp sistemos grandžių atliekami naudojant duomenų perdavimo saugumą užtikrinančias technologijas. Vadinasi, „Patikimo laiko“ sistema atitinka visus laiko žymos apibrėžimo „*Internet X.509 Public Key Infrastructure – Time Stamp Protocol* (TSP)“ pirminės redakcijos reikalavimus. Laiko žymos apibrėžimą ir ją reglamentuojančius dokumentus rengia IETF (angl. *Internet Engineering Task Force)* darbo grupė.



4 pav. Laiko žymos formavimo ir perdavimo schema „Patikimo laiko“ sistemoje
Šaltinis: <*http://www.elpasas.lt/gp/savokos.htm*>.

Skaitmeninis parašas ir elektroninė laiko žyma turi teisinę galią, taigi visa su jų formavimu susijusi įranga turi būti įrengta gerai saugomoje ir atitinkamų valstybinių žinybų kontroliuojamoje vietoje. Šiuo metu elektroninės laiko žymos „Trusted Time“ technologija įdiegta JAV, *DATUM*, bendradarbiaujant su *NIST* (angl. *National Institute of Standards)*.

Apibendrinant galima teigti, jog e. parašui laiko žymos dedamos siekiant įrodyti, kad parašas ar duomenys buvo sukurti iki žymoje nurodyto laiko, nes e. parašo naudotojams išduoti sertifikatai galioja ribotą laikotarpį. Šio pabaigos terminas nurodomas pateikiant sertifikatą, kurio galiojimas dėl įvairių priežasčių gali būti nutrauktas anksčiau, nei nurodytas jo pabaigos terminas. E. parašai, sukurti sertifikatui netekus galios, tampa negaliojantys. Norint įrodyti, kad e. parašas buvo sukurtas dar leistinu laikotarpiu, be laiko žymos, reikalingi ir to sertifikato duomenys. Taigi laiko žyma yra įrodymas, kad duomenys buvo sukurti iki joje nurodyto laiko. Laiko žymos yra svarbios elektroniniams parašams, nors gali būti naudojamos ir kitiems tikslams, pvz., kaip elektroninių duomenų autorių teisių įrodymo priemonė.

4 skirsnis. Elektroninio parašo reguliavimo poveikis kuriant elektroninius dokumentus

Pagal formą dokumentai skirstomi į rašytinius (popieriniai ir elektroniniai) ir į – garso, vaizdo bei garso ir vaizdo dokumentus. Nemažai dėmesio oficialiems elektroniniams dokumentams (toliau – elektroniniai dokumentai) valdyti skiriama ir tarptautinėje erdvėje.

Tarptautinės standartizavimo organizacijos patvirtintame tarptautiniame *ISO* 15489-1:2001 standarte nurodyta, kad būtina užtikrinti teisės aktų keliamus reikalavimus atitinkantį įstaigos veiklos tęstinumą, garantuoti atsiskaitomumą ir veiklos įrodymą, o įstaigos sukurti dokumentai turi būti autentiški, patikimi, galimi naudoti, be to, turi būti užtikrintas šių dokumentų integralumas visą jų gyvavimo ciklą *(ISO*, 2001). Taigi elektroninis dokumentas – fizinio asmens ar organizacijos gautas ir išsaugotas informacinis pranešimas kaip teisinių įsipareigojimų ir veiklos vykdymą įrodantys duomenys.

Pavyzdiniame *UNCITRAL* elektroninės komercijos įstatyme akcentuojama platesnė duomenų pranešimo sąvoka, apimanti ir elektroninį dokumentą *(UNCITRAL*, 2001). Duomenų pranešimas – elektroninėmis, optinėmis ar kitomis analoginėmis priemonėmis surinkta, išsiųsta, gauta ar išsaugota informacija, įskaitant ir elektroninį apsikeitimą duomenimis *(EDI – Electronic Data Interchange)*, elektroninį paštą, telegramas, teleksą ir telekopijas, tačiau neapsiribojama tik jais.

Duomenų pranešimas pats savaime negali būti laikomas popierinio dokumento ekvivalentu, nes ne kiekvienas pranešimas atlieka dokumento funkcijas. Kai įstatymai reikalauja rašytinės dokumento formos, el. pranešimas patenkina šį reikalavimą, jeigu jame esanti informacija yra prieinama tokiu būdu, kad ją būtų galima naudoti vėliau.

Todėl pavyzdiniame *UNCITRAL* elektroninės komercijos įstatyme buvo išplėsta dokumento sąvoka. Suformuluotas teiginys, kad ir popieriniai, ir elektroniniai dokumentai gali atlikti vienodas funkcijas:

- dokumentas yra visiems įskaitomas;
- net ir praėjus tam tikram laikui lieka nepakitęs;
- galima padaryti kopiją;
- galima autentifikuoti duomenis parašu;
- dokumentas gali būti parengiamas valstybės institucijoms priimtina forma *(UNCITRAL*, 2001).

Jeigu popierinis ar elektroninis dokumentas atitinka išvardytuosius kriterijus, jis turi tokią pat teisinę galią. Pavyzdiniame elektroninės komercijos įstatyme suformuluota nuostata, kad elektroninė forma negali būti diskriminuojama ir negali būti daroma jokio skirtumo tarp tokių dokumentų pripažinimo ir įrodomosios galios; elektroninis dokumentas negali būti diskriminuojamas dėl to, kad jis yra elektroninis, o elektroninės formos sutarties galiojimas negali būti paneigtas vien dėl to, kad ji sudaryta apsikeičiant duomenų pranešimais, t. y. svarbu ne dokumento forma, o jo funkcija *(UNCITRAL*, 2001).

Ši nuostata 2002 m. kovo 7 d. Europos Parlamento bei Tarybos direktyvoje 2002/21/EB dėl elektroninių ryšių tinklų ir paslaugų bendrosios reguliavimo sistemos (Pagrindų direktyvoje) ir Elektroninių ryšių įstatyme suformuluota kaip funkcinio lygiavertiškumo principas, kuris reiškia, kad teisės normos turi būti kuo vienodžiau taikomos elektroninių ryšių tinklams ar paslaugoms, atliekantiems analogiškas funkcijas. Kalbant apie rašytinius dokumentus, kriterijus turi būti rašytinio dokumento funkcijos: jis turi būti įskaitomas, laikui bėgant nepakisti, galimybė nukopijuoti dokumentą taip, kad kiekviena iš šalių turėtų tuos pačius duomenis.

Lietuvoje tokių dokumentų valdymas organizuojamas Lietuvos Respublikos dokumentų ir archyvų įstatymo, Lietuvos archyvų departamento prie Lietuvos Respublikos Vyriausybės generalinio direktoriaus tvirtinamų dokumentų tvarkymo ir apskaitos taisyklių nustatyta tvarka.

Dokumentų ir archyvų įstatymas dokumentą apibrėžia kaip „juridinio ar fizinio asmens veiklos procese užfiksuotą informaciją, nepaisant jos pateikimo būdo, formos ir laikmenos“ (Lietuvos Respublikos dokumentų ir archyvų įstatymas, 1995). Šiame įstatyme minima ir atsarginės kopijos –

„naudojimui skirtos dokumentų kopijos, pagamintos mikroformos ar skaitmeninėje laikmenoje“ – sąvoka. Taigi šis teisės aktas labai liberaliai apibrėžia dokumento sąvoką, kartu apimdamas ir elektroninio dokumento sampratą.

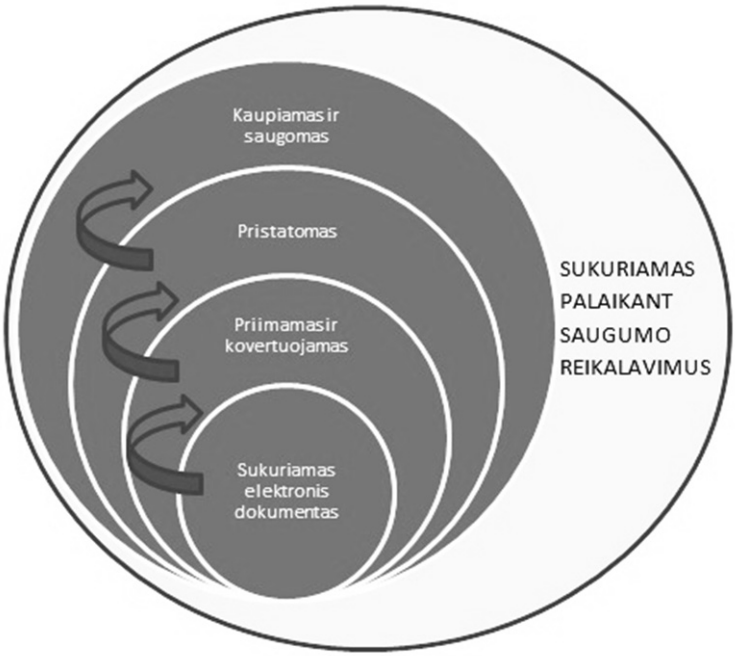
Teisės gauti informaciją iš valstybės ir savivaldybių įstaigų įstatymas apibrėžia oficialaus dokumento sąvoką – tai „rašytinis, grafinis, garsinis regimasis, kompiuterinės informacijos ar kitoks dokumentas“ *(Lietuvos Respublikos teisės gauti informaciją iš valstybės ir savivaldybių įstaigų įstatymas*, 2000), vadinasi, kompiuterinis, arba kitaip – e. dokumentas, jeigu jis yra išleistas, išduotas ar gautas arba saugomas valstybės institucijoje, turėtų būti pripažįstamas kaip įrodymas ir netgi oficialus.

E. dokumentas, kaip ir e. parašas, gali būti pateikiamas kaip įrodymas grindžiant faktus teisme. Tam, kad e. dokumentų naudojimosi sąlyga būtų patenkinta, Lietuvos archyvų departamentas prie Lietuvos Respublikos Vyriausybės dar 2005 m. parengė, o 2006 m. sausio 11 d. patvirtino Elektroninių dokumentų valdymo taisykles (Lietuvos archyvų departamento įsakymas „Dėl elektroninių dokumentų valdymo taisyklių patvirtinimo“). Siekiant užtikrinti e. parašu pasirašyto e. dokumento saugumą, slaptumą ir autentiškumą, naudojama kriptografija ir šifravimas. Tam, kad elektroninis dokumentas būtų ekvivalentiškas rašytiniam, jam keliami šie reikalavimai:

- dokumentas turi būti autentiškas. Būtina užtikrinti, kad jame užšifruota informacija nebuvo keičiama per visą jo gyvavimo ciklą;
- dokumentas turi būti patikimas. Jo sudarymo metu informacija turi būti teisinga ir tikra;
- dokumentas turi būti vientisas. Jis turi būti išbaigtas ir nekeičiamas;
- dokumentas turi būti prieinamas ir galimas naudoti;
- turi būti įmanoma autentifikuoti duomenis dėl parašo;
- dokumentas turi būti kaip aiškus įrodymas;
- galimybė jį dauginti;
- būtina užtikrinti, kad dokumentas būtų priimtinos formos teismams.

Elektroniniai dokumentai adresatui perduodami el. paštu, internetu ar kitomis e. priemonėmis, kurios turi būti atsparios informacijos iškraipymui siuntimo metu. Siunčiamas e. dokumentas turi būti parengtas ir perduodamas taip, kad jį gavusi įstaiga galėtų nustatyti jo sudarytoją (siuntėją), datą, registracijos numerį, atpažinti e. dokumento turinį ir identifikuoti elektroninį parašą. E. dokumento cirkuliacijos etapai pavaizduoti 4 paveiksle. Dokumentams pasirašyti elektroniniu būdu naudojamas skaitmeninis sertifikatas. Pasitelkę minėtąjį sertifikatą internetinėms operacijoms atlikti, galite įrodyti savo tapatybę, gauti patogų priėjimą prie jums reikalingos asmeninės informacijos. Siųsdami elektroniniu būdu pasirašytą informaciją

verslo partneriams ar draugams garantuosite, kad iš jūsų gaunami duomenys yra tikri.



5 pav. E. dokumento cirkuliacijos pavyzdys
Šaltinis: <*http://www.armedforces-int.com/article/digital-document-solutions.html*>.

Svarbiausias popierinio ir elektroninio pranešimo skirtumas yra tik laiško persiuntimo greitis, visais kitais atžvilgiais elektroninis laiškas atitinka visus popierinio rašto požymius. Elektroniniuose raštuose sukaupiama daugiau informacijos, ir jie dažniausiai yra patikimesni už popierinius. Pvz., sunaikinto popierinio rašytinio dokumento gali būti išvis neįmanoma atkurti. Sunaikinti e. dokumentą yra kur kas sunkiau. Nors šiek tiek su informacinėmis technologijomis susipažinusiam asmeniui yra aišku, kad paspaudus trynimo funkciją atliekantį kompiuterio klavišą kompiuterinis įrašas nebūtinai bus sunaikintas. Šiuolaikinės informacinės technologijos operatyvinėje kompiuterio atmintyje leidžia daryti momentines dokumento kopijas, be to, ištrinto elektroninio dokumento antrinis variantas lieka išsaugotas kaip rezervinė kopija kietajame diske, serveryje arba rezervinėje duomenų saugykloje ir, esant reikalui, toks dokumentas gali būti atkurtas tos pačios būklės ir išlikusi ta pati informacija, kaip ir buvo sukurta *(Petravičiūtė I.*, 2006, p. 169). Popierinė dokumento forma, jeigu jis nėra surašytas ranka, leidžia tik labai apytikriai nustatyti, kada jis sukurtas, ar

buvo keistas, kas atliko pakeitimus, o ekspertai, gavę ryšių tinklais persiųstą elektroninį dokumentą, daugeliu atvejų gali nustatyti, kada jis sukurtas ir kokioje šalyje, ar pakeitimai padaryti tuo pačiu įrenginiu, ar juos darė tas pats vartotojas *(Talbot J. Welsh D.*, 2006). Pakeitimus galima atsekti ir nuo jų atlikimo praėjus labai mažai laiko, ir gana daug, kai tas vartotojas, kuris juos padarė, ar galinis įrenginys, kuriuo įvesta informacija, tyrimo metu jau nebeegzistuoja.

5 skirsnis. Elektroninio parašo įtaka sudarant elektronines sutartis

Sparti informacinių technologijų plėtra didina elektroninių sandorių populiarumą, o vienas iš moderniųjų technologijų pritaikymo verslo komerciniams santykiams būdų – elektroninių sutarčių, kildinamų iš jau išanalizuotų e. dokumento kūrimo technologinių ir tarptautinės teisės standartų sureguliavimo, naudojimas. Pastaruoju metu elektroninių sutarčių daugėjimas rodo pasaulinę elektroninės komercijos ir verslo plėtrą.

Elektroniniai sandoriai dar kitaip vadinami elektronine sutarties forma – „tai pirkėjo (vartotojo) ir pardavėjo arba paslaugos teikėjo sudaryta sutartis keitimosi elektroniniais duomenų pranešimais būdu“ *(Sodžiūtė, Sūdžius*, 2006). Elektroninės sutartys atitinka rašytinių sutarčių juridinę galią ir yra sudaromos remiantis laisva abiejų šalių valia. Norint saugiai naudotis elektroninėmis sutartimis, būtina sukurti tinkamą e. parašo veikimo teisinę ir technologinę infrastruktūrą.

Elektroninėms sutartims sudaryti reikalingas e. parašas. Tam tikro pobūdžio sandoriams ir sutartims užtikrinti naudojamos kriptografinės sistemos. Pasitelkus tokio pobūdžio šifravimo priemones yra užtikrinamas e. parašo unikalumas ir patikimumas. Sandoriai, sudaromi apsikeičiant elektroninėmis žinutėmis, dažniausiai naudojami B2B modelyje arba uždarose sistemose. „Sandorio šalių suderintas galutinis sutarties tekstas turi būti pasirašytas abiejų šalių elektroniniais parašais“ *(Davidavičienė, Gatautis, Paliulis, Petrauskas*, 2009). Nustatyti sandorio sudarymo laiką gana sudėtinga, nes sutarties šalys gali būti skirtingose laiko zonose, todėl teikiama laiko žymos paslauga – sutartys tvirtinamos atskiru elektroniniu parašu, ir nė viena sandorio šalis negali pakeisti sutarties laiko, be to, tiek Lietuvoje, tiek kitose šalyse esantys sertifikavimo centrai, išduodantys atitinkamus kvalifikuotus sertifikatus, yra atsakingi už e. parašo konfidencialumą užtikrinančių reikalavimų atitikimą.

2001 m. gruodį paskelbtas elektroninių sutarčių konvencijos projektas, kuriuo siekiama nustatyti teisines priemones ir taip suteikti daugiau

pasitikėjimo virtualiomis sutartimis, nepažeidžiant sutarties laisvės ir šalies autonomiškumo principų. Bendros teisinės bazės, reglamentuojančios elektronines sutartis, nebuvimas yra įvardijamas kaip vienas iš veiksnių, trukdančių tarptautinei elektroninės komercijos ir verslo plėtrai.

Siekiant apsaugoti nuotolines sutartis sudarančius vartotojus, 1997 m. buvo priimta 97/7/EB direktyva. Vartotojų, vykdančių elektroninę (kaip ir įprastą) veiklą, reikalavimai ginami teisinėmis priemonėmis. Elektroninę sutartį sudaręs pirkėjas per nustatytą terminą elektronine forma turi gauti pardavėjo ar paslaugų teikėjo patvirtinimą apie sutarties sudarymą *(Sodžiūtė, Sūdžius*, 2006).

Kaip jau minėta, dėl sparčios informacinių technologijų plėtros įvyko pasaulinis ekonomikos perversmas. Rinkų transformacija ir naujų sukūrimas, kitokių prekių ir paslaugų įsigijimo ar informacijos pasiekimo būdų atsiradimas, nacionalinių sienų išnykimas – tik keli informacinių technologijų plėtros teikiami pranašumai. Tuo pat metu iškilo daugybė teisinių klausimų dėl elektroninių technologijų naudojimo sudarant komercinius sandorius. Dėl šios priežasties greta tradicinės atsirado ir elektroninė sutartis. Tai sukėlė daugybę diskusijų ne tik tarp teisės teoretikų, bet ir praktikų. Atsirado būtinybė išanalizuoti elektroninę sutartį, išskirti jos ypatybes ir palyginti su tradicine. Analogiškai kilo klausimas, ar tokie sandoriai neprieštarauja tradicinės sutarčių teisės principams *(Dontoglou*, 2002).

Pabrėžtina, kad elektroninės sutartys kaip specifinė sutarčių rūšis ar forma Lietuvoje nėra aiškiai reglamentuotos *(Kiškis, Štitilis, Rotomskis, Petrauskas*, 2006). Teisiniu pagrindu galėtume laikyti CK 6.192 str. 2 dalį. Remiantis šiuo straipsniu, kai pagal įstatymus ar šalių susitarimą sutartis turi būti paprastos rašytinės formos, ji gali būti sudaroma tiek surašant vieną šalių pasirašomą dokumentą, tiek ir apsikeičiant raštais, telegramomis, telefonogramomis, telefakso pranešimais ar kitokiais telekomunikacijų galiniais įrenginiais perduodama informacija, jeigu yra užtikrinama teksto apsauga ir galima identifikuoti jį siuntusios šalies parašą. Ilgą laiką teisės doktrinoje buvo diskutuojama dėl šios teisės normos taikymo internetu sudaromoms sutartims. M. Civilka teigė, kad „iš šios nuostatos nėra aišku, ar jos formuluotė apima ir sandorius, sudaromus internete“. Problemą iš esmės išsprendė Elektroninių ryšių įstatymas[36], kuris pakeitė jau nebegaliojantį Telekomunikacijų įstatymą. Šio įstatymo 3 str. 58 d. nurodo, kad galinis telekomunikacijų įrenginys – tai palaikyti ryšį leidžiantis įrenginys ar atitinkama jo dalis, skirti tiesiogiai ar netiesiogiai bet kokiomis priemonėmis prisijungti prie viešųjų telekomunikacijų tinklų (visiškai ar iš dalies skirtų viešosioms telekomunikacijų paslaugoms teikti). Tokiu būdu įstatymų

[36] LR elektroninių ryšių įstatymas, Valstybės žinios, 2004, Nr. 69-2382.

leidėjas jau nebediferencijuoja elektroninių pirkimo–pardavimo sutarčių pagal panaudotas informacines technologijas prisijungiant prie interneto ir išplečia „telekomunikacijų galinių įrenginių“ sąvoką. Todėl klausimas dėl CK 6.192 str. 2 d. taikymo internetu sudaromoms pirkimo–pardavimo sutartims neturėtų kilti. Informacinės visuomenės paslaugų įstatymo[37] 4 skyriuje yra minima sąvoka „sutarčių sudarymas elektroninėmis priemonėmis“. M. Kiškis *(Katuoka, Kiškis, Pranevičius ir kt.*, 2006) teigia, kad šiame įstatyme vartojama sąvoka gali būti suprantama dvejopai:

- „kaip sutartis, kurios sąlygos pateikiamos šalims elektronine forma ir šalys išreiškia savo valią elektronine forma;
- kaip sutartis (žodinė, rašytinė ir 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 ne elektronine forma.“

M. Kiškis mano, kad sistemiškai analizuojant informacinės visuomenės paslaugų įstatymo ir CK nuostatas „sutartimi, sudaroma elektroninėmis priemonėmis“ laikytina tik pirmoji sutarčių kategorija. Manytina, kad su tokia nuomone reikėtų sutikti, todėl šiame darbe nagrinėsime tik elektronines sutartis, kurių sąlygos šalims pateikiamos elektronine forma, o šios savo valią irgi išreiškia elektroniniu būdu.

„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 ar pareigūnų kompetencijos ir techninių galimybių ribų. Ilgainiui būtina tarptautiniu mastu spręsti teisines problemas elektroninėje erdvėje“ *(Kiškis, Štitilis, Rotomskis, Petrauskas*, 2006). ES ir tarptautiniu lygiu yra priimami e. komerciją reglamentuojantys teisės aktai. Tačiau nei rekomendaciniame Jungtinių Tautų Tarptautinės prekybos teisės komisijos pavyzdiniame elektroninės komercijos įstatyme *(UNCITRAL,* 1996), nei 2000 m. Europos Parlamento ir Tarybos direktyvoje dėl kai kurių informacinės visuomenės paslaugų, ypač e. komercijos teisinių aspektų vidaus rinkoje (Europos Parlamento ir Tarybos direktyva Nr. 2000/31/EB, 2000) (toliau – Elektroninės komercijos direktyva), nėra šios sutarties apibrėžimo. Šiais teisės aktais yra siekiama, kad elektroninė sutartis dėl savo formos neprarastų teisinės galios, t. y. turėtų tokią pačią teisinę galią kaip ir tradicinė sutartis. Todėl, kitaip nei teisės doktrinoje, teisės aktuose nesiekiama pateikti elektroninės sutarties sąvokos, tai paliekama teisės mokslui.

[37] LR informacinės visuomenės paslaugų įstatymas, Valstybės žinios, 2006, Nr. 65-2380.

Pabrėžtina, kad remiantis UNCITRAL buvo priimta Konvencija dėl elektroninių komunikacijų naudojimo tarptautinėse sutartyse *(UNCITRAL*, 2005). Šis teisės aktas yra taikomas sudarant *B2B* sandorius. Tačiau kol kas nė viena ES valstybė šios konvencijos neratifikavo.[38] P. P. Polanskis teigia, kad šios konvencijos tikslas – pasiūlyti praktinių problemų sprendimų būdų ne tik per sandorių sudarymo procesą, bet ir vykstant deryboms bei vykdant sutarčių sąlygas *(Polanski*, 2007). Valstybėms rekomenduotina ratifikuoti šį teisės aktą, nes jis šiuolaikinei e. komercijai suteiks daugiau tikrumo ir prognozavimo galimybių. Tačiau šis teisės aktas irgi nepateikia „elektroninės sutarties" sąvokos.

Kaip jau minėta, sutartis yra įprasta skirstyti į rūšis. Tai turi svarbią ne tik teorinę, bet ir praktinę reikšmę, nes „leidžia civilinių santykių dalyviams surasti ir panaudoti savo veikloje esmines vienos ar kitos sutarčių rūšies savybes, panaudoti praktikoje tokį sutarties modelį, kuris geriausiai atitinka siekius ir poreikius" *(Ambrasienė, Baranauskas*, 2006). Pagal sudarymo būdą sutartys yra skirstomos į sudaromas prisijungimo ir derybų būdu.

Vartotojų elektroninėje aplinkoje (konkrečiai internete) sudaromoms sutartims gana svarbūs vadinamieji *Click-wrap* susitarimai. Taip dažniausiai vadinamos sutartys, sudarytos „išskirtinai elektroninėje aplinkoje, tokioje kaip internetas, nustatantis šalių teises ir pareigas. Pavadinimas kilo iš fakto, kad tokių susitarimų sudarymui reikalingas pelės paspaudimas ant ekrane esančio paveikslėlio *(Icon)* arba mygtuko *(Button),* išreiškiantis šalies valią prisiimti įsipareigojimus". *Click-wrap* sutarčių atveju pirkėjas (vartotojas) sutinka įsipareigoti pagal nurodytas sutarties sąlygas. Šiuo atveju nereikalingas nei rašytinis, nei koks nors kitas dokumentas, nei pirkėjo parašas *(Samson*, 1998). Pabrėžtina, kad prisijungimo būdu sudaromos sutartys nėra tradicinės komercijos naujovė. Jos plačiai naudojamos bankų, draudimo įstaigų, mobiliojo ryšio ar interneto paslaugų teikėjų ir daugelyje kitų sričių. Didžiausias tokių sutarčių pranašumas – jos sudaromos lengvai, greitai ir patogiai. Tokiais atvejais nereikia su kiekvienu klientu aptarinėti konkrečių sąlygų ir derinti pozicijų. Laikas ir kitos sąnaudos, kurių sutaupoma dėl minėtųjų sutarčių sudarymo galimybių, gali būti skiriami prekės ar paslaugos kokybei gerinti, rinkodaros efektyvumui didinti ir pan.

Tokie susitarimai dažniausiai yra sudaromi dviem būdais:

a) **įrašyti ir paspausti** (angl. *Type and Click)* – vartotojas, ketindamas sudaryti sutartį, turi į nurodytą langelį įrašyti „sutinku", paskui paspausti paveikslėlį ar mygtuką, patvirtinantį sutikimą su visomis sutarties sąlygomis;

[38] Jungtinių tautų organizacijos UNCITRAL komisijos tinklalapis: <http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2005Convention_status.html>.

b) **paspaudimas** (angl. *Icon Clicking)* – šiuo atveju vartotojas, ketindamas sudaryti sutartį, tiesiog peržiūri jos sąlygas ir paspaudžia paveikslėlį ar mygtuką „aš sutinku“, taip išreikšdamas savo valią prisiimti įsipareigojimus.

Kita didelė e. sutarčių grupė – sudarytos derybų būdu. Pats derybų procesas iš esmės nesiskiria nuo tradicinių popierine forma sudaromų sutarčių: vyksta bendravimas, derinamos pozicijos, sutarties sąlygų punktai ir pan. Vienintelis skirtumas – visa tai daroma e. erdvėje. Dažniausiai pasitelkiamas elektroninis paštas, įvairios bendravimo programos (pvz., *Skype*, *Msn* ir pan.). Skirtingai nei bendros pozicijos suderinimą patvirtinantis tradicinis rankų paspaudimas, sudarant elektronines sutartis apsikeičiama laiškais (žinutėmis), kur matyti galutinis sutarties variantas. Nors nesklandumų dėl vienodų sutarties sąlygų pavyzdžio taikymo nekyla, atsiranda kitokia problema – kaip įsitikinti, kad vienos šalies siųstas galutinis variantas iš tiesų toks ir liko, kitaip tariant, ar šalis, gavusi elektroninį sutarties variantą, savo nuožiūra jos nepataisė. Kita problema yra susijusi su šalių identifikavimu ir jų valios išreiškimu pasirašant tokias sutartis. Elektroninių pirkimo–pardavimo sutarčių nederėtų painioti su sutartimis, kurių sąlygos derinamos internetu, tačiau galutinai jos pasirašomos realiai susitikus. Nors kai kurie aspektai, pvz., derybų vedimo e. erdvėje įrodinėjimas, yra glaudžiai susiję su e. komercija, tokios sutartys nėra elektroninių sutarčių objektas, nes galutinė sutartis yra tradicinės popierinės formos. Derybų būdu sudaryta elektroninė pirkimo–pardavimo sutartis yra pasirašoma (išreiškiama valia sutikti su sutarties sąlygomis) e. erdvėje. Pati sutartis irgi išlieka elektroninio formato. Dėl šių specifinių sutarties ypatybių ir kyla minėtųjų problemų. Šiuo atveju ieškoti atsakymų į tokius daug diskusijų keliančius klausimus padeda programinės įrangos gamintojai – jie siūlo įvairių programų, suteikiančių galimybę kontroliuoti e. sutarties sudarymo procesą. Konkrečiau – pateikiama įvairių e. parašo variantų. Šiuo atveju kalbama apie elektroninius dokumentus, pasirašytus kvalifikuotu e. parašu, turinčiu tokią pat teisinę galią kaip ir pasirašymas ranka.

Kvalifikuoti e. parašai negali būti sudaromi automatiškai, jie sukuriami pasirašančiojo asmens išreikštiniu veiksmu, patvirtinant ketinimą pasirašyti duomenis naudojant instrumentines priemones, kurios adekvačiai ir saugiai vizualizuoja ar kitaip pateikia pasirašomus duomenis.

Kvalifikuotus e. parašus sudarančia taikomąja sistema negalima pasirašyti bet kokio formato duomenų todėl, kad netinkamo formato duomenys negali būti adekvačiai ir saugiai vizualizuoti ar kaip nors kitaip pateikti.

Vadinasi, problema kyla tada, kai kalbama apie konkrečią kvalifikuotus e. parašus sudarančią taikomąją sistemą, kuri bet kokio formato duomenis pasirašančiam asmeniui padėtų atlikti kvalifikuoto e. parašo sudarymo veiksmą.

Geriausiu atveju galima kalbėti tik apie konkrečią taikomąją sistemą, sudarančią kvalifikuotus e. parašus pagrindiniams e. dokumentų formatams.

E. dokumentai ir jų pasirašymo reikalavimai yra tokie skirtingi, kad kiekvienam pasirašytam e. dokumentui taikyti bendrą formatą būtų gana sudėtinga, be to, nėra ir išvis negali būti bendro nepasirašyto elektroninio dokumento formato.

Kitokia padėtis yra kalbant apie parašo tikrinimą – šį veiksmą galima pavesti automatinėms procedūroms ar trečiosioms šalims. Kvalifikuotam e. parašui tikrinti gali būti sukurta atskira taikomoji kvalifikuotų e. parašų tikrinimo sistema.

Todėl keliami skirtingi kvalifikuoto e. parašo sudarymo ir tikrinimo reikalavimai.

A. Mitašiūnas abejoja dėl pasirašyto e. dokumento bendro formato vertės, nes mano, kad negalima kalbėti apie konkrečią kvalifikuotus e. parašus sudarančią taikomąją sistemą.

Kiekviena kvalifikuotus e. parašus sudaranti taikomoji sistema suformuoja tokį pasirašyto e. dokumento (konteinerio) formatą, koks yra tikslingesnis konkrečios kvalifikuotus e. parašus sudarančios taikomosios sistemos atveju, tačiau laikomasi visuotinai taikomų šios srities standartų.

Taikomoji kvalifikuotų e. parašų tikrinimo sistema turi būti universali, kad galėtų priimti bet kurios taikomosios sistemos, laikantis visuotinų šios srities standartų, kvalifikuotu e. parašu pasirašytą elektroninį dokumentą ir jį patikrinti.

Konkreti taikomoji kvalifikuotų e. parašų tikrinimo sistema taiko šiuos standartinius reikalavimus tokia apimtimi, kokią lemia taikymo specifika, į kurią yra orientuotos konkrečios taikomosios kvalifikuotų e. parašų sudarymo sistemos.

Universali taikomoji kvalifikuotų e. parašų tikrinimo sistema gali būti sukurta didėjant konkrečių kvalifikuotų e. parašų sudarymo taikomųjų sistemų reikalavimams ir turi priimti bet kurios taikomosios sistemos, laikantis standartinių reikalavimų, kvalifikuotu e. parašu pasirašytą elektroninį dokumentą ir jį patikrinti.

Apibendrinant tai, kas išdėstyta, galima teigti, kad vartotojų e. komercijoje bei ofertos ir akcepto ryšio priemonėmis sudaromoms sutartims tinkamai išreikšti Lietuvoje yra pakankamas (nors ir ne idealus, tačiau gana lankstus) teisinis pagrindas. Kai kuriuos neaiškumus ir reguliavimo trūkumus gali padėti užpildyti šiuo metu dar visiškai negausi šios srities teismų praktika ir vartotojų organizacijų veikla.

6 skirsnis. Elektroninio parašo įtaka įgyvendinant elektroninių sutarčių apsaugos teisinį reglamentavimą pasaulyje

1. Jungtinės Amerikos Valstijos

JAV prezidentas 2000 m. birželio 30 d. pasirašė e. parašo *E-Sign (Electronic Signatures in Global and National Commerce Act)* aktą. Šio įstatymo projekto e. parašai ir e. sutartys įgijo teisinį pripažinimą *(E-Sign legislation)*.

Elektroninio parašo įstatymu buvo sureguliuota visa teisinė e. parašo bazė. Bendros e. parašo teisinės bazės nebuvimas stabdė e. komercijos plėtrą, nes buvo baiminamasi, kad naudojamos elektroninės priemonės ir e. parašo technologijos neturi teisinio pagrindo ir gali būti laikomos negaliojančiomis *(Electronic Signature)*.

JAV Kalifornijos valstija viena pirmųjų patvirtino e. parašą. JAV Jutos valstijos statutas įteisina aiškios technologijos įtvirtinimą, kurio reglamentavimas labai detalus, jau įstatymų lygmeniu siejamas su konkrečia technologija, kuri pripažįsta tik skaitmeninį parašą, t. y. tokį e. parašą, kuris kuriamas ir naudojamas pasitelkus viešųjų raktų infrastruktūros (PKI) technologiją. Minėtasis statutas, reglamentuojantis skaitmeninius parašus, įtvirtina „pasirašančiojo“ ir „parašo turėtojo“ sąvokas (angl. *U. S. Electronic Signature)*. Parašo turėtojas atsako už privataus rakto saugojimą ir turi užtikrinti jo saugumą. Be to, jis turi sertifikatą ir privatų raktą, kuris atitinką viešąjį, o parašo gavėjas (pasirašantysis) sukuria parašą, pasirašydamas dokumentą.

1999 m. JAV nacionaliniai konferencijos dalyviai, atsakingi už bendrąją šalies teisę (angl. *NCCUSL – National Conference of Commissioners on Uniform State Law)*, priėmė elektroninių sandorių aktą (angl. *UETA – Uniform electronic transactions act)*. Šis aktas buvo rekomenduotinas visoms šalies valstijoms, siekiant suvienodinti skirtingai veikiančius tuometinius elektroninių sandorių įstatymus.

Elektroninių sandorių aktas buvo pritaikytas keturiasdešimt septyniose JAV valstijose, tačiau vėliau ta pati teisės komisija pabrėžė, kad elektroninių sandorių aktas neturėtų būti laikomas pagrindiniu šalies įstatymų rinkiniu, apibrėžiančiu skaitmeninį parašą, nes akte yra pateikiama ir kitų elektroninių, ne vien šifravimo metodu veikiančių, priemonių (angl. *Electronic contracts in the U. S.)*.

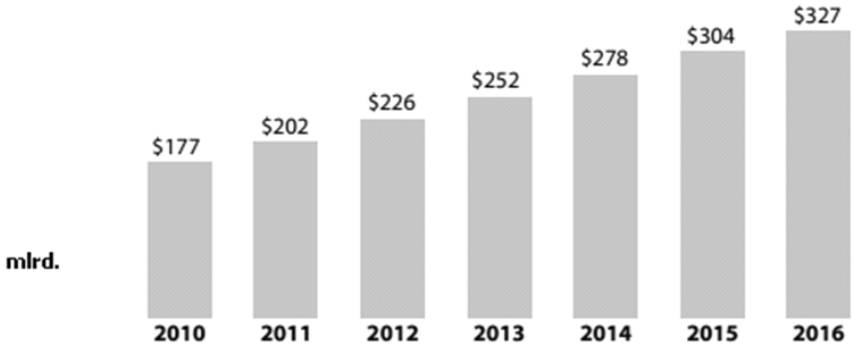
Elektroninio verslo plėtra JAV yra populiari nuo 2000 m. birželio, kai buvo priimtas aktas „Dėl elektroninių parašų naudojimo pasaulinėje ir nacionalinėje veikloje“. Remiantis šiuo aktu yra nustatomos sąlygos, pagal kurias turi būti tvarkomi e. dokumentai ir pabrėžiama jų saugumo svarba *(U. S. Federal Trade Commission, Department of Commerce*, 2001). 2000

m. buvo patvirtintas Elektroninio parašo įstatymas (angl. *E-Sign)*, apibrėžiantis e. sandorius, e. parašo naudojimą, e. kontraktų ir kitų elektroninių priemonių teisinę bazę.

JAV rinkoje e. komercija daro didelę įtaką sektoriams, kur vykdomas verslas – vartotojui skirti (B2C) sandoriai. E. komercija – svarbus segmentas, užtikrinantis sandorių vykdymo procesus. JAV gyventojų surašymo biuro (angl. *Census Bureau)* 2001 m. pateiktoje statistikoje matyti, kad šalyje e. komercijos būdu vykdomas pardavimas per pirmąjį ketvirtį sudarė 7 mlrd. JAV dolerių, o e. komercijos sandoriai – 0,91 proc. visų mažmeninės prekybos sandorių. Iš viso e. komercijos sandoriai siekė 25,8 mlrd. dolerių *(U. S. Federal Trade Commission, Department of Commerce, 2000).*

JAV komercijos departamentas apskaičiavo, kad 2011 m. vartotojai internete išleido 194 mlrd. dolerių – 16,1 proc. daugiau, palyginti su 2010 m., kai pardavimas siekė 167,3 mlrd. dolerių. Šie skaičiai rodo, kad e. komercija JAV užima vis didesnę mažmeninės prekybos dalį. Remiantis Komercijos departamento pateikta statistika, 2011 m. mažmeninės prekybos dalis išaugo iki 7,9 proc. ir sudarė 42 trln. JAV dolerių *(U. S. Commerce Department,* 2011).

Pasaulinė mokslinių tyrimų ir konsultavimo bendrovė „Forrester" pateikė mažmeninės prekybos iki 2016 m. prognozę, kuria remiantis pirkimas internetu padidėtų iki 327 mlrd. dolerių. Žemiau pateikiama 2011–2016 m. statistikos lentelė (žr. 6 pav).



6 pav. Internetinės prekybos prognozė iki 2016 metų
Šaltinis: *<http://mashablel.com/2012/02/27/ecommerce-327-billion-2016-study>.*

Įstatymų leidėjai sukūrė *E-Sign* aktą, kad suteiktų galimybę JAV įmonėms teisiškai naudotis e. parašu. *E-Sign* akto atsiradimas buvo grindžiamas motyvu, kad JAV bendrovės neatsiliktų nuo pasaulio verslo. Įstatymų leidėjai kaip paskatą ir paramą verslo įmonėms priėmė teisės aktą, kuris

skatintų e. parašo naudojimą sudarant tarptautinius verslo sandorius, kaip būtinybę ir galimybę naudoti įvardydami autentifikavimo technologijas, kurios teisiškai galiotų pasirašomiems sandoriams.

2. Vokietija

Vokietija yra viena iš pirmaujančiųjų Europos internetinės prekybos rinkose. Beveik pusė mažmeninės prekybos sektoriaus generuojamų pajamų yra gaunamos iš e. verslo rinkos. Vis didėjantis vartotojų, kurie perka internete, kiekis, skatina e. verslo plėtrą. Didžiąją dalį visos Vokietijos apyvartos generuoja dešimt didžiausių interneto prekiautojų, tokių kaip „Amazone“, „Otto Group“ ir kt.

E. verslo plėtros ir racionalių sprendimų, kurie padėtų optimizuoti įmonės veiklą, mažinant išlaidas ir išteklių sąnaudas, pakilimas Vokietijoje prasidėjo 2011 metais. E. verslas pasitelkia informacines technologijas savo procesams remti ir gerinti. Siekiama, kad sandoriai, sutartys ir su verslu susijusi informacija būtų perduodama elektroniniu būdu. Automatizavimo procesų sprendimai greitina ir efektyvina verslo procesus *(E-business standards in Germany)*.

Vokietija yra viena iš stipriausią ekonomiką turinčių šalių, ji užima penktąją vietą pasaulyje. Vis didėjanti interneto prieiga skatina e. verslo klestėjimą. Plačiajuosčio ryšio skverbtis yra viena didžiausių Europoje, tai skatina e. sandorius ir daro juos greitesnius ir išbaigtesnius *(Blythel*, 2012).

Vokietijoje Elektroninio parašo įstatymas priimtas 1997 metais. Kaip ir Lietuvoje, šioje šalyje yra pripažįstamas saugus parašas, sukurtas patikima parašo formavimo įranga. Pasak M. Civilkos ir T. Lamanausko, „skirtingose valstybėse narėse teks pasitelkti skirtingus technologinius standartus iš esmės tiems patiems verslo tikslams, o tai neabejotinai gali sukelti disharmoniją valstybių narių nacionalinėse sistemose ir taip iškraipyti bendrosios rinkos veikimą. Tokios disharmonijos pavyzdžiu galėtų tapti Vokietijos 1997 m. įstatymas (Informations- und Kommunikationsdienste-Gesetz - IuKDG, 1997), teisinį pripažinimą ir teisinę galia suteikęs tik skaitmeniniam parašui“ *(Civilka, Lamanauskas,* 2004). Elektroninio parašo įstatymas įtvirtina technologinio neutralumo principą, vadinasi, elektroniniai duomenys gali būti pasirašomi neatsižvelgiant į naudojamą technologiją. Vokietija, taikydama aiškios technologijos principą, pripažįsta e. parašo veikimo būdą, kuris paremtas viešojo rakto technologija, kai skaitmeninis parašas sietinas su viešuoju raktu, o tai prieštarauja technologinio neutralumo principui.

Vokietijoje, kaip ir daugelyje kitų šalių, priimtas e. parašas nebuvo plačiai naudojamas ir populiarus verslo rinkoje dėl teisinio ir technologinio sudėtingumo aspektų.

Elektroninio parašo įstatymo pakeitimas Vokietijoje buvo priimtas 2001 m. gegužės 16 d., jis pakeitė senesnįjį 1997 m. rugpjūčio 1 d. Skaitmeninio parašo įstatymą. Minėtasis įstatymas nustato būtiną e. parašo saugumo infrastruktūrą ir apibrėžia reikalavimus, pagal kuriuos e. parašas būtų teisiškai prilyginamas ranka rašytam parašui (angl. *EU electronic signature regulation)*. Vokietijos elektroninio parašo įstatyme nurodyta, kad sertifikato savininku teisiškai gali būti laikomas tik fizinis asmuo, o juridinis – negali būti įvardijamas kaip sertifikato savininkas. Skaitmeninio parašo aktas nurodo, kad skaitmeninis parašas, sietinas su viešuoju raktu, yra išduodamas fiziniam asmeniui. Tačiau Vokietijos elektroninio parašo įstatymas įtvirtina trečiojo asmens teisę reikalauti panaikinti sertifikatą, kuriame yra informacija apie šį asmenį. Taip juridinis asmuo gali panaikinti savo buvusiam darbuotojui suteiktą sertifikatą *(Tumalavičiūtė*, 2009).

Vokietija, ragindama įmones naudotis e. parašo teikiamomis galimybėmis, skatina e. parašų naudojimą e. versle, tačiau, siekdama užtikrinti išduodamų sertifikatų saugumo aspektus, sertifikavimo paslaugų teikėjams kelia gana griežtus reikalavimus.

Beveik visi kvalifikuotus sertifikatus išduodantys sertifikavimo paslaugų teikėjai Vokietijoje yra akredituoti. Siekiant užtikrinti ne tik vidaus, bet ir išorės, rinkos funkcionavimą bei siekiant dalyvauti tarptautinėje e. komercijos plėtroje ES valstybėse narėse išduoti sertifikatai, kurie atitinka direktyvoje nustatytus reikalavimus, pripažįstami ekvivalentiškais Vokietijos sertifikavimo paslaugų teikėjo išduotam kvalifikuotam sertifikatui, jei atitinka el. parašų direktyvos 5 str. 1 d. reikalavimus, kurie atitinka e. parašo teisinę galią: Valstybės narės užtikrina, kad saugūs yra tie e. parašai, kurie paremti kvalifikuotu sertifikatu ir sukurti saugia parašo formavimo įranga *(Tumalavičiūtė*, 2009):

- atitiktų teisinius parašo reikalavimus dėl elektronine forma pateiktų duomenų, kaip rašytiniai parašai atitinka tokius reikalavimus dėl duomenų popieriuje;
- būtų leistini kaip įrodymas teisme.

Be to, ekvivalentiškomis Vokietijos paslaugų teikėjų teikiamomis paslaugomis, susijusiomis su e. parašu, laikomos kitų ES valstybių narių teikiamos paslaugos, kurios atitinka Direktyvos reikalavimus.

Direktyvos reikalavimus atitinkančias laiko žymos paslaugas teikia Vokietijos paslaugų teikėjai.

Vokietija e. versle „nustato dviejų lygių apsaugą – aukštą vartotojų apsaugą ir žemesnę profesionaliems verslo subjektams“ *(Civilka*, 2001). Vokietijoje yra keliami itin griežti reikalavimai:

– „produkto sertifikavimui;
– sertifikavimo paslaugų teikimui (kai jos kilusios iš Vokietijos);
– savanoriškai akreditacijai („akredituotas e. parašas“).“ *(Civilka*, 2001).

Apytiksliai apskaičiuota, kad Vokietijos bendrovės kasmet išsiunčia per šešis milijardus įvairių popieriniu būdu pateiktų sąskaitų. Ši tendencija skatina pereiti prie keitimosi elektroninėmis sutartimis. Keturios iš penkių Vokietijos bendrovių kaip lemiamus perėjimo prie elektroninių sandorių ir sutarčių veiksnius nurodo išlaidų ir sąnaudų mažinimo pranašumą *(Germany el. invoice)*, tai skatina ir efektyvina e. parašo naudojimą e. versle. Kaip veiksnys, skatinantis patogesnį ir efektyvesnį e. parašo naudojimą e. versle, yra elektroninė asmens tapatybės kortelė. Dėl minėtosios kortelės, įskaitant e. parašo projektų plėtrą, Vokietijoje buvo diskutuojama dar 2002 m., o svarbiausias ilgų diskusijų aspektas – e. parašas nebuvo intensyviai, plačiai ir efektyviai naudojamas. 2006 m. rugsėjo 13 d. buvo suformuluoti projekto tikslai elektroninei tapatybės kortelei įvesti ir 2007 m. pabaigoje buvo tikimasi galutinai ją įtvirtinti.

Apibendrinant galima daryti išvadas, kad Vokietijoje e. parašas jau yra gana efektyviai naudojamas. Valstybė tokį parašą skatina naudoti kaip patogų ir saugų e. dokumentų bei e. sandorių sudarymo įrankį taupant įmonės lėšas. E. verslo įmonių subjektai supranta e. parašo naudą ir jo teikiamus pranašumus, tai didina e. parašo naudojimo perspektyvas Vokietijos e. versle.

3. Estija

Nors Estija yra nedidelė šalis, jai būdinga viena iš pažangiausių e. parašo sistemų pasaulyje. E. parašo naudojimas neatsiejamas nuo interneto, taigi svarbu paminėti, kad Estija pagal interneto vartotojų skaičių pirmauja tarp Baltijos šalių. Remiantis 2011 m. gruodžio 31 d. duomenimis, net 77,5 proc. gyventojų naudojasi internetu, kai Lietuvoje – 59,5, Latvijoje – 69,9 procento. Elektroninio parašo įstatymas Estijoje įsigaliojo 2000 m. pabaigoje. Minėtojoje šalyje, kaip ir kitose Europos valstybėse, šis įstatymas parengtas pagal 1999/93/EB Europos direktyvą ir juo įteisinti e. parašo reikalavimai, kurie jam suteikia tokį pat teisinį statusą kaip ir rašytiniam parašui. Estijos visuomenės atvirumas naujovėms, gana aukštas informacinių technologijų lygis sudaro palankias e. parašo infrastruktūros kūrimo sąlygas.

E. parašui keliami reikalavimai Estijoje, kaip ir kitose ES valstybėse, iš jų ir Lietuvoje, mažai kuo skiriasi, tačiau galime matyti skirtumų pritaikant e. parašą viešosioms paslaugoms.

E. parašo naudojimą Estijoje labiausiai skatina išduodamos asmens identifikavimo (ID) kortelės. Ši ID kortelė privaloma visiems gyventojams ir, be identifikavimo, atlieka dar ir elektronines funkcijas. Vadinasi, kortelės turėtojui suteikiama galimybė naudoti e. parašą. Kiekvienoje kortelėje yra du sertifikatai ir jų privatūs raktai, apsaugoti PIN kodais. Vienas iš sertifikatų skirtas identifikuoti, o kitas – skaitmeniniam pasirašinėjimui.

Suprantama, kai kuriems vartotojams gali kilti abejonių dėl e. kortelės naudojimo saugumo. Todėl yra numatytos tam tikros kortelių turėtojų gynimo teisės, kurios suteikia galimybę sustabdyti savo sertifikatų galiojimą – atlikus tokį veiksmą, šios kortelės nebeįmanoma naudoti elektroniniu būdu. Šis metodas, kuriuo stengiamasi paskatinti visuomenę aktyviau naudoti e. parašą, taikomas ir Lietuvoje, į naujosios kartos asmens tapatybės korteles įdiegiant e. parašo technologiją, tačiau mūsų valstybėje tai nelabai pasitvirtino.

Kaip jau buvo minėta, kiekviena išduota asmens tapatybės kortelė turi du sertifikatus: identifikavimo ir skaitmeninio pasirašymo. Be to, yra du susiję privatūs raktai, apsaugoti dviem atskirais PIN kodais. Sertifikatams nėra jokių naudojimo apribojimų: jie yra universalūs ir skirti naudoti labai įvairiai, t. y. tarp privačių asmenų, organizacijų ar kortelės turėtojų ir viešojo sektoriaus organizacijų. Be to, reikėtų atkreipti dėmesį, kad Estijoje suteikiama teisė naudotis e. parašu ne tik ID kortelių turėtojams, bet ir įsigijus specialią mobiliojo telefono SIM kortelę.

Aptarus pagrindines priemones, naudojamas e. parašui, svarbu paminėti ir būdus, kuriais galima pasirašyti e. dokumentus. Taigi Estijoje plačiausiai naudojama *DigiDoc* – speciali į vartotojo kompiuterį instaliuojama programa, skirta e. dokumentams pasirašyti ir patikrinti. Vartotojas, naudodamas ID kortelę arba mobilųjį telefoną, gali prisijungti prie *DigiDoc* sistemos ir įkelti bet kokį dokumentą, pasirašyti jį skaitmeniniu būdu ir perduoti kitoms šalims.

Ši sistema labai aktyviai naudojama Estijos viešajame sektoriuje tiek tvarkant teismo dokumentus, tiek įvairias savivaldybių sutartis. E. paslaugoms teikti nuo 2003 m. sukurtas interneto tinklalapis *www.eesti.ee*, kur galima rasti įvairių paslaugų fiziniams ir juridiniams asmenims.

Aktyviausiai e. parašas Estijoje naudojamas šiose srityse:

- elektroninei įmonių registracijai;
- elektroniniam balsavimui;
- elektroniniam mokesčių deklaravimui;
- sveikatos priežiūros srityje:
- elektroniniai vaistų receptai;
- skaitmeninė ligos istorija.

Estijoje 2005 m. įvykę vietos rinkimai buvo pirmieji pasaulyje, įvykdyti internetu, nors juose dalyvavo vos 2 proc. iš visų balsavusiųjų, šis bandymas pasitvirtino, nes vis dažniau per rinkimus balsuojama internetu. Tokiu būdu suteikiama galimybė pareikšti savo valią net šalyje nesantiems rinkėjams.

Taigi e. parašo infrastruktūra Estijoje yra labai toli pažengusi. Sričių, kur pasirašoma e. parašu, gana daug, o gyventojai aktyviai skatinami juo naudotis. Todėl Estija gali būti pavyzdys, kaip tobulinti Lietuvos e. parašo infrastruktūrą.

4. Latvija

Šios valstybės e. parašo padėtis gana panaši į Lietuvos. Nors Elektroninių dokumentų įstatymas Latvijoje įsigaliojo 2003 m. (šiek tiek vėliau nei Lietuvos Respublikos elektroninio parašo įstatymas) šiandien galime matyti, kad tai jai nesutrukdė gana sėkmingai pralenkti Lietuvą plėtojant e. parašo infrastruktūrą. Interneto vartotojų skaičius Latvijoje gana nedaug skiriasi nuo Europos vidurkio. 2010 m. galima matyti labai didelę šios šalies e. valdžios pažangą, tai rodo elektroninių paslaugų perkėlimo į e. erdvę lygis. 2010 m. net 89 proc. paslaugų gyventojams ir 100 proc. juridiniams asmenims jau buvo pasiekiamos ir visiškai suteikiamos internetu (Europos Komisija).

Latvijoje 2011 m. atidaryta virtualioji svetainė *www.eparaksts.lv*, kurioje pateikiamas unikalus naudojimosi e. parašu sprendimas. Šiam būdui nereikalingi specialūs įrenginiai, išmaniosios kortelės ar programinė įranga. Minėtąjį projektą sukūrė Latvijos nacionalinis radijo ir televizijos centras (LNRTC), kuris nuo 2009 m. birželio šalyje yra oficialus sertifikavimo paslaugų teikėjas. Šis e. parašas visose ES valstybėse turi juridinę galią. Norint naudotis šia technologija, reikalingas banko kortelės numeris, kodų kortelė arba generatorius. Pasirašantysis asmuo įveda savo PIN kodą, kuris suteikiamas tapus e. parašo naudotoju. E. parašo svarbą pabrėžia ir Latvijos informacijos ir komunikacijos technologijų asociacijos prezidentė S. Balina: „Šis technologijos sprendimas neabejotinai paskatins e. parašo naudojimą ir elektroninės aplinkos plėtrą Latvijoje. Aš esu įsitikinusi, kad dėl šių elektroninio parašo technologijų suteikiamų galimybių labai greitai bus pradėti naudoti kiti pažangūs sprendimai“. Vienas iš e. paslaugų prieinamumą palengvinsiančių sprendimų – interneto svetainės *www.eriga.lv*, kur galima rasti visas teikiamas viešąsias paslaugas, sukūrimas.

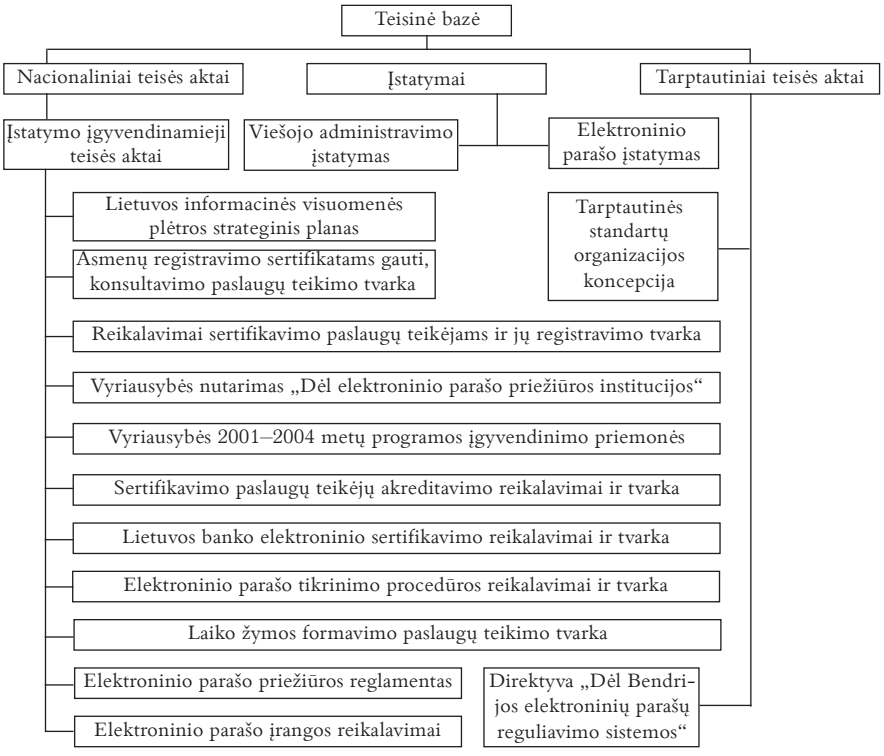
Elektroninių dokumentų įstatymas Latvijoje suteikia galimybę e. parašui būti pripažintam visose viešosiose institucijose, be to, žinoma, kad e. paslaugų teikimas neįsivaizduojamas neturint e. parašo, todėl sudaromos kuo palankesnės sąlygos juo naudotis. Siekiant veiksmingos ekonomikos,

atviro ir demokratinio valstybės valdymo, skatinama plėtoti e. paslaugas: elektroninių rinkimų informacinės sistemos plėtrą, gyventojų registro informacinių sistemų koordinavimą, elektroninio identifikavimo patvirtinimo įvedimą, kurie neatsiejami nuo e. parašo *(Technologijos.lt*, 2011).

5. Lietuva

1999 m. priimta Europos Parlamento ir Tarybos direktyva „Dėl Bendrijos elektroninių parašų reguliavimo sistemos“ paskatino Lietuvoje priimti Elektroninio parašo įstatymą. Praėjus metams po Direktyvos priėmimo, 2000 m. gegužės 25 d. buvo pateiktas Eektroninio parašo įstatymo projektas ir netrukus po to, 2000 m. liepos 11 d., priimtas Elektroninio parašo įstatymas, kuris reglamentuoja e. parašo kūrimo, tikrinimo, galiojimo, taip pat parašų naudotojų ir sertifikavimo paslaugų teises bei atsakomybę, e. parašo priežiūros institucijai keliamus reikalavimus.

E. parašą ir laiko žymos naudojimą reglamentuojanti teisinė bazė, kurioje e. parašą ir laiko žymą reglamentuojantys teisės aktai išskaidyti pagal aktų kilmę, pavaizduota 7 paveiksle.



7 pav. E. parašą ir laiko žymą reglamentuojanti teisinė bazė (Garuckas, Kaziliūnas, 2008)

2002 m. birželio 6 d. Seimas priėmė Elektroninio parašo įstatymo 4, 8, 14, 16 straipsnių pakeitimo ir papildymo įstatymą. Pagrindiniai pakeitimai skirti e. parašo galiai tarp šalių sustiprinti, taip pat – galimybei pasirašyti juridinio asmens vardu. Šiame įstatyme įtvirtinta nuostata, kad e. parašas visais atvejais turi tokią pat teisinę galią kaip ir rašytinių dokumentų parašas, jeigu parašų naudotojai tarpusavyje dėl to susitaria. Tuo metu juridinio asmens atstovo parašui suteikiama tokia pat teisinė galia kaip ir rašytiniam atstovo parašui kartu su įmonės antspaudu rašytiniuose dokumentuose. Kituose straipsniuose reglamentuojama, kad e. parašo priežiūros institucija Vyriausybei ir Seimui turi teikti kasmetines ataskaitas apie e. parašo diegimą.

Šis Elektroninio parašo įstatymo pakeitimo įstatymas suteikė galimybių efektyviau naudotis e. parašu.

Pagal minėtojo įstatymo 2 str. 4 d., e. parašas suprantamas kaip duomenys, kurie susiejami su kitais e. duomenimis pastarųjų autentiškumui patvirtinti ir (ar) pasirašančiajam asmeniui identifikuoti. Kadangi tokio parašo, kuris atlieka tik identifikavimo funkciją, juridinė galia yra gana abejotina, pateikiama ir „saugaus elektroninio parašo“ sąvoka. Ji atitinka keturis tarptautiniu mastu pripažintus reikalavimus: unikalumą (parašas vienareikšmiškai susietas su pasirašančiuoju asmeniu), identifikavimą (leidžia identifikuoti pasirašantįjį asmenį), saugumą (parašas sukurtas priemonėmis, kurias savo valia gali tvarkyti tik pasirašantysis asmuo) ir integralumą (parašas susijęs su pasirašytais duomenimis taip, kad bet koks pakeitimas yra matomas).

E. parašo atsiradimas pirmiausia reiškia naujų teisės ir teisės aiškinimo principų suformavimą. Valstybės pareiga – rengti teisės aktus (ar valstybės politiką), sieti juos su konkrečiomis technologijomis ir atitinkamai aiškinti galiojančias normas. Vadinasi, paprastas parašas ir elektroninė jo forma turi būti pripažįstami kaip lygiaverčiai. Lygiavertiškumas pripažįstamas lyginant tik tai, kad informacijos teisinis efektyvumas, galiojimas ir įgyvendinimas negali būti paneigtas vien tik tuo pagrindu, kad ši informacija yra elektroninis duomenų pranešimas *(Kunigėlis*, 2011).

E. parašo infrastruktūrą kuria: vartotojai, pasirašantys ir tikrinantys parašus, įranga, reikalinga parašams kurti ir tikrinti, sertifikavimo paslaugų teikėjai, garantuojantys pasirašančiojo tapatybę, ir Vyriausybės įgaliota institucija, atliekanti priežiūros funkcijas. Elektroninio parašo įstatymas nustato atskirų infrastruktūros dalių reikalavimus.

Elektroninio parašo įstatyme yra numatyti dvejopi e. parašo naudojimo subjektai – pasirašantysis asmuo ir parašo naudotojas. Šio įstatymo 2 str. 1 d. teigiama, kad „asmuo – įmonė, neturinti juridinio asmens teisių,

fizinis arba juridinis asmuo, įskaitant ir užsienio asmenis". Pasirašantysis apibūdinamas kaip veiksnus fizinis asmuo (galintis savo veiksmais įgyti civilines teises ir susikurti civilines pareigas), kuris turi parašo formavimo įrangą ir, veikdamas savo valia ir savo arba kito asmens, kuriam jis atstovauja, vardu, sukuria e. parašą. ES elektroninio parašo direktyvoje „pasirašančio asmens" sąvoka apibrėžiama lygiai taip pat, tik nereikalaujama būti veiksniu fiziniu asmeniu. Parašo naudotoju gali būti asmuo, savo veikloje naudojantis e. parašą arba iš kitų asmenų gaunantis pasirašytus duomenis. Šių sąvokų apibūdinimas įstatymo nuostatose rodo, kad pasirašyti e. parašu gali tik fizinis asmuo, o šį parašą naudoti – jau bet kokio teisinio statuso asmenys.

Paanalizavus Elektroninio parašo įstatymo 2 skirsnį „Parašo kūrimas, tikrinimas, galiojimas, parašo naudotojų teisės ir atsakomybė", galima suprasti, kad parašo formavimo ir tikrinimo duomenys skirti tik fiziniam asmeniui, kuris vienintelis gali jais disponuoti. Be to, šio įstatymo projekto aiškinamajame rašte teigiama, kad e. parašas susiejamas su fiziniu asmeniu. Taigi juridiniams asmenims ir įmonėms, neturinčioms juridinio asmens teisių, naudotis e. parašu gana sudėtinga dėl formos reikalavimų ir aiškaus įgaliojimų patvirtinimo trūkumo.

Duomenys e. parašu pasirašomi tada, kai yra naudojami e. parašo formavimo duomenys, o patikrinami – juos atitinkančiais e. parašo tikrinimo duomenimis. T. Lamanauskas straipsnyje „Elektroninio parašo įstatymas Lietuvoje: privalumai ir trūkumai" pabrėžia, kad Elektroninio parašo įstatymas atstovauja moderniųjų šios srities įstatymų grupei, įtvirtindamas atvirumo arba technologinio neutralumo principą. Šis principas reiškia, kad įstatymas, nepriklausomai nuo naudojamos technologijos, gali būti pasitelkiamas e. duomenų pasirašymui reglamentuoti.

Per pasirašymo procesą svarbus vaidmuo tenka ir e. parašo formavimo įrangai. Tai – kompiuterių programinė ir (arba) techninė įranga, kurią pasitelkus saugomi e. parašo formavimo duomenys, o šiuos panaudojus dėl pasirašomų duomenų, yra suformuojamas parašas. Elektroninio parašo įstatymo 2 str. keliama papildomų saugios įrangos reikalavimų, tačiau jeigu ji nepanaudojama, tai nepanaikina juridinės e. parašo galios.

Asmenį su jo e. parašu sieja šio sertifikatas, kuris suprantamas kaip elektroninis liudijimas, parašo tikrinimo duomenis susiejantis su pasirašančiuoju asmeniu ir patvirtinantis arba leidžiantis nustatyti pasirašančiojo asmens tapatybę. Sertifikato galiojimas gali būti sustabdomas, jeigu pasirašantysis asmuo praranda sertifikatą atitinkančių parašo formavimo duomenų kontrolę ar sertifikavimo paslaugų teikėjas gauna pranešimą, kad pasirašantysis asmuo tapo neveiksnus ir dėl kitų Elektroninio parašo įstatymo

4 str. 6 d. nurodytų priežasčių. Norint geriau užtikrinti e. parašo naudotojų teises, yra naudojamas kvalifikuotas sertifikatas, kuriam, kaip ir šio sertifikato išdavėjui (sertifikavimo paslaugų teikėjui), Elektroninio parašo įstatymas kelia papildomų reikalavimų (tačiau šiuo metu kvalifikuotus sertifikatus teikiančių subjektų Lietuvoje nėra).

Elektroninio parašo įstatymo projekto aiškinamajame rašte nurodyta minėtojo įstatymo paskirtis – e. parašui suteikti tokią pat teisinę galią kaip ir rašytam ranka. Tai reglamentuojama įstatymo 8 str. „Elektroninio parašo galia“, kuris atitinka ES elektroninio parašo direktyvos 5 str. „Elektroninio parašo teisinė galia“. Šių straipsnių nuostatose suformuluota, kad saugus e. parašas, kuris sukurtas patikima formavimo įranga ir yra patvirtintas galiojančiu kvalifikuotu sertifikatu, e. duomenims turi lygiai tokią pat teisinę galią kaip ir rašytinių dokumentų parašas, tad yra leistinas kaip įrodinėjimo priemonė teisme. Parašas nepraranda savo teisinės galios tik dėl to, kad yra elektroninis, neparemtas kvalifikuotu sertifikatu ar akredituoto sertifikavimo paslaugų teikėjo išduotu kvalifikuotu sertifikatu arba nėra sukurtas saugia parašo formavimo įranga.

T. Lamanauskas, remdamasis Elektroninio parašo įstatymu, išskiria tris sertifikavimo paslaugų teikėjų rūšis: paprastus, registruotus (išduodančius kvalifikuotus sertifikatus) ir akredituotus, kurių veikla įvertinama e. parašo priežiūros institucijoje. Kvalifikuotus sertifikatus sudarantys Lietuvos Respublikos sertifikavimo paslaugų teikėjai privalo užsiregistruoti, tačiau akreditacija nėra būtina sertifikavimo paslaugų teikėjų veiklos sąlyga. ES elektroninio parašo direktyvoje dar akcentuojama savanoriško akreditavimo svarba, siekiant sertifikavimo paslaugų teikėjams pasiūlyti tinkamus pagrindus toliau plėtoti savo paslaugas, užtikrinant pasitikėjimą, saugumą ir kokybę.

Užsienio valstybių sertifikatų galiojimas įtvirtinamas Elektroninio parašo įstatymo 5 str., kuris analogiškas ES elektroninio parašo direktyvos 7 straipsniui. Užsienio valstybių sertifikavimo paslaugų teikėjų sudaryti kvalifikuoti sertifikatai yra teisiškai lygiaverčiai Lietuvos Respublikos sertifikavimo paslaugų teikėjų sudarytiems kvalifikuotiems sertifikatams, jeigu:

- yra sudaryti sertifikavimo paslaugų teikėjo, akredituoto Lietuvos Respublikoje, arba sertifikavimo paslaugų teikėjo, akredituoto ES valstybėje (Lietuvos Respublikai tapus ES nare);
- už sertifikatą laiduoja Lietuvos Respublikos kvalifikuoto sertifikavimo paslaugų teikėjas arba ES valstybės kvalifikuoto sertifikavimo paslaugų teikėjas (Lietuvos Respublikai tapus ES nare);
- sertifikatų pripažinimas paremtas Lietuvos Respublikos tarptautinėmis sutartimis.

Svarbu yra tai, kad pagal šį straipsnį akreditavimas, o ne registravimas, yra sąlyga užsienio paslaugų teikėjams sudaryti kvalifikuotus sertifikatus.

Ketvirtasis Elektroninio parašo įstatymo skirsnis yra skirtas Vyriausybės įgaliotosios e. parašo priežiūros institucijos funkcijoms ir teisėms apibrėžti.

2002 m. Lietuvos Respublikos Vyriausybė priėmė du nutarimus, užtikrinančius e. parašo diegimą. Balandžio 23 d. nutarimu Nr. 568 „Dėl elektroninio parašo priežiūros institucijos" e. parašo priežiūros institucijos funkcijos pavestos Informacinės visuomenės plėtros komitetui prie Lietuvos Respublikos Vyriausybės (toliau – Informacinės visuomenės plėtros komitetas), kuris koordinavo e. parašo įgyvendinimo politiką iki 2011 m., kai ši funkcija buvo perleista Lietuvos Respublikos ryšių reguliavimo tarnybai. Būtent šiam komitetui buvo patikėta parengti Elektroninio parašo įstatymui reikalingus įstatymo įgyvendinamuosius teisės aktus. Tų pačių metų gruodžio 31 d. buvo priimtas nutarimas Nr. 2108 „Dėl reikalavimų kvalifikuotus sertifikatus sudarantiems sertifikavimo paslaugų teikėjams, reikalavimų elektroninio parašo įrangai, kvalifikuotus sertifikatus sudarančių sertifikavimo paslaugų teikėjų registravimo tvarkos bei elektroninio parašo priežiūros reglamento patvirtinimo".

2003 m. Informacinės visuomenės plėtros komiteto direktorius išleido penkis įsakymus, reglamentuojančius e. parašą. 2003 m. sausio 29 d. buvo patvirtinti keturi įsakymai:

1. „Dėl asmenų registravimo sertifikatams gauti ir konsultavimo paslaugų teikimo tvarkos patvirtinimo", kuris taikomas sertifikavimo paslaugų teikėjams, jame aprašoma asmenų registravimo sertifikatams gauti, sutarties sudarymo ir konsultavimo tvarka.
2. „Dėl reikalavimų elektroninio parašo tikrinimo procedūrai patvirtinimo", kurio svarbiausias tikslas – parašo naudotojams nurodyti, kaip turi būti tikrinami saugūs parašai ir kaip naudojamos parašų laiko žymos.
3. „Dėl sertifikavimo paslaugų teikėjų akreditavimo reikalavimų ir tvarkos patvirtinimo", nustatantis sertifikavimo paslaugų teikėjų akreditacinius reikalavimus ir akreditavimo tvarką.
4. „Dėl laiko žymos formavimo paslaugų teikimo tvarkos patvirtinimo", apibrėžiantis laiko žymos formavimo paslaugų teikimą, reikalavimus sertifikavimo paslaugų teikėjams, kuriantiems laiko žymas saugiems e. parašams, abonentų bei laiko žymos naudotojų pareigas ir atsakomybę.

2003 m. kovo 31 d. Informacinės visuomenės plėtros komitetas išleido įsakymą „Dėl minimalios draudiminės sumos kvalifikuotus sertifikatus

sudarantiems sertifikavimo paslaugų teikėjams nustatymo", kuriame buvo nustatyta, jog „kvalifikuotus sertifikatus sudarančių paslaugų teikėjų civilinės atsakomybės draudimo suma turi būti ne mažesnė kaip 100 000 litų vienam draudiminiam įvykiui, vienerių metų laikotarpiui".

E. parašo priežiūros institucija kasmet rengia Elektroninio parašo įstatymo įgyvendinimo ataskaitas. Remiantis šiomis ataskaitomis, galima išskirti keletą svarbiausių priežasčių, kurios daugiau ar mažiau trukdo sėkmingai kurti e. parašo infrastruktūrą:

- vartotojų žinių ir kompetencijos stoka;
- paslaugų, teikiamų e. erdvėje, trūkumas arba neišbaigtumas;
- tarptautinio techninio nesuderinamumo problema;
- sertifikatų ir e. parašo naudojimo įrangos kaina;
- motyvacijos stoka.

Tam, kad kliūtys būtų pašalintos, pirmiausia reikia jas identifikuoti. Išsiaiškinus, kas trukdo tinkamai plėtoti e. parašo infrastruktūrą, yra priimami atitinkami sprendimai. Visuomenės žinių ir kompetencijos trūkumo problemai spręsti internete buvo sukurta visiems pasiekiama nuotolinė e. parašo ir e. dokumento mokymo sistema – kol kas vienintelė lengvai prieinama priemonė, suteikianti galimybę asmenims gauti informacijos apie e. parašą ir e. dokumentą, tačiau norint, kad sistemoje būtų nuolat pateikiama aktuali informacija, šios sistemos plėtrai būtina skirti reikiamą finansavimą. Naudodamiesi minėtąja sistema, asmenys gali ne tik įgyti žinių, bet ir jas pasitikrinti spręsdami testus. Išbandyti šią programą gali kiekvienas interneto vartotojas tinklalapyje *www.elektroninisparasas.lt* (Ryšių reguliavimo tarnybos informacija apie e. parašą). Nuotolinio mokymo sistema 1999 m. buvo sukurta Ciuricho universitete naudojant OLAT mokymo valdymo sistemą. Šiandien ja naudojasi keli Šveicarijos universitetai ir akademijos. OLAT yra atviro kodo programa, ja galima naudotis ir ją modifikuoti nemokamai (e. parašas Lietuvoje).

Lietuvos archyvų departamentas prie Lietuvos Respublikos Vyriausybės 2006 m. sausio 11 d. patvirtino Elektroninių dokumentų valdymo taisykles. Šios taisyklės buvo parengtos pagal Europos Komisijos IDA programos nustatytą specifikaciją *MoReq (Model Requirements for the Management of Electronic Records, MoReq Specification*, 2001). Taisyklės dar nustato subjektus, įgaliotus vykdyti viešojo administravimo funkcijas. Šis dokumentas yra vienas iš svarbiausių teisės aktų, reglamentuojančių e. dokumentą ir visą jo gyvavimo ciklą (įskaitant ilgalaikį saugojimą).

2005 m. birželio 9 d. Seimas patvirtino Lietuvos Respublikos viešojo administravimo įstatymo 19 str. pakeitimą, kuris teigia, kad „Asmenų

prašymai, pateikti elektroniniu būdu, turi būti pasirašyti elektroniniu parašu. Atsakymas elektroniniu paštu turi būti pasirašytas institucijos vadovo arba jo įgaliotojo asmens saugiu elektroniniu parašu". Šiuo įstatymo papildymu siekiama paskatinti piliečius ir valstybės institucijas bendrauti elektroniniu būdu, naudojant e. parašą.

2008 m. birželio 26 d. priimtas ir nuo 2009 m. sausio 1 d. įsigaliojęs Lietuvos Respublikos asmens tapatybės kortelės įstatymo 2, 4, 5 str. pakeitimo bei papildymo ir įstatymo papildymo 1^1 str. įstatymas (Žin., 2008, Nr. 76-3007), suteikęs pagrindą išduoti naujo pavyzdžio lustines asmens tapatybės korteles su kontaktiniame luste įrašytu asmens atpažinimo e. erdvėje sertifikatu ir kvalifikuotu sertifikatu elektroniniams duomenims pasirašyti.

2006 m. gruodžio 12 d. buvo priimta Europos Parlamento ir Tarybos direktyva 2006/123/EB dėl paslaugų vidaus rinkoje valstybėms narėms, kuri nustatė paprastesnius administracinius įpareigojimus: palengvino procedūras ir formalumus, taikomus norint įgyti teisę verstis paslaugų teikimo veikla ir vykdant šią veiklą, be to, užtikrino, kad paslaugų teikėjai, naudodamiesi kontaktinių centrų paslaugomis, tas procedūras ir formalumus galėtų lengvai atlikti nuotoliniu būdu ir elektroninėmis priemonėmis. Siekiant perkelti Paslaugų direktyvos nuostatas, Lietuvoje 2009 m. gruodžio 15 d. (įsigaliojo 2009 m. gruodžio 28 d.) priimtas Lietuvos Respublikos paslaugų įstatymas (Žin., 2009, Nr. 153-6901). Europos Komisijos 2009 m. spalio 16 d. sprendimas 2009/767/EB, kuriuo pagal Paslaugų direktyvą siekiama nustatyti paprastesnes elektroninių priemonių naudojimo priemones, įpareigoja kiekvieną valstybę narę pagal Europos Komisijos sprendimo priede pateiktas technines specifikacijas sudaryti, tvarkyti ir skelbti sąrašą, kuriame pateikiama būtina informacija apie tos valstybės narės prižiūrimus ir akredituotus sertifikavimo paslaugų teikėjus, visuomenei išduodančius kvalifikuotus sertifikatus. Remiantis šiuo sprendimu, Lietuvoje nuo 2009 m. gruodžio 28 d. pradėjo veikti Elektroninio parašo priežiūros institucija, atsakinga už Europos Komisijos sprendimo vykdymą. Siekiant padėti tarpvalstybiniu mastu veiksmingai naudoti saugius e. parašus, patvirtintus kvalifikuotu sertifikatu, turi būti sustiprintas pasitikėjimas šiais e. parašais, kad ir kokioje valstybėje narėje būtų įsisteigęs pasirašantysis asmuo arba kvalifikuotą sertifikatą išduodantis sertifikavimo paslaugų teikėjas. Tai galima pasiekti suteikiant galimybę lengviau gauti patikimos informacijos, reikalingos e. parašui patikrinti, pirmiausia informacijos apie sertifikavimo paslaugų teikėjus, kuriuos prižiūri ir (arba) yra akreditavusi valstybė narė, ir apie jų teikiamas paslaugas. Būtina užtikrinti, kad valstybės narės, naudodamos bendrąją formą, šią informaciją skelbtų viešai ir taip palengvintų naudojimąsi ja bei užtikrintų tinkamą išsamumo lygį, kad gavėjas galėtų įsitikinti, ar e. parašas yra tikras.

2002 m. gruodį buvo priimtas Lietuvos Respublikos Vyriausybės nutarimas, kuris nustato reikalavimus kvalifikuotus sertifikatus sudarantiems sertifikavimo paslaugų teikėjams, e. parašo įrangai, kvalifikuotus sertifikatus sudarančių sertifikavimo paslaugų teikėjų registravimo tvarką. Šie reikalavimai sudaryti remiantis EESSI sukurtais standartais. Pasirašantieji asmenys turi turėti sertifikatų centro išduotus sertifikatus. Juose šalia kitų duomenų yra sertifikato galiojimo pradžios ir pabaigos terminai. Tačiau sertifikato galiojimas dėl įvairių priežasčių gali būti nutrauktas anksčiau už jame nurodytą pabaigos terminą. Parašas, sukurtas iki sertifikato išdavimo ir po jo galiojimo nutraukimo, yra negaliojantis. Todėl ateityje būtina turėti galimybę patikrinti, ar asmenys juos pasirašė atitinkamų sertifikatų galiojimo laikotarpiu. Dėl to parašams gali būti dedamos laiko žymos (angl. *Time Stamp Token)*. Tokias žymas kuria laiko žymų tarnybos (angl. *TSA – Time Stamping Authorities*). Laiko žymos tarnyba, kaip trečioji patikima šalis (angl. *TTP – Third Trusted Party)*, tokias žymas teikia kaip įrodymus, kad tam tikri duomenys (pvz., e. parašas) jau egzistavo iki žymoje užfiksuoto laiko. Šių tarnybų veiklos procedūros ir naudojama įranga turi atitikti nustatytus reikalavimus. Laiko žymos formavimo paslaugų teikimo tvarkos aprašas, patvirtintas Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus 2011 m. balandžio 19 d. įsakymu Nr. 1V-407[39], nustato laiko žymos formavimo paslaugų teikimą ir reikalavimus sertifikavimo paslaugų teikėjams, kuriantiems (formuojantiems) laiko žymas saugiems e. parašams, sukurtiems patikima parašo formavimo įranga ir patvirtintiems kvalifikuotais sertifikatais, abonentų bei laiko žymos naudotojų pareigas ir atsakomybę. Aprašo privalo laikytis visi paslaugų teikėjai, kuriantys (formuojantys) laiko žymas saugių e. parašų sukūrimo laikui patvirtinti, laiko žymos naudotojai ir abonentai. Apraše nustatyta, kad Laiko žymos taisykles renkasi laiko žymos naudotojai, o jų laikosi paslaugų teikėjas. Minėtosios taisyklės rengiamos laiko žymos naudotojų grupės ar paslaugų teikėjo iniciatyva arba pasirenkamos iš Lietuvos standarto LST ETSI TS 102 023 „Strateginiai reikalavimai, keliami laiko žymėjimo paslaugų teikėjams“. Laiko žymos taisykles, kuriose vienareikšmiškai nurodomas identifikatorius, laiko žymų sudarymo ir tvarkymo procedūros, paslaugų teikimo sąlygos ir taisyklės bei kita susijusi informacija (jeigu tokia yra), tvirtina jas parengęs asmuo. Visi, kuriems reikalingos laiko žymos, kreipiasi į paslaugų teikėją. Jeigu asmenį tenkina nustatytos laiko žymos teikimo sąlygos, paslaugų teikėjas ir asmuo (abonentas) sudaro sutartį. Jeigu sutartis tarp abonento

[39] Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus 2011 m. balandžio 19 d. įsakymas Nr. 1V-407 „Dėl Laiko žymos formavimo paslaugų teikimo tvarkos aprašo patvirtinimo“.

ir paslaugų teikėjo sudaroma elektronine forma, ji turi būti pasirašyta saugiu e. parašu, sukurtu patikima parašo formavimo įranga ir patvirtinta galiojančiu kvalifikuotu sertifikatu. Paslaugų teikėjas turėtų užtikrinti:

1. Laiko žymoms pasirašyti naudojamų parašo formavimo ir tikrinimo duomenų valdymą:
   - laiko žymoms pasirašyti naudojamų parašo formavimo duomenų konfidencialumą ir vientisumą, laiko žymos naudotojams platinamų atitinkamų parašo tikrinimo duomenų ir bet kurių kitų susijusių duomenų vientisumą ir autentiškumą;
   - laiko žymoms pasirašyti skirtų parašo formavimo duomenų ir juos atitinkančio sertifikato naudojimą ribotą laiką, nustatytą laiko žymos taisyklėse;
   - laiko žymoms pasirašyti naudojamos parašo formavimo įrangos saugumą jos naudojimo metu.
2. Patikimą laiko žymos kūrimą (formavimą):
   - saugų laiko žymų kūrimą (formavimą) ir teisingo laiko į jas įtraukimą;
   - paslaugų teikėjo laikrodžio sinchronizaciją su Lietuvos koordinuotuoju laiku UTC(LT) Laiko žymos teikimo nuostatuose paskelbtu tikslumu.
3. Patikimą valdymą ir darbą:
   - tinkamą kaupiamos informacijos ir laiko žymos paslaugoms teikti reikalingos įrangos apsaugą;
   - Laiko žymos teikimo nuostatuose nustatytų taisyklių laikymąsi ir Laiko žymos formavimo paslaugų teikimo tvarkos pažeidimo galimybės sumažinimą;
   - fizinės prieigos prie kritinių paslaugos vietų (laiko žymos formavimo ir pasirašymo) kontrolę, laiko žymoms formuoti naudojamos įrangos teisingą naudojimą ir apsaugą nuo modifikavimo ar fizinio sugadinimo;
   - tinkamą abonentų informavimą atsitikus įvykiams, turintiems įtakos laiko žymos formavimo paslaugų teikimo saugumui, arba esant laikrodžio sutrikimų;
   - nepertraukiamą informacijos, reikalingos abonentų sukurtų parašų laiko žymoms tikrinti, teikimą;
   - asmens duomenų, kuriuos jam yra pateikę abonentai, apsaugos reikalavimų, nustatytų Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatyme ir kituose Lietuvos Respublikos teisės aktuose, laikymąsi bei kitos jiems pateiktos abonentų informacijos be jų sutikimo ar teismo sprendimo neplatinimą;

- Laiko žymos taisyklėse nurodytos informacijos užrašymą ir saugojimą šiose taisyklėse nurodytą laiką.

Reikia pabrėžti, kad jeigu paslaugų teikėjai laiko žymos paslaugas teikia pagal Lietuvos standarto LST ETSI TS 102 023 „Strateginiai reikalavimai, keliami laiko žymėjimo paslaugų teikėjams“ nuostatas, teigiama, kad paslaugų teikėjas atitinka apraše išdėstytas nuostatas.

Apibendrinant galima pabrėžti, kad naudojant e. parašą ir laiko žymos funkciją e. versle šiuo metu susiduriama su šiomis teisinėmis problemomis:

– teisės aktų kūrimas yra lėtas procesas;
– nėra reglamentuotų atitinkamų mechanizmų, kurie skatintų e. parašo naudojimą e. versle;
– bendros teisinės bazės, apimančios naujas veiklos sritis, nebuvimas;
– „nėra kai kurių e. verslui būtinų santykių ir procesų reglamentavimo“;
– teisinės bazės, reglamentuojančios sankcijas už elektroninius nusikaltimus, nebuvimas.

Galima teigti, kad dabartinė teisinė e. parašo aplinka nepakankamai pritaikyta e. parašo Lietuvos e. versle ir tarptautinėse rinkose plėtrai. Nors e. parašas yra gana gerai žinomas jau ne vienus metus ir labai išsamiai analizuojamas teisės požiūriu, apžvelgiant pagrindinius įstatymus ir e. parašą aprašančias direktyvas, realiai juo besinaudojančių įmonių nuo e. parašo įteisinimo nėra daug, o šį parašą e. versle naudojančių įmonių patirtis vidutiniškai apima nuo dvejų iki penkerių metų. Laiko žyma teisės aktuose pradėta reglamentuoti tik 2011 m. (pasikeitus e. parašo priežiūros institucijai), o verslo subjektams tai – vis dar naujas reiškinys. E. verslo ir e. parašo plėtrą stabdo tai, kad nėra tinkamos teisinės bazės, reguliuojančios e. operacijas. Nors derinant vidaus įstatymus su tarptautiniais standartais ir žengta tam tikrų žingsnių, e. sandorių srityje Lietuva, palyginti su pasauliu, atsilieka pagal reikiamų teisės aktų priėmimą. Atsižvelgiant į teisės aktams, reguliuojantiems internetą ir elektronines operacijas, keliamus formalius reikalavimus, teisinė bazė turėtų būti suderinta su tarptautiniais standartais, be to, užtikrinta, kad naudojant e. parašą atliekamos skaitmeninės operacijos būtų įmanomos ir e. versle.

Tam, kad Lietuvoje saugiai gyvuotų ir kurtųsi naujos e. paslaugos, reikia išplėsti teisinį dokumentų autentifikavimo būdų pripažinimą (e. parašo arba kituose įstatymuose) numatyti mechanizmus, kaip nekvalifikuotais e. parašais ir kitomis autentifikavimo technologijomis pasirašyti dokumentai prilyginami rašytinei formai. Toks technologinis sprendimas didintų e. parašo plėtrą, suteikdamas vartotojams daugiau galimybių pasirašyti e. parašu, nes rašytinei formai prilyginamas tik kvalifikuotas e. parašo sertifikatas yra laikomas viena iš priežasčių, stabdančių efektyvią e. parašo plėtrą.

Siekiant teisiškai reglamentuoti e. parašą ir išlaikyti jį „patogiu“ e. verslo įrankiu, galima pritaikyti šiuo metu Europos Komisijos kuriamo atviro kodo taikomą programinės įrangos sprendimą. Jį išanalizavusi Europos Komisija pateikė išvadą, kad ši taikomoji programinė įranga bus diegiama ne lokaliai naudotojų kompiuteriuose, o tarnybinėse stotyse, suteikiant galimybę teikti e. parašo kūrimo, tikrinimo ir išplėtimo paslaugas internetu. Tai būtų tinkamas sprendimas e. versle plačiau naudoti e. parašą, tačiau pabrėžtina, kad visų pirma reikėtų įvertinti, ar Lietuvoje diegiant šią programinę įrangą būtų tenkinami visi teisiniai ir techniniai reikalavimai.

Lietuva pirmoji iš visų Baltijos valstybių pritaikė Vyriausybės informacinę elektroninio pasirašymo sistemą. Valstybių kaimynių – Latvijos ir Estijos – Vyriausybės savo veikloje e. parašu naudojasi ne taip aktyviai kaip Lietuvos Vyriausybė.

E. parašo reglamentavimas, remiantis Direktyvos reikalavimais, iš dalies suvienodino visų ES narių e. parašo įstatymus, tačiau šios technologijos plėtra skiriasi. Vienos šalys greičiau, kitos lėčiau prisitaiko prie technologinių naujovių. Estiją, palyginti su kitomis Baltijos valstybėmis, galime vadinti e. parašo infrastruktūros plėtros ir jo naudojimo pažangos lydere, tačiau technologijos greitai tobulėja ir keičiasi, taigi kiekviena šalis privalo nesustoti ir suteikti daugiau naudojimosi e. parašu galimybių.

Žinių įtvirtinimo klausimai

1. Kokios yra pagrindinės e. dokumentų ir e. sutarčių technologinės apsaugos priemonės?
2. Kokie yra e. parašo technologiniai veikimo principai?
3. Kokios yra e. parašo rūšys?
4. Kokiu būdu naudojami privatusis ir viešasis raktai pasirašant e. dokumentus ir e. sutartis?
5. Kokios yra svarbiausios laiko žymos funkcijos?
6. Kokia yra įrodomoji e. parašo ir laiko žymos vertė?

/VI/ *skyrius*

Teisiniai intelektinės nuosavybės elektroninėje erdvėje aspektai

/ 235–326 / *puslapiai*

1 skirsnis. Intelektinės nuosavybės elektroninėje erdvėje samprata

Intelektinė nuosavybė e. erdvėje arba elektroninės intelektinės nuosavybės objektai yra svarbiausia žinių visuomenės ir ekonomikos vertybė. Intelektinės nuosavybės objektai e. erdvėje sudaro daugumą elektroninės civilinės apyvartos objektų, tokių kaip kompiuterių programos (įskaitant operacines sistemas, žaidimus ir mobiliųjų įrenginių programas), duomenų bazės ir pavieniai duomenys, elektroninis garso ir vaizdo ar kūrybinis turinys (pvz., interneto tinklalapiai, elektroniniai garso ar vaizdo įrašai), nauji technologiniai sprendimai visose žmonių veiklos srityse (pvz., efektyvesnis duomenų perdavimo metodas tinklais ar skaitmeninė PET tomografija ligų diagnostikai).

Intelektinės nuosavybės teisės yra pagrindinis minėtųjų e. objektų teisinės apsaugos instrumentas, nustatantis teisinį jų naudojimo režimą.

E. turinio reguliavimą intelektinės nuosavybės teisės normomis lėmė e. objektų panašumas į tradicinius intelektinės nuosavybės teisių objektus.

Visus intelektinės nuosavybės teisių e. erdvėje objektus galima skirstyti į dvi dideles grupes:

1. **Tradiciniai intelektinės nuosavybės teisių objektai perkelti į elektroninę formą** (pvz., tradicinė knyga, išleista e. knygos formatu, arba analoginis garso ir vaizdo kūrinys, suskaitmenintas į realaus laiko garso ir vaizdo duomenų srautą);
2. **Išimtinai tik elektroniniai intelektinės nuosavybės teisių objektai**, kurie neturi analogiškų atitikmenų (pvz., kompiuterių programos arba kompiuteriniai 3D modeliai).

Sparčiai tobulėjant technologijoms, vyksta visuotinis žinių ir informacijos perkėlimas į e. erdvę (virsmas į e. formą).

Absoliuti naujų intelektinės nuosavybės objektų dauguma kuriama ir tvarkoma tik e. forma (pvz., nauji muzikos, kino ar fotografijos kūriniai).

Pagrindinė elektroninės intelektinės nuosavybės objektų civilinės apyvartos terpė yra kompiuterių tinklai ir internetas, kur kyla specifinių intelektinės nuosavybės apsaugos problemų.

Elektroninės intelektinės nuosavybės formos ir civilinės apyvartos terpės ypatumai lemia šio teisės instituto savitumą ir specialų reguliavimą. Intelektinės nuosavybės e. erdvėje reguliavimas yra neatsiejamas nuo tradicinės intelektinės nuosavybės reguliavimo ir jo ištakų. Principinės intelektinės nuosavybės teisės nuostatos yra taikomos ir reguliuojant intelektinės nuosavybės teises e. erdvėje.

Analizuojant intelektinės nuosavybės e. erdvėje institutą, vertinant ir tobulinant intelektinės nuosavybės teisių e. erdvėje reguliavimą, jį aiškinant ir užpildant spragas, kaip atskaitos taškas yra moderni intelektinės nuosavybės teisių doktrina.

Teisių nustatymas ir gynimas, pasitelkus valstybės institutus, nėra savitikslis, jis yra motyvuotas socialinės gerovės, kurią reprezentuoja atitinkamos teisės. Nuosavybės teisės istoriškai buvo suteikiamos atlyginant už indėlį į visuomenės galios ir socialinės bazės išplėtimą, siekiant efektyvaus išteklių valdymo, kultūrinio dominavimo ir pan. Šiuolaikinėje visuomenėje tam tikrų teisių turėjimas nustato ir atitinkamas pareigas: nuo bendrųjų – nepažeisti kitų teisių turėtojų teisių (derinti su kitų subjektų teisėmis), iki konkrečių – pvz., mokėti mokesčius nuo teisių objekto vertės.

Žinių visuomenėje nuosavybės teisių į intelektinę nuosavybę nustatymas ir apsauga yra paaiškinamos modernia intelektinės nuosavybės doktrina.

Pasitaiko atvejų, kai prisidengus intelektinės nuosavybės teisių absoliutumu, pažeidžiamumu ir pan. siekiama savanaudiškų tikslų, taip nulemiant ilgalaikę didelę žalą viešiesiems socialiniams interesams ir kitų asmenų subjektinėms teisėms. Viena iš spekuliacijos priežasčių – intelektinės nuosavybės žinių visuomenėje nesupratimas. Moderni intelektinės nuosavybės teisių doktrina turi būti atskaitos taškas vertinant naujas intelektinės nuosavybės teisių reguliavimo iniciatyvas, ypač atkreipiant dėmesį, ar jos nepažeis ilgalaikių visuomenės socialinės, ekonominės ir kultūrinės plėtros interesų.

Dominuojanti intelektinės nuosavybės teisių doktrina žinių visuomenėje yra epistemologinė, ji akcentuoja intelektinės nuosavybės teisės kaip žinių apsaugos nuo nusavinimo ir jų maksimalaus panaudojimo bendriesiems visuomenės tikslams mechanizmą. Minėtoji doktrina pabrėžia žinių prieinamumą (A2K[40]), jų svarbą ir būtinybę panaudoti naujiems kūriniams bei inovacijoms. Prie šios teorijos plėtros ypač prisidėjo prof. L. Lessigas, o ją praktikuoja atvirosios programinės įrangos ir visuomeniniai kūrybinių bendrijų judėjimai. Kai kurie kūrybinių bendrijų aspektai toliau nagrinėjami detaliau. Deja, Lietuvoje ši doktrina yra mažiausiai žinoma ir taikoma Lietuvos intelektinės nuosavybės teisėkūrai ir jurisprudencijai.

Kitose šalyse epistemologinė ir kita senesnioji ekonominė doktrinos daro didžiausią įtaką šiuolaikinei intelektinės nuosavybės teisėdarai, teisės taikymui ir teisės jurisprudencijai. Šios doktrinos yra išsamiausiai pagrįstos empiriniais tyrimais. Be minėtųjų doktrinų, egzistuoja ir kitos, tačiau dauguma jų nebeatitinka žinių visuomenės realijų, todėl atskirai nenagrinėjamos.

---

[40] Žinių prieinamumas anglų kalba dažnai žymimas santrumpa A2K *(Access to Knowledge)*. Šios idėjos pagrindu susiformavo ir aktyviai veikia visuomenis A2K judėjimas. Prieiga per internetą: <http://en.wikipedia.org/wiki/Access_to_Knowledge_movement>.

Ekonominė (utilitarinė) doktrina labiausiai buvo paplitusi laikotarpiu prieš informacinę visuomenę ir savo reikšmės iki šiol nėra praradusi. Jos esmė – intelektinės nuosavybės teisinė apsauga yra būtina ekonominė paskata visuomenės gerovei kilti, nes ji skatina kūrybiškumą ir inovacijas visos visuomenės labui, t. y. intelektinės nuosavybės teisės yra ekonominis atlygis (taip pat ir paskata) kūrybai ir inovacijai. Ekonominė doktrina grindžiama prielaida, kad intelektinė nuosavybė laisvosios rinkos sąlygomis (jos specialiai nesaugant) iš esmės negali būti civilinės apyvartos objektas, nes ji būtų nesąžiningai pasisavinama, platinama ir naudojama, todėl, nustatant intelektinės nuosavybės teises, reikalingas valstybės įsikišimas.

Epistemologinės doktrinos esmė – intelektinės nuosavybės teisinė apsauga turi būti ribota, nes būtina užtikrinti jos (informacijos ir žinių) sklaidą dėl visuomenės kultūrinės ir technologinės pažangos. Anot epistemologinės doktrinos, intelektinės nuosavybės sistemos turi užtikrinti, kad:

- visuotinai prieinama informacija nebūtų nesąžiningai pasisavinama (pasitelkiant nuosavybės, prievolines teises ar techninės apsaugos priemones);
- intelektinė nuosavybė numatytų adekvačių išimčių – objekto, galiojimo laiko ir nekomercinio naudojimo prasme;
- intelektinės nuosavybės teisės būtų suteikiamos tik atlyginant už kūrybą ir inovacijas bei suteikiant maksimalias galimybes pačiam autoriui ir (ar) inovatoriui disponuoti savo teisėmis be tarpininkų pagalbos.

Intelektinės nuosavybės ribojimas turi būti įgyvendinamas trimis kryptimis – ribojant saugomus objektus (pvz., nesuteikiant apsaugos idėjoms), nustatant teisių ribojimą laiku (pvz., maksimalų teisių apsaugos terminą) ir specialias intelektinės nuosavybės teisių naudotojų (visuomenės) teises (intelektinės nuosavybės teisių išimtis ar apribojimus).

Epistemologinė teorija kaip svarbiausią intelektinės nuosavybės apsaugos sąlygą pabrėžia šios nuosavybės saugomos informacijos prieinamumą visuomenei ir naujai kūrybai ir (ar) inovacijoms. Intelektinės nuosavybės sistema turi skatinti informacijos atskleidimą ir sklaidą bei maksimaliai plėsti informacijos, prieinamos visuomenei, apimtį.

Kai kuriuos epistemologinės doktrinos aspektus praktiškai įgyvendina atvirosios programinės įrangos judėjimas (angl. *Open Source Software movement)*. Šio judėjimo pradininkai yra L. Torvaldsas ir R. Stallmanas, jie sukūrė *Linux* operacinę sistemą ir atvirąją licenciją, kurioje autorių teisės į programinės įrangos kodą naudojamos kaip programinio kodo „laisvės“ (nepriklausymo konkrečiam subjektui) priemonė. R. Stallmanas išpopuliarino *GNU* bendrąją viešąją licenciją (angl. *General Public Licence, GNU)*,

skirtą sukurti aplinkai, kurioje laisvai, be atlygio ir įprastinių nuosavybės teisių keliamų suvaržymų, galima dalytis inovacijomis. Taigi galima sakyti, kad intelektinės nuosavybės teisės vykstant atvirosios programinės įrangos judėjimui yra naudojamos ne ekonominei naudai gauti, bet siekiant plėtoti bendrąją kultūrą. Pastaraisiais metais Atvirosios programinės įrangos judėjimo filosofija buvo išplėsta ir kitoms e. kūrybos formoms, siekiant laisvo jų apsikeitimo, be to, atsirado ir išplito kūrybinių bendrijų *(Creative Commons, www.creativecommons.com)* iniciatyva, kuri siekia valdyti intelektinės nuosavybės teises taip, kad būtų užtikrintas laisvas arba labai paprastas priėjimas prie intelektinės nuosavybės teisėmis saugomos informacijos.

Nors istoriškai intelektinės nuosavybės teisių institutas nuolat kinta (keičiasi ir objektas, ir subjektinės teisės, ir teisių subjektai, ir teisių apribojimai), tai atspindi ir pats intelektinės nuosavybės e. erdvėje institutas, o bendrieji intelektinės nuosavybės instituto socialiniai tikslai – užtikrinti visuomenės technologinę ir kultūrinę raidą – iš esmės lieka nepakitę.

Reikėtų pabrėžti, kad dėl ypač sparčios technologinės pažangos teisinis intelektinės nuosavybės teisių reguliavimas gerokai atsilieka nuo technologinių iššūkių, todėl tik modernios doktrinos ir intelektinės nuosavybės socialinių tikslų suvokimas bei jų tiesioginis taikymas gali užpildyti reguliavimo spragas.

Nukrypstant nuo intelektinės nuosavybės teisių socialinių tikslų arba juos interpretuojant neteisingai (pvz., teikiant prioritetą ekonominiams autorių teisių turėtojų interesams), visuomenei gresia kultūrinė ir technologinė stagnacija.

Deja, Lietuvoje gausu atvejų, kai įstatymų leidėjas ar teismai prioritetą teikia siauriems ekonominių tarpininkų, o ne visuomenės ar autorių ir (ar) išradėjų interesams. Tai lemia didelė intelektinės nuosavybės teisių koncentracija šiuolaikinėje visuomenėje, ypač teisių į garso ir vaizdo kūrinius, kompiuterių programas, muzikos įrašus srityse. Teisių turėtojai, kurie dažniausiai yra ekonominiai tarpininkai tarp autoriaus ir vartotojo (visuomenės) ar antstatinės organizacijos (pvz., kolektyvinio administravimo asociacijos), neatsižvelgdamos į visuomenės ir autorių interesus, siekia be saiko didinti pelną ir pajamas iš intelektinės nuosavybės teisių. Tokių teisių turėtojų tikslas – ne visuomenės pažanga, o absoliučios ir neriboto galiojimo intelektinės nuosavybės teisės, leidžiančios nedidelei subjektų grupei uždirbti monopolinius pelnus. Siekiant šio tikslo, iš esmės spekuliuojama intelektinės nuosavybės teisių išimtinumu, pažeidžiamumu, autorių gynimu, net atvirai falsifikuojami autorių teisių pažeidimų duomenys, finansuojamos plačių užmojų lobistinės kampanijos. Per pastaruosius du dešimtmečius, prisidengus autorių ir išradėjų gynimu bei intelektinės

nuosavybės teisių prioritetu, taip pat naudojantis įstatymų leidėjų ir teismų intelektinės nuosavybės instituto žinių trūkumu, intelektinės nuosavybės teisėdara ir teisės aiškinimas aiškiai pakrypo visuomenės interesams priešinga linkme – pvz., autorių teisių termino pratęsimas visuomenei ir autoriams neatnešė jokios naudos, tačiau užkirto kelią kultūros ir švietimo plėtrai bei užtikrino tik teisių turėtojų ekonomines pajamas iš kūrinių, prie kurių sukūrimo jie visiškai neprisidėjo. Tai geriausiai parodo J. Joyce'o („Uliso" autoriaus, mirusio dar 1941 m.) autorių teisių atvejis Airijoje, kai dėl teisių galiojimo pratęsimo 1998 m. jų turėtojai sustabdė valstybinę J. Joyce'o jubiliejaus šventę, viešus kūrinių skaitymus ir t. t. Galiausiai prireikė specialaus Airijos įstatymų leidėjo įsikišimo, kuris ir vėl apribojo autorių teises. Minėtųjų teisių išimčių ribojimas, besąlygiška techninių priemonių apsauga, laikmenų ir įrangos mokesčiai gerokai pabrangino ir suvaržė viešąją prieigą prie kūrinių ir techninės informacijos (ypač viešosiose bibliotekose ir universitetuose), apmokestino vartotojus, kurie apskritai nesinaudoja intelektinės nuosavybės teisėmis. Atkreiptinas dėmesys ir į tai, kad teismų praktikoje kaip argumentai įsitvirtina abstrakčios intelektinės nuosavybės teisių pažeidžiamumo ir išimtinumo (prioriteto teisių turėtojams) kategorijos, nepagrįstos nei įrodymais, nei įstatymu, nei doktrina (žr. pvz., civilinėje byloje *LATGAA v. „Trajektorija"* (3K-3-4/2008) teismas, aiškindamas ATGTĮ 78 str. 3 d. numatytą galimybę kolektyvinio administravimo asociacijoms priteisti didesnį žalos atlyginimą, argumentavo, kad „įstatymo leidėjas, nustatydamas atsakingai asociacijai teisę į ATGTĮ 78 straipsnio 3 d. tris kartus didesnį atlyginimą, siekė suteikti galimybę kuo veiksmingiau ginti pažeistas autoriaus teises, atsižvelgdamas į autorių teisių specifiką ir jų didelį pažeidžiamumą)".

Visa tai rodo, kad įstatymų leidėjams ir teismams yra nežinoma ar menkai žinoma šiuolaikinė intelektinės nuosavybės doktrina.

Mokslinėje literatūroje galima identifikuoti keletą skirtingų intelektinės nuosavybės sampratų, kuriose ši traktuojama kaip:

Objektinis supratimas	objektyvia forma išreikšta nauja informacija (kūryba ar techninė inovacija) nematerialioji vertybė intelektinio darbo rezultatas
Subjektyvus supratimas	išimtinės asmens teisės į jo intelektinės veiklos rezultatą, autoriaus santykis su kūrybos rezultatu ir interesas į jį
Socialinės funkcijos supratimas	kūrybos ir inovacinių procesų žaliava ir elementas

Objektyviąja prasme intelektinė nuosavybė yra žmogaus intelektinio darbo rezultatas – suvoktos ir išreikštos jo mintys. Abstrahuojant šią nuostatą, galima teigti, kad intelektinė nuosavybė – žmogaus sukurta informacija, atliekanti estetinę, intelektinę, techninę ar kitokią funkciją. Nors funkcinis (racionalios paskirties) reikalavimas intelektinei nuosavybei formaliai nekeliamas, jį lemia žmogaus intelekto, intelektinės veiklos ir žmogiškosios komunikacijos (minčių išraiškos) sąvybės. Paprastai suvokiama ir išreiškiama būtent ta informacija, kuri atlieka vienokią ar kitokią funkciją, arba, kitaip tariant, informacija apskritai neatsiejama nuo funkcijos, nes priešingu atveju ji tėra tik triukšmas ar trukdžiai. Apibendrintai galima teigti, kad intelektinė nuosavybė kaip objektas – bet kokia žmonėms ar techniniams įrenginiams suprantama ir vertinga informacija.

Tam, kad informacija (intelektinė nuosavybė) būtų ekonomiškai ir socialiai naudinga, ji turi būti žinoma ir naudojama. Informacija gali būti naudojama keliais būdais: vartotojams – per naujus produktus, procesus, paslaugas (vartojimą) ir švietimą; ūkio subjektams – naujiems produktų procesams ir paslaugoms kurti bei kaip tolesnių inovacijų pagrindas. Būtina tokio informacijos naudojimo sąlyga – ji turi būti vieša ir viešai prieinama. Kita vertus, tolesnės investicijos ir ekonominės naudos gavimas iš informacijos reikalauja, kad jos atžvilgiu būtų įtvirtintos subjektyvinės teisės ir informacija būtų subrandinta bei paversta praktinėmis inovacijomis.

Dar viena informaciją ir intelektinę nuosavybę iš kitų socialinių vertybių išskirianti ypatybė – informacija yra viešoji vertybė tiesiogine techine prasme, t. y. vieno asmens naudojimasis informacija nekliudo kam nors kitam tuo pat metu naudotis ta pačia informacija, be to, toks papildomas naudojimasis iš esmės nereikalauja papildomų išteklių ar išlaidų (išskyrus pridėtines platinimo išlaidas, kurios e. erdvėje iš esmės yra artimos nuliui). Kitais žodžiais tariant, informacijos naudojimas yra nekonkuruojantis, be to, labai sudėtinga apsisaugoti nuo neteisėtų viešai platinamos informacijos vartotojų.

Subjektyviąja prasme intelektinė nuosavybė – tai kompleksas išimtinių subjektyvinių teisių, leidžiančių kontroliuoti informacijos (intelektinės nuosavybės objektyviąja prasme) naudojimą. Teisės moksle dominuoja intelektinės nuosavybės supratimas subjektyviąja prasme. Teisėje intelektinę nuosavybę įprasta apibrėžti remiantis įvairiomis subjektyvinėmis teisėmis, įtvirtintomis įstatymuose, pvz., patentais, autorių teisėmis, gretutinėmis teisėmis, prekės ženklais, dizainu ir t. t. Tokį požiūrį įtvirtina dauguma tarptautinių teisinių dokumentų dėl intelektinės nuosavybės. Absoliuti dauguma nacionalinių, regioninių ir tarptautinių teisės aktų reglamentuoja būtent subjektyvines intelektinės nuosavybės teises.

Mikroekonominiu ar vadybos požiūriu intelektinės nuosavybės teisės gali būti suvokiamos kaip ekonominės skatinimo sistemos, taikomos moderniose kapitalistinėse visuomenėse ir skirtos inovatyvių produktų ar paslaugų apsaugai nuo kopijavimo, neinovatyvios konkurencijos ar piratavimo. Intelektinė nuosavybė, suteikdama teisinėmis priemonėmis užtikrinamas monopolines teises tiems, kurie gamina kūrybinius ir intelektualinius produktus, kartu sukuria ir paskatas įsitraukti į tokią veiklą bei užtikrina investicijų į kūrybinę ir intelektualinę veiklą saugumą. Kuriant ir parduodant naujus produktus bei paslaugas pasaulinėse rinkose, ypač svarbu, kad inovatyvios žinos ir idėjos bei investicijos į jas būtų pakankamai apsaugotos. Taigi šia prasme intelektinė nuosavybė yra dirbtinė socialinė ir teisinė kliūtis, sukurta tam, kad žinių rinka galėtų būti apsaugota ir leistų kūrėjui ar inovatoriui gauti tam tikro monopolinio pelno, kuris konkurencinėje rinkoje negalėtų būti prieinamas be minėtosios kliūties. Dauguma intelektinės nuosavybės sistemų kūrėjui ir (ar) inovatoriui ribotam laikotarpiui suteikia išskirtines monopolines teises į jo ar jos kūrinį ir apibrėžia veiklą, kuriai vykdyti reikia gauti teisių turėtojo leidimą. Būtina pabrėžti, kad ekonomine prasme intelektinės nuosavybės teisės iš esmės yra negatyvios, nes jos suteikia teisę užkirsti kelią kitiems asmenims neleistinai naudotis saugomu objektu. Be to, ekonominiu požiūriu intelektinė nuosavybė yra asmeninė ir su ja savininkas gali elgtis taip pat, kaip ir su kitomis nuosavybės formomis, įskaitant pardavimą, perdavimą ar licencijavimą.

Absoliuti inovacijų modelių dauguma remiasi prielaida, kad ekonominė ir kultūrinė raida priklauso nuo mokslinių ir technologinių žinių tobulinimo, kuris skatina inovacijų plėtrą, o vėliau – ir tolesnį ekonomikos kilimą. Intelektinės nuosavybės vaidmuo – užtikrinti informacijos daugėjimą, sklaidą ir gynimą visuomenėje, todėl ji tiesiogiai susijusi su technologine pažanga ir ekonomikos kilimu. Intelektinė nuosavybė, nors ir ne vienintelis, bet labiausiai paplitęs socialinis mechanizmas, taikomas socialiai valdant informaciją. Ji įsiterpia į informacijos kaupimo, sklaidos ir vartojimo procesus, todėl yra viena iš paskatų kurti naują informaciją arba kliūtis ją vartoti. Epistemologiniu požiūriu principinis intelektinės nuosavybės poveikis informacijai yra tas, kad kūrėjai laisvosios rinkos sąlygomis tikisi iš informacijos, ginamos intelektinės nuosavybės teisėmis, gauti didesnį pelną. Intelektinė nuosavybė skatina investicijas ir pastangas kurti naują informaciją, be to, mažina individualių investicijų riziką. Šis intelektinės nuosavybės vaidmuo yra esminis norint ją suprasti. Idealiai intelektinės nuosavybės sistemos turi būti orientuotos į naujos informacijos kūrimo skatinimą, tačiau tuo pat metu užtikrinti pakankamą prieigą prie esamos informacijos.

Nagrinėjant intelektinę nuosavybę, svarbus bendras informacijos, taip pat ir intelektinės nuosavybės, socialinių ir ekonominių požymių supratimas. Svarbiausi intelektinės nuosavybės socialiniai ir ekonominiai požymiai yra šie:

1) **viešumas** (išskyrus komercines paslaptis) – intelektinės nuosavybės saugomos informacijos viešumas yra būtina intelektinės nuosavybės teisių gavimo sąlyga. Viešumo reikalavimas gali būti tiek tiesioginis (patentai, prekės ženklai), tiek netiesioginis (pvz., autorių teisėmis ginama infromacija turi būti objektyviai išreikšta). Viešumas būtinas tam, kad vartotojai, valdžios atstovai ir konkurentai žinotų, į ką reiškiamos nuosavybės teisės, o tam tikrais atvejais dar ir tam, kad būtų įvertinta, ar saugomas objektas atitinka privalomus intelektinės nuosavybės apsaugos kriterijus (pvz., naujumas patentų atveju, originalumas saugant autorių teisėmis ar draudimas išduoti prekių ženklus bendriniams žodžiams, vaizdams ir t. t.). Be to, viešumas užtikrina, kad informacija, saugoma intelektinės nuosavybės teisėmis, bus žinoma net ir tada, kai nustos galioti intelektinės nuosavybės teisės ir ją bus galima naudoti kaip tolesnės kūrybos ir inovacijų pagrindą. Kita vertus, kartais tinkamiausia infromacijos apsaugos priemonė yra slaptumas, nes visos informacijos, kuri yra atskleista ir į ją pareikštos intelektinės nuosavybės teisės, neįmanoma apginti. Rinktis slaptumą tinka tik tada, kai saugoma informacija negali būti lengvai atskleidžiama ir nėra akivaizdžiai susijusi su produktu ar paslauga, kuriuos numatoma platinti viešai, ir tokią informaciją labai sudėtinga ar brangu savarankiškai sukurti. Komercinės paslaptys yra tinkamos kalbant apie specifinę, paslaptimi laikomą informaciją (pvz., kokakolos receptūrą), tačiau jos nepadės efektyviai apsisaugoti nuo reversinės galutinio produkto inžinerijos, kai patentai, kuriais saugomų išradimų požymiai yra vieši, efektyviai užkerta kelią naudotis informacija, gauta reversinės inžinerijos būdu;
2) **nekonkurentiškumas**: ekonomine prasme intelektinės nuosavybės nekonkurentiškumas reiškia, kad intelektualinių produktų pateikimo papildomam vartotojui pridėtinės išlaidos yra artimos nuliui. Iš esmės neribotas vartotojų skaičius vienu metu gali naudotis intelektine nuosavybe, vieni kitiems nekliudydami ir neskatindami papildomų išlaidų (kurios yra būtinos materialinių vertybių atveju, nes kiekvienam naujam vartotojui reikalingas atskiras egzempliorius, pateikimo išlaidos ir pan.). Intelektinė nuosavybė yra absoliučiai privaloma, kad būtų sukurta ir išlaikyta veikianti nematerialiųjų intelektualinių produktų, kurie pasižymi nekonkurentiškumu,

rinka. Kita vertus, nekonkurentiškumas leidžia po pradinių investicijų iš informacijos gauti didžiausią ekonominę naudą, jeigu ši, be abejonės, atitinka rinkos poreikius;

3) **ribotos monopolistinės teisės**: ribotos laiko ir apimties (teisių naudojimo ir išimčių prasme); galiojant intelektinės nuosavybės teisėms, teisiniai, sutartiniai ir techniniai mechanizmai užtikrina, kad šių teisių savininkai turi galią kontroliuoti informacijos, ginamos intelektinės nuosavybės teisėmis, naudojimą. Šis požymis iš dalies prieštarauja intelektinės nuosavybės viešumo požymiui, nes šios nuosavybės teisių galiojimo metu yra ribojamas priėjimas prie intelektinę nuosavybę sudarančios informacijos (pvz., prieiga suteikiama tik už tam tikrą licencinį mokestį) ir laisvas jos naudojimas. Nors monopolis iš esmės yra neigiamas intelektinės nuosavybės padarinys, jis yra šioje nuosavybėje glūdinčio kūrybos ir inovacijų skatinimo mechanizmo šerdis;
4) **konkurencingumas ir veiksmingumas** ta prasme, kad intelektinės nuosavybės rinkos vertė ir rinkos poveikis yra tiesiogiai susietas su jos socialine verte ir socialiniais poreikiais; kūrėjai ir inovatoriai, spręsdami, į ką investuoti bei ką kurti, iš esmės gali palyginti potencialių investicijų išlaidas ir socialinę vertę, kurią jomis sukurs. Taip skatinama savo kūrybinį ir inovacinį potencialą investuoti į tas sritis, kurios kuria didžiausią socialinę vertę. Be to, laisvosios rinkos sąlygomis intelektinės nuosavybės vartotojai savanoriškai ir savarankiškai pasirenka intelektinę nuosavybę, kuria jie nori naudotis, ir savo nuožiūra sprendžia, ar ji sukurs jiems pageidaujamą socialinę vertę. Investicijos į intelektinę nuosavybę turi būti efektyvios, nes tuo atveju, jeigu gautas intelektualinis produktas neturės socialinės paklausos, investuotojas (kūrėjas ar inovatorius) patirs reikšmingą nuostolį, neatsižvelgiant į intelektinės nuosavybės teises. Paminėtina, kad dėl didelės intelektinės nuosavybės teisių koncentracijos ir natūralios monopolijos iš esmės įgyjama galia primesti vartotojams savo intelektinės nuosavybės pasirinkimą už monopolistui (o ne vartotojui) priimtiną kainą. Tokia padėtis pastaruoju metu tampa vienu svarbiausių intelektinės nuosavybės kritikos atspirties taškų. Atskirai paminėtina ir tai, kad intelektinė nuosavybė yra akivaizdžiai nepakankama inovacijų diegimo paskata į tas socialines sritis, kur tikėtina socialinė vertė yra menka (pvz., nors maliarija besivystančiame pasaulyje yra viena labiausiai paplitusių mirtinų ligų, išsivysčiusiose šalyse į minėtosios ligos ir jos gydymo metodų tyrimus investuojama labai mažai, nes nesitikima gauti pelno iš vaistų nuo maliarijos pardavimo trečiojo pasaulio šalyse, o išsivysčiusio

pasaulio šalyse tokiems vaistams nėra rinkos). Vien jau tai lemia, kad intelektinė nuosavybė valstybės politikoje turi būti derinama su kitais kūrybos ir inovacijų skatinimo mechanizmais.

Formaliąja prasme intelektinė nuosavybė dažniausiai suprantama tiesiog kaip subjektyvių asmeninės nuosavybės teisių forma. Toks intelektinės nuosavybės supratimas koncentruojasi į teises, suteikiamas autoriams už jų kūrybinių ar intelektualinių pastangų rezultatus. Teisiniame kontekste nuosavybė apibrėžia ne konkretų objektą, o asmens ir objekto santykius, be to, intelektinė nuosavybė suteikia savininkui teises, kurios gali būti įgyvendinamos per santykį su jo ar jos kūrybinės ar intelektualinės veiklos rezultatu, ir leidžia kontroliuoti, kaip kiti asmenys naudos atitinkamą kūrybinės ar intelektualinės veiklos rezultatą.

Apibendrinant išdėstytas mintis, intelektinė nuosavybė suprastina kaip kompleksinis socialinis ir teisinis institutas, skirtas naujos vertingos informacijos (intelektinės nuosavybės objekto) kūrybai, apsikeitimui ir civilinei apyvartai reguliuoti, užtikrinant kūrėjų, teisių turėtojų ir visuomenės interesų balansą.

Iš daugelio šiuolaikinės intelektinės nuosavybės teisių tik dvi, seniausios, tradicinės ir pripažįstamos tarptautiniu mastu, yra betarpiškai susijusios su naujos informacijos kūrimu – autorių teisės ir patentai. Be to, atsižvelgiant į Lietuvos teisės sistemos specifiką, reikėtų pabrėžti, kad su kūryba ir inovacijomis glaudžiai susijusios gretutinės ir pramoninio dizaino teisės, kurios daugelyje užsienio valstybių nėra išskiriamos kaip atskiri institutai (pvz., daugelyje bendrosios teisės tradicijos valstybių autorių teisės apima ir tai, ką mes Lietuvoje suprantame kaip gretutines teises, o pramoninis dizainas laikomas viena iš patentų rūšių). Likusios intelektinės nuosavybės teisės, tokios kaip prekių ženklai, firmų pavadinimai, geografinės nuorodos ir t. t., iš esmės yra subjekto, prekės ar paslaugos diferencijavimo instrumentai, o ne kūrybos ir inovacijų plėtros socialiniai ir teisiniai mechanizmai. Dėl šios priežasties autorių teisėms ir patentams turi būti teikiamas prioritetas prieš kitas intelektinės nuosavybės formas, pvz., neregistruojamos autorių teisės į anksčiau sukurtą kūrinį yra viršesnės už oficialiai įregistruotą prekės ženklą (kuriam panaudota ankstesnio kūrinio elementų). Ir autorių, ir patentų teisių faktinis lygis (registracijos ir gynimas) parodo ir konkrečios visuomenės ar valstybės kūrybiškumo ir inovatyvumo lygį. Pabrėžtina ir tai, kad intelektinės nuosavybės grupavimas į šias dvi grupes (prišliejant artimas teises) iki šiol yra plačiausiai pripažįstama intelektinės nuosavybės klasifikacija.

Kaip jau minėta, ne visa informacija gali būti intelektinės nuosavybės objektas. Tam tikra informacija, kuri nėra žmogaus mąstymo rezultatas, net

jeigu jai gauti ir įdėta intelektinių pastangų, nelaikoma intelektine nuosavybe. Tai ypač aktualu bendrojo fundamentalaus pobūdžio informacijai – atradimams ar idėjoms (nesant techninio įgyvendinimo), informacijai apie gamtos dėsnius ir pan., net jeigu ji yra visiškai nauja. Neišreikšta ar numanoma informacija irgi nelaikytina intelektinės nuosavybės objektu, nes ji neturi jokios socialinės vertės.

2 skirsnis. Teisinė intelektinės nuosavybės elektroninėje erdvėje sąvoka

Tradiciškai teisės moksle intelektinė nuosavybė apibūdinama kaip kompleksas ribotų išimtinių subjektinių teisių į intelektinės ir kūrybinės veiklos rezultatus, išreikštus objektyvia forma. Intelektinės nuosavybės, kaip ir nuosavybės apskritai, teisė jos turėtojui leidžia savarankiškai nulemti kūrybinės ir intelektinės veiklos rezultato likimą, naudoti jį išimtinai savo nuožiūra, ginti savo teises nuo trečiųjų asmenų, kontroliuoti kūrinio naudojimą ir gauti atlyginimą už trečiųjų asmenų naudojimąsi kūrybinės ir intelektinės veiklos rezultatu, taip skatinant kūrybingumą, inovacijas, intelektinį indėlį ir už tai atlyginant. Atkreiptinas dėmesys, kad greta minėtųjų teisių, kurios iš esmės yra turtinės, intelektinės nuosavybės kūrėjai turi ir ypatingų neturtinių (moralinių) teisių, neatskiriamų nuo paties kūrėjo asmenybės.

Intelektinės nuosavybės teisė, panašiai kaip ir teisė į nuosavybę, nėra ir negali būti absoliuti. Siekiant suderinti visuomenės ir kūrėjo interesus, būtini intelektinės nuosavybės teisių apribojimai šiais požiūriais: objekto, termino, subjektyvinių teisių apimties (išimčių) ir teritorijos. Intelektinė nuosavybė tradiciškai saugo tik išreikštą vertingą informaciją (sukurtus originalius kūrinius ar naujas idėjų technines implementacijas), tačiau nesaugo pačių idėjų, principų, gamtos dėsnių (pvz., nesaugoma dailininko paveikslo idėja, nes paties paveikslo dar nėra, ir kiekvienas dailininkas tą pačią idėją (pvz., peizažą) gali išreikšti labai individualiai ir originaliai, taip pat nesaugomi termobranduolinės sintezės dėsniai ar galaktikos struktūros teorija, nes ši informacija nepriklauso nuo žmogaus intelekto ir tėra atrandama, o ne sukuriama). Intelektinės nuosavybės teisių (autorių teisių, patentų) galiojimas yra apribotas laiko, suvaržytas nekomercinio pobūdžio išimčių, be to, dažnai priklauso nuo nacionalinių teisės aktų. Intelektinės nuosavybės ribotumas yra labai svarbus pamatinis intelektinės nuosavybės principas, nustatytas siekiant viešojo intereso, kurio tikslas – pakartotinis žinių naudojimas užtikrinant kultūrinę ir techninę pažangą, t. y. būtinybę intelektinę nuosavybę naudoti švietimui, naujai kūrybai ir inovacijoms. Jeigu intelektinės nuosavybės teisės būtų išplėstos daugiau nei reikia

kūrybai skatinti ir atlyginti už intelektinį bei finansinį indėlį, tai suteiktų galimybių intelektinės nuosavybės teisių turėtojams pasipelnyti visuomenės sąskaita, darytų neigiamą poveikį naujai kūrybai ir inovacijoms. Intelektinės nuosavybės teisių turėtojų ekonominis interesas – gauti didžiausią naudą iš turimų intelektinės nuosavybės teisių – nėra tinkamas pateisinimas intelektinės nuosavybės teisėms išplėsti (ypač teisių galiojimo terminui ilginti ir išimtims apriboti), nes jis nesuderinamas su viešuoju interesu – skatinti naują kūrybą ir inovacijas, užtikrinti informacijos prieinamumą mokymo ir švietimo tikslams.

Intelektinės nuosavybės teisinės sąvokos ir reglamentavimo principai formuluojami tarptautiniuose žmogaus teisių ir laisvių dokumentuose, pvz., Visuotinės žmogaus teisių deklaracijos 27 str. teigiama: „kiekvienas žmogus turi teisę laisvai dalyvauti visuomenės kultūriniame gyvenime, gėrėtis menu, dalyvauti mokslinėje pažangoje ir naudotis jos gėrybėmis; kiekvienas žmogus turi teisę į jo dvasinių ir materialinių interesų apsaugą, atsirandančių ryšium su mokslo, literatūros ar meno kūrinių, kurių jis yra autorius, sukūrimu“. Intelektinė nuosavybė ir būtinybė ją saugoti pripažįstama ir daugelio valstybių konstitucijose – pradedant 1787 m. JAV Konstitucija. 1992 m. Lietuvos Respublikos Konstitucijos 42 str. nuostatos padeda intelektinės nuosavybės apsaugos pamatus, jos deklaruoja, kad „Dvasinius ir materialinius autoriaus interesus, susijusius su mokslo, technikos, kultūros ir meno kūryba, saugo ir gina įstatymas“.

Teisėje įprasta intelektinę nuosavybę apibrėžti remiantis įvairiomis subjektyvinėmis teisėmis, įtvirtintomis įstatymuose, pvz., patentais, autorių ir gretutinėmis teisėmis, prekių ženklais, dizainu ir t. t. Absoliuti nacionalinių, regioninių ir tarptautinių teisės aktų dauguma reglamentuoja būtent subjektyvines intelektinės nuosavybės teises. Būtent tas, kurios laikomos intelektinės nuosavybės teisėmis, išvardija 1967 m. Pasaulinės intelektinės nuosavybės organizacijos (WIPO) steigiamosios konvencijos 2 str. nuostatos, jose teigiama, kad intelektinės nuosavybės teisės apima teises, susijusias su:

- literatūros, meno ir mokslo kūriniais;
- vaidybine artistų veikla, fonogramų įrašais, radijo ir televizijos laidomis;
- visų žmogaus veiklos sričių išradimais;
- mokslo atradimais;
- pramoniniais pavyzdžiais (pramoniniu dizainu);
- prekių ir paslaugų ženklais, firmų pavadinimais ir kitais komerciniais žymenimis;
- apsauga nuo nesąžiningos konkurencijos;

- kitas panašaus pobūdžio teises, kylančias iš intelektinės veiklos pramonės, mokslo, literatūros ar meno srityse.

Atsižvelgiant į intelektinės nuosavybės tendencijas, intelektinės nuosavybės e. erdvėje institutas taip pat apima teises, susijusias su:

- konfidencialia informacija;
- naudingais modeliais (mažaisiais arba inovaciniais patentais);
- kompiuterių programomis;
- duomenų bazėmis;
- puslaidininkinių gaminių topografijomis;
- teisine mikroorganizmų apsauga;
- techninės apsaugos priemonėmis;
- domenų vardais.

Aukščiau minėtosios intelektinės nuosavybės teisės iš esmės yra skirtingi institutai, kurie atskirai plėtojosi ir buvo skirti ne tiems patiems tikslams, vadovaujasi skirtingomis taisyklėmis ir remiasi nevienodais principais. Dauguma šių teisių yra sukurtos ne tam, kad skatintų kūrybą ar inovacijas, o veikiau tam, kad taptų verslo, produktų ar paslaugų diferencijavimo priemonėmis.

Svarbiausias bendras visų intelektinės nuosavybės sistemų požymis, kuris pagrindžia jų grupavimą į vieną apibrėžimą – bendrąja prasme intelektinės nuosavybės teisės orientuotos į kūrybines, intelektualines ar administracines pastangas kurti naujus produktus, procesus, dizainą ir medžiagas, kūrybinio proceso rezultatų platinimą ir rinkodarą.

Aukščiau minėtosios intelektinės nuosavybės teisės irgi skirstomos į stambesnes grupes – pagal jau minėtą visuotinai paplitusį intelektinės nuosavybės skirstymą į dvi dideles dalis:

- literatūros, meno ir mokslo kūrinius – autorių teisių ir gretutinių teisių objektus (daugiau estetinius, neatliekančius aiškios racionalios funkcijos);
- pramoninę nuosavybę – patentus, prekių ženklus, pramoninį dizainą ir t. t. (daugiau racionalios ir utilitarinės paskirties objektus).

Kai kurios intelektinės nuosavybės teisės (autorių ir gretutinės teisės, geografinės nuorodos) atsiranda savaime, nesant ypatingų autoriaus ar teisių įgijėjo pastangų, tačiau svarbiausios pramoninės nuosavybės teisės suteikiamos tik atlikus tam tikras registravimo ir ekspertizės procedūras. Šie formalumai taikomi patentams, prekių ženklams, pramoniniam dizainui ir kt. Jokių formalumų ir registracijos nereikalauja autorių ir gretutinės teisės, konfidenciali informacija. Tam, kad būtų galima naudotis teise į geografinę nuorodą, pakanka tik fizižkai turėti verslą ir gaminti prekes ar

teikti paslaugas apibrėžtame geografiniame regione. Norint įsigyti patentą (iš dalies ir prekės ženklą ar pramoninį dizainą), būtina pateikti nustatytos formos paraišką, nurodant patentuojamojo išradimo požymius, kuriais jis skiriasi nuo technikos lygio, ir sumokėti patento registracijos mokesčius, o patentas išduodamas tik atlikus formalią arba esminę išradimo požymių ekspertizę. Siekiant įvertinti, ar išradimas atitinka galimybės patentuoti reikalavimus, patento požymius privalo įvertinti atitinkamos technikos srities ekspertas. Paminėtina, kad dėl sudėtingos ekspertizės ar pareikštinėse sistemose nustatytų privalomų paraiškos paskelbimo terminų patento išdavimas (arba atsisakymas jį išduoti) dažniausiai užtrunka keletą metų. Kitas esminis pramoninės nuosavybės požymis – nacionalinis pobūdis. Patentas ar prekės ženklas, išduotas vienoje valstybėje, savaime negalioja kitose. Siekiant sukurti tarptautinius patentus, net ir pagal naujausius tarptautinius susitarimus yra būtinos specialios nacionalinės procedūros. Be to, pramoninės nuosavybės (ypač patentų) teisių įgijimas ir išlaikymas yra gana brangus – daugelyje valstybių būtina mokėti ir patentinės paraiškos, ir patento galiojimo metinius mokesčius (kurie didėja per patento galiojimo laikotarpį), net neįskaitant paraiškos vertimo ir mokesčių patentiniams patikėtiniams (jeigu norima, kad patentas galiotų užsienio valstybėse). Siekiant įsigyti patento teises, patentinio patikėtinio paslaugos iš esmės yra būtinos, nes išimtinių teisių apimtis priklausys nuo to, kaip suformuluoti išradimo požymiai. Deja, net ir esamos tarptautinės patentavimo sistemos (pareiškiant Europos patentą ar patentą pagal Patentinės kooperacijos sutartį) nepadeda išvengti ypač didelių patentavimo išlaidų. Kitoms pramoninės nuosavybės rūšims, ypač prekių ženklams ir pramoniniam dizainui, irgi būtinos nacionalinės procedūros, atliekamos kiekvienoje valstybėje, kur norima, kad šios teisės galiotų, ir registracijos mokesčiai. Kita vertus, kitos pramoninės nuosavybės teisės (įskaitant prekių ženklus ir pramoninį dizainą) nėra tiesiogiai susijusios su naujos informacijos kūrimu ir inovacijomis, todėl jos ne tokios svarbios kaip patentai.

Visiškai kitaip nei pramoninė nuosavybė, autorių ir gretutinės teisės iš esmės yra nemokamos ir savaime galioja tarptautiniu mastu (dėl Berno konvencijos ir kitų tarptautinių susitarimų). Autorių ir gretutinėms teisėms įsigyti nereikalingos jokios registravimo ar ekspertizės procedūros, be to, nereikalaujama, kad šių teisių objektai turėtų kokį nors praktinį pritaikymą ar atitiktų kokius nors objektyvius reikalavimus. Iš esmės didžiausios išlaidos, susijusios su autorių ir gretutinėmis teisėmis, yra šių teisių gynimo išlaidos, kurios tarptautiniu mastu gali prilygti sumai, skirtai patentui įgyti ir ginti. Paminėtina, kad ekonominiu požiūriu visos išlaidos, susijusios su intelektine nuosavybe, yra negrįžtami kaštai.

Skirtingos intelektinės nuosavybės teisės nekonkuruoja tarpusavyje, t. y. gali galioti ir būti taikomos vienu metu, todėl, siekiant maksimaliai apginti savo interesus dėl to paties objekto, gali būti įgyjamos kelios skirtingos intelektinės nuosavybės teisės, pvz., grafinis atvaizdas ar literatūrinio personažo vardas yra saugomi autorių teisių, tačiau gali būti registruojami ir kaip prekės ženklai. Naujos intelektinės nuosavybės formos, ypač kompiuterių programos ir duomenų bazės, vienu metu gali būti saugomos autorių teisėmis, teisėmis į konfidencialią informaciją, patentais (jeigu tenkinami galimybės patentuoti reikalavimai) ir *sui generis* teisėmis. Atskiri jų elementai irgi gali būti registruojami kaip prekių ženklai ar pramoninis dizainas. Skirtingos intelektinės nuosavybės teisės į tą patį objektą gali būti įgyjamos vienu metu arba paeiliui, pvz., produkto idėja ir prototipai, saugomi kaip konfidenciali informacija, šio produkto brėžiniai ir verslo planai bus saugomi autorių teisėmis, veikiantis produktas ar procesas gali būti patentuojamas, produkto pavadinimas registruojamas kaip prekės ženklas, o įmonės verslas, susijęs su šiuo produktu, saugomas nuo nesąžiningos konkurencijos.

Autorių teisių ir gretutinių teisių objektų (intelektine nuosavybe siaurąja prasme) ir pramoninės nuosavybės palyginimas pateiktas lentelėje:

Autorių teisės ir gretutinės teisės	**Pramoninė nuosavybė**
Saugomi bet kokie originalūs ar pirmą kartą atlikti objektai.	Saugomi tik objektai, atitinkantys specialius reikalavimus.
Suteikiamos automatiškai ir nemokamai, be jokių 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 lygiagretus analogiško (panašaus) objekto sukūrimas.	Bet koks analogiško (panašaus) objekto sukūrimas ar naudojimas laikomas teisių pažeidimu.

3 skirsnis. Intelektinės nuosavybės raida elektroninėje erdvėje

Intelektinės nuosavybės raida e. erdvėje neatsiejama nuo svarbiausių technologinių laimėjimų. Dar XIX–XX a. ypač sparčiai vyko intelektinės nuosavybės objektų ekspansija ir diversifikacija, nulemta šių technologinių proveržių: fotografijos, kino, garso įrašų, radijo, televizijos, palydovinių ir kabelinių transliacijų, galiausiai kompiuterių ir jų tinklų atsiradimo bei masinio paplitimo. Kiekviena iš šių technologinių sričių skatino naujus intelektinės nuosavybės objektus, juos lydinčias subjektyvines teises ir iš to kylančias kitas teisines problemas.

Nuo XX a. aštuntojo dešimtmečio prasidėjusi informacinių technologijų revoliucija informaciją ir intelektinę nuosavybę pavertė masine preke, kuri minimaliomis sąnaudomis gali būti ypač lengvai atgaminama ar perduodama internetu į bet kurį pasaulio kampelį. Internete ypač aktuali tapo interneto tarpininkų, kurie perduoda e. informaciją (tarp jų ir intelektinės nuosavybės turinį), įtaka intelektinės nuosavybės platinimui ir apsaugai. Intelektinės nuosavybės pažeidimai internete dėl savo paprastumo pasiekė neregėtą mastą, kita vertus, gana akivaizdus intelektinės nuosavybės teisių turėtojų noras maksimaliai išplėsti savo intelektinės nuosavybės teises ir, pasitelkus informacines technologijas, pasipelnyti vartotojų sąskaita (reikalaujant nepagrįstos kainos už intelektinės nuosavybės teises ar atlyginimo už tradiciškai neatlygintiną – asmeninį ir nekomercinį – naudojimąsi intelektine nuosavybe ir siekiant neterminuotų intelektinės nuosavybės teisių).

Kompiuterių ir tinklo technologijos pakeitė ir intelektinės nuosavybės vieneto sampratą – vietoj muzikos albumo tapo įmanoma įsigyti ir vartoti konkretų aktualų kūrinį, vietoj viso žurnalo – tik reikiamą straipsnį, be to, vietoj įprastų mokamų intelektinės nuosavybės šaltinių atsirado nemokami (pvz., tinklaraščiai vietoj dienraščių) arba nemokami naujienų (išlaikomi vien iš reiklamos pajamų) kvaziportalai. Be to, globalių kompiuterių tinklų ir galimybių greitai platinti elektroninę intelektinę nuosavybę kontekste tapo labai sudėtinga diferencijuoti rinkas (skirtingose šalyse analogiškiems intelektinės nuosavybės objektams nustatyti skirtingas kainas). Tai lėmė labai didelį pinigų srauto sumažėjimą intelektinės nuosavybės tarpininkams, kurie iki šiol iš esmės negebėjo prisitaikyti prie žinių visuomenės poreikių, tačiau dėl to dažniausiai kaltina tik intelektinės nuosavybės teisių pažeidimus internete. Šie pokyčiai paskatino visiškai naujų elektroninės intelektinės nuosavybės platintojų atėjimą į rinką (pvz., didžiausias muzikos portalas elektroninėje erdvėje – *Itunes* – buvo įsteigtas tik 2003 m., tačiau pardavimu ir apyvarta gerokai pralenkė visus tradicinius muzikos pardavėjus).

Naudojant naujus skaitmeninius formatus ir informacijos glaudinimo standartus *(MP3, DivX, MP4)* intelektinės nuosavybės objektai ir kita informacija gali būti išsaugoma nedidelės apimties bylose, be to, eksponentiškai didėjant elektronių informacijos laikmenų talpumui ir mažėjant kainai, bylų dydis (megabaitų skaičius) tampa vis mažiau aktualus fizinis apribojimas. Pasitelkus glaudinimo algoritmus, net į įprastines laikmenas (pvz., įrašomąsias kompaktines plokšteles *(CD-R)* galima įrašyti gerokai daugiau informacijos – atitinkamai ilgesnės trukmės fonogramas ar net kelis garso ir vaizdo kūrinius, o informacijos perdavimas kompiuterių tinklais ir internetu tampa itin greitas ir efektyvus. *MP3, DivX, MP4* glaudinimo algoritmai sukurti naudoti teisėtiems tikslams, tokiems kaip interneto radijas ar skaitmeninė televizija, tačiau intelektinės nuosavybės pažeidėjai netruko naudotis šiais technologiniais laimėjimais. *MP3, DivX, MP4* algoritmai įgalino ir visiškai naujus teisėtus intelektinės nuosavybės platinimo ir naudojimo būdus – iš esmės realus tapo ir milžiniškos sėkmės sulaukė intelektinės nuosavybės (elektroninių įrašų, knygų, filmų) teisėtas platinimas internete, atsirado ir suklestėjo specializuotų skaitmeninės informacijos grotuvų rinka. Paprastai tik dėl minėtųjų technologijų galima įsigyti intelektinės produkcijos, pritaikytos individualiems vartotojų poreikiams ir apskritai neprieinamos jokiais kitais būdais, pvz., tai gali būti konkrečios dainos muzikos e. įrašas vietoj viso albumo. Paminėtina, kad tokios individualios prekės ir paslaugos yra ypač patrauklios ir reikalingos vartotojams – 2013 m. vasarį *Itunes* populiariausias legalių skaitmeninių muzikos įrašų pardavimo portalas internete *www.itunes.com* minėjo 25 mlrd. parduotų muzikos įrašų, o 2013 m. balandį – veiklos dešimtmečio sukaktį (žr. *<http://www.apple.com/pr/library/2013/02/06iTunes-Store-Sets-New-Record-with-25-Billion-Songs-Sold.html>)*. Be to, pastaraisiais metais *Itunes* pradėjo platinti e. knygas, filmus ir TV serialų įrašus. Tokia sparti plėtra neturi analogų ir precedentų.

Plačiajuosčio tinklo ir duomenų glaudinimo technologijos iš esmės išstūmė fizines intelektinės nuosavybės objektų laikmenas, nes intelektinės nuosavybės objektai tapo prieinami ir vartojami srautiniu realaus laiko režimu ir jiems visiškai nereikalinga fizinė laikmena. Tokiu būdu klausantis kūrinio, tam tikru laiko momentu vartotojui yra prieinama tik skambanti ar rodoma šio kūrinio dalelė, kuri tiesiogiai siunčiama į jo galinį įrenginį, o visas kūrinys yra saugomas tik nutolusiame tiekėjo serveryje.

XXI a. pirmąjį dešimtmetį intelektinės nuosavybės pažeidimams masiškai naudotos įrašomosios kompaktinės plokštelės ir kitos įrašymo laikmenos (pvz., daugkartinio naudojimo atmintinės (angl. *flash memory)*, nešiojamieji kietieji diskai ir pan.) šiandien beveik prarado reikšmę piratams,

tačiau plačiai naudojamos nepiratavimo tikslams, pvz., asmeniniam turiniui (šeimos fotografijoms, asmeniniams dokumentams ir pan.) saugoti. Neatsižvelgiant į šiuos pokyčius, įrašomos kompaktinės plokštelės ir atminties įrenginiai yra plačiai apmokestinami laikmenų bei įrangos mokesčiais ir tai aiškiai rodo tokių mokesčių neadekvatumą. Laikmenų ir įrangos mokesčiai turėtų būti renkami tik už teisėtas svetimų kūrinių asmenines, o ne piratines, kopijas ar juo labiau asmeninį turinį.

E. erdvėje iš esmės išnyko skirtumas tarp kūrinio kopijos ir originalo. Analoginiame pasaulyje kopija visada buvo prastesnės kokybės nei originalus įrašas, tai ir padėdavo parduoti originalius įrašus kaip pranašesnius. Duomenų glaudinimo technologijos šiuos skirtumus labai sumažino. Paprastas vartotojas nemato, negirdi ir negali pajusti skirtumo tarp teisėtos ir neteisėtos elektroninio turinio kopijos – šie objektai tapo visiškai ekvivalentiški.

Patys e. turinio vartojimo galiniai įrenginiai iš esmės tapo universalūs, t. y. tinkami labai įvairioms komunikacijos, informacijos ir pramogų funkcijoms (pvz., asmeniniai kompiuteriai ar išmanieji telefonai).

Kitas labai svarbus aspektas – per pastaruosius du dešimtmečius technologijų raida iš esmės labai supaprastino ir atpigino intelektinės nuosavybės kūrimą. Kūrybinius darbus, kuriems atlikti prieš du dešimtmečius buvo reikalingos milijoninės investicijos ir įvairių specialistų komandos, šiuo metu galima padaryti įprastu nešiojamuoju kompiuteriu (pvz., muzikos ar vaizdo įrašų kūryba ar redagavimas, kompiuterių programavimas ir pan.).

Galiausiai e. erdvė iš esmės pakeitė intelektinės nuosavybės verslo modelius – patys intelektinės nuosavybės kūrėjai, prisijungę prie interneto, gali be tarpininkų platinti savo intelektinę nuosavybę ir gauti už tai atlyginimą. Šie technologijų nulemti pokyčiai išryškino pasenusią ir neefektyvią kolektyvinio administravimo sistemą, kuri prieš informacinės eros visuomenėje priverstine tvarka už kūrėjus administruodavo jų teises.

Be to, greta minėtųjų technologinių proveržių labai sustiprėjo intelektinės nuosavybės teisių, kaip leidžiančių kontroliuoti teisėtą informacijos naudojimą, įtaka. Be teisinių, atsirado ir techniniai mechanizmai – techninės apsaugos priemonės, leidžiančios automatizuoti intelektinės nuosavybės teisių administravimą.

Naujos technologinės galimybės ir minėtieji pokyčiai pamažu atsispinti ir teisiškai reguliuojant intelektinę nuosavybę. Per kelis pastaruosius dešimtmečius teisiniai pokyčiai yra labai akivaizdūs.

Galima identifikuoti tris ryškiausias teisinių pokyčių kryptis:

1) atsirado ir buvo teisiškai reglamentuota daug naujų intelektinės nuosavybės formų ir su jomis susijusių objektų: kompiuterių programos, duomenų bazės, tinklalapiai, domeno vardai ir kt.;

2) į e. erdvę išsiplėtė su intelektine nuosavybe susijusios subjektyvinės teisės ir jų apribojimai, be to, atsirado naujų subjektyvinių teisių ir specifinių intelektinės nuosavybės apribojimų e. erdvėje;
3) intelektinės nuosavybės teisė reglamentavo ir suteikė teisinę apsaugą objektams, tiesiogiai nesusijusiems su intelektine nuosavybe: investicijoms į informaciją, techninėms apsaugos priemonėms ir teisėms gauti papildomą atlyginimą nuo potencialių intelektinės nuosavybės laikmenų.

Bręstantis naujas intelektinės nuosavybės reglamentavimo e. erdvėje pokytis – intelektinės nuosavybės kūrėjų ir naudotojų (vartotojų ir visuomenės) teisių nustatymas ir reglamentavimas, atkuriant balansą tarp intelektinės nuosavybės kūrėjų ir šių teisių turėtojų (tarpininkų) bei tarp teisių turėtojų (tarpininkų) ir teisių naudotojų (vartotojų ir visuomenės).

Apskritai galima konstatuoti, kad intelektinės nuosavybės teisių turinys ir principai e. erdvės ir žinių visuomenės sąlygomis gerokai pakito – išaugo į gana platų ir savarankišką intelektinės nuosvybės e. erdvėje institutą.

Pokyčių apimtį ir kitas minėtąsias tendencijas geriausiai atspindi įstatymų leidėjų dėmesys ir įstatymų leidimo apimtys intelektinės nuosavybės klausimais. Per pastaruosius du dešimtmečius tarptautinės organizacijos ir regioniniai blokai (ES) priėmė daugiau teisės aktų, susijusių su intelektinės nuosavybės klausimais e. erdvėje, nei per ankstesnį intelektinės nuosavybės teisinio reglamentavimo šimtmetį.

Svarbiausi šio etapo tarptautiniai teisės aktai, tiesiogiai susiję su elektroninės intelektinės nuosavybės reglamentavimu, yra šie: 1996 m. Pasaulinės intelektinės nuosavybės organizacijos (WIPO) autorių teisių sutartis bei 1996 m. Pasaulinės intelektinės nuosavybės organizacijos (WIPO) atlikimų ir fonogramų sutartis. Ypatingą dėmesį intelektinės nuosavybės problemoms skiria ES. Nuo 1991 m. ji yra priėmusi net dešimt direktyvų, reglamentuojančių intelektinės nuosavybės klausimus e. erdvėje, tarp jų – Direktyvą 91/250/EEC dėl teisinės kompiuterių programų apsaugos (nuo 2009 m. šią direktybą pakeitė konsoliduotoji Direktyva 2009/24/EB), Direktyvą 93/83/EEC dėl autorių teises ir gretutines teises reglamentuojančių taisyklių harmonizavimo palydovinių bei kabelinių transliacijų srityje, Direktyvą 93/98/EEC dėl autorių teisių ir gretutinių teisių apsaugos terminų suvienodinimo, Direktyvą 96/9/EC dėl teisinės duomenų bazių apsaugos, Direktyvą 2001/29/EC dėl kai kurių autorių teisių ir gretutinių teisių aspektų informacinėje visuomenėje, Direktyvą 2004/48/EC dėl intelektinės nuosavybės teisių gynimo. Šiuo metu rengiama dar keletas direktyvų projektų, glaudžiai susijusių su intelektinės nuosavybės klausimais internete, iš jų – ir direktyvos projektas dėl intelektinės nuosavybės teisių administravimo e. erdvėje.

4 skirsnis. Intelektinės nuosavybės elektroninėje erdvėje teisinio reglamentavimo ypatumai

Kaip jau minėta, pirmoji intelektinės nuosavybės e. erdvėje reglamentavimo kryptis – objekto plėtra. Visų pirma į e. erdvę buvo perkelti tradiciniai intelektinės nuosavybės objektai, pvz., tekstiniai kūriniai, fotografijos, garso ir vaizdo objektai ir pan. Todėl intelektinės nuosavybės e. erdvėje objektas yra tradiciniai kūriniai, pateikiami e. forma, pvz., e. tekstai, e. muzikos įrašai, e. paveikslėliai ir pan.

Vėliau atsirado specifinių, vien elektroninių, intelektinės nuosavybės objektų. Populiariausi iš minėtųjų objektų yra kompiuterių programos ir duomenų bazės. Pati e. erdvė iš esmės yra kompiuterių ir kompiuterių programų veikimo (sąveikos) rezultatas. Savarankiškomis intelektinės nuosavybės e. erdvėje formomis tam tikrais atvejais galima laikyti ir domeno vardus – simbolinius interneto adresų pavadinimus ir interneto turinį – įvairialypės terpės (multimedijos) objektus.

Ryškėja tendencija, kad tradiciniai analoginiai intelektinės nuosavybės objektai yra išstumiami jų skaitmeninių formų (pvz., skaitmeninė fotografija beveik išstūmė analoginę fotografiją).

Antra kryptis yra specialus intelektinės nuosavybės teisių išplėtimas e. erdvėje – elektroninės teisės, nes autoriams, išradėjams ir kitiems intelektinės nuosavybės teisių turėtojams būtina kontroliuoti intelektinės nuosavybės naudojimą ir tradicinėje, ir e. erdvėje. Be to, būtinos ir specialios intelektinės nuosavybės teisių išimtys, susijusios su techninėmis e. erdvės savybėmis. Specialios bendrosios subjektyvinės intelektinės nuosavybės teisės e. erdvėje yra šios (teisės leisti ar drausti):

- intelektinės nuosavybės e. erdvėje atgaminimą (kopijavimą), apimantį specialias kvaziatgaminimo formas, tokias kaip interneto nuorodos, langų elementai (angl. *frames)*, integruotą įvairialypį turinį;
- intelektinės nuosavybės platinimą e. erdvėje, įskaitant platinimą telefono linijomis, interneto serveriuose, tinklalapiuose, *P2P* tinklais ir pan.;
- intelektinės nuosavybės padarymą viešai prieinamą kompiuterių tinklais (įdėjimą į internetą).

Specialios intelektinės nuosavybės subjektyvinės teisės e. erdvėje yra susijusios su tam tikrais intelektinės nuosavybės e. erdvėje objektais, pvz., kompiuterių programomis ar duomenų bazėmis. Tokios specialios teisės, pvz., yra *sui generis* teisės riboti reikšmingos duomenų bazės turinio dalies atgaminimą, naudojimą ir pan.

Specialios intelektinės nuosavybės teisių išimtys e. erdvėje yra susijusios su būtinybe užtikrinti e. erdvės, interneto ar kompiuterių funkcionavimą, suderinamumą ir galimybes juos naudoti pagal paskirtį. Tokios išimtys yra:

- laikinas intelektinės nuosavybės atgaminimas e. erdvėje, kuris būtinas, pvz., kompiuterių programai paleisti (laikinoji kopija operatyviojoje atmintyje *(RAM)*, informacijai perduoti internetu (laikinos kopijos tarpiniuose serveriuose) ir pan.;
- intelektinės nuosavybės atgaminimas ir naudojimas suderinamumo, klaidų taisymo ir pasiekiamumo tikslams, pvz., teisė dekompiliuoti kompiuterių programą (atkurti pirminį jos kodą) suderinamumo tikslams, pasidaryti atsarginę ar asmeninę kopiją, taisyti programos klaidas ir kt.

Kiti aktualūs intelektinės nuosavybės klausimai e. erdvėje, kurie ją taip pat atskiria nuo tradicinės intelektinės nuosavybės problematikos, yra:

- techninių apsaugos priemonių naudojimas intelektinės nuosavybės apsaugai;
- teisių administravimas e. erdvėje;
- intelektinės nuosavybės teisių suderinimas su naujomis kūrybos ir inovacijų formomis e. erdvėje – atviro kodo, kūrybinių bendrijų ir kt. judėjimais.

Techninės apsaugos priemonės – 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 šios: specialūs techniniai raktai, papildomi elektroniniai signalai ir vandenženkliai, speciali programinė įranga, net sąmoningai paliekamos naudingos informacijos klaidos.

XX a. paskutiniojo dešimtmečio pabaigoje e. erdvėje atsirado ir įsitvirtino minėtieji alternatyvūs intelektinės nuosavybės judėjimai, tokie kaip atvirosios programinės įrangos (angl. *Open source)* ir kūrybinių bendrijų (angl. *Creative Commons)*, akcentuojantys intelektinės nuosavybės svarbą socialiniam informacijos prieinamumui, planavimui, kultūros ir technologijų plėtrai. Šie judėjimai pabrėžia pamatinį intelektinės nuosavybės teisių balanso (kūrėjų-teisių turėtojų-naudotojų (visuomenės) principą, be to, teigia, kad intelektinės nuosavybės subjektyvinių teisių išplėtimas į e. erdvę pažeidė balansą intelektinės nuosavybės teisių turėtojų naudai, taip suvaržydamas viešąjį interesą ir intelektinės nuosavybės instituto socialinę naudą. Ši pozicija sulaukė palaikymo ir naujausioje intelektinės nuosavybės e. erdvėje jurisprudencijoje JAV ir ES. Nauji ekonominiai tyrimai rodo, kad esama tam

tikrų intelektinės nuosavybės e. erdvėje reglamentavimo iniciatyvų (pvz., laikmenų ir įrangos mokesčio), darančių žalingą poveikį žinių visuomenei.

Atvirosios programinės įrangos judėjimas yra kompiuterių programų, kurių kodas pateikiamas viešai analizuoti ir tobulinti, virtuali autorių bendruomenė. Kiekvienas asmuo gali laisvai naudotis atvirąja programine įranga, ją perdirbti, tobulinti ir pan., tačiau jo panaudotas ar perdirbtas programinės įrangos kodas turi likti atviras – laisvai prieinamas ir viešas. Atvirosios programinės įrangos judėjimas neturi būti tapatinamas su nemokamomis kompiuterių programomis, nes atviroji programinė įranga nebūtinai platinama ir prieinama nemokamai, tik svarbu, kad programos kodas būtų laisvai viešai prieinamas ir būtų galimybė šį kodą ar jo elementus naudoti naujoms kompiuterių programoms kurti. Atvirosios programinės įrangos judėjimo tęstinumas paprastai užtikrinamas specialiomis atvirosios programinės įrangos licencijomis (susitarimais dėl atvirosios programinės įrangos teisinio statuso ir naudojimo sąlygų). Atvirosios programinės įrangos judėjimas neprieštarauja ir jokiu būdu neneigia intelektinės nuosavybės teisių reikalingumo, priešingai, jis iš esmės priklausomas nuo intelektinės nuosavybės teisių, kurios naudojamos ginant atvirosios programinės įrangos (ir jos pagrindu sukurto naujo kodo) viešumą ir prieinamumą.

Kūrybinių bendrijų (angl. *Creative Commons)* judėjimas – atvirosios programinės įrangos principais pagrįsta bet kokios informacijos (kūrinių, inovacijų) apsikeitimo ir tobulinimo licencijavimo sistema, leidžianti pagal aiškiai apibrėžtas licencijas pateikti viešai platinti ir naudoti intelektinės nuosavybės teisėmis saugomą turinį. Kiti asmenys, atsižvelgdami į autoriaus ar teisių turėtojo pasirinktas licencijos sąlygas, kūrybinių bendrijų informacija gali naudotis nemokamai ar už atlyginimą, gali jį perdirbti, naudoti nekomerciniams projektams ir pan. Kūrybinės bendrijos gerokai supaprastina intelektinės nuosavybės naudojimą, nes išlaisvina jos naudotojus nuo būtinybės individualiai derinti licencijos sąlygas, kontaktuoti su autoriumi (teisių turėtoju ir pan.).

Svarbi intelektinės nuosavybės e. erdvėje instituto dalis – specifiniai intelektinės nuosavybės pažeidimai e. erdvėje (ypač *P2P* tinkluose). Lietuvoje atsakomybės už intelektinės nuosavybės pažeidimus e. erdvėje reglamentavimas yra nespecifinis (šie pažeidimai priskiriami bendriesiems intelektinės nuosavybės teisių pažeidimams), nors veikų pavojingumas yra didesnis.

Atskira intelektinės nuosavybės e. erdvėje tema – prekių ženklų apsauga e. erdvėje. Informacinės technologijos ir e. erdvė prekių ženklams iškėlė visiškai naujų iššūkių, tokių kaip prekių ženklų naudojimas domenų vardams, nematomiems tinklalapių ir interneto išteklių elementams,

interneto raktažodžių reklamai (elektroninei rinkodarai), be to, neteisėtų ar falsifikuotų prekių ir paslaugų ženklinimas bei platinimas internete. Detaliau šie iššūkiai, kylančios teisinės problemos ir teisiniai jų sprendimai nagrinėjami žemiau.

5 skirsnis. Intelektinės nuosavybės elektroninėje erdvėje reglamentavimas Lietuvoje

Intelektinės nuosavybės e. erdvėje reguliavimo specifika Lietuvoje labiausiai pasireiškia dviejose reguliavimo srityse – reguliuojant technines apsaugos priemones ir laikmenų bei įrangos mokesčius.

Siekdami užkirsti kelią intelektinės nuosavybės teisių pažeidimams e. erdvėje, intelektinės nuosavybės gamintojai ir platintojai greta įprastinių teisinių priemonių (teisinės atsakomybės) pradėjo naudoti įvairias technines apsaugos priemones, teisių valdymo mechanizmus ir sutartinius autorinių kūrinių ir gretutinių teisių objektų laikmenų, jų atgaminimo ir net įprastinio naudojimo apribojimus. Tokios techninės apsaugos priemonės dažnai gali būti veiksmingesnės nei atitinkami teisiniai draudimai ar ribojimai. Techninėmis apsaugos priemonėmis laikoma bet kokia technologija, įtaisai ar jų sudėtinės dalys, skirti normaliai veikiant uždrausti arba riboti su autorių, gretutinių ar *sui generis* teisių objektais atliekamus veiksmus, kurių neleidžia autorių, gretutinių ar *sui generis* teisių subjektai. Techninės apsaugos priemonės laikomos veiksmingomis, jeigu yra saugomos autorių, gretutinių ar *sui generis* teisių; objekto naudojimą teisių subjektai kontroliuoja pasitelkdami prieigos kontrolę ar apsaugą (kodavimą, elementų perstatymą arba kitokį intelektinės nuosavybės objekto transformavimą) arba kopijų kontrolės būdą, užtikrinantį apsaugą.

Įsipareigojama užtikrinti techninių priemonių ir informacijos apie autorių ir gretutinių teisių valdymą, teisinę apsaugą įtraukti į TRIPS sutartį ir WIPO interneto sutartis bei minėtuosius ES teisės aktus.

Pradėjus naudoti technines kūrinių ir gretutinių teisių objektų apsaugos priemones, atsirado ir naujų neteisėtos veiklos formų – įrenginių, skirtų techninėms apsaugos priemonėms pašalinti ar joms apeiti, gamyba ir platinimas. Nors tokia veikla tiesiogiai ir nepažeidžia autorių ar gretutinių teisių į techninėmis priemonėmis saugomą objektą, siekiant išspręsti šį kazusą, buvo numatyta atskira teisinė techninių priemonių apsauga. Visose išsivysčiusiose valstybėse draudžiama pašalinti bet kokias autorių ar gretutinių teisių objekto technines apsaugos priemones, taip pat gaminti ar platinti prietaisus ar kitokius įrankius, skirtus minėtosioms techninėms priemonėms panaikinti. Pabrėžtina, jog tam tikrais atvejais technines

priemones pašalinti tiesiog būtina, kad būtų įgyvendintos įstatymais nustatytos autorių ir gretutinių teisių išimtys (pvz., teisės užtikrinti suderinamumą, apsaugotos informacijos prieinamumą moksliniams tikslams, padaryti atsarginę kopiją), todėl taikydami technines priemones intelektinės nuosavybės teisių turėtojai gali ir piktnaudžiauti.

Techninių priemonių ir informacijos apie teisių valdymą reglamentavimą Lietuvoje nustato Autorių teisių ir gretutinių teisių įstatymo 74–76 str., o baudžiamąją atsakomybę už jų pažeidimą papildomai numato BK 193–194 straipsniai. Techninių apsaugos priemonių pažeidimu yra laikomas bet kokių veiksmingų techninių apsaugos priemonių šalinimas ar vengimas, kai asmuo tai daro žinodamas ar turėdamas žinoti, kad jis siekia pašalinti autorių, gretutinių ar *sui generis* teisių subjektų taikomas technines apsaugos priemones ar jų išvengti. Pažeidimu laikoma ir įtaisų, gaminių ar jų sudėtinių dalių, suprojektuotų, pagamintų ar pritaikytų tam, kad sudarytų galimybę pašalinti bet kokias veiksmingas technines apsaugos priemones arba padėtų jų išvengti, taip pat įtaisų, gaminių ar jų sudėtinių dalių, kurių paskirtis ribota komerciniu požiūriu arba kuriuos galima naudoti kitiems tikslams nei techninių apsaugos priemonių šalinimas ar vengimas, gaminimas, platinimas ar kitoks disponavimas, taip pat paslaugų, susijusių su techninių apsaugos priemonių šalinimu ar vengimu, teikimas. Greta civilinio reglamentavimo BK XXX skirsnio nuostatos 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 (ir civilinėje, ir baudžiamojoje teisėje) keliamas komercinių tikslų reikalavimas. Subjektyviai šios veikos turi būti padaromos tiesiogiai, tyčia, kaltininkui suvokiant nusikalstamos veikos pobūdį ir norint taip veikti. Už šias veikas taikomos sankcijos: viešieji darbai arba bauda, arba laisvės apribojimas, arba areštas, arba laisvės atėmimas iki dvejų metų. Be to, atsakomybė gali būti taikoma ir juridiniam asmeniui. Paprastai viena iš 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, kūrinių, atliktų įrašų, fonogramų ar jų kopijų platinimas, importavimas, transliavimas, viešas paskelbimas ar padarymas viešai prieinamais, be leidimo panaikinus arba pakeitus informaciją apie teisių valdymą, yra laikomas autorių teisių ir gretutinių teisių pažeidimu.

Deja, Lietuvoje nustatyta teisinė techninių apsaugos priemonių apsauga yra besąlygiška ir nenumato jokių išimčių, dėl to beveik neįgyvendinamos tampa autorių teisių ir gretutinių teisių išimtys – teisė atgaminti

asmeniniams, švietimo ir mokslo tikslams ir kt. Lietuvos įstatymai nenumato jokio realaus mechanizmo, kaip vartotojui įgyvendinti savo juridines teises (pvz., asmeninės kopijos teisę ar teisę intelektine nuosavybe naudotis mokslo ir švietimo tikslams). Tokia padėtis akivaizdžiai lemia intelektinės nuosavybės naudotojo (vartotojo) teisių ir intelektinės nuosavybės teisių pažeidimo normų koliziją, t. y. vartotojas, norėdamas įgyvendinti savo teises, iš esmės neturi kitos išeities, kaip tik pažeisti technines apsaugos priemones. Kadangi už techninių apsaugos priemonių pažeidimus numatyta net baudžiamoji atsakomybė, ši teisių kolizija turėtų būti sprendžiama.

Dar viena ryškėjanti intelektinės nuosavybės e. erdvėje problema – kolektyviai administruojami laikmenų ir įrangos mokesčiai. Kolektyvinis teisių administravimas yra intelektinės nuosavybės teisių turėtojų pavedimas centralizuotoms asociacijoms tvarkyti ir ginti jų intelektinės nuosavybės teises, rinkti pinigus 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. Deja, sparčiai tobulėjant technologijoms, ypač plintant techninėms apsaugos priemonėms bei autorių teisių ir gretutinių teisių valdymo technologijoms, didėja pačių autorių ir gretutinių teisių turėtojų galimybės administruoti savo teises ir kontroliuoti saugomų kūrinių naudojimą. Kaip jau minėta, techninių apsaugos priemonių bei autorių ir gretutinių teisių valdymo priemonių teisinė apsauga yra atskirai reglamentuojama, o šios priemonės tampa svaria kolektyvinio teisių administravimo alternatyva. Be to, kaip kolektyvinio administravimo alternatyva yra ir minėtasis kūrybinių bendrijų judėjimas, orientuotas į paties autoriaus galimybes licencijuoti savo kūrinį ir individualiai nustatyti jo naudojimo režimą.

Kolektyvinis intelektinės nuosavybės teisių administravimas iš esmės yra tinkamas teisėms tvarkyti prieš informacinės eros, bet ne žinių, visuomenėje. Kolektyvinis administravimas ypač netinkamas ir net žalingas e. erdvėje. Svarbiausios to priežastys – kolektyvinio administravimo ir technologinių intelektinės nuosavybės teisių administravimo mechanizmų nesuderinamumas.

Svarbiausi kolektyvinio e. erdvės administravimo iššūkiai šiuo metu yra nesuderinamumas su individualiu technologiniu teisių administravimu ir dvigubas ar nepagrįstas tų pačių intelektinės nuosavybės naudojimo formų apmokestinimas per laikmenų ir įrangos mokesčius. Techninių apsaugos priemonių bei autorių teisių ir gretutinių teisių valdymo technologijų naudojimas – plintantis individualus teisių administravimas – lemia

dvigubą ar net apskritai nepagrįstą autorinio atlyginimo mokėjimą už intelektinės nuosavybės naudojimą. Geriausiai šią problemą Lietuvoje parodo kolektyvinio administravimo asociacijų renkamas atlyginimas už garso ir vaizdo ar į fonogramas įrašytų kūrinių atgaminimą asmeniniams tikslams, kuris dažnai vadinamas „laikmenų ir įrangos mokesčiu“ arba „tuščios laikmenos mokesčiu“. Pagal galiojančias taisykles, nustatytas Autorių teisių ir gretutinių teisių įstatymo 20 str. ir 2012 m. birželio 13 d. Lietuvos Respublikos Vyriausybės nutarime Nr. 699 „Dėl Kompensacinio atlyginimo už audiovizualinių kūrinių ar fonogramose įrašytų kūrinių atgaminimą asmeniniais tikslais surinkimo, paskirstymo, mokėjimo ir grąžinimo tvarkos aprašo patvirtinimo“, laikmenų ir įrangos mokesčiai turi būti mokami:

- už visas laikmenas, tarp jų ir tas, kurios naudojamos su intelektine nuosavybe visiškai nesusijusiems tikslams (pvz., verslo informacijai saugoti, asmeninėms fotografijoms, šeimos filmui ir pan.);
- tais atvejais, kai asmeninis kūrinio atgaminimas yra uždraustas techninėmis priemonėmis, t. y. teisėtai atgaminti kūrinio asmeniniams tikslams iš esmės neįmanoma. Paminėtina, kad šiuo metu apie 90 proc. viešai platinamų kūrinių dėl taikomų techninių apsaugos priemonių negali būti teisėtai atgaminami asmeniniams ar kitiems tikslams;
- neatsižvelgiant į tai, kad mokestis už atitinkamas laikmenas ar įrangą jau buvo sumokėtas kitose ES 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).

Laikmenų ir įrangos mokesčių administracinė našta mokesčio mokėtojams yra ypač didelė ir biurokratiška. Nors numatyta galimybė tam tikrais atvejais mokestį susigrąžinti, dėl itin neaiškios reguliavimo ir komplikuotos procedūros ja pasinaudoti iš esmės neįmanoma. Verslo asociacijų vertinimu, laikmenų ir įrangos mokesčiai daro kelių šimtų milijonų litų žalą Lietuvos ūkiui, skatina šešėlinį verslą ir iš esmės stabdo žinių ekonomikos plėtrą Lietuvoje.

Intelektinės nuosavybės e. erdvėje subjektyvinių teisių ir apribojimų balansas, techninės apsaugos priemonės, laikmenų ir įrangos mokesčiai yra priemonės, turinčios milžinišką socialinę ir ekonominę įtaką. Netinkamas jų reglamentavimas, pvz., perdėta e. informacijos apsauga nuo socialinio jos naudojimo, per didelė laikmenų ir įrangos mokesčių našta ar netinkamas atlygis už intelektinės nuosavybės objektų elektroninį naudojimą turi

tiesioginę įtaką žinių visuomenės ir žinių ekonomikos plėtrai – nepalankios sąlygos lemia stagnaciją, verslo ir investicijų mažėjimą bei migraciją į palankesnes jurisdikcijas, o tinkamas reglamentavimas skatina atvirkštinius (pageidautinus) procesus. Atsižvelgiant į Lietuvos valstybės deklaruojamą ilgalaikės darnios plėtros, pagrįstos žinių ekonomika, tikslą, tinkamas intelektinės nuosavybės e. erdvėje reglamentavimas yra ypač svarbus.

Be to, aukščiau aptarta intelektinės nuosavybės e. erdvėje instituto specifika, transformacijos ir reikšmė žinių visuomenėje geriausiai pagrindžia intelektinės nuosavybės e. erdvėje instituto savarankiškumą nuo tradicinės intelektinės nuosavybės teisės institutų ir atskirų studijų būtinybę.

Apibendrinant reikia konstatuoti, kad intelektinė nuosavybė e. erdvėje yra specifinis, naujai susiformavęs intelektinės nuosavybės teisės institutas, kuris turi ypatingą reikšmę žinių visuomenės plėtrai, jos socialinei ir ekonominei raidai. Šis institutas kelia specifinių problemų ir reikalauja specialaus reglamentavimo. Tiek tarptautiniu mastu, tiek ES intelektinės nuosavybės e. erdvėje reglamentavimo ir apsaugos klausimai yra akcentuojami kaip svarbiausias žinių ekonomikai palankios teisinės aplinkos elementas. Reglamentuojant intelektinę nuosavybę e. erdvėje, dėl skubotumo bei elektroninės intelektinės nuosavybės vaidmens žinių visuomenėje nesupratimo Lietuvoje buvo padaryta ir klaidų: neišsamus reguliavimas, nustatytas techninėms intelektinės nuosavybės apsaugos priemonėms, be ekonominio pagrindimo ir perdėtai taikomi laikmenų ir įrangos mokesčiai, nepakankama atsakomybė už intelektinės nuosavybės pažeidimus. Esama rizikos, kad toks netobulas reglamentavimas gali sukelti nemažai neigiamų padarinių – užuot skatinama, žinių ekonomikos raida bus ribojama. Dėl šios priežasties būtina tęsti intelektinės nuosavybė teisinio reglamentavimo reformą. Pamatinis reglamentavimo principas turėtų būti intelektinės nuosavybės teisių turėtojų ir visuomenės interesų (subjektyvinių teisių ir pareigų) balansas ir žinių ekonomikos plėtra.

Atsižvelgiant į aptartas reglamentavimo problemas, Lietuvoje tikslinga aiškiai įteisinti individualų teisių administravimą, panaikinti arba sumažinti laikmenų ir įrangos mokesčių naštą, išplėsti teisių išimtis (naudotojų teises), nustatyti techninių intelektinės nuosavybės apsaugos priemonių apribojimus ir specialias atsakomybės už intelektinės nuosavybės pažeidimus e. erdvėje taisykles.

6 skirsnis. Intelektinės nuosavybės pažeidimai elektroninėje erdvėje

Intelektinės nuosavybės pažeidimu laikomas šios nuosavybės produktų atgaminimas, platinimas, naudojimas, laikymas ir gabenimas, neturint teisių turėtojo sutikimo ar sutarties su teisių turėtoju (ar jo atstovu), ir apskritai bet koks intelektinės nuosavybės įstatymų (įskaitant ir neturtinių teisių) pažeidimas. Pažeidimų gali būti padaroma komerciniais ir nekomerciniais tikslais. Komerciniais tikslais laikomi šie atvejai: kai siekiama betarpiškai pasipelnyti ir kai intelektinės nuosavybės teisių objektas naudojamas kitai su komercija susijusiai veiklai.

Intelektinės nuosavybės pažeidimai e. erdvėje yra specifiniai intelektinės nuosavybės teisių pažeidimai, tarp jų:

- tradiciniai intelektinės nuosavybės pažeidimai, kurių padarymo terpė ar priemonė yra e. erdvė arba jos technologijos;
- specifiniai intelektinės nuosavybės pažeidimai, padaromi tik e. erdvėje:
  - nuorodų į neteisėtas intelektinės nuosavybės kopijas įdėjimas ir platinimas;
  - intelektinės nuosavybės neteisėtų kopijų skelbimas ir platinimas kompiuterių tinklais;
  - techninių apsaugos priemonių ir teisių valdymo informacijos pažeidimai;
  - priemonių, skirtų intelektinės nuosavybės pažeidimams e. erdvėje, kūrimas, palaikymas ir platinimas.

Paplitus elektroniniams turinio formatams, e. erdvėje platinami iš esmės bet kokie intelektinės nuosavybės objektai – elektroninis turinys: kompiuterių ir išmaniųjų įrenginių programos, duomenų bazės, garso ir vaizdo produkcija, fonogramos, e. knygos, įvairių erdvinių detalių ir įrenginių 3D modeliai, kurie gali būti atgaminami 3D spausdintuvais, ir įvairiausia kita neteisėta informacija. Vis labiau plintant srauto technologijoms, neteisėtas e. turinys gali būti ne tik lengvai atgaminamas, bet ir pasauliniu mastu platinamas bei perduodamas kompiuterių tinklais be jokių fizinių informacijos laikmenų ir nesukuriant neteisėtų itelektinės nuosavybės skaitmeninių kopijų.

Intelektinės nuosavybės pažeidimais galima laikyti bet kokius intelektinės nuosavybės teisių pažeidimus, nes dauguma iš jų gali būti padaromi tiek e. erdvėje, tiek tradiciniais būdais. Apskritai minėtuosius pažeidimus yra įprasta tapatinti su intelektinės nuosavybės produktų atgaminimu,

platinimu, naudojimu, laikymu ir gabenimu komerciniais tikslais, t. y. tokiais veiksmais, kurie daro ypač didelę žalą intelektinės nuosavybės teisių turėtojams, valstybei ir visuomenei, nors kaip pažeidimai yra pripažintini ir tie atvejai, kai tokios veikos vykdomos nesiekiant pasipelnyti. Komerciniais tikslais laikomi šie atvejai: siekimas betarpiškai pasipelnyti, intelektinės nuosavybės teisių objektas naudojamas kitai su komercija susijusiai veiklai (pvz., įmonės dokumentams rengti), nors pats intelektinės nuosavybės teisių objekto naudojimas nėra komercinis, t. y. neskatina tiesioginių pajamų ar konkretaus taupymo. Pažeidimu laikytinas ir bet koks intelektinės nuosavybės įstatymų ar intelektinės nuosavybės licencinės sutarties pažeidimas, tarp jų intelektinės nuosavybės teisių objekto naudojimas be teisių turėtojo sutikimo (sutarties).

Pažeidimus komerciniais tikslais praktikoje įprasta vadinti „piratavimu“. Ši sąvoka ypač tinkama intelektinės nuosavybės pažeidimams e. erdvėje apibūdinti, nes „piratai“ grobia svetimą intelektinę nuosavybę ir ją naudoja savo tikslams, beveik nedėdami jokių pastangų šioms vertybėms sukurti. Intelektinės nuosavybės sukūrimo sąnaudos dažniausiai išreiškiamos vos ne astronominėmis sumomis, o intelektinės nuosavybės produktų neteisėto atgaminimo ir platinimo (ypač internetu) išlaidos nepalyginimai mažesnės.

Neteisėta (piratine) intelektine produkcija laikomos visos neteisėtai įgytos (nesant įsigijimo dokumentų ir (ar) licencijos), atgamintos (neturint autoriaus, teisių turėtojo ar jiems atstovaujančios organizacijos sutikimo) intelektinės produkcijos (autorinių kūrinių, garso ir vaizdo produkcijos, fonogramų, kompiuterių programų, atlikimų, transliacijų ir kt.) fiksacijos, kopijos, papildomos legaliai 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 e. erdvėje visų pirma turi būti kvalifikuojami taip pat, kaip ir tradiciniai intelektinės nuosavybės pažeidimai, o atsižvelgiant į aptartą jų specifiką ir daromą žalą kai kuriais atvejais vertintini ir kaip pavojingesnės veikos rūšys. Minėtieji pažeidimai įtraukti į daugelio išsivysčiusių valstybių baudžiamuosius ir administracinius kodeksus, tarp jų ES ir Jungtinių Tautų Organizacijos rekomendacijas dėl neteisėtų ir nusikalstamų veikų kvalifikavimo. Intelektinės nuosavybės pažeidimai visose valstybėse, iš jų ir Lietuvoje, laikomi civilinių teisių pažeidimu. Lietuvos Respublika yra pasirašiusi ir ratifikavusi pagrindines tarptautines konvencijas, reglamentuojančias intelektinės nuosavybės teisių pažeidimus,

bei ES direktyvas intelektinės nuosavybės klausimais. Naujausia ES direktyva 2004/48/EB dėl intelektinės nuosavybės teisių gynimo šiuo metu baigiama įgyvendinti Lietuvos intelektinės nuosavybės teises reglamentuojančiuose įstatymuose.

Vienas išsamiausiai intelektinės nuosavybės pažeidimus Lietuvoje reguliuojančių teisės aktų – Autorių teisių ir gretutinių teisių įstatymas, kuris konkrečiai reglamentuoja autorių teisių ir gretutinių teisių pažeidimus ir jų gynimą.

Vadovaujantis minėtojo įstatymo 64 str. nuostatomis, autorių teisių pažeidimu yra laikomi šie veiksmai:

1) kūrinio ar gretutinių teisių objekto naudojimas (įskaitant išleidimą, atgaminimą, viešą atlikimą, transliavimą ir 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 ir eksportavimas, platinimas, gabenimas ar laikymas komerciniams tikslams;
3) įstatymu ar autorinėmis sutartimis 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 ar paslaugų tai padaryti siūlymas ir atitinkamų prietaisų, leidžiančių pašalinti tokias technines apsaugos priemones, gaminimas, importavimas, gabenimas ar laikymas, turint tikslą platinti, ir jų platinimas;
5) informacijos apie autorių teisių ar gretutinių teisių valdymą panaikinimas arba pakeitimas be autorių ar gretutinių teisių subjektų leidimo, taip pat kūrinių ir jų atlikimo įrašų, fonogramų ar jų kopijų platinimas, importavimas, transliavimas, viešas paskelbimas ar padarymas viešai prieinamais, neturint leidimo panaikinus arba pakeitus informaciją apie teisių valdymą; autoriaus ar atlikėjo asmeninių neturtinių teisių pažeidimas;
6) kitų įstatymo nuostatų pažeidimas.

Šios nuostatos Autorių teisių ir gretutinių teisių įstatyme įtvirtintos vadovaujantis ES direktyvomis, TRIPS ir WIPO interneto sutarčių nuostatomis.

Atkreiptinas dėmesys, kad įstatyme pateiktas pažeidimų sąrašas nėra baigtinis.

Labai panašų autorių teisių ir gretutinių teisių pažeidimų sąrašą pateikia ir galiojantys administraciniai bei baudžiamieji įstatymai. Vis dėlto minėtieji įstatymai specialiai nereglamentuoja ir nekriminalizuoja intelektinės nuosavybės pažeidimų e. erdvėje, o specifinių, tik e. erdvėje padaromų, intelektinės nuosavybės teisių pažeidimų, tokių kaip nuorodų į neteisėtai platinamas intelektinės nuosavybės kopijas teikimas interneto svetainėse, taip pat operacijos *P2P* tinkluose ir pačių šių tinklų operatorių su neteisėtu intelektinės nuosavybės turiniu atliekami veiksmai, šiuo metu specialiai nenustato ir nereglamentuoja. Pvz., administracinė atsakomybė už autorių teisių ir gretutinių teisių pažeidimus reglamentuojama ATPK 214[10] str., atsakomybė numatyta už neteisėtą literatūros, mokslo ar meno kūrinio (įskaitant kompiuterių programas ir duomenų bazes) ar gretutinių teisių objekto arba jų dalies viešą atlikimą, atgaminimą, viešą paskelbimą, kitokį naudojimą bet kokiais būdais ir priemonėmis nekomerciniais tikslais, taip pat neteisėtų kopijų platinimą, gabenimą ar laikymą komerciniais tikslais. Iki 2009 m. liepos 15 d. galiojusioje šio straipsnio redakcijoje administracinė atsakomybė buvo nustatyta tik už autorių teisių ir gretutinių teisių saugomų objektų naudojimą, siekiant turtinės naudos – šio požymio atsisakymas aktualus užkardant intelektinės nuosavybės teisių pažeidimus e. erdvėje, nes gerokai palengvina jų įrodinėjimą.

Dėl intelektinės nuosavybės tarptautiškumo su ja susiję pažeidimai jau patys savaime yra tarptautinis reiškinys. Atsižvelgiant į menkas išlaidas, susijusias su intelektinės nuosavybės pažeidimais, pvz., masinių intelektinės nuosavybės produktų (fonogramų ar kompiuterių programų) atgaminimu ir tiražavimu, net ir sąlygiškai maža valstybė (pvz., Bulgarija) piratinę produkciją gali tiekti ne tik savo vidaus rinkai – pasitelkusi internetą ja gali aprūpinti visą pasaulį. Todėl intelektinės nuosavybės pažeidėjų pelnai yra milžiniški, tokia neteisėta veikla tampa patraukli organizuotiems nusikaltėliams ir yra glaudžiai susijusi su kitomis visuomenei itin pavojingomis nusikalstamomis veikomis: pinigų plovimu, prekyba žmonėmis ir narkotinėmis medžiagomis, tarptautiniu terorizmu.

Dėl minėtųjų priežasčių efektyvi kova su intelektinės nuosavybės teisių pažeidimais e. erdvėje iš esmės reikalauja tarptautinių pastangų ir naujų tarptautinės teisės normų. Tokia tarptautinė iniciatyva kovojant su intelektinės nuosavybės teisių pažeidimais internete galėjo būti 2012 m. pasirašyta Prekybos sutartis dėl kovos su klastojimu (angl. *Anti-Counterfeiting Trade Agreement,* ACTA). Viena iš ACTA nustatytų naujovių, ypač aktualių ginant autorių ir gretutines teises internete, buvo įpareigojimas interneto paslaugų teikėjams dalyvauti nustatant pažeidimus darančius abonentus. Pagal ACTA 27 str. 4 d., interneto paslaugų teikėjai gali būti įpareigoti

atskleisti informaciją apie abonentus, kurių paskyros buvo naudojamos intelektinės nuosavybės teisių pažeidimams, kad juos būtų galima patraukti atsakomybėn.

Deja, ACTA dėl savo neskaidrumo ir nedemokratiškumo irgi yra netinkamo teisinio proceso pavyzdys. Šio tarptautinio dokumento nuostatos buvo visapusiškai sukritikuotos dėl nekonkretumo ir didelės žmogaus teisių pažeidimo rizikos. Norint iš esmės atskleisti informaciją apie abonentą, prieš tai būtina ją surinkti ir sutvarkyti, todėl kyla klausimas, kokios apimties informacija, kokiomis sąlygomis ir kaip ilgai turėtų būti saugoma. Dar labai padidėja galimybės turimą informaciją neteisėtai naudoti kitiems tikslams, be to, tokios informacijos tvarkymas pasunkintų viešųjų tinklų infrastruktūrą ir interneto paslaugų teikėjai dėl jo patirtų didelių ekonominių sąnaudų, kurios tikriausiai būtų perkeltos vartotojams. Abejonės, ar tokios nuostatos neprieštarauja pagrindinėms žmogaus teisėms, ypač teisei į privataus gyvenimo neliečiamumą ir žodžio laisvę, lėmė, kad 2012 m. liepą Europos Parlamentas nepritarė ACTA.

Apibendrinant dėl intelektinės nuosavybės pažeidimų e. erdvėje susiklosčiusią padėtį, reikia pripažinti, kad kol kas nei nacionalinė, nei tarptautinė teisė neturi veiksmingų mechanizmų, padedančių apginti elektroninę intelektinę nuosavybę, ypač privatiems asmenims, kuriems sunku orientuotis esant tokiam sudėtingam teisiniam intelektinės nuosavybės teisių reguliavimui, be to, teisinė gynyba yra labai brangi ir reikalauja didelių laiko sąnaudų. Teisminės procedūros keliose Lietuvos instancijose gali užtrukti ne vienus metus, o elektroninių intelektinės nuosavybės objektų komercinio atsiperkamumo laikotarpis (ypač kompiuterių programų) paprastai neviršija dvidešimt keturių mėnesių. Akivaizdu, kad ginti intelektinės nuosavybės teises, kurios dar nesibaigus gynimo procesui praranda savo komercinę vertę, yra neefektyvu ar netgi beprasmiška.

Dar viena paminėtina intelektinės nuosavybės teisių gynimo problema – vis dar nepakankama teismų kompetencija intelektinės nuosavybės teisės srityje. Kartais ginčai dėl intelektinės nuosavybės teisių sprendžiami teisėjų, kurie neturi tokių bylų nagrinėjimo patirties, dėl to teisių gynimas tampa dar sunkesnis, ilgesnis ir brangesnis. Minėtoji aplinkybė lemia ir kitą žalingą problemą – perdėtą intelektinės nuosavybės teisių gynimą, paremtą paviršutiniškais įrodymais ir tendencingu jų vertinimu.

7 skirsnis. Intelektinės nuosavybės pažeidimai *P2P* tinkluose

Prieš dešimtmetį atsiradę pažeidimai *P2P* tinkluose, šiandien yra labiausiai paplitusi ir daugiausia žalos daranti intelektinės nuosavybės pažeidimų e. erdvėje forma. Naujausia jų atmaina tapo pažeidimai naudojant srautinį neteisėto e. turinio pateikimą ir e. debesijos įrankius, tokius kaip debesijos duomenų įkėlimo paslaugos, kurios prieinamos bet kuriam interneto vartotojui, ir taip suteikiama galimybė anonimiškai platinti neteisėtą e. turinį.

P2P tinklais gali būti platinamas bet koks e. turinys – tiek įprastas (muzikos ar garso ir vaizdo kūriniai), tiek naujas (išmaniųjų telefonų programėlės). Nuo 2011 m. viename populiariausių *P2P* tinklų – *the Pirate Bay* – jau yra platinami elektroniniai *3D* modeliai. Bet koks elektroninis turinys skaitmeninių bylų forma yra *P2P* piratavimo taikinys. Neteisėtos elektroninės intelektinės nuosavybės kopijos (neteisėtas e. turinys) iš esmės yra tapačios originalui (ar bent jau pirmajai kopijai), nesusidėvi jas naudojant, be to, leidžia vartotojui nedelsiant pasiekti bet kurią įrašytos informacijos dalį ir gali būti vienu metu (lygiagrečiai) naudojamos neriboto kiekio vartotojų. Be to, neteisėto e. turinio paklausą didina dar ir tai, kad jis gali būti pasiekiamas bet kokiu išmaniuoju įrenginiu.

Dar vienas svarbus intelektinės nuosavybės pažeidimų *P2P* tinkluose arba debesijos saugyklose ypatumas – iš šių pažeidimų dažnai gaunama milžiniškos komercinės naudos, tačiau ji gaunama netiesiogiai, t. y. ne už patį e. turinį, o, pvz., reklamos paslaugas atitinkamuose interneto portaluose arba kaip „parama“ ar portalo narystės mokestis. *P2P* pažeidėjai itin sėkmingai naudoja naujausius teisėtus verslo modelius ir technologinius sprendimus: socialinius tinklus, elektroninius interneto aukcionus, bylų beserverinio apsikeitimo protokolus (kurie yra *P2P* tinklų, tokių kaip *Bittorent*, pagrindas), pokalbių programas *(ICQ, IRC)*, vartotojų forumus ir naujienų grupes, sujungdami juos į visaapimančius interneto portalus, kur vykdoma labai įvairi teisėta veikla.

P2P tinklai iš esmės yra tapę specializuotais socialiniais tinklais ar interneto pramogų portalais. Tokia padėtis kelia didelę grėsmę ir ta prasme, kad tam tikros visuomenės grupės, ypač intelektinės nuosavybės teisių turėtojai, bet kokias naujas interneto technologijas, neatsižvelgdami į jų teisėto naudojimo galimybes, sieja būtent su intelektinės nuosavybės pažeidimais, taip iš esmės kliudydami technologinei pažangai ir plėtrai. Geriausiai tai rodo JAV patirtis, kur muzikos industrijos atstovai buvo iškėlę teismines bylas pirmiesiems vaizdo arba *MP3* grotuvų gamintojams, siekdami užkirsti kelią šių technologijų plėtrai ir paplitimui tarp vartotojų, nes buvo baiminamasi, kad minėtieji įrenginiai bus daugiausia naudojami

piratavimo tikslams. Būtina aiškiai suvokti, kad modernūs *P2P* duomenų perdavimo protokolai ir platformos yra labai svarbūs teikiant daugelį teisėtų interneto paslaugų (pvz., populiari interneto telefonijos paslauga *Skype* naudoja tuos pačius beserverinius duomenų perdavimo protokolus kaip ir *Bittorent P2P* tinklai), dėl to besąlygiški draudimai ar *P2P* platformų veiklos apribojimai turi būti nustatomi itin atsargiai.

Naujausia skaitmeninio informacijos pateikimo tendencija tiek teisėtuose, tiek neteisėtuose *P2P* tinkluose yra ne tik beserverinis duomenų apsikeitimas, bet ir vadinamasis srautinis elektroninio turinio pateikimas (angl. *streaming)*, kuris apsiriboja tik laikinomis tarpinėmis intelektinės nuosavybės objektų mažų fragmentų fiksacijomis ir vienu metu vartotojui nepateikia viso intelektinės nuosavybės objekto.

Populiariausias modernus *P2P* protokolas šiuo metu yra *Bittorent*. Jis buvo sukurtas kaip efektyvesnis (greitesnio ir mažiau išteklių naudojančio) duomenų perdavimo protokolas. *Bittorent P2P* tinklai yra decentralizuoti, juose duomenimis apsikeičiama beserveriniu būdu, todėl esamomis techninėmis priemonėmis sukontroliuoti jais vykdomų neteisėtų intelektinės nuosavybės kopijų apsikeitimų ir jų platinimo beveik neįmanoma. E. turinio bylų sklaida naujausiais *P2P* tinklais yra beveik nekontroliuojama, o duomenys gali būti lengvai persiunčiami ir platinami internete pasauliniu mastu nesant jokių tarpinių serverių, konkrečios infrastruktūros ar duomenų, apsiribojant tik laikinomis srautinėmis duomenų struktūromis, kurios nuolat kinta, priklausomai nuo tam tikrus duomenų apsikeitimo protokolus ir platformas naudojančių galinių įrenginių. Nauji *P2P* e. ryšių protokolai, tokie kaip tiesioginis apsikeitimas adresais (angl. *Peer Exchange, PeX)*, paskirstytos duomenų struktūros ar paskirstyto duomenų žemėlapio (angl. *distributed hash table*, *DHT)* platformos, veiksmingai naudojami keičiantis duomenimis tarp atsitiktinių nutolusių kompiuterių be jokių tarpinių serverių, konkrečios infrastruktūros ar netgi tam tikro (kiekybiškai didesnio) duomenų kiekio viename galiniame įrenginyje. Tokių tinklų duomenų fragmentai yra pasklidę globaliame tinkle. Netgi tuo atveju, jeigu nė vienas į *P2P* tinklą susijungusių galinių įrenginių tam tikru laiko momentu neturi 100 proc. e. turinio bylos, visa ši byla gali būti sukomponuota iš tinkle pasklidusių atskirų jos fragmentų.

Naudojant *PeX* ir *DHT* šiuolaikiniuose *P2P* tinkluose, e. turinio sklaida ir atsisiuntimas yra visiškai decentralizuoti, t. y. juose iš esmės nebėra konkrečios infrastruktūros (serverio ar tinklo dalies), kurią atjungus tinklas nebeveiktų. Vartotojai, norintys platinti e. turinį, turi tik specialiu formatu suformuluoti e. turinio objekto ir savo kompiuterio adresą (sukurti specialią *torrent* bylą, kuri savo esme yra tinklo kodas ir nuorodų į naudojamus

duomenų apsikeitimo protokolus bei platformas rinkmena). Bet kuris kitas vartotojas, kuriam prieinama *torrent* byla, pasitelkęs specialią programinę įrangą, galės atkoduoti šį kodą ir naudodamas nurodytus protokolus bei platformas parsisųsti tą e. turinį, kuriam sukurta *torrent* byla, ir joks tarpinis serveris nebus reikalingas. Tarpiniai serveriai gali būti naudojami tik apsikeičiant *torrent* bylomis (koduotais adresais), bet ne neteisėtu turiniu. Pabrėžtina, kad *torrent* bylos gali būti platinamos absoliučiai bet kokiu būdu, kuris naudojamas keistis duomenimis tarp dviejų kompiuterių (pvz., elektroniniu paštu). Vartotojas, norintis parsisiųsti neteisėtą turinį, turi susirasti atitinkamą *torrent* bylą bet kuriame jam prieinamame šaltinyje ir taip galės parsisiųsti norimą turinį iš bet kurio kito vartotojo (nebūtinai iš sukūrusiojo šią *torrent* bylą), kurio kompiuteryje yra atitinkama *torrent* byla ir bent mažiausias joje koduojamo e. turinio fragmentas. *Torrent* byloje koduojamo turinio fragmentai gali būti laisvai pasklidę interneto tinkle. Be to, kiekvienas vartotojas, atsisiunčiantis e. turinį *Bittorent P2P* tinklu, tokį turinį lygiagrečiai siunčia ir kitiems vartotojams (ir atgamina, ir platina tuo pat metu).

Modernaus *Bittorent P2P* tinklo ypatumai lemia, kad tarpiniai serveriai, valdomi trečiųjų asmenų ar tarpininkų, iš esmės nereikalingi tarp vartotojų vykstant neteisėto turinio mainams. Jų paskirtis gali būti palengvinti vartotojų galimybes apsikeisti tik *torrent* bylomis. Neteisėto turinio mainai gali sėkmingai vykti net ir nesant palaikomojo tarpininko serverio. Netgi visiškai pašalinus tarpinius *P2P* tinklo serverius, atskiri vartotojai neteisėtą turinį gali siųsti *P2P* tinklu ir jį gauti.

Deja, teisinės sistemos dalyviai (tarp jų patys teisių turėtojai ir jiems atstovaujantys teisininkai) minėtųjų šiuolaikinių *P2P* ypatumų dažniausiai išvis nesupranta, suvokia miglotai arba, stokodami techninės kompetencijos, interpretuoja juos visiškai neteisingai.

Vartotojui Lietuvoje iškeltoje pirmojoje administracinio teisės pažeidimo byloje policijos pareigūnai surašė administracinio teisės pažeidimo protokolą už tai, kad jis, naudodamasis *uTorrent* protokolu, parsisiuntė kompiuterių programos kopiją ir padarė ją viešai prieinamą kompiuterių tinklais (internete) nekomerciniams tikslams. Pabrėžtina, kad *uTorrent* yra ne protokolas (duomenų apsikeitimo formatas), o viena iš daugelio taikomųjų programų, kuri leidžia tvarkyti *torrent* bylas. Ši ir kitos šiurkščios techninės bei procesinės klaidos lėmė, kad 2010 m. kovo 15 d. Kauno miesto apylinkės teismas priėmė visiškai teisingą nutarimą nutraukti administracinio teisės pažeidimo bylą Nr. A-785-311/2010. Vėliau tokį sprendimą patvirtino ir Lietuvos vyriausiasis administracinis teismas.

Dėl tokių techninės kompetencijos spragų teisinė *P2P* tinklo kontrolė yra itin sudėtinga. Pirmoji priemonė, kuri istoriškai buvo pasitelkta

siekiant suvaldyti *P2P* tinklų veiklą – *P2P* tinklų ir jų veiklos pripažinimas intelektinės nuosavybės pažeidimų e. erdvėje įrankiais. Būtent tokią poziciją suformulavo JAV teismai, dar 1999 m. sprendimu pripažindami *Napster* tinklą iš esmės prisidėjus prie intelektinės nuosavybės teisių pažeidimų, kuriuos naudodamiesi tinklu padarė jo vartotojai. Kadangi *Napster* centralizuotai kontroliavo (indeksavo) neteisėtą tinklo turinį ir jo vartotojų veiksmus, be to, žinojo apie intelektinės nuosavybės teisių pažeidimus ir juos ignoravo, jis buvo pripažintas atsakingu už intelektinės nuosavybės teisių pažeidimus taikant solidariosios atsakomybės (kartu su pačiais vartotojais) ir netiesioginės atsakomybės doktrinas. Žiūrinti iš perperktyvos, *Napster* byla yra gana triviali, nes *P2P* serveris veikė visiškai centralizuotai ir buvo būtinas apsikeičiant neteisėtu turiniu (be serverio apsikeitimas buvo neįmanomas). 2005 m. *Grokster* byloje buvo susidurta su iš dalies decentralizuotu *P2P* tinklu. *Grokster* nevykdė centralizuoto neteisėto turinio kontrolės, tačiau be *Grokster serverių neteisėto turinio apsikeitimas tarp vartotojų vis tiek nebuvo įmanomas.* Be to, *Grokster* atsakomybė konstatuota dar ir dėl to, kad šis aiškiai pozicionavo savo paslaugas ir reklamavo jas kaip intelektinės nuosavybės teisių pažeidimų įrankį. Teismas konstatavo, kad asmuo, kuris *suteikia įrankį ir pats skatina trečiuosius asmenis šį įrankį naudoti autorių teisių ir gretutinių teisių pažeidimams, akivaizdžiai sudarydamas įspūdį arba kitaip parodydamas galimybes daryti pažeidimus, yra atsakingas dėl trečiųjų asmenų daromų pažeidimų*. Minėtojoje byloje teismas nustatė, kad *Grokster* veiksmų negalima laikyti pasyviais, nes nuo pat tinklo naudojimo pradžios buvo imtasi aktyvių rinkodaros veiksmų naudoti tinklą neteisėto turinio sklaidai.

Visiškai decentralizuotų *P2P* tinklų atžvilgiu pagal esamas teisės normas (net ir taikant solidariosios ir netiesioginės atsakomybės doktrinas) atsakomybės taikymas iš esmės yra neįmanomas. Tą parodė *KaZaA P2P* tinklo byla Olandijoje. Teismas netaikė teisinės draudimų ar atsakomybės *KaZaA* atžvilgiu, motyvuodamas išsamia decentralizuoto *P2P* tinklo veikimo principų analize, galimybe tokį tinklą naudoti teisėtiems tikslams ir tai, kad tinklo valdytojas neturi galimybės kontroliuoti vartotojų veiksmų.

Apskritai sprendžiant, atsakomybės už intelektinės nuosavybės teisių pažeidimus *P2P* tinkluose būtina atsiriboti nuo pačios *P2P* platformos neigiamo vertinimo, o vietoj to ypač išsamiai išanalizuoti konkretaus subjekto, valdančio *P2P* platformą, veiksmus ir vaidmenį darant pažeidimus tiek teisine, tiek technine prasme.

Visi asmenys, teikiantys paslaugas e. erdvėje, tam tikra prasme yra tarpininkai (pvz., universitetas tarpininkauja teikdamas studentams interneto prieigos ir elektronio pašto paslaugas, o interneto naujienų portalas

– skelbdamas trečiųjų šalių turinį ir suteikdamas vartotojams galimybę komentuoti naujienas). *P2P* platformų veikla pati savaime niekuo nesiskirtia nuo kitų e. erdvės tarpininkų. *P2P* platforma irgi veikia kaip tarpininkas tarp vartotojų, kurie keičiasi e. turiniu. Yra daugybė *P2P* platformų, išimtinai orientuotų tik į apsikeitimą teisėtu specializuotu e. turiniu.

Dėl nurodytųjų priežasčių vienas iš pamatinių e. erdvės teisinio reguliavimo principų yra tarpininkų – interneto paslaugų tiekėjų ir kitų e. erdvės tarpininkų – atsakomybės ribojimas. Tarpininkų atsakomybės apribojimai nustatyti ES elektroninės komercijos direktyvoje bei Informacinės visuomenės paslaugų įstatyme ir jie galioja visiems e. erdvės tarpininkams, iš jų ir *P2P* platformoms. Tarpininkų atsakomybės apribojimai plačiau analizuojami skyriuje „Interneto teisė".

Atsižvelgiant į *P2P* platformos kaip tarpininko atsakomybės apribojimą, ypač svarbu nustatyti, ar asmens, valdančio *P2P* platformą ir veikiančio kaip e. erdvės tarpininkas, dalyvavimas pažeidžiant intelektinės nuosavybės teises yra būtinas – ar be šio asmens dalyvavimo tretieji asmenys galėjo padaryti analogišką pažeidimą. Be to, svarbu nustatyti, ar asmuo galėjo imtis priemonių, siekdamas užkirsti vartotojams kelią padaryti pažeidimą, ar jis kaip nors skatino ir kurstė juos nusikalsti. Vien tai, kad asmuo net ir aktyviai valdo tam tikrą interneto infrastruktūrą, kurią naudodami tretieji asmenys daro intelektinės nuosavybės teisių pažeidimus, nėra pakankama prielaida teisinei atsakomybei nustatyti.

Būtina akcentuoti, kad intelektinės nuosavybės pažeidimai internete ir juos palengvinančios technologijos neturi būti suabsoliutinami. Dalis pažeidimų padaroma dėl pačių intelektinės nuosavybės teisių turėtojų konservatyvios ar net neteisėtos politikos, piktnaudžiavimo turimomis intelektinės nuosavybės teisėmis. Be to, technologijos, reikalingos intelektinės nuosavybės pažeidimams, nepalyginamai efektyviau gali būti naudojamos teisėtai ir yra ypač reikšmingos užtikrinant visos visuomenės informacijos ir socialinių paslaugų prieinamumą bei ilgalaikę jos socialinę ir ekonominę plėtrą.

Lietuvoje *P2P* tinklų pažabojimas vis dar yra atvira problema. Visi ligšioliniai mėginimai suvaldyti *P2P* tinklus iš esmės yra nekoordinuoti, nors ir skatinami pozityvių tikslų, tačiau teisiškai yra skuboti ir menkai pagrįsti.

Esama intelektinės nuosavybės teisių gynimo doktrina Lietuvoje neatspindi šiuolaikinių *P2P* tinklų ypatumų, nes iš esmės yra pagrįsta pirmųjų *P2P* tinklų, kurie išsiskyrė centralizuota infrastruktūra ir centralizuoto serverio būtinimu, supratimu. Šiuo atveju serverio vadytojo atsakomybė už prisidėjimą prie intelektinės nuosavybės pažeidimų yra akivaizdi, tačiau šiuolaikiniai visiškai decentralizuoti *Bittorent P2P* ar srautiniai *P2P* tinklai

yra kokybiškai kitokie. Jiems išvis nebūtini serveriai, todėl teisiniu požiūriu serverio valdytojas nedalyvauja pažeidžiant intelektinės nuosavybės teises. Priešingas interpretavimas iš esmės prilygtų bet kurių modernių interneto paslaugų (tokių kaip socialiniai tinklai ar interneto paieška), kurios pelnosi iš to, kad suteikia vartotojams galimybę apsikeisti vienam iš kito gaunama informacija (beje, dažniausiai neteisėta), uždraudimui.

Atsižvelgiant į aukščiau išdėstytus dalykus, modernių decentralizuotų *P2P* tinklų atveju, pagal esamus įstatymus, remiantis CK 6.279 str., teisiškai yra nepagrįstas solidarios civilinės atsakomybės taikymas interneto serverių valdytojams. Norint juos patraukti atsakomybėn, būtini įstatymų pakeitimai, nustatantys aktyvias pareigas tarpininkui kontroliuoti apsikeitimą neteisėtu e. turiniu ir sankcijas už nekontroliuojamą pelnymąsi iš trečiųjų asmenų vykdomų neteisėtų veikų e. erdvėje ir tiesioginio poveikio sankcijas (tokias kaip interneto domenų areštas). Domenų arešto praktika sparčiai plinta JAV nuo 2010 metų. Areštavus domeną, buvo uždarytas vienas didžiausių *P2P* piratavimo tinklų *Demonoid.com*.

Kelios administracinių teisės pažeidimų bylos (neskaitant jau minėtosios pirmosios), iškeltos *P2P* tinklų vartotojams, net kelia abejonių dėl teisinio proceso režisavimo, pvz., pažeidėjai, akivaizdžiai veikiantys prieš savo interesą ir galbūt susitarę su teisių turėtojais, prisipažįsta padarę pažeidimą, bendrai siekdami suformuluoti precedentą, kuris būtų tinkamas ir toliau ginant teises.

Vienintelė byla, nukreipta prieš asmenis, kurie pelnosi iš trečiųjų asmenų vykdomų neteisėtų veikų e. erdvėje, Lietuvoje yra *Microsoft v. UAB N5 ir K. E.* (civ. byla Nr. 2-742-262/2012), plačiai žinoma kaip *Linkomanijos P2P* tinklo byla. Joje 2012 m. pabaigoje priimtas pirmosios instancijos sprendimas, o šiuo metu byla yra apeliacinės stadijos. Šioje byloje pirmosios instancijos teismas galbūt nepakankamai įsigilino į modernių *P2P* tinklų veikimo esmę, todėl kyla abejonių dėl galimo pavojingai plataus solidarios atsakomybės pagal CK 6.279 str. taikymo interneto serverių valdytojams (kai serveris nėra būtinas pažeidimams) ir globalių bet kokio *P2P* platformos naudojimo apribojimų (besąlygišku įpareigojimu nutraukti *Linkomanijos P2P* platformos veiklą, neatsižvelgiant į tai, kad ji gali būti teisėta). Be to, kyla abejonių dėl gana abstrakčių įrodymų ir civilinės atsakomybės (ypač priežastinio ryšio) standartų. Nors *Linkomanijos P2P* tinklas Lietuvos visuomenėje yra bendrai laikomas piratavimo avangardu, tokios nuostatos neturi būti kaip pagrindas, siekiant paminti esminius teisingo proceso principus ir nustatyti lengvesnes atsakomybės taisykles. Pabrėžtina, kad aptartoji teismų praktika JAV (net ir *Napster* atveju, kur tinklo valdytojo atsakomybė nekėlė jokių abejonių) apsiribojo

tik teisinės atsakomybės taikymu, o ne globaliu *P2P* platformų veiklos uždraudimu. Legalizavęsis *Napster* kaip teisėto e. turinio platinimo platforma veikia iki šiol.

Atskirai būtina pabrėžti, kad intelektinės nuosavybės teisių gynimas e. erdvėje beveik visada konfliktuoja su kitomis žmogaus teisėmis, ypač privatumo teise ir asmens duomenų teisine apsauga, žodžio ir saviraiškos laisve. Nustatant labai plačias solidarios atsakomybės taisykles interneto serverių valdytojams (kai serveris nėra būtinas pažeidimams) rizikuojama, kad šios taisyklės bus taikomos bet kokiems teisių pažeidimams internete ir taip sutrikdys laisvą informacijos cirkuliaciją – pamatinę interneto demokratinę vertybę.

Vartotojų atsakomybės atveju būtina pabrėžti, kad *P2P* tinklų vartotojus geriausiai identifikuoja *IP* adresas, kurį sudaro vartotojo asmens duomenys. Šių duomenų tvarkymas yra galimas tik esant griežtai iš anksto nusatytoms teisėto tvarkymo sąlygoms ir kriterijams. Neteisėtai apie vartotojų *IP* adresus surinkta informacija kaip įrodymai yra negalima ir neleistina. Vartotojų *IP* adresų rinkimas be jų žinios, vien dėl įtariamo civilinio intelektinės nuosavybės delikto, vienareikšmiškai nėra teisėtas asmens duomenų tvarkymo pagrindas.

Minėtąsias teisių kolizijas pripažįsta ir teismai. Pagal esamą *ESTT* praktiką C-275/06 *Promusicae v. Telefonica* byloje, pabrėžiama, kad privatumo teisės yra fundamentalios asmenų teisės ir jų apribojimas yra leistinas tik išimtiniais įstatymuose nustatytais atvejais, laikantis proporcingumo principo. Siekiant paneigti interneto vartotojo privatumą – atskleisti asmens duomenis, būtinus teisminei gynybai – nepakanka vien įtarimų dėl galimo intelektinės nuosavybės teisių pažeidimo. Iš esmės tai reiškia, kad teisių turėtojas pažeidimą turi įrodyti kitomis priemonėmis (pvz., vykstant administraciniam procesui). Ši pozicija visiškai teisingai priimta ir Vilniaus apygardos teismo 2012 m. birželio 28 d. nutartimi civilinėje byloje Nr. 2S-1416-302/2012, kurioje autorių teisių ir gretutinių teisių turėtojas, surinkęs *IP* adresų duomenis dėl galimo jo teisių pažeidimo, kreipėsi į teismą su prašymu atskleisti ir kitus pažeidėjų asmens duomenis. Teisių turėtojas prašė taikyti įrodymų užtikrinimo institutą ir ATGTĮ 79 str. įstatymo analogiją – įpareigoti interneto ryšio paslaugos teikėją pagal pateiktus duomenis nustatyti ir pateikti asmenų, kurie padarė kūrinius viešai prieinamus, tapatybės duomenis. Teismas teisių turėtojo prašymą atmetė ir konstatavo, jog nagrinėjamuoju atveju teisių turėtojas siekė ne įrodymų užtikrinimo, o teismo padedamas gauti duomenis, reikalingus tam, kad galėtų identifikuoti asmenis, kurie neteisėtai atgamino kūrinius ir pasitelkę *P2P* tinklą padarė juos viešai prieinamus, siekdamas šiems asmenims

pareikšti turtinius reikalavimus. Duomenys apie galimų pažeidimus padariusių asmenų tapatybę ir jų gyvenamąją vietą nelaikyti įrodymais CPK 177 str. 1 d. prasme, nes jie nepagrindžia tam tikrų aplinkybių ir nepatvirtina kokių nors faktų buvimo ar nebuvimo, jie susiję tik su konkrečių asmenų tapatybės bei gyvenamosios vietos nustatymu. Interneto ryšio paslaugos teikėjo įpareigojimas pateikti tokius duomenis akivaizdžiai prieštarautų imperatyvioms asmens duomenų apsaugos nuostatoms.

Apibendrinant Lietuvoje susiklosčiusią padėtį dėl intelektinės nuosavybės teisių pažeidimų *P2P* tinkluose, manytina, kad yra reikalingos naujos esminės materialinės teisės normos ir nauji teisių gynimo būdai. Mėginimai teismuose nustatyti atsakomybę pagal esamą teisine bazę (solidarios ir netiesioginės atsakomybės doktrinas) yra nevykę, nes iš esmės remiasi interpretaciniu žaismu, peržengia teisės aiškinimo ribas, sukuria prielaidas galimiems ypač svarbių žmogaus teisių pažeidimams ir tokiu būdu iš esmės iškreipia intelektinės nuosavybės teisių reguliavimą.

Teisinė problema yra ir tai, kad esamas reguliavimas daugiausia dėmesio skiria galutiniams neteisėto turinio vartotojams, tačiau nenumato specialių kovos su subjektais, kurie tiesiogiai ar netiesiogiai pelnosi iš dalijimosi neteisėtu turiniu internete (pvz., *P2P* svetainių valdytojais), priemonių. Intelektinės nuosavybės teisių gynimo sutelkimas į vartotojus yra neproduktyvus, pavojingas ir nepageidautinas, nes jis tiesiogiai supriešina intelektinės nuosavybės teisių turėtojus ir vartotojus, skatina intelektinės nuosavybės radikalizmą.

8 skirsnis. Teisinės kompiuterių programų apsaugos ypatumai

Kompiuterių programos (angl. *software)* yra svarbiausias naujas elektroninis intelektinės nuosavybės objektas. Populiariausios kompiuterių programos yra kompiuterio darbui naudojamos operacinės sistemos, taikomoji programinė įranga ir įvairių e. duomenų: skaičių, tekstų, piešinių, garsų ir kt., masyvai. Visa ši informacija kompiuterio viduje yra suskaitmeninta ir išreikšta dvejetaine skaičiavimo sistema (nuliukais ir vienetukais). Būtent programinė įranga suteikia kompiuteriui dirbtinio intelekto elementų ir jis tampa intelektualiu informacijos apdorojimo įrankiu.

Kompiuterių programos plačiausia prasme suprantamos kaip visuma elementų ir efektų, susijusių su kompiuterių programos kūrimu ir veikimu, išskyrus reikalingą techninę įrangą. Šiuolaikinė kompiuterių programos samprata apima ir duomenų struktūras bei šiuolaikinius įvesties ir išvesties elementus – sąsajas kaip savarankiškas kompiuterių programos

sudėtines dalis. Šiandien kompiuterių programa galima laikyti kompiuterių programos elementų visumą ir jų tarpusavio sąveikas, pirminį ir objektinį programos kodą, specifikacijas ir veikimo schemą, elektroniniu būdu išsaugotą informaciją (failus), duomenis ir kompiuterių programa valdomo kompiuterio veikimo rezultatus: išspausdintą medžiagą, garso ir vaizdo išraiškas, grafinę vartotojo sąsają, failų ir grafinių vaizdų struktūras, interneto sąsajas ir kt.

1. Kompiuterių programos elementai, kuriems taikytina teisinė apsauga

Autorių teisių ir gretutinių teisių įstatyme pateikiamas kompiuterių programos apibrėžimas – tai 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 būtų galima sukurti minėtąją instrukcijų visumą. Deja, šis apibrėžimas yra morališkai pasenęs ir neatspindi svarbiausių saugotinų elementų.

Teisininkui labai svarbu suvokti dualistinę kompiuterių programų prigimtį ir jas sudarančius elementus, nes šiems elementams galiausiai ir taikoma teisinė apsauga. Teisiniu požiūriu svarbūs ir saugotini kompiuterių programos elementai yra tiek jų tekstinė išraiška (pirminis kodas, objektinis kodas), tiek kompiuterių programa valdomo kompiuterio veikimo rezultatai (vartotojo ir kitos sąsajos, failų ir grafinių vaizdų išdėstymas, garso ir vaizdo programos prezentacija). Tekstinė kompiuterių programos išraiška tiesiogiai lemia jos veikimo rezultatus ir, priešingai, kompiuterių programos tekstinė išraiška ir veikimo rezultatai tuo pat metu yra nepriklausomi, nes analogiškus veikimo rezultatus įmanoma pasiekti pasitelkiant kitokios tekstinės išraiškos kompiuterių programą, o visiškai skirtingų išraiškų kompiuterių programos gali atlikti tuos pačius uždavinius (pasiekti tų pačių rezultatų). Kūrybinis procesas apima abu šiuos kompiuterių programos aspektus.

Atsižvelgiant į dualistinę kompiuterių programų prigimtį, jas galima apibūdinti kaip techninius mechanizmus, išreikštus tekstinėmis priemonėmis. Tokiais „tekstiniais mechanizmais“ galima pasiekti konkrečių naudingų rezultatų, sudarytų iš visumos veiksmų, kuriuos gali atlikti kompiuteris, vykdydamas kompiuterių programos instrukcijas. „Tekstiniams mechanizmams“, kaip ir bet kokiems kitiems techniniams mechanizmams, gali būti taikomi inžineriniai sprendimai ir naujovės. Kompiuterių programas, kaip ir techninius mechanizmus, sudaro visuma tarpusavyje suderintų ir sąveikaujančių elementų – algoritmų ir duomenų struktūrų, kurių kiekvieno

„gedimas“ dažniausiai lemia viso mechanizmo veiklos sutrikimą. Be to, rezultatai, pasiekiami naudojantis kompiuterių programomis, gali būti įmanomi pasiekti ir grynai techninėmis priemonėmis.

Teisine kompiuterių programų apsauga moksliniu ir įstatymų leidybos lygmeniu pradėta aktyviai domėtis XX a. šeštajame dešimtmetyje. 1971 m. kompiuterių programų teisinės apsaugos klausimams spęsti prie Pasaulinės intelektinės nuosavybės organizacijos (toliau – PINO) buvo sudaryta speciali darbo grupė, kuri pateikė gana kontroversiškų siūlymų ir šie nebuvo praktiškai įgyvendinti. 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 pastangų pateikti kokių nors kompiuterių programų teisinės apsaugos rekomendacijų. Tuo pat metu kaip ir PINO, kompiuterių programų teisinės apsaugos klausimais aktyviai domėjosi Tarptautinė pramoninės nuosavybės apsaugos asociacija (toliau – AIPPI). 1975 m. AIPPI rekomendavo kompiuterių programų teisinei apsaugai taikyti autorių teises.

Pirmuosius mėginimus nustatyti teisinę kompiuterių programų apsaugą galima apibendrinti kaip pastangas apsispręsti, ar kompiuterių programoms turi būti taikomos jau esamos tradicinės intelektinės nuosavybės teisės normos, ar turi būti ieškoma naujų *sui generis* teisinių instrumentų. Tradicinės intelektinės nuosavybės normų šalininkai kaip teisinės kompiuterių programų apsaugos modelį siūlė jau esamus intelektinės nuosavybės teisės institutus: autorių teises, patentų ir komercinių paslapčių teisę. Pradedant 1980 m. JAV autorių teisių aktų pakeitimais ir įtvirtinant ES direktyvą 91/250/EEB dėl kompiuterių programų teisinės apsaugos (nuo 2009 m. šią direktyvą pakeitė konsoliduotoji Direktyva 2009/24/EB), autorių teisės tapo svarbiausia kompiuterių programų teisinės apsaugos forma.

Kompiuterių programoms autorių teisės taikomos vadovaujantis trimis teisinės apsaugos principais:

1) programa pagal autorių teisę saugoma taip pat, kaip ir literatūros kūrinys;
2) programa saugoma neatsižvelgiant į jos išraiškos formą;
3) programa saugoma tik tuo atveju, jeigu yra originali.

Kompiuterių programos pagal Berno konvenciją dėl literatūros ir meno kūrinių apsaugos turi būti saugomos autorių teisės normomis kaip literatūros kūriniai. Nuoroda į Berno konvenciją suprantama kaip autorių teisių principų, nustatytų šioje konvencijoje, galiojimas kompiuterių programoms, tačiau ji nereiškia, kad kompiuterių programa visiškai sutapatinama su literatūros kūriniu. Teisinė kompiuterių programos apsauga

taikoma ir programos parengiamajai medžiagai, ir sąsajoms, tai iš esmės apima aukščiau aptartus techninius kompiuterių programos elementus, kurių visuma sudaro kompiuterių programą. Pabrėžtina, kad kai kurios šiuolaikinės programos, pvz., tvarkyklės, pagal savo atliekamas funkcijas gali būti prilyginamos sąsajoms, todėl jų teisinė apsauga ypač svarbi.

Pagal bendrą autorių teisių principą, autorių teisės į kompiuterių programą atsiranda nuo pat jos sukūrimo momento, t. y. nuo kompiuterių programos išeities kodo užbaigimo. Visiškai sukurta programa turi būti užfiksuota bet kokioje materialiojoje išraiškos laikmenoje, kad galėtų būti suvokta kitų asmenų. Kompiuterių programos kūrimo parengiamosios medžiagos atžvilgiu teisinės apsaugos atsiradimo momentas turėtų būti nustatomas nuo tada, kai parengiamoji medžiaga pasiekia tokį kokybinį lygį, kad ją naudojant vėlesniu etapu būtų galima sukurti baigtinę kompiuterių programą, o teisinė apsauga, taikytina parengiamajai medžiagai, prilyginama teisinei apsaugai, kuri bus taikoma baigtinei kompiuterių programai. Teisinė apsauga taikytina kompiuterių programoms, išreikštoms bet kokia forma. Atsižvelgiant į autorystės nustatymo sunkumus, autorių teisių turėtojams rekomenduotina pasirūpinti autorystės užfiksavimo mechanizmu, pvz., įtraukti į kompiuterių programą individualizuotų programos kodo eilučių, įterpti komentarų, sąmoningų klaidų ir kt. Kompiuterių programų registravimas dažnai yra sudėtingas ir menkavertis jų autorystės ir sukūrimo laiko įrodymas.

Idėjos ir išraiškos dichotomijos doktrina ypač svarbi kompiuterių programoms. Ši doktrina daugeliu atvejų lemia kompiuterių programų teisinės tekstinių ir netekstinių išraiškos elementų apsaugos ribas. Idėjos ir išraiškos dichotomijos doktrinos taikymas kompiuterių programoms komplikuojasi tada, kai programuotojas turi labai ribotas išraiškos priemones, kad kompiuterių programai būtų pritaikytos tos pačios idėjos ir principai.

Vadovaujantis svarbiausiu autorių teisių principu, kompiuterių programa turi būti saugoma, jeigu ji yra originali, t. y. ji yra paties autoriaus intelektualinės veiklos rezultatas. Jokie kiti kriterijai negali būti taikomi, siekiant nustatyti, ar programa yra saugotina. Programos originalumui patikrinti negali būti taikomi jokie kiekybiniai ar estetiniai kriterijai.

Berno konvencija ar kiti tarptautiniai dokumentai nepateikia jokių kriterijų, kas laikytina „kūriniu“ kiekybės ir kokybės prasme, be to, nėra jokių „originalumo“ kriterijų. Deja, visa, kas sudaro kūrinį, o konkrečiai kompiuterių programų atveju – kelių eilučių kodas yra laikytinas programa – turi būti vertinama individualiai, ir aiškių objektyvių kriterijų tam nėra. Nagrinėjant tokias situacijas reikėtų įvertinti, ar konkretus kodas yra naujas, ar jis pakeičiamas (ar galimi kitokie išraiškos būdai), ar nustatytas

atgaminimo faktas ir kokiems tikslams jis buvo atliktas, o sprendžiant klausimą, ar konkretus kodas gali būti pripažįstamas kaip savarankiška kompiuterių programa, būtina įvertinti, ar šis kodas yra pakankamas, kad atliktų tam tikrą savarankišką funkciją ir pasiektų konkretų rezultatą.

Teisinei kompiuterių programų apsaugai taikomos ir yra ypač aktualios autorių teisės objekto ribojimo, idėjos ir išraiškos dichotomijos bei *scenes-a-faire* doktrinos.

Apibendrinant galima teigti, kad kompiuterių programų ir literatūros kūrinių autorinės apsaugos rūšys viena kitos atžvilgiu yra analogiškos. Svarbiausia kompiuterių programų autorinės apsaugos problema (ir ribotumas) – kompiuterių programų netekstinių elementų apsauga. Atsižvelgiant į tradicinius autorių teisių principus, ši 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 labai ribota. Ši aplinkybė tapo viena svarbiausių patentinės kompiuterių programų apsaugos prielaidų.

Neturtinių autorių teisių – ypač teisės į kūrinio pavadinimą ir autoriaus vardo nurodymą, 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 pabrėžiamas dar XX a. devintajame dešimtmetyje. Atsižvelgiant į utilitarinį ir techninį kompiuterių programų pobūdį ir teisės jurisprudenciją, 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 analogiškos turtinėms teisėms į bet kokius kitokius kūrinius. Turtinių teisių išimtys kompiuterių programoms iš esmės yra svarbesnės. Kompiuterių programų, kaip teisinės apsaugos objekto, technologiniai ypatumai lemia skirtingas autoriaus (teisių turėtojo) teisių į šias programas išimtis. Šių išimčių turinys tarptautiniu mastu yra palyginti bendras, o bendrasis jų principas – būtinumas sąžiningai naudoti kompiuterių programas pagal jų tiesioginę paskirtį. Ypač specifinė išimtis iš autoriaus (teisių turėtojo) teisių yra ir programos naudotojo teisė dekompiliuoti programą ar jos dalį suderinamumo tikslais. Programos įprastinis naudojimas – įkėlimas į kompiuterio techninę įrangą ir paleidimas bei techninė jos priežiūra 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, jeigu įgyta teisė naudotis pačia programa ar jos kopija. Dar svarbu atkreipti dėmesį į informacinės visuomenės paslaugų teikėjų atsakomybės problemas. Interneto prieigos ar informacijos perdavimo ir jos įkėlimo paslaugų teikimas technine prasme reikalauja siunčiamos informacijos (ir kompiuterių programų) laikino atgaminimo, panašiai kaip ir kompiuterių programos įprastinis naudojimas kompiuteryje, todėl būtina numatyti specialią laikino techninio atgaminimo išimtį. Be to, turi būti apribota paslaugų teikėjų atsakomybė tuo atveju, kai šių paslaugų vartotojai teikėjo kompiuterių tinklais perduoda ar į paslaugų teikėjo serverį įkelia neteisėtas kompiuterių programų kopijas, kur šios gali būti viešai prieinamos.

Kompiuterių programų autorių teisių turėtojai paprastai reglamentuoja minėtųjų programų naudotojų teises licencinėmis sutartimis, kuriomis šios teisės į kompiuterių programą gali būti perduodamos visiškai ar iš dalies. Kompiuterių programų atveju plačiai paplitusios ir teisiškai pripažįstamos vadinamosios atplėšiamosios pakuotės (angl. *shrink-wrap)* ir elektroninės licencinės sutartys.

Kompiuterių programų atgaminimas, adaptavimas ir keitimas gali būti atliekami neturint teisių turėtojo sutikimo, jeigu tokie veiksmai yra būtini teisėto įgijėjo kompiuterių programai naudoti pagal paskirtį (įkelti, paleisti ir pan.) bei klaidoms ištaisyti. Tai galioja tik teisėtam programos įgijėjui (asmeniui, kuris teisėtai turi programos kopiją ir teisę naudotis šia programa). Reikėtų atkreipti dėmesį, kad programos paskirtis gali būti apibrėžta licencinėje sutartyje, kur gali būti numatytos ir programos naudojimo sąlygos (vartotojų skaičius, įranga, vieta ir pan.) bei jos atliekamos funkcijos (pvz., teksto procesorius, interneto naršyklė ir pan.). Ne taip jau retai licencinėmis sutartimis programą leidžiama naudoti tik konkrečiame kompiuteryje, iš anksto nustatoma, kiek kartų galima ją paleisti, arba įsigytą programą leidžiama naudoti tik tam tikrą laikotarpį (pastarosios nuostatos ypač dažnai pasitaiko kompiuterių programų demonstracinių versijų (angl. *shareware)* ar preliminarių kompiuterių programų versijų (vadinamųjų *beta* versijų) licencinėse sutartyse). Jeigu sutartyje nieko nenurodyta, programos paskirtį nulems faktinės aplinkybės, pvz., programos gebėjimas atlikti tam tikras užduotis, galimybė jos nepakeitus perkelti iš vienos sistemos į kitą, techniniai apribojimai, kurie gali būti nustatyti vartotojų skaičiui ir pan. Klaidų taisymas irgi gali būti papildomai reglamentuotas licencinėje sutartyje. Šios sutarties nuostatas, reglamentuojančias programos klaidų taisymą, būtina suderinti su nuostatomis, leidžiančiomis vartotojui atskleisti ir taisyti programos kodą, nes techniškai gali būti labai sunku ar net neįmanoma ištaisyti programos klaidų nekeičiant jos kodo.

Kadangi kompiuterių programų autorių teisių turėtojai visapusiškai stengiasi išvengti būtinybės atskleisti programos kodą, plačiai paplitusi praktika licencinėse sutartyse tiesiogiai uždrausti pačiam vartotojui taisyti klaidas, numatant tam tikras klaidų taisymo ir vartotojo aptarnavimo paslaugas. Dėl minėtųjų priežasčių apskritai galima matyti vis labiau didėjančią licencinių sutarčių svarbą kompiuterių programų apsaugai.

Teisėtam kompiuterių programos vartotojui turi būti leidžiama sukurti atsarginę programos kopiją. Tokios kopijos sukūrimas negali būti draudžiamas sutartimis, jeigu asmuo turi teisę naudoti programą ir minėtoji kopija jam iš tiesų reikalinga. Tais atvejais, kai atsarginę programos kopiją pateikia pats programos platintojas, naujos atsarginės kopijos sukūrimas negali būti pateisinamas. Jeigu teisė naudoti programą nebegalioja, jokia kopija (įskaitant ir atsarginę) negali būti sukuriama. Netekus teisės naudoti programą, visos atsarginės kopijos turi būti sunaikinamos. Tai aktualu ir įvairių ribotų programos versijų atveju, pvz., bandomoji programos kopija turėtų būti sunaikinama (ištrinama) pasibaigus jos bandomajam laikotarpiui.

Kaip jau minėta, autorinė kompiuterių programų apsauga yra paprasčiausias ir pigiausias teisinės kompiuterių programų apsaugos būdas, iš gamintojų nereikalaujantis jokių papildomų pastangų ar investicijų. Kūrinio – kompiuterių programos ar net jos dalių arba funkcinių schemų – sukūrimo faktas yra vienintelė ir pakankama sąlyga taikyti teisinę autorių apsaugą. Šios teisinės autorių apsaugos ypatybės lemia, kad minėtoji apsauga išlieka gana svarbi kompiuterių programų teisinės apsaugos forma. Tokios apsaugos pakanka ir norint apsaugoti kompiuterių programas nuo tiesioginio neteisėto atgaminimo bei platinimo – piratavimo. Kita vertus, autorių teisės negali apsaugoti inovatyvių ribotos išraiškos sprendimų, panaudotų kompiuterių programose, be to, tradiciškai autorių teisės numato nemažai išimčių, kurios sumažina investicijų grąžą.

2. Patentinės kompiuterių programų apsaugos principai

Noras apsaugoti kompiuterių programų elementus, kurių nesaugo autorių teisės, ir siekis išvengti tradicinių autorių teisių išimčių lėmė alternatyvių teisinės kompiuterių programų apsaugos formų paiešką. Kaip autorių teisių alternatyva buvo pasitelkta patentinė apsauga. Ši apsauga iš pradžių pradėta taikyti techniniams mechanizmams, į kurių sudėtį įėjo kompiuterių programa valdomas kompiuteris, vėliau – atskiriems kompiuterių programų techniniams elementams, o šiuo metu ir kompiuterių programoms *per se* ir net matematiniams algoritmams bei matematiniams ir verslo metodams, išreiškiamiems pasitelkus kompiuterių programas. Tradicinė patentų teisė skirta techniniams išradimams apsaugoti – inovatyvių idėjų techniniam

pritaikymui, sukuriančiam 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 išradimams e. erdvėje apsaugoti. Kompiuterių programų patentinė apsauga iki šiol yra kontroversiška problema, iš esmės nacionalinių patentų biurų pozicijos šiuo klausimu skiriasi. Skirtingai nei autorių teisės, patentai yra registruojami, brangūs ir riboti nacionaliniu lygiu.

Patentinė kompiuterių programų apsauga ypač įsigalėjusi JAV, kur šiuo metu iš esmės leidžiamas kompiuterių programų patentavimas *per se*, su sąlyga, kad patento objektas atitinka tradicinius patentui keliamus reikalavimus: naujumą, išradimo lygį ir yra naudingas (techninio pritaikomumo kriterijus iš tiesų pakeistas naudingumo kriterijumi). Europoje kompiuterių programų patentinė apsauga ne taip plačiai paplitusi kaip JAV, tačiau prieinama netiesiogiai. Tokią padėtį iš dalies lemia ES patentinės politikos nenuoseklumas. Kompiuterių programoms patentuoti Europoje ypač reikšminga 1973 m. Europos patentų konvencija, kurios 52 str. 2 d. 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.

Didžioji dalis kontroversiškų pasiūlymų dėl kompiuterių programų patentinės apsaugos nagrinėja klausimą, ar galima įsigyti patentą matematiniams algoritmams, kurie sudaro bet kokios kompiuterių programos pagrindą.

Naujausia praktika pripažįsta, kad jeigu įprastinis 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, jeigu tenkinami įprastiniai patentavimo galimybių kriterijai. Tik svarbu, kad patentinė paraiška būtų suformuluota apimant procesą, kuris vykdomas kompiuterių programą įkėlus į kompiuterį ir atliekant tam tikras funkcijas, arba paraiška būtų suformuluota apimant gaminį, kuris parduodamas kompiuterių programą susiejant su tam tikra materialiąja struktūra, pvz., magnetine laikmena ar kompiuterio atmintimi. Tam, kad atitiktų patentavimo galimybių kriterijus, patentavimui pareikštas procesas turi arba sukelti tam tikrų fizinių transformacijų ne kompiuteryje, arba turi būti apribotas konkrečiu naudojimo būdu ir technologijos sritimi. Šiuo metu kompiuterių programai patentuoti pakanka vienintelio kriterijaus – „naudingo, konkretaus ir materialaus rezultato“.

Nors aukščiau išdėstyta kompiuterių programų patentavimo logika iš esmės yra pagrįsta, praktinė problema, su kuria susiduria kompiuterių programų patentai, yra tradicinių patentavimo galimybių kriterijų, ypač naujumo ir išradimo lygio reikalavimų, vertinimo sudėtingumas kompiuterių programų atveju. Vien dėl šios priežasties išduota daugybė patentų, kurie gana akivaizdžiai neatitinka tradicinių patentavimo galimybių kriterijų, tačiau dėl didelių sąnaudų ir tradicinių patentų teisėtumo prezumpcijų juos sudėtinga paneigti. Be to, kompiuterių programų patentai pradėti aktyviai naudoti ne dėl inovacijų apsaugos, o siekiant apriboti konkurenciją. Kompiuterių programų (matematinių algoritmų ir verslo metodų) patentavimo kritikai nurodo, kad tokie patentai prieštarauja socialiniams patentų teisės tikslams ir, užuot skatinę inovacijas, ekonomikos plėtrą ir konkurenciją, juos nepagrįstai suvaržo, lemia rinkos monopolizaciją, užkerta kelią ateiti naujiems rinkos dalyviams, ypač nedidelėms ir vidutinėms įmonėms, bei stabdo atvirosios programinės įrangos plėtrą.

Nors ir būta kontroversiškų vertinimų, vis dėlto galima daryti išvadą, kad kompiuterių patentavimas pernelyg įsišaknijo, kad jo būtų galima taip lengvai atsisakyti. Kita vertus, atsirado akivaizdus poreikis užtikrinti nuoseklų tradicinių patentavimo galimybių kriterijų taikymą ir efektyvias apsaugos nuo piktnaudžiavimo patentų sistema priemones.

Labai panašias taisykles ilgainiui sukūrė ir Europos patentų biuras, interpretuodamas Europos patentų konvencijos 52(3) str. numatytą *per se* išlygą. Minėtojo biuro praktika šiandien beveik atmetė Europos patentų konvencijos 52(2)(c) str. draudimą patentuoti kompiuterių programas. Draudimo, įtvirtinto Europos patentų konvencijos 52(2)(c) str., ištakos glūdi europietiškoje patentų teisės tradicijoje, kuri numato tik techninio pobūdžio išradimų patentinę apsaugą. Tradiciškai kompiuterių programos laikytos literatūros kūrinių analogu, todėl pagal šį tradicinį supratimą net ir be esamos tiesioginės išimties jos neturėtų patekti į patentuotino išradimo sampratą. Kita vertus, toks aiškinimas lemia, kad išradimai, susiję su kompiuterių programomis, arba juose kompiuterių programos sudaro tik dalį, jeigu jie atitinka bendruosius patentavimo galimybių kriterijus, gali būti patentuojami. Naujausia praktika EPO *de facto* panaikino 1973 m. Europos patentų konvencijoje numatytą kompiuterių programų *per se* patentavimo galimybių išimtį.

JAV patentų ir prekių ženklų biuro pozicija (naudingumo teorija) ir Europos patentų biuro pozicija (techninio efekto teorija) dėl kompiuterių programų patentinės apsaugos iš esmės yra labai artimos. Nors Europos Parlamentas 2005 m. ir nepritarė pateiktam direktyvos dėl kompiuterinių išradimų patentinės apsaugos projektui, iš esmės tai neriboja kompiuterių

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

Šiuo metu kompiuterių programų patento objektu gali būti kompiuterių programa *per se*, su sąlyga, jeigu tokia kompiuterių programa atitinka įprastinius naujumo, išradimo lygio kriterijus ir specialų naudingumo ar techninio įnašo kriterijų, kuris pasireiškia tuo, kad kompiuterių programą vykdanti įprastinė techninė įranga gali sukelti tam tikrų techninių padarinių ar pakitimų.

Patentinė apsauga negali ir neturi pakeisti teisinės kompiuterių programų autorių apsaugos. Ji gali būti taikoma papildomai, kai kompiuterių programai yra panaudotas išradimas. Didžiausias patentinės apsaugos pranašumas – tvirta ir besąlygiška teisinė apsauga, beveik neturinti išimčių, tokia kaip autorių teisės (įskaitant idėjos ir išraiškos sutapimo, *scenes-a-faire* doktrinas). Bet koks patentuoto kompiuterių programos elemento naudojimas bus laikomas patento pažeidimu. Kita vertus, nereikėtų pamiršti esminių patentų trūkumų – patento gavimo procedūra, skirtingai nei autorių teisės įgyvendinimo mechanizmas, yra formalizuota, brangi ir reikalauja daug laiko, be to, yra ribojama valstybės sienų. Tam, kad būtų palaikomas patento galiojimas, per visą jo galiojimo laikotarpį reikia mokėti patento palaikymo mokesčius, kurie progresyviai didėja kartu su patento galiojimo terminais. Dauguma šiuolaikinių kompiuterių programų inovacijų yra inkrementinio pobūdžio, todėl gali neatitikti išradimo lygio kriterijų, be to, inkrementinio pobūdžio inovacijos pagrįstos tokių pat ankstesnių inovacijų naudojimu. Inkrementinių inovacijų patentavimas nepaprastai apkrautų patentų sistemą, be to, jų licencijavimas (dėl daugybės licencijų būtinybės) būtų beveik neįmanomas. Tokioje sparčiai besivystančioje srityje kaip kompiuterių programų kūrimas nepriimtina ir tai, kad nuo patentinės paraiškos padavimo momento iki patento išdavimo dažniausiai praeina gana daug laiko, o pats patento galiojimo laikas (dvidešimt metų) yra akivaizdžiai per ilgas kompiuterių programoms (iš esmės morališkai jos pasensta per metus). Patentinės paraiškos daugelyje jurisdikcijų skelbiamos viešai (taip atskleidžiant informaciją konkurentams). Dėl patentinės apsaugos brangumo ir sudėtingumo pavieniai programuotojai ir smulkios firmos beveik prarado galimybes savarankiškai įsigyti patentus, o kompiuterių programų jautrumas natūraliai monopolizacijai lėmė šiuolaikinės kompiuterių programų industrijos koncentraciją, kuri savo ruožtu sudaro ypač palankias sąlygas konkurencijos ir vartotojų teisių pažeidimams.

3. Kitos teisinės kompiuterių programų apsaugos formos

Kaip jau minėta, prognozuotas autorių teisių ribotumas ir patentinės apsaugos kontroversiškumas dar XX a. aštuntajame dešimtmetyje lėmė siūlymus kompiuterių programoms taikyti ypatingą – *sui generis* – teisinę apsaugą. Tačiau išsivysčiusioms pasaulio valstybėms kaip pagrindinę kompiuterių programų teisinės apsaugos formą pasirinkus autorių teisę, *sui generis* teisinės apsaugos siūlymai buvo laikinai užmiršti.

Šiuo metu kompiuterių programoms pritaikytos modifikuotos autorių teisių ir patentų teisės normos, kurios ilgainiui įgijo esminių skirtumų nuo tradiciniams kūriniams taikomų taisyklių ir leidžia kalbėti apie *de facto* kompiuterių programų *sui generis* teisinę apsaugą. Pagrindą daryti tokią išvadą 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 Direktyvoje dėl duomenų bazių teisinės apsaugos 96/9/EB.

S*ui generis* teisinei apsaugai galima priskirti ir siūlymus kompiuterių programoms teikti labai ribotą teisinę apsaugą arba jos išvis atsisakyti. Pastaruoju metu šie siūlymai labai aktyviai reiškiami per atvirosios programinės įrangos ir kūrybinių bendrijų judėjimus. Atviroji programinė įranga reikalauja tik tiek teisinės apsaugos, kad būtų užtikrintas nuolatinis šių programų kodo atvirumas, t. y. viešumas ir nevaržoma galimybė juo naudotis toliau diegiant naujoves. Reikėtų atkreipti dėmesį, kad atvirumas nesiejamas su neatlygintinumu. Kitokia teisinė kompiuterių programų apsauga, ypač patentai kompiuterių programų algoritmams, atvirajai programinei įrangai kelia tiesioginę grėsmę, nes riboja galimybes šiomis inovacijomis naudotis diegiant kitas inovacijas. Šis argumentas buvo viena iš svarbiausių priežasčių, dėl kurių Europos Parlamentas nepritarė direktyvos dėl išradimų, susijusių su kompiuteriais, projektui. Svarbiausią atvirosios programinės įrangos apsaugos vaidmenį šiuo metu atlieka licencinės sutartys, o ne intelektinės nuosavybės įstatymai. Nenuoseklus ir išimtinai nacionalinis licencinių sutarčių reglamentavimas (ir su tuo susijusios jų įgyvendinimo problemos) yra viena iš atvirosios programinės įrangos plėtros kliūčių.

Kaip pagalbinės teisinės kompiuterių programų apsaugos formos įvairiose valstybėse dar taikomos komercinių paslapčių apsauga, prekių ir paslaugų ženklai. Šie intelektinės nuosavybės institutai padeda apsaugoti atskirus kompiuterių programų elementus, pvz., originalias grafines, vaizdo ir garso išraiškas, be to, gina kompiuterių programas, apribodami galimybes gaminti neteisėtas jų kopijas, o tokias kopijas pagaminusiems asmenims užtraukia papildomą teisinę atsakomybę.

Kompiuterių programų apsaugai dar pasitelkiamos ir 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 ir ES direktyvoje 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, pvz., kompiuterių programoms atgaminti ar dekompiliuoti, siekiant užtikrinti šios kompiuterių programos suderinamumą su naujai kuriamąja. Deja, esamas techninių apsaugos priemonių reguliavimas iš esmės nenumato efektyvių mechanizmų, užtikrinančių sąžiningo vartotojo teises.

Svarbi kompiuterių programų ypatybė – jos yra savo forma ir turiniu itin sparčiai besivystantis intelektinės nuosavybės objektas. Kaip jau minėta, autorių teisė ir patentai sunkiai dera su šia kompiuterių programų savybe – jų naudojimo ciklas yra labai trumpas (dažniausiai mažiau nei penkeri metai), o patentų ir ypač autorių teisių galiojimo terminai gerokai viršija šį laikotarpį, be to, kompiuterių programos neturi jokios išliekamosios ar kultūrinės vertės. Vien dėl šių priežasčių galima pritarti nuomonėms, kad esamos kompiuterių programų teisinės apsaugos formos bent iš dalies yra nepakankamos ir negali patenkinti informacinės visuomenės poreikių, todėl būtina ir toliau vykdyti teisinės kompiuterių programų apsaugos reformą.

4. Civilinė naudotų kompiuterių programų apyvarta

Vienas naujausių kontroversiškų klausimų, kylančių dėl visų intelektinės nuosavybės elektroninių objektų, – vartotojų teisės disponuoti teisėtai įsigytais ypač brangiai kainuojančiais e. turinio objektais, tokiais kaip kompiuterių programos. Palyginti su kitais e. turinio objektais, kompiuterių programų kaina yra gerokai didesnė, todėl tiek individualiems, tiek verslo vartotojams, kurie dėl įvairių priežasčių sustabdo kompiuterių programos naudojimą (pvz., verslas likviduojamas arba individualiam vartotojui nepatiko įsigytas kompiuterinis žaidimas) yra labai aktualu atgauti bent dalį pinigų, išleistų kompiuterių programos licencijai (teisei naudotis kompiuterių programa) įsigyti.

Kai kurie kompiuterių programų gamintojai vartotojams, įsigijusiems kompiuterių programos licenciją, suteikia teisę vienu metu naudoti ne vieną, o kelias kompiuterių programos kopijas skirtinguose kompiuteriuose, pvz., *Microsoft Office* licencija suteikia teisę vienu metu instaliuoti ir naudoti tris kopijas. Tokiu būdu vartotojas iš esmės įsigyja tris ar daugiau kompiuterių programų licencijų, nors jam galbūt reikalinga tik viena. Bent

jau *Microsoft Office* neleidžia įsigyti licencijos tik vienam kompiuteriui. Tokia padėtis prilyginama reikalavimui vienu metu įsigyti tris poras batų ir iš karto už juos visus sumokėti, nors vartotojui reikia tik vienos poros ir jis norėtų mokėti tik už ją. Akivaizdu, kad draudžiant vartotojui disponuoti jam nereikalingomis kompiuterių programų licencijomis yra šiurkščiai pažeidžiami vartotojų interesai.

Dėl šios priežasties JAV teismai palengva įgalino vienareikšmę vartotojų teisę laisvai disponuoti nebereikalingomis kompiuterių programų licencijomis. JAV netgi leidžiama laisvai parduoti nenaudojamas licencijas, kai kompiuterių programų gamintojas vartotojams nesuteikia galimybės įsigyti vienos licencijos vienam kompiuteriui, o platina tik minimalų susijusių licencijų kiekį. Tokiu atveju vartotojui suteikiama teisė pačiam atsieti minėtąsias licencijas ir parduoti tas, kurios nereikalingos (pvz., parduoti *Microsoft Office* licenciją vienam kompiuteriui, o pasilikti licencijas dviem kompiuteriams). Šios teisės galioja ir individualiems, ir verslo vartotojams su sąlyga, jeigu jie neturėjo galimybės įsigyti konkretaus reikalingų licencijų kiekio.

Naudotų kompiuterių programų pardavimo teisėtumas ES ilgą laiką buvo neaiškus. Tik 2012 m. liepos 3 d. *UsedSoft GmbH v. Oracle International Corp* byloje ESTT byloje C128/11 pagaliau išaiškino, kad vartotojai turi teisę laisvai disponuoti nereikalingomis kompiuterių programų licencijomis.

Pagal *ESTT UsedSoft* sprendimą, tiek vartotojas fizinis asmuo, tiek verslininkas, tiek viešasis subjektas gali laisvai disponuoti jam nereikalingų kompiuterių programų licencijomis, jeigu jam pačiam nelieka galimybės naudotis atitinkama kompiuterių programa. Tai ypač aktualu verslininkams, kurie nutraukia savo veiklą, turėdami brangias verslo valdymo programų licencijas, ir likviduojamoms ar bankrutuojančioms įmonėms, kurioms anksčiau turėtą gana nepigią verslo programinę įrangą prireikė tiesiog nurašyti. Svarbu, kad pirminis kompiuterių programos licencijos pirkėjas nustotų naudoti šią kompiuterių programą, ją ištrintų ar kaip nors kitaip pašalintų iš savo kompiuterių.

UsedSoft sprendimas nustato, kad sutartiniai kompiuterių programų pardavimo ar perleidimo apribojimai yra neteisėti, t. y. vartotojas gali parduoti naudotą kompiuterių programą (jos licenciją), net jeigu sutartyje tai daryti jam uždrausta. Be to, kompiuterių programų licencijų pardavimas neturi būti susijęs su būtinybe (pareiga) sudaryti jų priežiūros sutartis – įsigyti naudotą programą galima ir nesudarant brangių priežiūros sutarčių. Parduoti naudotą kompiuterių programos licenciją galima tik tuo atveju, jei ji yra galiojanti (pvz., nėra pasibaigęs ribotas licencijos galiojimą terminas),

tačiau naudota programos licencija apima visus programos atnaujinimus ir pataisymus, kurie yra aktualūs pardavimo metu, net jeigu pirkėjas nesudaro naujos techninės priežiūros sutarties.

Vis dėlto *ESTT* apibrėžė vartotojų teisę disponuoti kompiuterių programų licencijomis siauriau nei JAV. *Usedsoft* sprendimas palieka atvirą klausimą, ar ES vartotojai gali savo nuožiūra išskaidyti susietas kompiuterių programų licencijas. *ESTT* nurodė, kad jeigu vartotojas savo nuožiūra įsigijo kompiuterių programos licenciją penkioms darbo vietoms, o iš tikrųjų naudoja tik dvi, jam neleidžiama išskaidyti licencijos ir parduoti likusių nenaudojamų darbo vietų licencijų, tačiau *ESTT* nenagrinėjo tų atvejų, kai vartotojas neturėjo galimybės įsigyti jam reikalingo konkretaus licencijų kiekio dėl paties kompiuterių programų gamintojo nustatytų sąlygų. Tikėtina, kad ateityje šis klausimas turėtų būti galutinai išspręstas taip, kaip ir JAV – vartotojų naudai.

Svarbu pabrėžti, kad vartotojų teisės disponuoti naudotomis kompiuterių programomis iš esmės turėtų galioti ir kitokiam e. turiniui (pvz., e. knygoms, garso įrašams ir pan.), nes nėra reikšmingų esminių skirtumų tarp įvairių e. turinio formų, tačiau nesant konkrečių teisinių nuostatų ar teismų praktikos teisinio aiškumo irgi trūksta.

5. Teisinės kompiuterių programų apsaugos ypatumai Lietuvoje

Teisinė kompiuterių programų apsauga Lietuvoje iš esmės užtikrinama autorių teisėmis, dar įmanoma ir patentinė kompiuterių programų apsauga. Kompiuterių programų apsaugos autorių teisėmis teisinis pagrindas Lietuvoje yra ES direktyva 91/250/EEB dėl kompiuterių programų teisinės apsaugos (nuo 2009 m. šią direktybą pakeitė konsoliduotoji Direktyva 2009/24/EB), kuri yra įgyvendinta Autorių teisių ir gretutinių teisių įstatyme (ATGTĮ). Šio įstatymo 2 str. nuostatos pateikia legalines jame vartojamų terminų sąvokas, tarp jų – ir kompiuterių programos sąvoką. Kompiuterių programa apibrėžiama kaip visuma instrukcijų, pateikiamų žodžiais, kodais, schemomis ar kitu pavidalu, kurios leidžia kompiuteriui 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, tik keliama sąlyga, kad iš jos būtų galima sukurti minėtąją instrukcijų visumą. Sąvoka atskiria kompiuterių programą ir prie jos pridedamą medžiagą (aprašymus, vartotojų instrukcijas ir pan.), 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 nei pati kompiuterių programa, todėl tuo atveju, kai

jie pateikiami kartu su kompiuterių programa arba yra į ją integruoti, neišnyksta kaip savarankiški kūriniai ir turėtų būti saugomi kaip savarankiški įprastiniai autoriniai kūriniai ar gretutinių teisių objektai. Tais atvejais, kai kompiuterių programos garso ir vaizdo apipavidalinimas sudaro kompiuterių programos sąsajos (dažniausiai vartotojo) sudėtinę dalį, jis laikytinas kompiuterių programos sudėtine dalimi.

Iš esmės AGTGĮ kompiuterių programoms taikomos bendrosios autorių teisių normos, iš jų išskyrus keletą specifinių. Kompiuterių programoms ir duomenų bazėms taikomos šios 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 AGTGĮ nuostatos dėl kompiuterių programų, sukurtų atliekant tarnybines pareigas. Pagal ATGTĮ 10 str. 2 d. nuostatas turtinės teisės į kompiuterių programą, sukurtą darbuotojui einant savo tarnybines pareigas ar vykdant tarnybinę užduotį, priklauso darbdaviui visą jų galiojimo laiką, išskyrus atvejus, kai kitokios nuostatos nustatytos šalių sutartimi. Ši prezumpcija skiriasi nuo tos, kuri taikoma įprastiniams literatūros ir meno kūriniams – į šiuos darbdavys savaime įgyja turtines teises tik penkerių metų laikotarpiui (ATGTĮ 9 str. 2 d.). Šis skirtumas pabrėžia kompiuterių programos kaip utilitarinio (taikomojo) kūrinio prigimtį.

Deja, AGTGĮ neatsižvelgta į prieštaravimą tarp įstatyme įtvirtintų autoriaus asmeninių neturtinių ir turtinių teisių, nes įstatyme nustatytos turtinės autorių teisės į kompiuterių programas (pvz., teisė adaptuoti ar dekompiliuoti kompiuterių programą (ATGTĮ 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 (vartotojų teisės) Lietuvoje iš esmės reglamentuojamos analogiškai kaip ir ES teisės aktuose.

Nors ATGTĮ 20 str. leidžia atgaminti kūrinį asmeniniams tikslams, 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 str. 2 d. 3 p. tiesiogiai nustato, kad išradimais nelaikomos „kompiuterių programos“. Šios nuostatos yra perimtos iš 1973 m. Europos patentų konvencijos, kurios narė Lietuva yra nuo 2004 m. spalio 5 dienos. Lietuvos Respublikos patentų įstatymo 2 str. 2 d. iš esmės atkartoja Europos patentų konvencijos 52(2) str. nuostatas, tačiau labai svarbu atkreipti dėmesį, kad kompiuterių programų patentavimo išimtis Patentų įstatyme suformuluota kur kas plačiau nei 1972 m. Europos patentų konvencijoje, nes Lietuvos

įstatymas nenumato jokių išlygų, kad minėtasis apribojimas *per se* taikomas tik kompiuterių programoms.

Praktinė kompiuterių programų patentavimo problema Lietuvoje nekyla dėl to, kad šalis yra pernelyg maža ir nereikšminga jurisdikcija, taip pat dėl to, kad joje neatliekama pateiktų patentuoti išradimų paieška ir ekspertizė. Pabrėžtina, kad bendra Lietuvos patentų kokybė yra ypač prasta dėl šių priežasčių:

1) užsienio subjektams – daugianacionalinių patentų savininkams – Lietuvos jurisdikcija ir ekonominė rinka yra pernelyg mažos, todėl išlaidos, susijusios su Lietuvos patento gavimu ir išlaikymu, gali paprasčiausiai neatsipirkti;
2) nacionalinė kompiuterių programų industrija yra dar neseniai atsiradusi, nauji produktai dažnai nėra tokie novatoriški, kad atitiktų griežtus patentavimo galimybių kriterijus;
3) potencialūs nacionaliniai išradėjai ir patentuotojai dažnai neturi užtektinai žinių apie galimybes apginti savo intelektinę nuosavybę patentų teisės priemonėmis;
4) esamas teisinis režimas neskatina daugianacionalinių patentų savininkų pateikti patentines paraiškas Lietuvoje, nes tas pats rezultatas (teisinė apsauga Lietuvos teritorijoje) gali būti pasiektas per Europos patentus, išplečiant jų galiojimą Lietuvoje, nes jau nuo 1995 m. Europos patentų biuro išduotų patentų (Europos patentų) galiojimas gali būti išplėstas Lietuvoje, atlikus nesudėtingą nacionalinę procedūrą, kuri neapima patento teisėtumo ar jo objekto patentavimo galimybių tikrinimo.

9 skirsnis. Teisinė duomenų bazių apsauga

Dideliems duomenų ir informacijos masyvams tvarkyti bei sisteminti naudojami specialūs duomenų formatai ir programų paketai, vadinamosios duomenų bazių valdymo sistemos. Jos leidžia kurti įvairių duomenų rinkinius, peržiūrėti duomenis ir juos keisti, pateikti ataskaitas. Techniniu požiūriu duomenų bazę sudaro jos turinys (patys duomenys) ir sąsaja (duomenis valdančios programos). *Windows* terpėse tam dažniausiai naudojama *MS Access* programa.

Šiandien duomenų bazės yra svarbiausia informacijos tvarkymo forma ir instrumentas, vienas dažniausiai pateikiamų pavyzdžių, kaip modernios informacinės technologijos pritaikomos kasdienei aplinkai. Šiuolaikinės verslo įmonės, valstybės institucijos ir kitos organizacijos susiduria su nuolat didėjančiais informacijos srautais bei būtinybe juos tvarkyti, todėl

duomenų bazės tampa svarbiausia informacijos tvarkymo ir kontrolės priemone, neatskiriamu informacijos vadybos elementu.

Duomenų bazės yra būtinos norint atlikti ir daugumą verslo valdymo funkcijų, tokių kaip apskaita ir sąskaityba, atsargų planavimas, ryšių su klientais palaikymas, pardavimo ar personalo vadyba ir t. t. Šiuo metu įsitvirtino ir tiesiogiai nuo duomenų bazių priklausomos verslo rūšys: įmonių katalogai, kredito biurai, įdarbinimo agentūros, bankai ir draudimo bendrovės.

Duomenų bazę galima apibrėžti tiesiog kaip informacijos rinkinį ar kompiliaciją, išdėstytą ar organizuotą sisteminiu ar metodologiniu būdu. Minėtoji bazė susieja pavienę (individualią) informaciją į kokybiškai naują visumą. Pabrėžtina, kad duomenų bazę turi sudaryti informacijos daugetas, t. y. būtinas tam tikras minimalus sistemiškai organizuotas informacijos kiekis. Duomenų baze laikytinas tiek automatizuotai tvarkomas, tiek neautomatizuotas (net ir ranka užrašytas) informacijos rinkinys, jeigu jis išreikštas kokia nors forma.

Duomenų bazės santykis su kompiuterių programomis gali būti dvejopas. Jeigu duomenų bazėms tvarkyti naudojama kompiuterių programa integruota į duomenų bazę taip, kad ja perteikiama duomenų bazės struktūra, tokia programa iš esmės prilyginama duomenų bazei (savo ruožtu duomenų struktūros laikomos kompiuterių programų elementu). Tuo atveju, kai kompiuterių programa yra tik duomenų bazės kūrimo ir (arba) tvarkymo (prieigos, keitimo, išsaugojimo) priemonė, tokia programa nelaikoma duomenų bazės dalimi.

Duomenų bazės, kaip ir kompiuterių programos, pripažįstamos savarankišku intelektinės nuosavybės apsaugos objektu.

Teisinė duomenų bazių apsauga įtvirtinta dar 1886 m. Berno konvencijoje dėl literatūros ir meno kūrinių apsaugos. Šios konvencijos 2 str. 5 d. nustato, kad teisinė apsauga (nepažeidžiant autorių teisės į kiekvieną kūrinį) taikoma literatūros ir meno kūrinių rinkiniams, kurie dėl turinio parinkimo ir išdėstymo yra intelektualiosios kūrybos rezultatas, pvz., enciklopedijoms ir antologijoms. Literatūros ir meno kūrinių arba tiesiog informacijos rinkiniai iš esmės yra neautomatizuotos duomenų bazės, pvz., Lietuvos Aukščiausiojo Teismo praktikoje duomenų baze vienareikšmiškai pripažįstami spausdintiniai žodynai. Duomenų bazėmis laikytini šie informacijos šaltiniai: chrestomatijos, poezijos rinkiniai, bibliotekų katalogai ir bet kokie kiti informacijos rinkiniai, pvz., telefonų direktorija ar įmonių katalogas. Duomenų bazės būtinos norint atlikti ir daugumą verslo valdymo funkcijų, tokių kaip apskaita ir sąskaityba, atsargų planavimas, ryšių su klientais palaikymas, pardavimo ar personalo vadyba ir t. t.

ATGTĮ 2 str. 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 tokioms duomenų bazėms kurti ar valdyti. AGTGĮ 4 str. 3 d. 2 p. kūrinių ar duomenų rinkiniai, duomenų bazės (išreikštos techninėmis priemonėmis skaityti pritaikyta ar kita forma), kurie dėl turinio parinkimo ar jo išdėstymo pateikiami kaip autoriaus intelektinės kūrybos rezultatas ir yra įvardijami kaip autorių teisių objektas. Kūrinių rinkiniams ir duomenų bazėms autorių teisės 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.

Pagrindiniai duomenų bazės elementai yra duomenų bazės turinys (informacija – duomenys, kūriniai ir pan.) ir jų tvarkymo priemonės (sąsajos). Automatizuotų duomenų bazių tvarkymo priemonės (sąsajos) dažniausiai yra specializuotos kompiuterių programos. Duomenų bazės santykis su kompiuterių programomis gali būti dvejopas. Jeigu duomenų bazėms tvarkyti naudojama kompiuterių programa į duomenų bazę integruota taip, kad ja perteikiama duomenų bazės struktūra, tokia programa iš esmės prilyginama duomenų bazei (savo ruožtu, duomenų struktūros laikomos kompiuterių programų elementu). Tuo atveju, jeigu kompiuterių programa yra tik duomenų bazės kūrimo ir (arba) tvarkymo (prieigos, keitimo ir išsaugojimo) įrankis, tokia programa nelaikoma duomenų bazės dalimi. Atkreiptinas dėmesys, kad ir duomenų bazės turinys, ir jos tvarkymo priemonės, atskirai paėmus gali būti skirtingų intelektinės nuosavybės teisių objektas ir gali priklausyti skirtingiems intelektinės nuosavybės teisių turėtojams, tačiau teisėtai naudojant šiuos elementus gali būti sukuriamas kokybiškai naujas intelektinės nuosavybės objektas – duomenų bazė.

1. Teisinės duomenų bazių apsaugos formos ir jų principai

Teisinė duomenų bazių apsauga visų pirma užtikrinama autorių teisėmis – kaip jau minėta, AGTGĮ 4 str. 3 d. 2 p. duomenų bazes įvardija kaip autorių teisių objektą. Duomenų bazės, remiantis bendraisiais autorių teisių principais – laikantis bendrųjų originalumo, teisių naudojimo, riboto teisių galiojimo laiko ir teritorijos bei turtinių teisių išimčių taisyklių, yra saugomos kaip originalūs kūrinių rinkiniai. Kaip ir bet kokia kita informacija, duomenų bazės gali būti saugomos kaip komercinės paslaptys. Jų apsaugai šiuo metu pasitelkiamos gausios techninės apsaugos priemonės. Specifinės duomenų bazės gali būti papildomai saugomos ir taikant asmens privatumo, valstybės paslapties ir kt. apsaugos taisykles. Nuo 1996 m. ES

duomenų bazėms gali būti taikoma ir ypatinga teisinė *sui generis* apsauga, numatyta ES direktyvoje 96/9/EB.

Visos minėtosios teisinės duomenų bazių apsaugos formos: autorių ir *sui generis* teisės, komercinių paslapčių apsauga, nereikalauja registracijos ar kokių nors kitų formalių procedūrų, atsiranda tik sukūrus duomenų bazę ir yra lygiagrečiai taikomos. Tarptautiniu mastu *sui generis* teisės paprastai galioja vadovaujantis vienodumo ir abipusiškumo principais.

Duomenų bazių *sui generis* teisinė apsauga iš esmės skiriasi nuo autorių teisių, nors ir reglamentuojama autorių teisių įstatymuose (pvz., AGTGĮ IV skyriuje (61–64 str.). ES nustatant specialią teisinę duomenų bazių *sui generis* apsaugą, siekiama apsaugoti investicijas į duomenų bazių gamybą, ypač tais atvejais, kai galutinė duomenų bazė negali būti saugoma tradicinės autorių teisės (pvz., dėl neoriginalumo, idėjos ir išraiškos sutapimo ar jos ribotumo ir pan.). Duomenų bazių atveju išraiška tradicinių autorių teisių požiūriu iš esmės yra duomenų bazės struktūra, kurią gali nulemti labai 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). Teisinei duomenų bazių apsaugai taikant tradicines autorių teises, saugoma tik originali duomenų bazės struktūra (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 – individualios duomenų bazę sudarančios informacijos vienetai, kurie kaip savarankiški kūriniai gali būti autorių teisių objektai, tačiau gali būti ir išvis nesaugomi autorių teisės, jeigu jie nėra autorių teisių objektai. Kaip alternatyva originaliai parinktas ir išdėstytas toks pat turinys (informacija) gali būti laikomas nauja duomenų baze ir nepažeisti pirmosios duomenų bazės kūrėjo autorių teisių (pvz., tos pačios poezijos rinktinės, išdėstytos tematiškai ir chronologiškai, iš esmės yra dvi skirtingos duomenų bazės). Tradicinė autorių teisė nesaugo ir neoriginalių informacijos rinkinių (pvz., sudarytų remiantis funkciniais kriterijais – telefonų sąrašo, išdėstyto abėcėline tvarka) ir tai net nepriklauso nuo investicijų į juos.

Be to, kartu su tradicinėmis autorių teisėmis neišvengiamai taikomos ir turtinių teisių išimtys, kurios gerokai riboja duomenų bazių gamintojų galimybes greitai susigrąžinti duomenų bazių kūrimo investicijas. Tradicinės autorių teisės požiūriu duomenų bazės gali būti naudojamos švietimo ir mokslinio tyrimo tikslams, daromos jų asmeninės kopijos ir kt. Teisėtas duomenų bazės ar jos kopijos naudotojas be autoriaus arba kito autorių teisių subjekto leidimo turi teisę atlikti bet kokius veiksmus, įskaitant ir

duomenų bazės atgaminimą, adaptavimą bei perdavimą, kurie reikalingi norint sužinoti duomenų bazės turinį ir pradėti tinkamai juo naudotis. Reikėtų atkreipti dėmesį, kad tradicinių turtinių autorių teisių išimčių, taikomų duomenų rinkiniams ir bazėms, apimtis yra gana neaiški.

Šie argumentai ir spekuliatyvios nuostatos (duomenų bazių verslo skatinimas) lėmė ES sprendimą nustatyti duomenų bazių *sui generis* teisinę apsaugą.

2. Duomenų bazių *sui generis* teisinės apsaugos ypatumai

Duomenų bazių *sui generis* teisinė apsauga remiasi vadinamąja esminių investicijų doktrina. Ši doktrina teigia, kad duomenų bazės gamintojas turi teisę uždrausti duomenų bazės turinio (viso ar esminės dalies) perkėlimą į kitą laikmeną, viešą platinimą ar perdavimą, jeigu įrodo, kad parinkdamas, sudarydamas, tikrindamas ir pateikdamas duomenų bazės turinį padarė esminių kokybinių ir (ar) kiekybinių investicijų. Šios gali būti intelektinės, finansinės ir organizacinės, o jų svarbą lemia kokybiniai ir kiekybiniai kriterijai. Minėtoji doktrina dėl visiško neapibrėžtumo, nekonkretumo ir objektyvių kriterijų nebuvimo gali būti vertinama labai kritiškai. Nors nuo šios ES direktyvos 96/9/EB priėmimo praėjo dešimtmetis, nė vienoje ES valstybėje įstatymų leidėjai, teismai ar jurisprudencija nesugabėjo suformuluoti aiškių esminių investicijų kriterijų. Pabrėžtina, kad rinkos sąlygomis funkcionuojančioje visuomenėje bet koks informacijos tvarkymas reikalauja nemažų intelektinių, finansinių ir organizacinių sąnaudų. Viena svarbiausių to priežasčių – eksponentiškai didėjantis informacijos kiekis ir duomenų bazių naudojimas kasdieniams socialiniams procesams. Kyla klausimas, ar toks kasdienis įprastinių duomenų tvarkymas, kuris kartkartėmis gali būti net pareiga, o daugeliu atvejų – ir socialinė būtinybė, be to, šių duomenų integravimas į masinius produktus ar paslaugas, yra svarbi esminė investicija.

Sui generis teisės galioja penkiolika metų po duomenų bazės sudarymo datos (skaičiuojant nuo sausio 1 d. po tų metų, kuriais duomenų bazė buvo sudaryta arba pirmą kartą tapo viešai prieinama), tačiau šis terminas gali būti neribotai pratęstas kiekvieną kartą papildžius ar atnaujinus duomenų bazės turinį, t. y. padarius esminių papildomų investicijų. Tokia *de facto* neterminuota duomenų bazių apsauga yra viena iš kontroversiškiausių duomenų bazių *sui generis* teisinės apsaugos nuostatų, ji ypač kritikuojama ES ir kitų valstybių mokslininkų. Neterminuotas *sui generis* teisių galiojimas kelia rimtą grėsmę šių teisių socialinei funkcijai ir gali iš esmės suvaržyti socialinę informacijos kaitą, būtiną švietimui, inovacijoms ir kūrybai, visuomenės kultūrinei ir technologinei pažangai. Pabrėžtina, kad duomenų

bazės turinio pildymas ir atnaujinimas rinkos sąlygomis yra absoliuti būtinybė, kurią lemia šiuolaikinės visuomenės poreikiai, o ne laisvas duomenų bazių gamintojo pasirinkimas. Neterminuotos *sui generis* teisės sunkiai suderinamos su žmogaus teise į informaciją ir žodžio laisvę. Dėl duomenų bazių, kuriose saugomi ir tvarkomi ypatingi (asmens ar medicininiai) duomenys, kyla ir etinių klausimų.

Sui generis teisinei apsaugai yra nustatyta specifinių apribojimų ir išimčių. Duomenų bazės, kuri teisėtai bet kuriuo būdu tapo viešai prieinama, gamintojas negali kliudyti teisėtiems jos naudotojams bet kokiems tikslams į kitas laikmenas perkelti ar naujai naudoti nedideles (vertinant kokybiniu ar kiekybiniu požiūriu) duomenų bazės turinio dalis, tačiau teisėtas duomenų bazės naudotojas neturi teisės atlikti veiksmų, kurie prieštarautų įprastam duomenų bazės naudojimui, pažeistų teisėtus duomenų bazės gamintojo interesus arba autorių teisių ir gretutinių teisių subjektų teises į kūrinius ir gretutinių teisių objektus, kurie sudaro duomenų bazės turinį. Duomenų bazių gamintojui draudžiama sutartimi (licencija) suvaržyti minėtąsias duomenų bazės gamintojo teises. Neleidžiama daryti pakartotinių ar sistemingų ištraukų ir naudoti nedidelių duomenų bazės turinio dalių, kai šie veiksmai prieštarauja tos duomenų bazės normaliam naudojimui arba pažeidžia teisėtus duomenų bazės gamintojo interesus. Nedidelės duomenų bazės dalys nėra aiškiai apibrėžtos. Remiantis ES valstybių praktika, nedidelė dalis kiekybine prasme neturėtų viršyti dešimt procentų viso duomenų bazės turinio, o kokybine prasme turėtų būti vertinamas duomenų bazės turinio dalies vertingumas, unikalumas ir pakeičiamumas (lyginant su likusiąja dalimi).

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

be to, nenumatytas joks techninių apsaugos priemonių ir naudotojo teisių suderinimo mechanizmas.

Analizuojant minėtuosius *sui generis* teisių apribojimus, išryškėja akivaizdus jų neadekvatumas – iš esmės absoliučioms ir neterminuotoms duomenų bazės gamintojo teisėms priešpriešinamos minimalios naudotojo teisės, kurios gali būti lengvai eliminuojamos techninėmis apsaugos priemonėmis ar licencijos sąlygomis. Atkreiptinas dėmesys, kad nedidelių duomenų bazių turinio dalių naudojimą riboja duomenų bazių gamintojų interesai, o esminės dalies asmeninio naudojimo teisės apskritai taikomos tik neelektroninių duomenų bazių turiniui. Taip nepagrįstai diskriminuojamos neelektroninės duomenų bazės (nors kultūrine prasme jos gali būti vertingesnės ir reikalauti didesnių investicijų). Duomenų bazių turinio esminės dalies naudojimas mokymo ar įvairių sričių mokslinio tyrimo tikslams irgi yra apribotas tik pavyzdžio pateikimu.

Iš esmės didžiausias *sui generis* teisių į duomenų bazes apribojimas yra bendras šių teisių neapibrėžtumas (teisinis reikalavimas įrodyti esmines investicijas į duomenų bazės turinį), o ne jau minėtosios duomenų bazių naudotojų teisės. Būtent tokią praktiką formuoja ES valstybių nacionaliniai teismai ir ESTT. Dėl ES direktyvoje 96/9/EB įtvirtintų duomenų bazių *sui generis* teisinės apsaugos principų neapibrėžtumo dauguma nacionalinių bylų, susijusių su šių teisių taikymu, keliauja į ESTT, kuris formuoja vadinamąją šalutinio produkto (angl. *spin-off)* doktriną, kuria vadovaujantis *sui generis* teisės netaikomos tuo atveju, jeigu duomenų bazė sukuriama kaip veiklos, kurios svarbiausias tikslas nėra sukurti duomenų bazę, subproduktas. Šalutinio produkto doktrina iš esmės eliminuoja *sui generis* teisinę duomenų bazių, apimančių sporto varžybų tvarkaraščius, televizijos programas ir jų sąvadus, telefono numerių duomenų bazes ir pan., apsaugą. Kaip jau minėta, tokios duomenų bazės nėra saugomos ir autorių teisėmis, nes jos netenkina originalumo kriterijaus ir yra nulemtos funkcinių reikalavimų. Deja, teismų praktika kol kas nepateikia atsakymų į esminius *sui generis* teisių neapibrėžtumus – esminių investicijų kriterijus suteikia galimybę neterminuotai pratęsti *sui generis* teises ar išplėsti naudotojų teisių apimtį (teises į nedidelės ar didesnės duomenų bazių turinio dalies naudojimą), tačiau akivaizdi tendencija siaurinti duomenų bazių *sui generis* teisinės apsaugos apimtį.

Apskritai duomenų bazių *sui generis* teisinė apsauga net ir pačioje ES atvirai vertinama kaip abejotinas socialinis eksperimentas – taikydama duomenų bazių *sui generis* teisinę apsaugą ji liko vieniša, nes kitos išsivysčiusios šalys, tokios kaip JAV, Japonija, Kanada ir Australija, bei besivystančios valstybės šios iniciatyvos nepalaikė. Per dešimt metų ES direktyva

96/9/EB nesukėlė jokio apčiuopiamo duomenų bazių industrijos ar su ja susijusių verslų proveržio ES, o JAV duomenų bazių industrija nepatiria jokių sunkumų ir iš esmės klesti, nors duomenų bazės saugomos tik tradicinėmis autorių teisėmis, komercinėmis paslaptimis ir techninėmis apsaugos priemonėmis. Dėl šių priežasčių iš esmės įšaldytas ir ES inicijuotas PINO duomenų bazių sutarties, kuri nustatytų tarptautinę duomenų bazių *sui generis* teisių apsaugą, siūlymas.

3. Teisinė duomenų bazių apsauga Lietuvoje

Kaip jau minėta, Lietuvoje šiuo metu aiškiai įtvirtinta teisinė duomenų bazių apsauga autorių teisėmis ir *sui generis* teisinė apsauga. Duomenų bazių *sui generis* teisinės apsaugos normos yra tik pažodžiui perkeltos iš ES direktyvos 96/9/EB, jų nė trupučio nepaaiškinant ir neišplėtojant. Autorių teisių normos, taikomos duomenų bazėms, irgi gana rudimentinės ir prieštaringos – ypač neaiškus bendrųjų turtinių autorių teisių išimčių santykis su specifiniu duomenų bazių teisiniu reglamentavimu ir duomenų bazių autorių teisių išimčių santykis su duomenų bazių *sui generis* teisinės apsaugos taisyklėmis (AGTGĮ 32 str. ir 61–64 str.). Lietuvoje nėra nei teisinių duomenų bazių apsaugos taikymo apribojimų, nei komercinių paslapčių (neviešoms duomenų bazėms), nei techninių apsaugos priemonių, 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, kol kas Lietuvoje nėra jokios teismų praktikos dėl duomenų bazių *sui generis* teisinės apsaugos apimties, galiojimo ar apribojimų, tačiau prireikus turėtų būti vadovaujamasi ESTT praktika ir ES jurisprudencija, be to, turėtų būti įvertinti duomenų bazių *sui generis* teisinės socialinės apsaugos tikslai ir būtinybė užtikrinti teisių turėtojų, naudotojų ir visuomenės interesų balansą.

10 skirsnis. Teisiniai intelektinės nuosavybės techninių apsaugos priemonių aspektai

Siekdami užkirsti kelią intelektinės nuosavybės teisių pažeidimams e. erdvėje, intelektinės nuosavybės gamintojai ir platintojai greta įprastinių teisinių priemonių (teisinės atsakomybės) pradėjo naudoti įvairias technines apsaugos priemones, teisių valdymo mechanizmus ir sutartinius autorinių kūrinių bei gretutinių teisių objektų laikmenų atgaminimo ir net įprasto jų naudojimo apribojimus. Tokios techninės apsaugos priemonės dažnai gali būti veiksmingesnės nei atitinkami teisiniai draudimai ar

ribojimai. Techninėmis apsaugos priemonėmis laikoma bet kokia technologija, įtaisai ar jų sudėtinės dalys, skirti normaliai veikiant uždrausti arba riboti su autorių teisių, gretutinių teisių ar *sui generis* teisių objektais atliekamus veiksmus, kurių neleidžia autorių teisių, gretutinių teisių ar *sui generis* teisių subjektai. Techninės apsaugos priemonės laikomos veiksmingomis, jeigu autorių teisių, gretutinių teisių ar *sui generis* teisių saugomo 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 trikdyti normalios elektroninės įrangos veiklos ir jos technologinio tobulėjimo.

Įsipareigojimai užtikrinti techninių priemonių ir informacijos apie autorių ir gretutinių teisių valdymą teisinę apsaugą yra įtraukti į TRIPS sutartį ir WIPO interneto sutartis bei ES norminius aktus.

Skaitmeninėse garso ir vaizdo informacijos laikmenose (kompaktinėse plokštelėse, *DVD* laikmenose) plačiausiai naudojamas techninis apribojimas – draudimas skaitmeniniu formatu atkurti skaitmeninę informaciją. Vartotojui naudojant tokią informacijos laikmeną, informacija (fonograma, garso ir vaizdo kūrinys bei pan.) atkuriama tik analogine forma, taip užkertant kelią atgaminti informaciją skaitmenine forma. Tam, kad analoginė informacija būtų paversta skaitmenine (tam, kad būtų pagaminta skaitmeninė fiksacija), būtina sudėtinga konversijos procedūra, kurios metu nukenčia ir informacijos tikslumas, ir 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 būdingas televizijos ir radijo veiklai, kabelinėms ir palydovinėms transliacijoms. Tam, kad atgamintų užšifruotus garso ir vaizdo kūrinius bei fonogramas, naudojamas televizijos, radijo, kabelinėms ar palydovinėms transliacijoms, vartotojas turi įsigyti specialų dekoderį, dekodavimo kortelių ir pan., kartu sumokėdamas ir už šių kūrinių naudojimą. Techninių šifravimo priemonių grupei dar priklauso ir aukščiau minėtoji *Macrovision*, taip pat specialios apsaugos sistemos, užkertančios kelią kopijuoti kompaktines plokšteles ir *DVD* laikmenas (pvz., *CSS* kodavimas, žr. žemiau). Visos šios techninės priemonės gana 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 naujų neteisėtos veiklos formų – įrenginių, skirtų techninėms apsaugos priemonėms pašalinti ar apeiti, 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 savarankiška teisinė apsauga. Visose išsivysčiusiose valstybėse draudžiama panaikinti bet kokias autorių ar gretutinių teisių objekto technines apsaugos priemones, taip pat gaminti ar platinti prietaisus ar kitokias priemones, skirtas minėtosioms techninėms priemonėms pašalinti. Pabrėžtina, kad tam tikrais atvejais techninių priemonių pašalinimas yra būtinas, siekiant įgyvendinti įstatymais nustatytas autorių ir gretutinių teisių išimtis (pvz., būtų užtikrinamas suderinamumas arba galimybė atgaminti atsarginę kopiją), todėl techninių priemonių taikymas ir apsauga iki šiol kelia 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 identifikuojanti kūrinį ir jo autorių, kitą autorių teisių subjektą arba atlikėją, kūrinio atlikimą, fonogramą ir jos gamintoją, kitą gretutinių teisių subjektą, taip pat informacija apie kūrinio, atlikimo ar fonogramos naudojimo sąlygas ir tvarką. Tokia informacija paprastai pateikiama kaip 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. Šios informacijos pašalinimas ar pakeitimas gali suklaidinti vartotoją ir paskatinti neteisėtą veiką. Pats informacijos pašalinimas ar apkeitimas irgi pažeidžia autorių ar gretutinių teisių turėtojo interesus. Dėl šių priežasčių informacijai apie autorių ir gretutinių teisių valdymą taikoma speciali teisinė apsauga.

E. turinio bylose techninės apsaugos priemonės ir informacija apie teisių valdymą dažnai įdiegiama pasitelkus specialius šifravimo algoritmus. Tokie algoritmai turi būti atpažįstami specialios programinės ar aparatinės įrangos ir tik tada e. bylos turinys gali būti atgamintas. Pvz., vis dar naudojamose *DVD* laikmenose išsaugotas e. turinys apsaugotas specialiu *CSS* (angl. *Contents Scrambling System)* kodu, kuris turi užkirsti kelią atgaminti įrašą skaitmenine, tačiau leidžia tai padaryti analogine (prastesnės kokybės) forma. 1999 m. *DVD* laikmenoms net nespėjus paplisti rinkoje interneto kompiuterių tinkle pasirodė *DeCSS* kompiuterių programa, kurią pasitelkus e. turinys, išsaugotas *DVD* laikmenose, gali būti atgamintas skaitmenine forma be apribojimų. Minėtoji programa buvo sukurta teisėtiems tikslams – siekiant užtikrinti *DVD* standarto suderinamumą su *Linux* ir kitomis nekomercinėmis kompiuterių operacinėmis sistemomis, tačiau ji atvėrė kelią ir *DVD* laikmenose išsaugotos informacijos pažeidimams.

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

Viena iš techninės apsaugos priemonių yra informacijos apie teisių valdymą įdiegimas į intelektinės nuosavybės objektus, t. y. į patį e. turinį. 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, irgi yra laikomas autorių teisių ir gretutinių teisių pažeidimu.

Šiuo metu vis plačiau naudojamos naujosios kartos techninės apsaugos priemonės, kurios iš esmės decentralizuoja e. turinį – tam tikros turinio dalys vartotojui yra pateikiamos srautiniu realaus laiko režimu ir tik tuo atveju, jeigu vartotojo turimos dalies koduotė serverio yra atpažįstama kaip teisėta. Tokios techninės apsaugos priemonės ypač efektyvios, tačiau jomis norinčio naudotis vartotojo galinis įranginys turi būti nuolat prijungtas prie interneto. Be to, reikalaujama, kad interneto ryšys būtų gana greitas ir leistų be trikdžių į vartotojo laikmeną ar bylą parsiųsti trūkstamus e. turinio elementus. Šios techninės apsaugos priemonės yra labai efektyvios ir negali būti apeinamos, tačiau didžiausias jų trūkumas – ribotos pačių vartotojų galimybės naudoti e. turinį, nes tai yra įmanoma tik turint greitą ir patikimą interneto ryšį. Vis dėlto galima teigti, kad tokio tipo techninės apsaugos priemonės taps e. turinio verslo standartu, pvz., bendrovė *Blizzard*, kurianti populiariausius kompiuterinius žaidimus, 2012 m. pareiškė, kad visiems naujiems žaidimams naudos būtent nuolat prie interneto prijungtas technines apsaugos priemones. Populiariausios žaidimų ir e. turinio įrenginio *Xbox* gamintoja *Microsoft,* 2013 m. pristačiusi naujosios kartos įrenginį *Xbox One*, irgi nustatė, kad juo bus galima naudotis tik tada, jeigu e. turinys kasdien bus autentifikuojamas interneto ryšiu.

Teisinės nuostatos dėl techninių apsaugos priemonių ir teisių valdymo informacijos Lietuvos civiliniuose įstatymuose įtvirtintos iš esmės atkartojant PINO interneto sutarčių taisykles.

Techninių apsaugos priemonių apsauga įtvirtinama ir BK XXX skirsnio nuostatomis, 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 jos turi būti padaromos tiesiogiai, kaltininkui tyčia suvokiant nusikalstamos veikos pobūdį ir norint taip veikti. Už minėtąsias veikas taikomos tokios sankcijos: 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, dėl to iš esmės neįmanomos tampa autorių teisių ir gretutinių teisių išimtys – teisė atgaminti asmeniniams ar švietimo ir mokslo tikslams ir kt. Daugumos valstybių, tarp jų ir Lietuvos, įstatymai nenumato jokio realaus mechanizmo, kaip vartotojui įgyvendinti savo juridines teises (pvz., asmeninės kopijos teisę ar teisę intelektine nuosavybe naudotis mokslo ir švietimo tikslams). Tokia padėtis akivaizdžiai lemia intelektinės nuosavybės vartotojo teisių ir intelektinės nuosavybės teisių pažeidimų koliziją, t. y. vartotojas, norėdamas įgyvendinti savo teises, iš tikrųjų neturi jokios kitos išeities – tik pažeisti technines apsaugos priemones. Kadangi už techninių apsaugos priemonių pažeidimus numatyta net ir baudžiamoji atsakomybė, būtina nedelsiant spręsti šią teisių koliziją.

11 skirsnis. Kolektyvinio intelektinės nuosavybės administravimo elektroninėje erdvėje sunkumai

Kolektyvinio administravimo asociacijos dažniausiai atlieka dvi pagrindines funkcijas – rūpinasi užmokesčio už autorių teisių ar gretutinių teisių naudojimą (visų pirma teisės atgaminti kūrinį) surinkimu ir autorių bei gretutinių teisių apsauga. Tradiciškai įgaliojimus atstovauti autorių ar gretutinių teisių turėtojui kolektyvinio administravimo institucija įgyja sudarydama atitinkamą (pavedimo) sutartį su autorių ar gretutinių teisių turėtoju ar jam atstovaujančiąja institucija, todėl kolektyvinio administravimo asociacijų teisės tiesiogiai priklauso nuo šių asociacijų narių mandato. Vietoj tokio sutartinio mandato šiuo metu plačiai taikomas teisinio atstovavimo principas, kuris reiškia, kad kolektyvinio administravimo institucijos pagal įstatymą laikomos visų autorių teisių turėtojų atstovais ir administruoja visą atitinkamų teisių visumą.

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 – būtinybė centralizuotai nustatyti retransliacijos licencijos tarifus ir išvengti ypač sudėtingo individualaus licencijavimo. Šia prasme kolektyvinis administravimas užtikrina ir viešąjį interesą –

visuomenės galimybę per transliacijas susipažinti su visais kūriniais už tinkamą kainą. Jeigu reikėtų individualiai derėtis su kiekvieno kūrinio teisių turėtoju, tai labai pasunkintų ir pabrangintų visuomenės galimybę gauti šią informaciją. Kitose srityse, ypač kai autorių ir gretutinių teisių turėtojai ekonominiu ir organizaciniu požiūriu yra pajėgūs subjektai, kolektyvinio administravimo taikymas nepageidautinas, nes būtų neefektyvus bei dubliuotų pačių autorių ir gretutinių teisių turėtojų veiklą. Tokios sritys yra, pvz., autorių teisės į kompiuterių programas, autorių teisės ar *sui generis* teisės į duomenų bazes, pagrindinės teisės į garso ir vaizdo (kino, vaizdo įrašų, TV laidas) produkciją ir pan. Kolektyvinis administravimas iš esmės netaikomas ir pramoninės nuosavybės sričiai, tačiau joje gana aktyviai veikia teisių turėtojų interesus vienijančios ir jiems atstovaujančios organizacijos.

Sparčiai tobulėjant technologijoms – ypač plintant techninėms apsaugos priemonėms bei autorių teisių ir gretutinių teisių valdymo technologijoms – didėja pačių autorių ir gretutinių teisių turėtojų galimybės administruoti savo teises ir kontroliuoti saugomų kūrinių naudojimą. Šiuo metu ir autorių, ir gretutinių teisių valdymo techninių apsaugos priemonių teisinė apsauga yra reglamentuojama atskirai, o šios priemonės tampa svaria kolektyvinio teisių administravimo alternatyva. Be to, kūrybinių bendrijų judėjimas irgi orientuotas į paties autoriaus galimybes licencijuoti savo kūrinį ir individualiai nustatyti jo naudojimo režimą.

Pramoninės nuosavybės srityje veikia teisių turėtojų interesus vienijančios organizacijos – nors jos ir neatlieka formalių kolektyvinio administravimo funkcijų, yra joms artimos: organizuoja savo narių intelektinės nuosavybės teisių gynimą, inicijuodamos civilines, administracines ir (ar) baudžiamąsias bylas prieš intelektinės nuosavybės teisių pažeidėjus, bendradarbiauja su teisėsaugos institucijomis dėl intelektinės nuosavybės gynimo, užsiima aktyvia lobistine veikla, atstovauja atitinkamai industrijai ir koordinuoja veiklą nacionaliniu ar tarptautiniu mastu.

Kolektyvinis intelektinės nuosavybės teisių administravimas iš esmės parankus industrinei, bet ne žinių, visuomenei. Ypač kolektyvinis administravimas netinkamas e. erdvėje. Svarbiausios to priežastys – kolektyvinio administravimo ir technologinių intelektinės nuosavybės teisių administravimo mechanizmų nesuderinamumas. Šiuo metu didžiausi e. erdvės kolektyviniam administravimui keliami iššūkiai yra nesuderinamumas su individualiu technologiniu teisių administravimu ir dvigubas ar nepagrįstas tų pačių intelektinės nuosavybės naudojimo formų apmokestinimas.

Techninių apsaugos priemonių bei autorių teisių ir gretutinių teisių valdymo technologijų naudojimas – plintantis individualus teisių administravimas – lemia dvigubo ar net apskritai nepagrįsto autorinio atlyginimo

mokėjimą už intelektinės nuosavybės naudojimą. Geriausiai šią problemą parodo kolektyvinio administravimo asociacijų už garso ir vaizdo ar į fonogramas įrašytų kūrinių atgaminimą asmeniniams tikslams renkamas atlyginimas – laikmenų ir įrangos mokesčiai. Kaip jau minėta, pagal galiojančias taisykles (ATGTĮ 20 str.) bendriniai laikmenų ir įrangos mokesčiai yra mokami:

- už visas laikmenas, iš jų ir tas, kurios naudojamos su intelektine nuosavybe visiškai nesusijusiems tikslams (pvz., asmeninei kūrybai);
- tais atvejais, kai kūrinio asmeninis atgaminimas yra uždraustas techninėmis priemonėmis, t. y. kūrinio teisėtai atgaminti asmeniniams tikslams iš esmės neįmanoma. Pabrėžtina, kad šiuo metu apie 90 proc. viešai platinamo e. turinio dėl taikomų techninių apsaugos priemonių negali būti teisėtai atgaminama asmeniniams ar kitiems tikslams;
- neatsižvelgiant į tai, kad panašus tuščios laikmenos mokestis jau buvo sumokėtas kitose ES valstybėse, o nacionaliniams subjektams nėra realių galimybių jo atgauti;
- neatsižvelgiant į tai, kad autorinis atlyginimas buvo sumokėtas įsigyjant individualias licencijas (pvz., įsigyjant kūrinį interneto muzikos įrašų parduotuvėje).

Kita didelė kolektyvinio administravimo problema – tokio administravimo neskaidrumas ir neefektyvumas. Per kolektyvinio administravimo sistemą yra perskirstomos milijoninės lėšos, surinktos kaip visuotinio pobūdžio mokesčiai, tačiau nežinoma, kam konkrečiai jos naudojamos. Netgi neaiškūs lėšų paskirstymo konkretiems gavėjams kriterijai. Netiesioginė informacija ir Lietuvoje bei kitose valstybėse nuolat kylantys skandalai leidžia daryti prielaidas, kad didžiausios išmokos skiriamos ne tiems asmenims, dėl kurių teisių gauta daugiausia įplaukų, be to, didelė dalis kolektyvinio administravimo asociacijų surinktų lėšų apskritai naudojama ne išmokoms už teises, o su tuo nesusijusiems tikslams, pvz., prabangiai išlaikyti asociacijų vadovybę ir pan.

Atsižvelgiant į pasaulinę patirtį, efektyvia lėšų perskirstymo sistema laikoma ta, kuri perskirstydama lėšas sunaudoja ne daugiau kaip dešimt ar dvylika procentų visos surenkamos sumos. Deja, kolektyvinio administravimo sistemos analizė rodo, kad faktinės perskirstymo sąnaudos gana dažnai viršija dvidešimt penkis procentus surenkamų pinigų. Iš esmės sąnaudos yra dar didesnės, nes didelė dalis už intelektinės nuosavybės teises surinktų lėšų iš jų gavėjų yra nusavinamos įvairioms plėtros, kultūrinėms ir pan. programoms.

Būtinas visiškas kolektyvinio administravimo asociacijų perskirstomų lėšų skaidrumas, t. y. turi būti žinomos konkrečios sumos, išmokamos tam tikriems asmenims. Neskaidrumas negali būti dangstomas privatumu, nes per kolektyvinio administravimo sistemą yra perskirstomos *de facto* mokesčių pavidalu surinktos lėšos. Be to, reikalingos kolektyvinio administravimo sąnaudų lubos ir lėšų naudojimo būdų reglamentavimas.

Dar viena kolektyvinio administravimo problema – sistemos monopolizmas ir ribotas teritorinis pobūdis. Akivaizdu, kad jokios konkurencijos nebuvimas leidžia kolektyvinio administravimo asociacijoms intelektinės nuosavybės naudotojams diktuoti vienašališkas monopolistines sąlygas. Ribotas teritorinis kolektyvinio administravimo pobūdis pats savaime yra nesuderinamas su globalia e. turinio rinka. Be šio ribotumo dar atsižvelgus į monopolinę padėtį matyti, kad kolektyvinio administravimo asociacijos yra visiškai nesuinteresuotos globalios e. turinio rinkos ir konkurencijos plėtra.

Visos aptartos problemos rodo, kad kolektyvinio administravimo sistema yra morališkai pasenusi. Esama nuomonių, kad šios sistemos turėtų būti išvis atsisakyta, nes jos neįmanoma pritaikyti žinių visuomenės realijoms.

Minimalūs būtini kolektyvinio administravimo sistemos pakeitimai – jos išskaidrinimas ir konkurencijos įgalinimas, ypač skatinant skaidrų reguliuojamą individualų teisių administravimą pasauliniu mastu.

12 skirsnis. Atvirojo kodo ir kūrybinių bendrijų judėjimai

XX a. paskutiniojo dešimtmečio pabaigoje e. erdvėje dar atsirado ir įsitvirtino alternatyvūs intelektinės nuosavybės judėjimai, tokie kaip atvirosios programinės įrangos (angl. *Open source)* ir kūrybinių bendrijų (angl. *Creative Commons)*, akcentuojantys intelektinės nuosavybės svarbą socialiniam informacijos prieinamumui ir planavimui, kultūros bei technologijų plėtrai.

Atvirosios programinės įrangos judėjimas yra kompiuterių programų, kurių kodas pateikiamas viešai analizei ir tobulinimui, virtualioji autorių bendruomenė. Kiekvienas asmuo gali laisvai naudotis atvirąja programine įranga, ją perdirbti, tobulinti ir pan., tik keliama sąlyga, kad jo panaudotas ar perdirbtas kompiuterių programos kodas liks atviras, t. y. laisvai prieinamas ir viešas. Atvirosios programinės įrangos judėjimas neturėtų būti tapatinamas su nemokamomis kompiuterių programomis, nes atviroji programinė įranga nebūtinai turi būti platinama ir prieinama nemokamai, tik svarbu, kad programos kodas būtų laisvai viešai prieinamas ir būtų galima šį kodą ar jo elementus naudoti naujoms kompiuterių programoms kurti. Atvirosios programinės įrangos judėjimo tęstinumas užtikrinamas specialiomis atvirosios programinės įrangos licencijomis (susitarimais dėl

atvirosios programinės įrangos teisinio statuso ir naudojimo sąlygų). Atvirosios programinės įrangos judėjimas jokiu būdu neneigia intelektinės nuosavybės teisių reikalingumo ir tam neprieštarauja, priešingai, jis yra priklausomas nuo intelektinės nuosavybės teisių, kurios naudojamos ginant atvirosios programinės įrangos (ir jo pagrindu sukurto naujo kodo) viešumą ir prieinamumą.

Kūrybinių bendrijų (angl. *Creative Commons)* judėjimas yra atvirosios programinės įrangos principais pagrįsta bet kokios informacijos (kūrinių, inovacijų) apsikeitimo ir tobulinimo forma, t. y. pagal aiškiai apibrėžtas licencijas leidžianti pateikti viešai platinti ir naudoti intelektinės nuosavybės teisėmis saugomą turinį. Atsižvelgiant į autoriaus ar teisių turėtojo pasirinktas licencijos sąlygas, kiti asmenys nemokamai ar už tam tikrą atlygį gali naudotis kūrybinių bendrijų informacija, ją perdirbti, naudoti nekomerciniams projektams ir pan. Kūrybinės bendrijos gerokai supaprastina intelektinės nuosavybės naudojimą, nes išlaisvina jos naudotojus nuo būtinybės bendrauti su autoriumi (teisių turėtoju ir pan.) ir individualiai derinti licencijos sąlygas.

Atviro kodo judėjimas laikytinas pirmosiomis viosuomenės pastangomis bent iš dalies pašalinti autorių teisių ir gretutinių teisių sistemos trūkumus bei žinių visuomenės poreikių neatitikimą. Pabrėžtina, kad minėtasis judėjimas atsirado dar tada, kai teisininkai tik svarstė istorinio intelektinės nuosavybės teisinio režimo pakeitimus, ir pagrįstai paskatino sutartinių licencijų kaip alternatyvaus skaitmeninio turinio teisinės apsaugos būdo naudojimą kompiuterių programų kodo apsaugai. Atviro kodo licencijos iš pradžių buvo kuriamos siekiant užkirsti kelią pasisavinti kompiuterinį programinės įrangos kodą, kad jį būtų galima peržiūrėti ir pakartotinai naudoti, ir reikalauti, kad išvestiniai kūriniai (nauja programinė įranga su ankstesniu atviru kodu) irgi išliktų prieinami. Buvo sukurta daug atviro kodo licencijų versijų, iš jų geriausiai žinoma yra *GPL* (Bendra viešoji licencija).

Kūrybinių bendrijų judėjimu iš pradžių buvo siekiama atviro kodo licencijų principus pritaikyti visų rūšių skaitmeniniam turiniui (išskyrus kompiuterinį programinės įrangos kodą), kaip antai skaitmeninėms fotografijoms, skaitmeninei muzikai, tekstui, multimedijos turiniui, garso ir vaizdo klipams ir t. t. Kaip ir atviro kodo judėjimo atveju, kūrybinių bendrijų licencijos pirmiausia yra skirtos nustatyti sutartinį teisinės apsaugos režimą kūriniams, kuriems taikoma licencija. Šis licencijavimo režimas nesiremia teisine licencijuoto turinio apsauga, jis nustatomas sutartimi ir priklauso nuo sutartinių teisių gynimo priemonių, sutartinės atsakomybės ir bendrosios sutarčių teisės mechanizmų. Kadangi sutartis jau pati savaime

yra kur kas lengviau pritaikoma negu bendrasis teisinis režimas, ji gali ignoruoti įvairius autorių teisių ir gretutinių teisių teisinio reguliavimo apribojimus. Taikydamas sutartinio atsisakymo nuostatas, autorius gali nustatyti trumpesnius apsaugos terminus ar papildomų išimčių, o sutartines teises išdėstyti paprastai ir suprantamai. Šis pranašumas licencijos sąlygas supaprastina beveik iki semiotinio lygio. Tokiu būdu jos tampa suprantamos kiekvienam, net ir neturinčiam specialių žinių apie autorių teisę. Toks paprastumas ir prieinamumas tapo kūrybinių bendrijų judėjimo pagrindu.

Kūrybinių bendrijų organizaciją 2001 m. įsteigė L. Lessigas, H. Abelsonas ir E. Eldred'as *http://en.wikipedia.org/wiki/Creative_Commons - cite_note-1*. Pirmasis kūrybinių bendrijų autorių teisių licencijų rinkinys buvo išleistas 2002 m. gruodį JAV jurisdikcijai. 2008 m. 130 mln. kūrinių visame pasaulyje buvo licencijuota pagal kūrybinių bendrijų licencijų sutartis. Pabrėžtina, kad pirmosios kūrybinių bendrijų licencijos buvo specialiai sukurtos ir pritaikytos JAV autorių teisių sistemai. Svarbiausios kūrybinių bendrijų licencijų ypatybės, kaip antai autoriaus teisė būti nurodytam (teisė į autorystę), jau senokai pripažįstamos kitų valstybių (tarp jų Lietuvos) teisės aktuose ir yra nereikalingos daugeliui Europos autorių teisių ir gretutinių teisių sistemų. Europos valstybėse ir Lietuvoje yra numatytos tam tikros autoriaus specialiosios arba neturtinės teisės, kurios negali būti atskiriamos nuo autoriaus asmens ir perleidžiamos tretiesiems asmenims. Teisė į autorystę – vadintis ar būti nurodytam kaip kūrinio autoriui – yra nustatyta 1886 m. Berno konvencijoje dėl literatūros ir meno kūrinių apsaugos, kuri yra Europos autorių teisės pagrindas. Tačiau dėl to kūrybinių bendrijų licencijos netampa bevertėmis Europos autoriams, nes šie, remdamiesi kūrybinių bendrijų autorystės licencija, galėtų naudotis autorystės teisių apsauga jurisdikcijose, kurios kitais atvejais nepripažintų autorių neturtinių teisių apsaugos.

Tai yra tik vienas pavyzdys, rodantis, kad kūrybinių bendrijų licencijos priklauso nuo konkrečios jurisdikcijos. Dėl didelės neturtinių, pagrindinių turtinių teisių, išimčių ir teisių valdymo reglamentavimo įvairovės kūrybinių bendrijų licencijos turėtų būti pritaikomos kiekvienai jurisdikcijai, kad jas būtų galima naudoti teisme, o jų vykdymą užtikrinti teismine tvarka. Daugelyje šalių nacionalinės kalbos tekstas yra būtina teisminės gynybos ir vykdymo užtikrinimo teismine tvarka sąlyga, ypač vartotojams. Šie reikalavimai labai apriboja tarptautinių kūrybinių bendrijų licencijų taikymą, kuris yra svarbiausias atsižvelgiant į globalią e. turinio rinką.

Išoriškai kūrybinių bendrijų licencijų režimas žymimas bendrųjų simbolių ir santrumpų rinkiniu, kuris yra lengvai suprantamas net ne specialistui ir automatizuotoms kompiuterių sistemoms. Kūrybinių bendrijų

licencijų režimo negalima painioti su nekomerciniu kūrinio naudojimu arba jo apsaugos atsisakymu. Pavyzdžiui, kūrybinių bendrijų autorystės (BY) licencija leidžia asmeniui kurti išvestinius kūrinius ir jais dalytis netgi komerciniam naudojimui tol, kol nurodoma originali autorystė. Be to, kūrybinių bendrijų licencijavimo režimo nustatyti draudimai nėra absoliutūs ir gali būti licencijos davėjo (autoriaus arba teisių turėtojo) atšaukiami, atsižvelgus į individualų atvejį ir gavus prašymą, pvz., pagal „Autorystės nuoroda. Išvestiniai kūriniai negalimi. Platinimas leidžiamas tik tokiomis pat sąlygomis“, (BY-ND-SA) licenciją paprastai būtų visiškai uždrausta kurti komercinį išvestinį kurinį iš nekomercinio, tačiau licencijos davėjas individualiu atveju gali padaryti išimčių. Kūrybinių bendrijų licencijų režimas gali būti apibendrinamas kaip „tam tikros teisės saugomos“ režimas ir priešpriešinamas „visos teisės saugomos“ režimui, kuris paprastai yra taikomas didžiajai komerciniu būdu platinamo turinio daliai.

Visos pirminės kūrybinių bendrijų licencijos suteikia pagrindines teises, kaip antai teisę visame pasaulyje nemokamai platinti autorių teisių ginamą kūrinį, jame neatliekant jokių pakeitimų. Kiekvienos iš šių licencijų turinys susideda iš keturių pagrindinių sąlygų:

1) autorystės nuoroda (BY). Licencijos gavėjui leidžiama kopijuoti, platinti, demonstruoti ir atlikti kūrinį bei kurti išvestinius kūrinius originalo pagrindu tik tuo atveju, jeigu jų nustatytu būdu nurodomas autorius arba licencijos davėjas;
2) nekomercinis naudojimas (NC). Licencijos gavėjui leidžiama kopijuoti, platinti, demonstruoti ir atlikti kūrinį bei kurti išvestinius kūrinius originalo pagrindu tik nekomerciniams tikslams;
3) išvestiniai kūriniai negalimi (ND). Licencijos gavėjui leidžiama kopijuoti, platinti, demonstruoti ir atlikti tik pažodines kūrinio kopijas, tačiau draudžiama originalo pagrindu kurti išvestinius kūrinius;
4) platinimas leidžiamas tik tokiomis pat sąlygomis (SA). Licencijos gavėjui leidžiama platinti išvestinius kūrinius tik pagal analogišką licenciją, kuria pažymėtas kūrinio originalas.

Galimi keturių minėtųjų sąlygų deriniai. Kaitaliojant ir derinant šias sąlygas gaunama vienuolika galiojančių Kūrybinių bendrijų licencijų (likusieji deriniai yra teisiškai negalimi dėl tarpusavyje nesuderinamų sąlygų). Šešios dažniausiai naudojamos licencijos yra šios: Autorystės nuoroda (BY), Autorystės nuoroda + Nekomercinis naudojimas (BY-NC), Autorystės nuoroda + Išvestiniai kūriniai negalimi (BY-ND), Autorystės nuoroda + Platinimas leidžiamas tik tokiomis pat sąlygomis (BY-SA), Autorystės nuoroda + Nekomercinis naudojimas + Išvestiniai kūriniai negalimi

(BY-NC-ND), Autorystė + Nekomercinis naudojimas + Platinimas leidžiamas tik tokiomis pat sąlygomis (BY-NC-SA). Kaip jau minėta, paprasčiausiomis santrumpomis yra žymima speciali teisinė kalba, pritaikyta jurisdikcijos, kuriai ji naudojama, ypatumams.

Lietuvoje kūrybinių bendrijų judėjimas sunkiai skinasi kelią. Tam yra kelios priežastys:

1) dėl griežtos neturtinių teisių doktrinos ir reglamentavimo autoriams nėra svarbu sutartimis reguliuoti autorystės teisę;
2) savarankiškai sukurto nacionalinio turinio kiekis (neturint jokių išankstinių susitarimų) yra sąlygiškai mažas;
3) kūrybinių bendrijų licencijų pobūdis yra gana svetimas Lietuvos autorių teisei (kaip minėta, autorystės nuoroda (BY) Lietuvoje nėra reikšminga);
4) valstybės institucijos yra atsakingos už autorių teisių politiką, kai kurie autorių teisių ir gretutinių teisių mokslininkai, teismai ir ypač kolektyvinio teisių administravimo asociacijos smarkiai priešinasi bet kokiems alternatyviems autorių teisių ir gretutinių teisių apsaugos būdams ir neretai net sąmoningai tapatina juos su piratavimu;
5) kai kurios teisės aktų nuostatos dėl autorių teisių ir gretutinių teisių kolektyvinio administravimo visiškai pašalina individualaus susitarimo (individualaus administravimo) dėl to paties turinio galimybes (todėl kūrybinių bendrijų licencijavimas tampa neįmanomas).

Labai svarbu ir tai, kad kūrybinių bendrumų iniciatyvos Lietuvoje yra plėtojamos asmenų, kurie turi kitokių tikslų nei kūrybinių bendrumų plėtra, pvz., atvirai veikia siekdami maksimaliai riboti individualų teisių administravimą ir išsaugoti neefektyvų ir neskaidrų kolektyvinį intelektinės nuosavybės teisių administravimą. Tokie veiksmai iš esmės sabotuoja nuoširdžias pastangas dėl kūrybinių bendrumų Lietuvoje.

Su pastarąja iš minėtųjų problemų (konfliktu su kolektyvinio administravimo sistema) susiduriama ir kitose jurisdikcijose. Pagal galiojančius autorių teisių ir gretutinių teisių įstatymus, kolektyvinio teisių administravimo asociacijos turi teisę rinkti autorinius atlyginimus už visą turinį ir nedaryti jokių išimčių. Be to, kolektyvinio teisių administravimo asociacijos reikalauja, kad jų narys perleistų visas teises asociacijos žiniai. Tokiu būdu, remiantis individualia kūrybinių bendrijų licencija, nepriklausomam autoriui iš esmės yra uždraudžiama išduoti individualią licenciją bet kuriam kūriniui, jeigu jis irgi pageidauja būti kolektyvinio teisių administravimo asociacijos narys ir per kolektyvinio teisių administravimo asociaciją gauti autorinius atlyginimus kitiems savo kūriniams. Tokio antagonizmo pagrindai yra numatyti ATGTĮ 65 str., kuris tam tikrais atvejais nustato kolektyvinį

teisių administravimą net ir tada, kai autorius dėl to nesudarė sutarties su nė viena kolektyvinio teisių administravimo asociacija. Dar daugiau, individualaus teisių valdymo galimybė yra apribota sudarant autoriaus arba atlikėjo sutartis su kolektyvinio teisių administravimo asociacijomis. Galiausiai kūrybinių bendrijų licencijavimo naudingumą sumažina teismuose ir kai kuriuose moksliniuose darbuose dominuojantis autorių teisių fundamentalizmas. Alternatyvūs autorių ir gretutinių teisių apsaugos būdai ir individualūs susitarimai yra netgi sąmoningai įvardijami kaip piratiniai ir prieštaraujantys kūrybos skatinimo nuostatoms. Veikla, kuri yra priešinga kūrybinių bendrijų idėjoms, negali būti suderinama su tų pačių asmenų deklaruojamais mėginimais skatinti kūrybines bendrijas.

Tam, kad Lietuvoje būtų naudingos kūrybinių bendrijų licencijos, reikia ne tik vertimo ir teisinio licencijų tekstų suderinimo. Siekiant apriboti kolektyvinio teisių administravimo asociacijų savanaudiškumą ir godumą yra būtini teisės aktų pakeitimai. 2011 m. gruodžio 22 d. Lietuvoje priimti ATGTĮ pakeitimai yra visiškai priešingi žinių visuomenės ir kūrybinių bendrumų siekiams. Norint Lietuvoje paskatinti kūrybinių bendrijų licencijų naudojimą, esamiems ir būsimiems autoriams bei atlikėjams turi būti išaiškinti jų pranašumai, be to, turėtų būti pasitelkiama ir kitų kūrybingumą skatinančių priemonių.

Pabrėžtina, kad kūrybinių bendrijų licencijos neišsprendžia visų galiojančio autorių teisių ir gretutinių teisių režimo problemų. Pavyzdžiui, kūrybinių bendrijų licencijos *per se* neįveikia pernelyg ilgo apsaugos termino (nors autoriai iš anksto gali laisvai atsisakyti savo teisių, tačiau nėra organizuoto ir paprasto būdo, kaip tai padaryti). Iš pirmo žvilgsnio atrodo, kad kūrybinių bendrijų licencijos supaprastina autorių ir gretutinių teisių licencijavimą, tačiau užsienio praktika rodo, kad kūrybinių bendrijų licencijų įgyvendinimas ir gynimas gali būti sudėtingas procesas. Žemyninės Europos (ir Lietuvos) jurisdikcijose, kur dažniausiai veikia savanaudiškų interesų turinčios konservatyvios kolektyvinio teisių administravimo sistemos, dėl kūrybinių bendrijų licencijos autoriams gali kilti dar daugiau sudėtingų konfliktų. Galiausiai kūrybinių bendrijų licencijos tiesiogiai nepadeda atlyginti autoriui už kūrinį.

Aukščiau pateikta analizė leidžia daryti išvadą, kad dabartinio autorių teisių ir gretutinių teisių režimo visaapimanti reforma yra būtina tam, kad kūrybinių bendrijų licencijos ir kiti alternatyvūs teisių apsaugos būdai būtų visapusiškai taikomi Lietuvos ir Europos teisėje. Ši reforma būtų reikalinga supranacionaliniu lygiu, nes tam tikrų nesusipratimų kyla ne dėl nacionalinės teisės, o yra iš anksto užprogramuoti tarptautinėje arba Europos autorių teisių ir gretutinių teisių sistemoje.

13 skirsnis. Laikmenų ir įrangos mokesčiai

Laikmenų ir įrangos mokesčiai (kompensacinis atlyginimas autoriams ir gretutinių teisių turėtojams už kūrinių atgaminimą asmeniniams tikslams) yra viena jautriausių intelektinės nuosavybės e. erdvėje temų, kuria itin dažnai ir nepagrįstai spekuliuodami su kūryba tiesiogiai nesusiję asmenys (tarpininkai) siekia savanaudiškų tikslų.

Autorinius mokesčius – atlyginimą už kūrinių atgaminimą asmeniniams tikslams – Europos Komisija yra priskyrusi prie trylikos svarbiausių autorių ir gretutinių teisių klausimų, kurie laikomi prioritetiniais. 2004–2012 m. Europos Komisija organizavo viešas Valstybių narių ir suinteresuotų asmenų konsultacijas ir klausymus, buvo parengusi rekomendacijos projektą (kurį vėliau atsisakyta priimti motyvuojant reguliavimo formos netinkamumu), o šiuo metu laukiama specialaus projekto. Kiekvienu atveju autorių teisių ir gretutinių teisių turėtojų, kolektyvinio administravimo asociacijų bei informacinių technologijų ir kitų informacinės visuomenės industrijų atstovų nuomonės gana radikaliai išsiskyrė. 2011–2013 m. vyko oficiali mediacijos procedūra, kuri suformulavo labai aiškius siūlymus, kaip reformuoti mokesčių sistemą ir apriboti jos žinių visuomenei daromą žalą, tačiau teisių turėtojai ir kolektyvinio administravimo (ne patys autoriai ar atlikėjai, o jų vardu prisidengiantys tarpininkai) asociacijos atmetė racionalius tarpininko siūlymus.

Būtent taip poliarizuota ir mokslinė diskusija šiuo klausimu. Kai kurie konservatyvūs mokslininkai šiuos mokesčius vertina kaip užmokestį už privalomą licenciją teisių turėtojams (asmeninio atgaminimo teisę), nors tokią poziciją vienareikšmiškai paneigė ESTT 2012 m. pradžioje išspręstoje *Luksan* byloje C-277/10, jis konstatavo, kad tai yra visiškai atskira teisė, kuri suteikiama autoriams ir atlikėjams, bet ne tarpininkams. Atsižvelgiant į naujausią ESTT jurisprudenciją, konstatuotina, kad laikmenų ir įrangos mokesčiai yra neefektyvus ir neteisingas rinkos varžymas, ginantis tik autorių ir gretutinių teisių tarpininkų komercinį interesą.

ESTT *Luksan* byla C-277/10 yra ypač svarbi laikmenų ir įrangos mokesčių kontekste, nes šioje byloje ESTT konstatavo, kad autoriams ir atlikėjams už jų kūrinių naudojimą (taip pat ir asmeniniams tikslams) priklauso aiški atskira teisė į teisingą atlyginimą. Toks atlyginimas turi būti mokamas pirmiausia pačių esamų autorių teisių ir gretutinių teisių turėtojų (tarpininkų), kurie šiuo metu iš esmės nusavina autoriams ir atlikėjams priklausantį atlyginimą. Pats teisingas atlyginimas galėtų būti surenkamas įvairiomis formomis, nebūtinai apmokestinant visas rinkoje parduodamas laikmenas ir įrangą, o, pvz., skiriamas kaip valstybės dotacija. Būtent toks sprendimas nuo 2011 m. pabaigos sėkmingai įgyvendinamas Ispanijoje.

Laikmenų ir įrangos mokesčių klausimą kai kuriais aspektais narpliojo ir Lietuvos teismai, priėmę klaidingus ir nevienareikšmiškai vertinamus sprendimus.

Tinkamas teisingos kompensacijos sprendimas reikalauja teisinio įforminimo, tačiau esamos nuostatos Lietuvoje jų nesprendžia. Vietoj teisingos kompensacijos autoriams ir atlikėjams Lietuvos įstatymai (įskaitant naujausius 2011 m. gruodžio 21 d. ATGTĮ pakeitimus ir jo įgyvendinamuosius teisės aktus) laikmenų ir įrangos mokesčius nustato tarpininkų naudai. Be to, teisinės nuostatos yra nenuoseklios ir neaiškios.

Dėl teisingo atlyginimo teisingos kompensacijos stringančio klausimo sprendimas ne tik Lietuvoje, bet ir kitose ES valstybėse iš esmės persikėlė į teismus, tarp jų ir ESTT. Pradedant *Padawan* byla (*Sociedad General de Autores y Editores de España (SGAE) v. Padawan*, S.L. (byla Nr. C-467/08) ESTT laikmenų ir įrangos mokesčių klausimui suteikia naujų aspektų, kontroversijų ir ilgai laukto aiškumo.

Po *Padawan* bylos priimti ESTT sprendimai *EGEDA v. Magnatrading SL* (byla Nr. C-387/09), *Stichting de Thuiskopie v. Opus Supplies Deutschland GmbH* (byla Nr. C-462/09), *Luksan* (byla Nr. C-277/10) ir kitose bylose iš esmės parodo, kad laikmenų ir įrangos mokesčiai, iš kurių pelnosi daugiausia tarpininkai, ES yra netinkama teisingos kompensacijos autoriams ir atlikėjams forma.

Jurisprudencijoje vartojamos kelios laikmenų ir įrangos mokesčių institutui tapačios sąvokos: „tuščios laikmenos mokestis“, „kompensacija už kūrinių atgaminimą asmeniniams tikslams“, „atlyginimas už garso ir vaizdo ar fonogramose įrašytų kūrinių atgaminimą asmeniniams tikslams“, „kompensacinis atlyginimas“ ir pan., kurios iš esmės reiškia tą patį – teisingos kompensacijos autoriams ir atlikėjams išmokėjimo formas.

Laikmenų ir įrangos mokesčiai, kaip teisingos kompensacijos forma, Lietuvoje iš esmės nustatyti priėmus 2003 m. kovo 5 d. ATGTĮ pakeitimo įstatymą Nr. IX-1355 ir įsigaliojo nuo 2004 m. sausio 1 d. 2011 m. gruodžio 21 d. įstatymu Nr. XI-1833, ATGTĮ pakeitimais laikmenų ir įrangos mokesčių taisyklės buvo gerokai išplėstos, iš esmės apmokestinant visus e. turinio tvarkymo įrenginius ir laikmenas. Pakeitimai įsigaliojo 2012 m. kovo 1 d., tačiau dėl vėluojančių įstatymo įgyvendinamųjų teisės aktų pradėjo veikti tik nuo 2012 m. vidurio. Pakeitimų priėmimas buvo skubotas, o galutinės formuluotės labai neaiškios ir galbūt prieštaraujančios ES teisei, nes nustato ne teisingą kompensaciją autoriams ir atlikėjams, o pasenusią mokesčių, iš kurių pelnosi tik tarpininkai, sistemą. Tais pačiais pakeitimais nustatytas ir reprografinės įrangos apmokestinimas (ATGTĮ 20^1 str.), tačiau savo esme jis labai panašus į laikmenų ir įrangos mokesčius, todėl atskirai nenagrinėjamas.

Bet kokiu atveju 2013 m. rudenį ESTT sprendžiamos bylos laikmenų ir įrangos mokesčių klausimais *(Amazon* byla Nr. C-521/11 ir kt.) ir brėstanti ES teisės reforma šiuo klausimu turėtų koreguoti visų ES valstybių nacionalinę teisę, tarp jų ir Lietuvos. Jau paskelbtos generalinio advokato nuomonės nuteikia optimistiškai – tikėtina, kad teismas dar kartą akcentuos laikmenų ir įrangos mokesčių netinkamumą bei nustatys teisingą kompensaciją žinių visuomenės autoriams ir atlikėjams.

Galiojančio ATGTĮ 20 str. 4–5 d. (po 2011 m. gruodžio 21 d. pakeitimų) nustatyta, kad autorių teisių ir gretutinių teisių subjektai turi teisę gauti kompensacinį atlyginimą už garso ir vaizdo ar fonogramose įrašytų kūrinių atgaminimą asmeniniams tikslams. Kompensacinis atlyginimas turi būti mokamas už ATGTĮ priede nustatytus pirmą kartą Lietuvos Respublikoje parduodamus civilinėje apyvartoje esančius, pagamintus Lietuvos Respublikoje ar į jos teritoriją įvežtus atgaminti asmeniniam naudojimui skirtus įrenginius ir tuščias analogines ir skaitmenines garso bei garso ir vaizdo laikmenas. Mokestį (kompensacinį atlyginimą) privalo mokėti asmenys, Lietuvoje parduodantys šiuos įrenginius ir tuščias laikmenas. Mokesčio objektai ir tarifai yra nustatyti ATGTĮ priede. Konkrečiai apmokestinami bet kokie kompiuteriai, mobilieji telefonai ir kiti įrenginiai, kuriais galima tvarkyti e. turinį. Be to, apmokestinamos bet kokios e. turinio laikmenos, tarp jų ir *flash* atminties laikmenos bei kortelės. Mokesčio tarifai yra tiek fiksuoti (konkreti suma) (pvz., dvidešimt litų už bet kokį kompiuterį), tiek procentiniai, priklausomi nuo mokesčio objekto (pvz., šeši procentai nuo *CD* ar *DVD* laikmenų). Mokesčio objektų sąrašas ir tarifai turėtų būti peržiūrimi ne rečiau kaip kas dveji metai. Mokesčio mokėjimo sąlygas ir tvarką, atsižvelgdama į tai, taikomos ar netaikomos techninės apsaugos priemonės, nustato Vyriausybė, suderinusi su kompensacinio atlyginimo mokėtojams atstovaujančiomis ir autorių teisių bei gretutinių teisių kolektyvinio administravimo asociacijomis.

Naujovė, nustatyta 2011 m. gruodžio 21 d. ATGTĮ pakeitimais, yra teorinė galimybė susigrąžinti sumokėtą mokestį. Mokestis Vyriausybės nustatyta tvarka grąžinamas šiais atvejais:

1) kai tuščios laikmenos ir įrenginiai yra įsigyti profesionalioms reikmėms. Šiame straipsnyje tokiomis reikmėmis laikomos transliuojančiųjų organizacijų ir asmenų, tiražuojančių garso ir vaizdo bei fonogramose įrašytus kūrinius ar gretutinių teisių objektus garso ir vaizdo kūrinių bei fonogramų gamintojams, reikmės, susijusios su kūrinių ar gretutinių teisių objektų įrašymu, ir asmenų, kurie tuščias laikmenas ir įrenginius įsigyja akivaizdžiai kitiems tikslams negu kūrinių atgaminimas asmeniniam naudojimui, reikmės (pvz.,

kai kūriniai atgaminami viešojo valdymo ir gynybos įstaigose ir organizacijose, ligoninėse, švietimo įstaigose, bibliotekose ir valstybės archyvuose, muziejuose, mokslinių tyrimų įstaigose bei organizacijose ir kai kūrinių atgaminimas yra skirtas išimtinai tų įstaigų ir organizacijų veiklos reikmėms);

2) kai tuščios laikmenos ir įrenginiai yra įsigyjami neįgalių žmonių reikmėms;
3) kai tuščios laikmenos ir įrenginiai yra išvežami iš Lietuvos Respublikos teritorijos.

Dar viena šiais ATGTĮ pakeitimais nustatyta naujovė yra reikalavimas, kad apskaitos dokumentuose, kuriais įforminamas pirmas laikmenų ir įrangos pardavimas, kompensacinio atlyginimo suma būtų apskaičiuota, išskirta ir įrašyta atskira eilute, o išrašomų sąskaitų pastabose nurodoma, kad laikmenas ar įrangą įsigijęs asmuo įstatymo numatytais atvejais turi teisę susigrąžinti kompensacinį atlyginimą.

Reguliavimas plėtojamas įstatymo įgyvendinamajame teisės akte – Kompensacinio atlyginimo už audiovizualinių kūrinių ar fonogramose įrašytų kūrinių atgaminimą asmeniniais tikslais surinkimo, paskirstymo, mokėjimo ir grąžinimo tvarkos apraše, patvirtintame 2012 m. birželio 13 d. Lietuvos Respublikos Vyriausybės nutarimu Nr. 699. Nors pagal ATGTĮ 20 str. 6 d. nuostatas: „mokesčio mokėjimo sąlygas ir tvarką, atsižvelgdama į tai, ar taikomos, ar netaikomos techninės apsaugos priemonės, nustato Vyriausybė, suderinusi su kompensacinio atlyginimo mokėtojams atstovaujančiomis asociacijomis ir autorių teisių bei gretutinių teisių kolektyvinio administravimo asociacijomis“, iš esmės jos derinimas nevyko, o tai jau savaime kelia abejonių dėl Aprašo patvirtinimo teisėtumo.

Minėtajame Apraše nustatyta laikmenų ir įrangos mokesčio deklaravimo (pranešimų teikimo kolektyvinio administravimo asociacijai) ir mokėjimo tvarka, nuostatos dėl surinktų sumų paskirstymo ir sumokėto mokesčio grąžinimo tvarka, įsigijus laikmenas ir įrangą profesionalioms reikmėms.

Vienas esminių įstatymo įgyvendinamojo teisės akto reguliavimo aspektų yra profesionalių reikmių sąvokos, kai sumokėti laikmenų ir įrangos mokesčiai turi būti grąžinami, patikslinimas. Apraše patvirtintas pavyzdinis (turėtų būti nebaigtinis) profesionalių reikmių sąrašas. Vis dėlto šis sąrašas stebina savo ypatingu detalumu, jame išskirta trylika atskirų punktų. Į sąrašą, be kita ko, įtrauktos ir informacinių technologijų srities ūkio subjektų reikmės, susijusios su jų veikla kuriant kompiuterių programas ir duomenų bazes, kita informacinių technologijų srities veikla, kuriai vykdyti reikia tuščių laikmenų ir įrenginių, bei kitos profesionalios reikmės, susijusios su tuščių laikmenų ir (ar) įrenginių naudojimu akivaizdžiai kitiems tikslams

negu kūrinių atgaminimas asmeninėms fizinių asmenų reikmėms, nesiekiant tiesioginių ar netiesioginių komercinių tikslų. Tačiau sąraše nėra konkrečiai minimos su asmeniniu atgaminimu nieko bendro neturinčios verslo veiklos rūšys, tokios kaip apskaita ar rinkodara. Be to, minėtasis detalumus yra aiškiai perteklinis. Pavyzdinio profesinių reikmių sąrašo pateikimas, įtraukiant į jį tik kai kurias veiklos rūšis, gali būti paaiškinamas tik siekiu maksimaliai apriboti galimybes susigrąžinti mokesčius.

Pagal Aprašą sumokėtą mokestį (kompensacinį atlyginimą) gali susigrąžinti asmenys, kurie tuščias laikmenas ir (ar) įrenginius įsigijo profesionalioms ar neįgalių žmonių reikmėms arba išvežė iš Lietuvos Respublikos teritorijos. Deja, iš esmės grąžinimas yra labai sudėtingas ir biurokratiškas. Pagal Aprašo 25-28 punktus, grąžinimo klausimą iš esmės vienašališkai sprendžia kolektyvinio administravimo asociacija, be to, grąžinimas yra labai apribotas laiko (per metus ir iki kitų kalendorinių metų kovo 1 dienos).

ATGTĮ ir Apraše nustatyta profesionalių reikmių išimtis iš esmės yra nelogiška ir labai neaiški, nes didžioji dalis laikmenų ir įrangos yra išvis nesusijusios su kūrinių atgaminimu asmeniniams tikslams, todėl apskritai neturėtų būti apmokestinamos. Bet kurie verslo tikslai ar funkcijos (pvz., rinkodara) yra nesusiję su kūrinių atgaminimu asmeniniams tikslams, tačiau gali naudoti labai daug e. turinio duomenų (pvz., rinkodaros vaizdo klipai), todėl bet kuriam verslui turėtų būti galimybė susigrąžinti sumokėtus mokesčius arba jų išvis nemokėti.

Net ir fizinių asmenų įsigyjamos laikmenos bei įranga ne visada susijusios su asmeniniu kūrinių atgaminimu. Laikmenos ir įranga gali būti skirtos asmeninei kūrybai: šeimos fotografijoms ar filmavimui, o tai nesusiję su asmeninio atgaminimo tikslais. Deja, šiems atvejams jokių išimčių nenumatoma. Tokios nuostatos autorių teisių subjektams suteikia galimybę be pagrindo praturtėti – gauti mokestį, nors jų nuosavybe (autorių teisėmis) iš esmės nebuvo pasinaudota ir žalos jiems nebuvo padaryta.

Laikmenų ir įrangos mokesčiai turėtų būti renkami tik už teisėtas asmenines svetimų kūrinių kopijas, bet ne už asmeninį turinį ar neteisėtas kopijas.

ESTT *Padawan* byloje išaiškino „teisingos kompensacijos“ institutą pagal ES informacinės visuomenės direktyvą (Direktyvą 2001/29/EB). Šioje byloje ESTT padarė keturias išvadas:

1) teisinga kompensacija turi būti vienodai aiškinama ir taikoma visoje ES, vadinasi, laikmenų ir įrangos apmokestinimas – mokesčio bazė – turės būti suvienodinta visos ES lygiu;
2) mokesčio tarifai turi būti pagrįsti konkrečiu žalos apskaičiavimu;

3) mokestį turi mokėti mažmenininkai (subjektai, platinantys laikmenas ir įrangą vartotojams), o ne didmenininkai, kurie šiuo metu Lietuvoje jį jau moka;
4) laikmenų, skirtų neasmeniniams tikslams (pvz., verslo, valdžios, nevyriausybinio sektoriaus ir kitiems), apmokestinimas yra negalimas ir nesuderinamas su direktyva.

Kaip savo sprendime pabrėžė *ESTT Padawan*, bendrosios rinkos požiūriu esami skirtumai tarp įrangos ir laikmenų apmokestinimo ES valstybėse narėse yra nepriimtini ir iš esmės iškraipo bendrąją rinką. Suderinama turėtų būti tiek mokesčio bazės (už kokias laikmenas ir įrangą yra mokamas mokestis), tiek mokesčio tarifas (procentiniai tarifai ar absoliutūs dydžiai, ar jų kompleksas).

Lietuvos vartotojai beveik nesinaudoja asmeninio atgaminimo teise. Primintina ir tai, kad dalis kūrinių (pvz., garso ir vaizdo) platinami *DVD* ar *Blue-Ray* laikmenose, dėl visuotinai taikomų techninių apsaugos priemonių apskritai negali būti atgaminti asmeniniams tikslams. Tai kelia rimtų abejonių dėl ATGTĮ 20 str. 1–2 dalyse nustatytos asmeninio atgaminimo išimties reikalingumo, t. y. ar išimtis yra nustatyta dėl to, kad ji reikalinga vartotojams ir šie ja naudojasi savišvietos ir pan. tikslais, ar ji yra nominali ir nustatyta viso labo kaip pretekstas laikmenų ir įrangos mokesčiams taikyti Lietuvoje?

Pabrėžtina ir tai, kad Lietuva, nustatydama laikmenų ir įrangos mokesčius, tarptautiniu lygiu blogina savo vartotojų padėtį ir verslo konkurencingumą, nes tik nedaugelis valstybių pasaulyje turi nustačiusios analogiškus mokesčius. Didžiausios valstybės (JAV, Kinija, Japonija ir Australija), kuriose klesti teisėtos e. turinio platinimo platformos ir kitas e. turinio verslas, laikmenų ir įrangos mokesčių netaiko. Tuščios laikmenos mokesčių nenustato net septynios iš dvidešimt septynių ES valstybių: Airija, Didžioji Britanija, Kipras, Liuksemburgas ir Malta tokių mokesčių nenumato įstatymuose, Graikijoje ši sistema yra įšaldyta, o Ispanijoje nuo 2012 m. ji pakeista į alternatyvų valstybės administruojamą fondą. E. verslo subjektai, veikiantys šiose valstybėse, sėkmingai naudojasi neapmokestinamųjų statusu ir tiesiogiai parduoda laikmenas bei įrangą kitų valstybių (iš jų ir Lietuvos) vartotojams. Tokiu būdu Lietuva ne tik nesurenka tuščios laikmenos mokesčių, bet ir praranda PVM pajamas bei darbo vietas laikmenų ir įrangos gamybos bei platinimo verslo srityje.

Primintina, kad per pastaruosius dešimtmečius autorių teisės ir gretutinės teisės buvo tik plečiamos, pamirštant visuomenės ir vartotojų teises (geriausias to pavyzdys – autorių teisių galiojimo pratęsimas net dvidešimčiai metų). Kaip jau ne kartą pabrėžta, autorių teisės nėra savitikslės –

visuomenė suteikia joms teisinę apsaugą mainais į galimybę laisvai naudotis kūriniais, pasibaigus teisių galiojimo terminams, ir galimybę naudotis kūriniais nekomerciniams tikslams teisių galiojimo laikotarpiu, nes tik taip įmanoma nauja kūryba, mokslo ir kultūros plėtra.

Galiausiai būtina priminti, kad surinktos laikmenų ir įrangos mokesčio lėšos yra paskirstomos per neefektyvią ir neskaidrią kolektyvinio administravimo sistemą. Remiantis labai ribotais viešaisiais duomenimis, didžioji dalis surinktų lėšų (daugiau kaip 50 proc.) yra absorbuojama tarpininkų, bet ne autorių ir atlikėjų. Tai akivaizdžiai rodo, kad mokesčiai naudojami visiškai ne tiems tikslams, kokie deklaruoti ją nustatant, ir pagrindžia būtinybę nedelsiant peržiūrėti šią sistemą.

14 skirsnis. Prekių ženklų apsauga elektroninėje erdvėje

Prekių ženklai yra išskirtiniai žymenys, naudojami prekėms ir paslaugoms žymėti. Svarbiausios prekės ženklo funkcijos – atskirti vieno gamintojo ir (ar) tiekėjo prekes bei paslaugas nuo kito gamintojo prekių ir paslaugų. Be to, prekių ženklai nurodo prekių ir paslaugų kilmę (šaltinį), sukuria tam tikrą reputaciją, siejamą su prekių gamintoju ir (ar) paslaugų teikėju. Prekės ženklas gali būti bet koks žymuo: žodis, frazė, melodija, tam tikras dizainas, atvaizdas ar net erdvinė forma arba kvapas. Žymenų kombinacija irgi gali būti prekės ženklas.

Prekių ženklai nėra intelektinė nuosavybė siaurąja prasme, nes jie patys nebūtinai yra intelektinio darbo rezultatas ir nėra susiję su kūrybos ar inovacijų procesais. Vis dėlto teisės į prekių ženklus yra priskiriamos intelektinės nuosavybės teisėms dėl to, kad prekės ženklas yra nematerialus objektas, turintis daug panašumų į kitus pramoninės nuosavybės objektus (teritorialumą, registracijos reikalavimus, mokesčius ir t. t.). Kai kurie mokslininkai apskritai gana kritiškai vertina prekių ženklus žinių visuomenėje ir pabrėžia, kad šie prarado savo paskirtį (žymėti skirtingų gamintojų ir (ar) tiekėjų prekes bei paslaugas), vietoj to jie naudojami vartotojams klaidinti ir rinkai monopolizuoti.

Prekių ženklų naudojimas e. erdvėje paplitęs ne mažiau nei tradicinėje civilinėje apyvartoje. Išskirtiniai žymenys yra domenų vardų sistemos, informacijos paieškos internete ir reklamos internete socialinis bei techninis pagrindas. Be išskirtinių žymenų, šios sistemos būtų neįmanomos.

Pabrėžtina, kad žinių visuomenė ir suklestėjęs e. verslas apskritai pakeitė prekių ženklų pasaulį. 2013 m. į žinomiausių pasaulyje prekių ženklų *Top10* įėjo net aštuonių bendrovių prekių ženklai, tiesiogiai susiję su interneto ir e. erdvės technologijomis. Galima sakyti, kad e. erdvė suteikė

visiškai kitokių galimybių šiems prekių ženklams: *Apple, Samsung, Google, Microsoft, IBM, Amazon.com*. Prieš du dešimtmečius minėtieji prekių ženklai ir jais pasivadinusios bendrovės arba išvis neegzistavo, arba buvo niekam nežinomi.

Kita vertus, e. erdvė prekių ženklų savininkams sukėlė ir daugybę specifinių teisinių iššūkių. Svarbiausi iš jų yra prekių ženklų naudojimas domenų varduose, nematomuose tinklalapių ir interneto išteklių elementuose, interneto reklamos raktažodžiams (e. rinkodarai), taip pat neteisėtų ar falsifikuotų prekių ir paslaugų ženklinimas bei platinimas internete.

Prekių ženklų ir domenų vardų konfliktas istoriškai buvo pirmas iššūkis, su kuriuo internete susidūrė prekių ženklų savininkai. Pirmieji interneto vartotojai suprato svarbų domenų vardų vaidmenį internete, todėl pradėjo beatodairiškai registruoti domenų vardus, tarp jų ir tuos, kurie buvo tapatūs arba panašūs į ankstesnius prekių ženklus. Domenų vardų teisėms palengva įsitvirtinus kaip savarankiškoms, kilo ir daugybė kitų problemų, pvz., domenų vardų su asmenvardžiais (vardų ar pavardžių) konfrontacija su ankstesniais prekių ženklais ir pan. Plačiau konfliktai dėl domenų vardų ir prekių ženklų bei jų sprendimo būdai nagrinėjami skyriuje „Interneto teisė“.

Kita problema dėl prekių ženklų internete tapo jų (ypač konkurentų prekių ženklų) naudojimas nematomiems tinklalapių ir interneto išteklių elementams. Šie elementai, kitaip dar vadinami metaduomenimis, yra skirti automatiniams naršymo robotams (programinei įrangai), kuri indeksuoja ir klasifikuoja interneto tinklalapius bei išteklius tam, kad juos būtų galima rasti interneto paieškos sistemose, e. direktorijose ir pan. Be indeksavimo ir klasifikavimo interneto tinklalapis ar išteklius vartotojams būtų pasiekiamas tik tuo atveju, jeigu jie naršyklėje įrašytų tiesioginį interneto tinklalapio ar ištekliaus adresą. Dažniausiai tiesioginio adreso funkciją atlieka simbolinis adresas (domeno vardas). Toks metaduomenų naudojimas suteikia galimybę nesąžiningam interneto tinklalapio valdytojui savo tinklalapyje naudoti metaduomenis, kurie yra tapatūs plačiai žinomiems ir (arba) konkurentų prekių ženklams, tam, kad jų tinklalapis būtų surastas.

Kitas svarbus metaduomenų naudojimo būdas yra interneto tinklalapių ir išteklių reitingavimas paieškos rezultatuose, t. y. pateikimas kaip paieškos rezultato, labiau susijusio su paieškos užklausa. Nesąžiningi interneto tinklalapių ir išteklių valdytojai savo tinklalapiams ar ištekliams gali naudoti metaduomenis, kurie yra tapatūs plačiai žinomiems ir (arba) konkurentų prekių ženklams, siekdami ne tik to, kad jų tinklalapis būtų surastas, bet ir norėdami įgyti pranašumą prieš konkurentus dėl paieškos rezultatų.

Abiem šiais atvejais svetimų prekių ženklų naudojimas būtų akivaizdžiai neteisėtas ir užtrauktų atsakomybę už teisių į prekės ženklą pažeidimą. Paminėtina, kad šie pažeidimai kvalifikuotini pagal bendrąsias prekių ženklų teisės normas (Prekių ženklų įstatymą ir (ar) 2009 02 26 ES Reglamentą Nr. 207/2009 dėl Bendrijos prekių ženklų). Esamas teisinis prekių ženklų regamentavimas ir teisinės atsakomybės taisyklės jokių atskirų ar specialių normų dėl prekių ženklų naudojimo ar pažeidimo e. erdvėje nenumato.

Paprastų *HTML* puslapių metaduomenys iš esmės gali būti matomi ir žmogui, atgaminus ir išsamiai išnagrinėjus tinklalapio *HTML* kodą, tačiau moderniųjų tinklalapių ir interneto išteklių metaduomenys yra itin sudėtingi, naudojami ne tik *HTML* žymenys, tačiau ir milžiniški nematomi duomenų klodai, specialiai pritaikyti automatiniams naršymo robotams. Tinklalapių optimizavimas paieškos rezultatams (angl. *Search engine optimization, SEO*) tapo atskiru verslu, o modernius interneto puslapius galima palyginti su ledkalniu, kurio tik maža dalis yra matoma žmogui, naršančiam tinklalapį įprastomis interneto naršyklėmis.

Kadangi visų tinklalapių metaduomenų atitikties realiam puslapio turiniui neįmanoma patikrinti, naujosios kartos paieškos sistemos ribotai naudoja metaduomenis paieškos rezultatams reitinguoti, nes netinkamas tinklalapių reitingavimas yra paieškos sistemos kokybės problema. Tikėtina, kad vartotojas, nerandantis ieškomų išteklių dėl to, kad jam pateikiami paieškos rezultatai (tinklalapiai) savotiškai apgavo paieškos sistemą, nusivils paieškos sistemos kokybe ir norės naudoti kitą paieškos sistemą. Pabrėžtina ir tai, kad dėl eksponentinės interneto plėtros (internete esančių tinklalapių ir kitų išteklių bei duomenų kiekio didėjimo) paieškos sistemų reikšmė internete pastaraisiais metais labai smarkiai išsaugo. Paieškos sistemos yra pagrindinis ir daugeliu atvejų vienintelis būdas vartotojams pasiekti norimą turinį e. erdvėje. Dėl šios priežasies bent jau didžiausių interneto paieškos sistemų valdytojai *(Google, Microsoft)* patys aktyviai kovoja su nesąžiningu ir neteisėtu metaduomenų naudojimu ir SEO piktnaudžiavimu. Paieškos sistemos taiko specifines sankcijas – tokias kaip laikinas ar visiškas tinklalapio pašalinimas iš tos sistemos paieškos rezultatų. Iš esmės vyksta šaltasis technologijų karas tarp paieškos sistemų ir tinklalapių valdytojų bei SEO paslaugų teikėjų, siekiant aukštesnių paieškos rezultatų reitingo pozicijų.

Problemos dydį aiškiai parodo ir tai, kad net ypač gerai žinomos bendrovės nevengia naudotis metaduomenimis su konkurentų prekių ženklais, pvz., dar 2006 m. bendrovė BMW AG patyrė laikinų *Google* paieškos sankcijų dėl to, kad BMW tinklalapiai galbūt neteisėtai naudojo metaduomenis, susijusius su pagrindinio konkurento *Daimler AG (Mercedes-Benz)* prekių ženklais.

Suvokdamos prekių ženklų svarbą vartotojams susiejant konkretų ženklą su tam tikru e. turiniu, prekių ženklais netruko naudotis ir interneto paieškos bei e. rinkodaros sistemos. Prekių ženklai labai dažnai yra tie raktažodžiai, kuriais naudodamiesi vartotojai ieško susijusių tinklalapių, interneto išteklių ar net labai konkrečios informacijos bei e. turinio internete. Sėkmingiausia interneto paieškos sistema *Google* savo paieškos įrankius ir kitus produktus yra visiškai integravusi kartu su e. rinkodaros sprendimu. Galima teigti, kad *Google* e. rinkodara (vadinamoji *Adwords*) yra pagrįsta tais pačiais raktažodžiais kaip ir *Google* interneto paieška (tarp jų ir prekių ženklais). Reklama, pateikiama vartotojams *Google* ištekliuose, yra tų asmenų, kurie e. aukciono būdu daugiausia sumokėjo už savo reklamos pateikimą kartu su norimais raktažodžiais. Iš esmės *Google* parduoda raktažodžius asmenims, kurie nori įsigyti e. reklamą ir parodyti ją tada, kai vartotojas naudoja atitinkamus raktažodžius (pvz., pateikia užklausą interneto paieškai ar gauna e. žinutę su atitinkamu raktažodžiu ir pan.). Tokia integruota e. rinkodaros sistema ne tik suteikia galimybių, bet ir labai didina suinteresuotumą:

1) sistemos valdytojui „parduoti“ raktažodžius, tapačius ar panašius į prekės ženklus;
2) suinteresuotiems asmenims „pirkti“ raktažodžius, tapačius ar panašius į svetimus prekių ženklus, pvz., konkurentų prekių ženklus.

Akivaizdu, konkurentai yra suinteresuoti, kad vartotojui ieškant kito gamintojo ir (ar) prekių tiekėjo ir paslaugų teikėjo būtų parodyta jų reklama, pvz., tikėtina, kad sportinių batelių „Puma“ gamintojas bus suinteresuotas parodyti vartotojui savo reklamą, net jeigu šis ieško „Nike“ ar „Adidas“ sportinių batelių.

Aukščiau aptartas e. rinkodaros principas yra vadinamas raktažodžiais pagrįsta reklama (angl. *keyword advertising)* ir šiuo metu yra naudojamas beveik visoms e. rinkodaros sistemoms (ne tik paieškos sistemų e. rinkodarai). Moderniose e. rinkodaros sistemose kaip raktažodžiai gali būti naudojama ne tik žodinė ar simbolinė informacija, bet ir vaizdai ar vaizdo turinys arba kokia nors kita e. turinį sudaranti informacija.

Turint omenyje ypač spartų e. rinkodaros plėtros tempą ir svarbą, raktažodžiais pagrįsta reklama kelia vis didesnį prekių ženklų turėtojų nepasitenkinimą ir mėginimus uždrausti ar apriboti prekių ženklų kaip raktažodžių naudojimą e. rinkodarai (jų pardavimą ir pirkimą susijusiai e. rinkodarai). Šiuo metu *Google Adwords* yra didžiausia pasaulyje e. rinkodaros sistema, o *Google* – reklamos paslaugų teikėja. Jos pajamos vien tik iš e. reklamos paslaugų 2012 m. sudarė 42.5 mlrd. JAV dolerių.

Paminėtina, kad bet koks konkurento prekių ženklų naudojimas tradicinei rinkodarai prekių ženklų teisėje yra smarkiai ribojamas. Kita vertus, „raktažodžių" naudojimas tradicinei rinkodarai iš esmės yra neįmanomas – tai visiškai naujas tik e. erdvės technologijų įgalintas prekių ženklų ir kitos informacijos naudojimo būdas. Dėl to bendroji prekių ženklų teisė nepateikia aiškaus atsakymo, ar minėtasis prekių ženklų kaip raktažodžių e. rinkodarai „pardavimas" ir jų „pirkimas" yra teisėti. Be to, primintina ir tai, kad dėl globalaus e. erdvės pobūdžio e. rinkodara irgi yra globali, o prekių ženklų teisė, kaip ir kitos tradicinės pramoninės nuosavybės formos, iš esmės yra nacionalinės teisės, galiojančios tik tam tikroje teritorijoje.

Nesant aiškios doktrinos ir teisinių nuostatų, prekių ženklų naudojimo raktažodžiais pagrįstoje e. reklamoje teisėtumą iki šiol narplioja įvairaus lygio teismai. Paminėtinos dvi reikšmingos ESTT bylos, kurios padėjo pamatus šiam besiformuojančiam prekių ženklų teisės e. erdvėje institutui.

ESTT sujungtose bylose C-236, 237 ir 238/08 *(Google France, Google Inc. v. Louis Vuitton Malletier; Google France v. Viaticum Luteciel; Google France v. CNRRH Pierre-Alexis Thonet Bruno Raboin Tiger, a Franchisee of Unicis)* nagrinėjo prekių ženklų kaip raktažodžių „pardavimą", kurį vykdo e. rinkodaros paslaugų teikėjai, tokie kaip *Google*. Šiose bylose ESTT pripažino, kad prekių ženklų kaip raktažodžių „pardavimas" nepažeidžia prekių ženklų turėtojų teisių, nes *Google* šiuo atveju veikia tik kaip reklamos platforma (analogiškai žurnalui ar TV kanalui, o konkrečių prekių ženklų naudojimas ir jo teisėtumas priklauso nuo reklamos užsakovo (prekės ženklo raktažodžio „pirkėjo").

Vis dėlto teismas pabrėžė, kad asmenys, „nusipirkę" prekės ženklams tapačius raktažodžius ir juos naudoję savo e. turinio reklamai, tam tikrais atvejais gali būti laikomi neteisėtai panaudoję prekės ženklus ir atitinkamai pažeidę teises į minėtuosius prekės ženklus. Tokiais atvejais turėtų būti vertinamas pats e. reklamos, pateikiamos pagal atitinkamą raktažodį, ir reklamuojamojo elektroninio ištekliaus turinys ir pobūdis. Konkretus pažeidimo atvejis galėtų būti, jeigu vidutiniam interneto vartotojui paspaudus e. reklamą ir pamačius reklamuojamą interneto išteklių susidarytų įspūdis, kad reklamuojamos prekės ar paslaugos yra susijusios su pačiu prekės ženklo turėtoju, o ne trečiuoju asmeniu, kuris tik „nusipirko" reklamą, susietą su atitinkamu raktažodžiu. Vis dėlto aiškių pažeidimo kriterijų ESTT nenustatė, jis tik nurodė, kad kiekviena situacija nacionalinių teismų turėtų būti vertinama individualiai.

Naujesnėje 2011 m. pabaigoje išspręstoje byloje ESTT nagrinėjo būtent prekės ženklo raktažodžio „pirkėjo" veiksmų teisėtumą veikiant *Google* e. rinkodaros platformoje *Adwords*. Byloje C-323/09 *Interflora v.*

Marks & Spencer (M&S) Interflora kreipėsi į teismą, kad apgintų savo teises į prekės ženklą *Interflora*, kuris buvo nusipirktas *M&S* kaip raktažodis *Google Adwords* sistemoje reklamuojant tapačias *M&S* paslaugas (gėlių pristatymą). ESTT išaiškino, kad *M&S,* pasirinkdama raktažodį *Interflora,* iš esmės pasinaudojo prekės ženklu *Interflora*. Teismas išaiškino, kad toks pasinaudojimas gali būti laikomas prekės ženklo pažeidimu tik tuo atveju, jeigu jis turės kokį nors neigiamą efektą ar šio prekės ženklo turėtojui sukels negiamų padarinių, pvz., buvo nesąžiningai pasinaudota prekės ženklo išskirtinumu ar reputacija siekiant komercinės naudos (angl. *free-riding)* arba daroma neigiama įtaka prekės ženklo reputacijai (angl. *dilution)*.

ESTT pabrėžė, kad prekės ženklo turėtojo teisės ypač pažeidžiamos tais atvejais, kai su raktažodžiu susieta reklama apriboja protingo vartotojo galimybes atskirti, ar prekės ir paslaugos yra teikiamos prekės ženklo turėtojo ar trečiojo asmens. Todėl *M&S* pasinaudojimas prekės ženklu *Interflora* kaip raktažodžiu ir su šiuo raktažodžiu susieta konkreti reklama gali suklaidinti vartotojus dėl reklamuojamų paslaugų kilmės. Konkrečiu atveju atkreiptas dėmesys, kad *Interflora* bendradarbiauja su labai daug trečiųjų asmenų, todėl esama didesnės vartotojo suklaidinimo tikimybės manant, kad *M&S* yra *Interflora* tinklo dalis.

ESTT nurodė, kad kaip pažeidimai neabejotinai būtų vertinami ir tie atvejai, kai nesąžiningai naudojamasi prekės ženklo reputacija, t. y. jeigu reklama, susieta su prekės ženklui tapačiu raktažodžiu, naudojama (pvz., parduodant prastesnės kokybės prekes) ir ji neigiamai veikia prekės ženklo turėtojo galimybes dėl turimos ženklo reputacijos pritraukti vartotojų arba išsaugoti jų lojalumą. Vis dėlto ESTT padarė išlygą, kad prekės ženklo kaip raktažodžio naudojimas yra leistinas, jeigu siekiama pateikti aiškią alternatyvą prekės ženklo turėtojo prekėms ir paslaugoms. Alternatyva nelaikytina prekių ar paslaugų imitacija, pvz., labai panašios prekės ir paslaugos, tik teikiamos už mažesnę kainą.

Nesant vartotojų klaidinimo ar naudojimosi prekės ženklo reputacija, tik prekės ženklo kaip trigerio naudojimas e. reklamai *Google Adwords* ar panašioje sistemoje šio ženklo turėtojui nesukelia jokių neigiamų padarinių. Minėtoji išvada laikoma *Google* laimėjimu, nes ji iš esmės vindikuoja raktažodžių, atitinkančių prekės ženklus, „pardavimą“ ir „pirkimą“ *Google Adwords* sistemoje.

Reikėtų atkreipti dėmesį, kad ESTT sprendimas pabrėžė būtinybę detaliai išnagrinėti faktines aplinkybes ir atkreipti dėmesį į šiuos dalykus: prekės ženklų turimą reputaciją ir turėtojo investicijas į ją; faktinę reklamą, susietą su prekės ženklui tapačiu raktažodžiu, ir jos turinį; reklamuojamų prekių ir paslaugų esmę bei savybes. Tai yra esminės ESTT rekomendacijos

nacionaliniuose teismuose sprendžiant bylas, susijusias su teisių į prekės ženklus pažeidimu raktažodžių e. reklamos srityje. Pats ESTT faktinių aplinkybių nenagrinėjo ir negali nagrinėti, todėl jis nepateikė atsakymo į klausimą, ar *M&S* savo veiksmais pažeidė *Interflora* teises į prekės ženklą ar jų nepažeidė. Pirmosios instancijos teismas tik 2013 m. gegužę pripažino, kad *M&S* savo veiksmais pažeidė *Interflora* teises į prekės ženklą, tačiau galutinio Didžiosios Britanijos teismų verdikto ir atsakomybės, kuri bus pritaikyta *M&S*, dar teks palaukti.

Atskirai išskirtina ir neteisėtų ar falsifikuotų prekių ir (ar) paslaugų ženklinimo bei platinimo internete problema. Internetas labai palengvino globalų neteisėtų ar falsifikuotų prekių ir (ar) paslaugų pardavimą. E. prekybos platformos ir e. aukcionai, veikiantys kaip globalios prekybos tarpininkai, suteikia nemažai galimybių neteisėtoms ar falsifikuotoms prekėms ir (ar) paslaugoms plisti iš Kinijos į Vakarų rinkas, tačiau sudaro tik minimalias sąlygas kontroliuoti prekių legalumą ar autentiškumą. Tradicinėse rinkose prekių legalumą ir autentiškumą kontroliuoja valstybės institucijos bei prekių ženklų turėtojai. E. rinkoje tokia kontrolė yra neįmanoma, nes prekių pardavėjai dažnai yra skirtingose valstybėse nei pirkėjai, o pardavėjų valstybės institucijos pro pirštus žiūri į intelektinės nuosavybės teisių ir prekių ženklinimo pažeidimus.

Kai nesąžiningi pardavėjai yra nepasiekiami pirkėjų valstybės institucijoms ir prekių ženklų turėtojams, galimybė kontroliuoti prekės ar paslaugos legalumą lieka tik pačiam pirkėjui. Vadovaujantis tradicinėmis intelektinės nuosavybės teisės doktrinomis yra svarstytina, kad teisinė atsakomybė turėtų tekti ir asmeniui, kuris tarpininkauja sudarant neteisėtų ar falsifikuotų prekių pirkimo–pardavimo sandorį bei pelnosi iš tokio tarpininkavimo. Beveik visos e. verslo platformos gauna procentą nuo kiekvieno sandorio, sudaryto pasitelkus platformą. Didžiausios globalios e. verslo platformos *EBay* ar *Amazon* iš tokio tarpininkavimo uždirba milijardines sumas. Iš esmės tokios platformos veikia kaip globalus *P2P* tinklas tradicinėms prekėms ir paslaugoms. Pabrėžtina, kad e. verslo platformose gali būti platinamos ir e. prekės bei paslaugos, pvz., kompiuterių programos ar e. knygos. Ypač *EBay* platforma suteikia galimybių platinti specifinius elektroninius objektus, tokius kaip naudota programinė įranga. Dar 2010 m. *EBay* platforma visame pasaulyje turėjo daugiau nei 94 mln. vartotojų, kolektyviai perkančių ir parduodančių prekes, kurių vertė kiekvieną sekundę viršija du tūkstančius JAV dolerių.

Kaip jau minėta, interneto tarpininkų atsakomybė ir jos ribojimas yra vienas iš kontroversiškiausių ir svarbiausių teisinio e. erdvės reguliavimo klausimų. Nors e. verslo platformos ir pelnosi iš bet kokių objektų

pardavimo, jos neatsako už vartotojų veiksmus pateikiant ir parduodant neteisėtus bei intelektinės nuosavybės teises (tarp jų ir teises į prekės ženklus) pažeidžiančius objektus, jeigu apie juos nežino (aktyvios pareigos domėtis vartotojų veiksmų teisėtumo platforma neturi) ir jų nekontroliuoja. Taigi e. prekybos platformos nėra atsakingos už prekių ženklų teisių pažeidimus, kuriuos, naudodamiesi platforma, daro tretieji asmenys.

Garsus juvelyrinių dirbinių gamintojas *Tiffany & Co*, 2004–2005 m. ištyręs *EBay* platformoje vartotojų parduodamus *Tiffany & Co* gaminius, nustatė, kad daugiau nei 70 proc. šių gaminių yra padirbti. Savo teises į gaminių prekės ženklus ir firmos vardą *Tiffany & Co* mėgino apginti teisminiu būdu, ji teigė, kad *EBay* yra įsipareigojusi kontroliuoti savo platformos vartotojų veiksmus, pelnosi iš prekių ženklų pažeidimų ir dėl to atsako už platformos įgalintus neteisėtus vartotojų veiksmus, tačiau teismai iš esmės atmetė *Tiffany & Co* pretenzijas *EBay* tiek dėl tiesioginio, tiek dėl netiesioginio teisių į prekių ženklus pažeidimo, motyvuodami tuo, kad *EBay* platformai galioja e. erdvės tarpininkų atsakomybės išimtys. Tarpininkai e. erdvėje atsako tik griežtai įstatymų nustatytais atvejais ir jiems nenumatyta aktyvi pareiga kontroliuoti vartotojų, kurie naudojasi e. platforma, veiksmų teisėtumą. Plačiau apie e. erdvės tarpininkų atsakomybės apribojimus – skyriuje „Interneto teisės“.

Visų instancijų teismai, nagrinėję *Tiffany & Co v. EBay* bylą, atsisakė e. platformai *EBay* taikyti solidariosios (kartu su pačiais vartotojais) ir netiesioginės atsakomybės už intelektinės nuosavybės teisių pažeidimą doktrinas, nors ir pripažino, kad *EBay* gavo komercinės naudos (komisinį mokestį) iš falsifikuotų prekių pardavimo ir turėjo bendro pobūdžio informacijos, kad falsifikuoti *Tiffany & Co* produktai yra platinami *EBay* platformoje. Pabrėžtina, kad *EBay* preciziškai reagavo į visus individualius *Tiffany & Co* prašymus pašalinti iš platformos konkrečias prekes, kurios aiškiai pažeidė *Tiffany & Co* teises į prekės ženklus.

Be to, pabrėžė, kad e. erdvės tarpininkų atsakomybės apribojimai yra būtini ir esminiai netrikdomai teisėtai e. komercijai ir technologiniam progresui.

Panaši praktika taikoma ir ES. Gana panašiomis aplinkybėmis vienas didžiausių pasaulio kosmetikos koncernų *Loreal* nustatė, kad *EBay* platformoje platinama ir ES vartotojų gali būti įsigyjama falsifikuota kosmetika, paženklinta *Loreal* prekių ženklais ir išvis neskirta prekybai (mėginiai ir pavyzdžiai), taip pat kosmetika, skirta ne ES rinkoms (prekių ženklų teisėje teisių turėtojams suteikiama teisė riboti vadinamąjį paralelinį importą). Pagrindiniai bylos klausimai, tarp jų ir *EBay* kaip e. platformos, kuri pelnosi iš tokios galbūt neteisėtos prekybos, solidarios ir netiesioginės

atsakomybės klausimas, buvo nukreipti ESTT. Šis 2011 m. liepą išsprendė šią bylą Nr. C-324/09 ir konstatavo, kad tik patys pardavėjai, kurie prekiauja e. verslo platformoje, bet ne šios platformos operatorius naudojasi prekių ženklais ir daro jiems įtaką. E. platformos valdytojo atsakomybė turi būti vertinama pagal tuos pačius principus, kokie nustatyti visiems interneto tarpininkams ES elektroninės komercijos direktyvoje 2000/31/EB, t. y. tarpininkui atsakomybė gali kilti tik už aktyvų veikimą ir dalyvavimą pažeidžiant intelektinės nuosavybės teises. ESTT pabrėžė, jog e. tarpininkas neturėtų išvengti atsakomybės, jeigu jis žinojo faktus ir aplinkybes, kurių pagrindu atsakingas asmuo gali spręsti, kad vartotojų veiksmai yra neteisėti, ir tą žinodamas neatidėliodamas nesiėmė veiksmų pažeidimui apriboti. Ši ESTT pastaba aiškinama taip, kad tarpininkui turi būti prieinama pakankamai su pažeidimu susijusios informacijos, kurią turėdamas atidus asmuo į tai reaguotų.

Galiausiai *Loreal v. EBay* sprendime ESTT nurodė, kad Direktyvoje 2004/48/EB nustatyta galimybė įpareigoti tarpininką apriboti prieigą prie neteisėtų interneto išteklių gali būti naudojama užkertant kelią platinti neteisėtas prekes ateityje, pvz., iš e. verslo platformos pašalinti ne tik esamas neteisėtas prekės ženklus pažeidžiančias prekes, bet ir patį neteisėtų prekių pardavėją, taip užkertant jam kelią ateityje platinti nelegalias prekes. Teismas pabrėžė, kad, atsižvelgiant į efektyvumo, proporcingumo ir veiksmingumo principus, tokios priemonės iš esmės turi būti individualios. Jos neturėtų tapti legalaus verslo e. platformoje kliūtimis.

Apibendrinant prekių ženklų pažeidimų problematiką e. verslo platformose, reikia pabrėžti, kad e. erdvės tarpininkai (e. verslo platformų operatoriai) už vartotojų padarytus prekių ženklų pažeidimus yra atsakingi tik tuo atveju, jeigu tarpininko vaidmuo darant pažeidimą buvo aktyvus. Labai svarbu, kad tarpininkai nėra bendrai įpareigoti kontroliuoti vartotojų veiksmus e. platformose (tai yra techniškai neįmanoma ir bet kurią e. platformą padarytų nepelningą). Apie intelektinės nuosavybės teisių pažeidimą gavę pakankamai individualios informacijos, kuri vidutiniam atidžiam ir atsakingam asmeniui leidžia spręsti apie pažeidimo buvimą, tarpininkai privalo imtis priemonių užkirsti tam kelią.

Aukščiau akcentuoti principai yra bendri bet kokiems e. erdvės tarpininkams, iš jų ir fizinių prekių e. prekybos, *P2P* e. turinio platformoms, e. informacijos portalams ir pan.

Žinių įtvirtinimo klausimai

1. Kokių transformacijų patyrė intelektinės nuosavybės institutas e. erdvėje?
2. Kodėl žinių visuomenėje aktualiausias epistemininis intelektinės nuosavybės suvokimas?
3. Kokie yra intelektinės nuosavybės kaip informacijos socialiniai ir ekonominiai požymiai?
4. Kodėl intelektinė nuosavybė yra pranašiausias universalus kūrybos ir inovacijų skatinimo instrumentas?
5. Kokiais atvejais intelektinės nuosavybės nepakanka kūrybai ir inovacijoms skatinti?
6. Kokie didžiausi kūrybinės intelektinės nuosavybės (autorių teisių ir gretutinių teisių) bei pramoninės intelektinės nuosavybės panašumai?
7. Kokius žinote specifinius intelektinės nuosavybės objektus e. erdvėje?
8. Kokios specialios intelektinės nuosavybės teisės nustatytos e. erdvėje?
9. Kokios specialios intelektinės nuosavybės teisių išimtys nustatytos e. erdvėje?
10. Kaip techninės apsaugos priemonės naudojamos intelektinės nuosavybės apsaugai?
11. Kodėl kolektyvinis intelektinės nuosavybės teisių administravimas yra neefektyvus e. erdvėje?
12. Kokių naujos kūrybos ir inovacijų iniciatyvų yra atsiradę e. erdvėje? Kuo jos skiriasi nuo tradicinės intelektinės nuosavybės apsaugos?
13. Kokie yra svarbiausi intelektinės nuosavybės pažeidimų e. erdvėje ypatumai?
14. Kuo ypatingi intelektinės nuosavybės pažeidimai *P2P* tinkluose?
15. Kokie yra pagrindiniai kompiuterių programų elementai, kuriems taikoma teisinė apsauga?
16. Kodėl kompiuterių programos vadinamos „mechanizmais, kurių išraiškos forma yra tekstas“?
17. Kokie kompiuterių programų elementai gali būti patentuojami?
18. Kokių yra papildomų teisės į kompiuterių programas apsaugos būdų?
19. Kokiomis sąlygomis gali būti parduodamos naudotos kompiuterių programos?
20. Kaip suderinamos autorių ir *sui generis* teisės į duomenų bazes?

21. Kodėl *sui generis* teisės į duomenų bazes yra ribojamos teismų praktikoje?
22. Kaip sprendžiami intelektinės nuosavybės techninių apsaugos priemonių ir intelektinės nuosavybės teisių apribojimų konfliktai?
23. Kodėl laikmenų ir įrangos mokesčiai yra nepriimtini žinių visuomenei?
24. Kokios didžiausios prekių ženklų apsaugos e. erdvėje problemos?
25. Koks yra e. erdvės tarpininkų (e. verslo platformų operatorių) vaidmuo ir atsakomybė už intelektinės nuosavybės pažeidimus?

/VII/ *skyrius*

Teisinė privatumo ir asmens duomenų apsauga elektroninėje erdvėje

/ 327–378 / *puslapiai*

1 skirsnis. Privatumo ir asmens duomenų teisinės apsaugos elektroninėje erdvėje ypatumai

Pastaraisiais metais plintant informacinėms ir komunikacinėms technologijoms, elektroninėms paslaugoms bei virtualiems socialiniams tinklams ypač aktualus tapo privatumo ir asmens duomenų apsaugos e. erdvėje aspektas. Palaikant elektroninius ryšius, internete apdorojama vis daugiau duomenų, susijusių su konkrečiu asmeniu. Apie asmenį galima surinkti informaciją, kuri gali apibūdinti jo įpročius, pomėgius ir kt. Neteisėtai renkant ir netinkamai naudojant šiuos duomenis gali kilti didelė grėsmė tokių asmenų privatumui.

1890 m. JAV teisininkai S. Warrenas ir L. 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 plėtojosi kita linkme ir šiuo metu privatumas dažnai tapatinamas su asmens duomenų apsauga. Tačiau reikėtų paminėti, kad asmens duomenų apsauga sudaro tik vieną iš keturių privatumo elementų. Nepaisant to, 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 tiek tarptautinės teisės aktuose, tiek Lietuvos Respublikos Konstitucijoje. Ši teisė pagal jos įteisinimo laiką priskirtina prie vadinamųjų trečiosios kartos teisių, nes daugelyje šalių buvo įtvirtinta gerokai vėliau nei socialinės, ekonominės ar politinės teisės.

Paminėtini svarbiausi tarptautiniai dokumentai, kuriuose įtvirtinta teisė į privataus gyvenimo neliečiamumą. Visuotinės žmogaus teisių deklaracijos 12 str. 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[41] 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 str., kur nurodyta, kad „žmogaus privatus gyvenimas neliečiamas. Asmens susirašinėjimas, pokalbiai telefonu, tele-

[41] Lietuvoje įsigaliojo nuo 1995 metų.

grafo pranešimai ir kitoks susižinojimas neliečiami“. Lietuvos Respublikos Konstitucijos 22 str. 3 d. nuostata, kad „informacija apie privatų gyvenimą gali būti renkama tik motyvuotu teismo sprendimu ir tik pagal įstatymą“ bei 4 d. nuostata, jog „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, jog „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, skirtingai nei daugelyje kitų valstybių, įvirtinta teisė ne į privatumą, o teisė į privatų gyvenimą. Abi minėtosios teisės nėra tapačios. Tačiau preziumuotina, kad ši problema neturi didelės praktinės įtakos teisės į privatų gyvenimą e. erdvėje apsaugai, todėl nebus detaliau analizuojama.

Privatumo apsauga gali apimti daug aspektų, pvz., 2011 m. gegužės 31 d. LAT nutartimi civilinėje byloje Nr. 3K-3-262/2011 teismas apgynė ieškovės pažeistą teisę į atvaizdą ir privatumą. Ieškovė prašė pripažinti, kad atsakovas – mokykla, paviešindama jos nuotrauką mokyklos interneto tinklalapyje be ieškovės ir jos tėvų sutikimo, pažeidė teisę į atvaizdą ir privatumą, priteisti neturtinės žalos atlyginimą ir uždrausti atsakovui dėti jos atvaizdą į internetą ateityje. Pirmosios instancijos teismas ieškinį tenkino iš dalies, o apeliacinės instancijos teismas ieškinį atmetė. Ieškovė pateikė kasacinį skundą. LAT pabrėžė, kad būtina sąlyga naudotis konkretaus fizinio asmens atvaizdu – to asmens sutikimas tiek jį fotografuojant, tiek jo nuotrauką, portretą ar kitokį atvaizdą atgaminant, parduodant, demonstruojant, spausdinant, paviešinant interneto puslapyje. Nagrinėjamuoju atveju nuotrauka, kurioje nufotografuota ieškovė kartu su kitais klasės moksleiviais, buvo įdėta mokyklos interneto puslapyje nesant nepilnametės ieškovės ar jos juridinių atstovų sutikimo.

Tarptautinių teisės aktų analizė (žr. Visuotinės žmogaus teisių deklaracijos 12 str., Tarptautinio pilietinių ir politinių teisių pakto 17 str., Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos 8 str. 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 tvarkymu ir vadinamas asmens duomenų apsauga; t. y. kai asmuo pats savo iniciatyva gali disponuoti savo asmens duomenimis, žinoti apie savo duomenų tvarkymą, su jais susipažinti ar reikalauti juos ištaisyti ir pan.;
- *fizinis privatumas* (kūno neliečiamumas), t. y. nesant žmogaus sutikimo, su juo negali būti atliekami jokie medicininiai ar moksliniai bandymai (pvz., privaloma tvarka 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.

1. Pagrindinės asmens duomenų teisinės apsaugos elektroninėje erdvėje kategorijos ir principai

Asmens duomenų apsaugą galima tapatinti su vienu iš keturių privatumo elementų – informaciniu privatumu. Asmens duomenų apsauga ES laikoma fundamentalia teise. A. Saarenpaa *(Saarenpaa*, 2001) asmens duomenų apsaugą laiko atskira privatumo dalimi – informacinį privatumą, kuris reiškia fizinių asmenų privatumo ir jų sąmoningo apsisprendimo teisių apsaugą kontroliuojant, ribojant ir reguliuojant asmens duomenų tvarkymą pasitelkus asmens duomenų teisinės apsaugos norminius aktus.

Nors asmens duomenys gali būti tvarkomi tiek automatiniu, tiek neautomatiniu būdu (pvz., tvarkant asmens duomenų susistemintas rinkmenas: sąrašus, kartotekas ir pan.), pastarojo asmens duomenų tvarkymo atvejų sumažėjo iki minimumo ir dėl informacinių technologijų paplitimo, didžiąja dalimi asmens duomenys tvarkomi automatiniu būdu[42], kuris šiame skyriuje bus tapatinamas su asmens duomenų tvarkymu e. erdvėje (arba tiesiog asmens duomenų tvarkymu).

Kalbant apie asmens duomenų apsaugą, kyla vienas svarbiausių klausimų: kas yra asmens duomenys? Pavyzdžiui, keliaujant su mobiliuoju telefonu, telekomunikacijų operatoriai dažniausiai fiksuoja mobiliojo telefono buvimo vietą ir kartu tam tikro asmens 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 naudojantis tokiais duomenimis kaip asmens kodas, vienas arba keli asmeniui būdingi fizinio, fiziologinio, psichologinio, ekonominio, kultūrinio ar socialinio pobūdžio požymiai.

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

Akcentuotini du kriterijai – tiesioginis ir netiesioginis asmens tapatybės nustatymas, tai leidžia apimti daug duomenų, kurie iš pirmo žvilgsnio turi menką ryšį su konkrečiu asmeniu. Duomenys gali būti asmeniniai netgi tada, jeigu juos pasitelkus asmuo gali būti identifikuotas tik turint kitų duomenų kombinaciją – pagalbinius duomenis. Kita vertus, svarbu, kad asmens tapatybės nustatymas turi būti įmanomas be neprotingų laiko, darbo ir pan. sąnaudų.

Asmens duomenys, kurie tiesiogiai ir vienareikšmiškai nurodo konkretų asmenį, yra asmens kodas, paso ir 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 paėmus atskirus duomenų elementus asmens nebūtų įmanoma identifikuoti.

Skiriama ypatingų asmens duomenų kategorija. Jiems priskiriami 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. Ypatingų asmens duomenų sąrašas yra baigtinis. Šių duomenų apsaugai taikomi griežtesnis reikalavimai, nei saugant „įprastus“ asmens duomenis.

Yra 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 svarbiausius asmens duomenų subjekto interesus;
- įgyvendinami oficialūs įgaliojimai, suteikti valstybės ir savivaldybių institucijoms arba trečiajam asmeniui, kuriam teikiami asmens 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 nei asmens duomenų rinkimo metu ir paskesnis jų naudojimas turi būti apribojamas šiems tikslams pasiekti);
- *asmens duomenų naudojimo apribojimo* (asmens duomenys neturi būti atskleisti, padaryti prieinami ar kitaip panaudoti kitiems tikslams, negu tie, kurie nurodyti remiantis tikslo nustatymo principu, išskyrus atvejus, kai gaunamas asmens duomenų subjekto sutikimas, arba pagal įstatymą);
- *saugumo užtikrinimo* (asmens duomenys privalo būti saugomi protingomis saugumo priemonėmis prieš tokias rizikas ar pavojus kaip netekimas, praradimas, neteisėtas priėjimas 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).

Skiriami šie asmens duomenų tvarkymo proceso dalyviai: duomenų valdytojas, tvarkytojas ir 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 įgaliotas 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.

Vykstant asmens duomenų tvarkymo procesui, asmens duomenų subjektas turi tam tikras teises, iš kurių galima išskirti šias 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. Jeigu duomenų subjekto prašymas išreikštas rašytine forma, duomenų valdytojas turi pateikti jam atsakymą raštu.

Asmens duomenų tvarkymą, išskyrus asmens duomenų tvarkymą palaikant elektroninius ryšius, 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 į:

1) reguliavimas bendraisiais įstatymais;
2) sektorinis reguliavimas, kai tam tikroms sritims taikomi specialūs teisės aktai (pvz., elektroniniai ryšiai);
3) savireguliacija;
4) apsauga techninėmis priemonėmis.

2. Bendrieji asmens duomenų apsaugos elektroninėje erdvėje reguliavimo aspektai

Asmens duomenų apsaugą reglamentuojantys tarptautiniai aktai gali būti skirstomi į privalomuosius ir rekomendacinio pobūdžio. 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. Nustatant pagrindinius asmens duomenų apsaugos principus, šios gairės tampa atrama vyriausybėms ir verslui, siekiant geriau apsaugoti asmens duomenis bei nustatyti atitinkamą reguliavimą. Paminėtinos ir 1990 m. Jungtinių tautų kompiuterizuotų asmens duomenų bylų gairės, kurios atspindi *EBPO* gairėse įtvirtintus asmens duomenų apsaugos principus. Valstybėms narėms, įgyvendinančioms nacionalinius teisės aktus dėl kompiuterizuotų asmens duomenų bylų, patariama atsižvelgti į šiose gairėse numatytus principus.

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

Šia Konvencija siekiama užtikrinti, kad automatizuotai tvarkant asmens duomenis visų šalių teritorijose bus gerbiamos kiekvieno asmens (neatsižvelgiant į jo tautybę ir gyvenamąją vietą) 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 įtraukiamas principas, reikalaujantis atitinkamų apsaugos priemonių jautriems duomenims, t. y. tokiems duomenims, kurie atskleidžia rasinę kilmę, politinius įsitikinimus, religines nuostatas ar yra susiję su sveikata ir pan. Vis dėlto ši Konvencija neturi didelės reikšmės. Pastaraisiais metais technologijų ir komunikacijų pasaulyje atsirado esminių naujienų ir pasikeitimų, o tai reikalauja naujo teisės aktų leidėjų požiūrio.

Vienintelis bendro pobūdžio įpareigojantis teisės aktas ES – Europos Parlamento ir Tarybos direktyva dėl asmenų apsaugos tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo 95/46/EB. Ši direktyva taikoma tvarkant asmens duomenis automatiniais būdais, ištisai arba dalimis ir neautomatiniais būdais tvarkant asmens duomenis, kai tie duomenys sudaro arba yra skirti sudaryti rinkmenų sistemos dalį. Direktyvos tikslas yra dvejopas. Viena vertus, 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.

Galima išskirti šiuos direktyvoje įtvirtintus reglamentavimo principus:

1) *Duomenų kokybė* (direktyvos 6 str.). Asmens duomenys turi būti:
   - tvarkomi teisingai ir teisėtai;
   - surinkti įvardytais, aiškiai apibrėžtais ir teisėtais tikslais, paskui tvarkomi su šiais tikslais suderintais būdais;
   - adekvatūs, susiję ir savo apimtimi neviršijantys tikslų, kuriems jie renkami ir (arba) vėliau tvarkomi;
   - tikslūs ir, jeigu būtina, nuolat atnaujinami; turi būti imtasi visų reikalingų priemonių, kad duomenys, kurie yra netikslūs ar neišsamūs, palyginti su tikslais, dėl kurių jie buvo surinkti ar po to tvarkomi, būtų ištrinti arba ištaisyti;
   - laikomi tokio pavidalo, kad duomenų subjektų tapatybes būtų galima nustatyti ne ilgiau, nei tai yra reikalinga tiems tikslams, dėl kurių duomenys buvo surinkti arba paskui 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 nei 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 ir ištaisymą;
   - teisę prieštarauti dėl asmens duomenų tvarkymo;
   - teisę į kompensaciją, kai neteisėtai tvarkomi asmens duomenys.

Reikia paminėti, kad teisė į informacijos ištrynimą 2014 m. Europos Sąjungos Teisingumo Teismo buvo įvertinta naujame kontekste. 2014 m. gegužės 13 d. ES Teisingumo Teismas paskelbė sprendimą byloje Byloje C131/12 *Google prieš Ispanijos duomenų apsaugos agentūrą ir M. C. Gonzalez*, kurioje teismas pasisakė dėl „teisės būti pamirštam“ ir įtvirtino tam tikras sąlygas. Šis sprendimas galioja tik ES veikiantiems interneto paieškos varikliams ir įpareigoja juos esant atitinkamam prašymui pašalinti nuorodas į tinklalapius. Pagal ES Teisingumo Teismo sprendimą, paieškos variklio veikimo operacijos, kurias sudaro internete trečiųjų asmenų paskelbtos ar jau esančios informacijos suradimas, automatiškai atliekamas jos indeksavimas, laikinas laikymas ir galiausiai padarymas prieinamos interneto naudotojams tam tikra pasirinkta tvarka, laikytinos „asmens duomenų tvarkymu“, kaip jis suprantamas pagal Direktyvos 95/46 2 straipsnio b punktą, jei ši

informacija apima asmens duomenis, ir, kita vertus, paieškos variklio eksploatuotojas laikytinas tokių duomenų „valdytoju“, kaip jis suprantamas pagal minėtojo 2 str. d punktą. Taigi paieškos varikliai pripažinti asmens duomenų valdytojais, į kuriuos galima kreiptis įgyvendinant duomenų subjekto teises. Vis dėlto teisė būti pamirštam nėra absoliuti ir kiekvienu konkrečiu atveju turi būti įvertinta, surandant balansą su fundamentaliomis žmogaus teisėmis.

Bendrosios duomenų apsaugos direktyvos 29 str. darbo grupė 2014 m. lapkričio 26 d. priėmė darbinį dokumentą Nr. WP225, kuriame pateikė gaires kaip įgyvendinti minėtą ES Teisingumo Teismo sprendimą. Tuo metu bendrovė *Google* įsteigė patariamojo pobūdžio tarybą, kuri dirba susijusiais klausimais, įskaitant ir „kaip suderinti vieno žmogus teisę būti pamirštam su visuomenės teise žinoti informaciją“[43]. Pašalinimo iš paieškos rezultatų užklausą bendrovei *Google* galima pateikti per specialią nuorodą[44]. Teismo sprendimas galioja ir kitoms paieškos sistemos.

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 perduodami į trečiąją šalį tik tuo atveju, jeigu nepažeidžiant nacionalinių nuostatų, priimtų pagal kitas šios direktyvos nuostatas, ši trečioji šalis užtikrina adekvatų apsaugos lygį.“

Didelį atgarsį ir daug diskusijų sukėlė Europos Sąjungos Teisingumo Teismo 2015 m. spalio 6 d. sprendimas byloje Nr. C-362/14 *Maximillian Schrems prieš Airijos duomenų apsaugos pareigūną*, kuriuo Europos Komisijos sprendimas 2000/520/EB dėl pakankamo JAV „Saugaus uosto“ principų apsaugos lygio buvo pripažntas negaliojančiu. Tačiau šiuo sprendimu neuždraudžiama nacionalinėms duomenų apsaugos institucijoms nepriklausomai nuspręsti, ar tam tikra trečiojo pasaulio šalis atitinka Direktyvos nustatytus duomenų perdavimo reikalavimus. Remiantis sprendimu, Airijos duomenų apsaugos institucija turės įvertinti, ar Austrijos studento M. Schremso skundas yra pagrįstas, ir nuspręsti, ar duomenų perdavimas į JAV turėtų būti sustabdytas remiantis tuo pagrindu, kad JAV nėra užtikrinamas pakankamas asmens duomenų apsaugos lygis.

[43] <https://www.google.com/advisorycouncil>.

[44] <https://support.google.com/legal/contact/lr_eudpa?product=websearch>.

Reaguodama į šį sprendimą, Europos Komisija 2015 m. lapkričio 6 d. išleido komunikatą COM(2015)566 galutinis dėl asmens duomenų perdavimo iš ES į JAV pagal 95/46/EB direktyvą ir Teisingumo Teismo sprendimą byloje C-362/14 (Shrems). Šiame komunikate nurodoma, kad duomenų perdavimui iš ES į trečiąsias valstybes, tokias kaip JAV, įmonės gali naudoti alternatyvius įrankius ir dėl to perdavimas gali tapti teisėtu. Tačiau kaip pagrindinis prioritetas vis dėlto išlieka poreikis susitarti su JAV dėl asmens duomenų perdavimo modelio ir sąlygų. Toks modelis turėtų užtikrinti didesnę Europos piliečių duomenų apsaugą, juos perduodant į JAV. Tuo laikotarpiu, kol bus ieškoma tinkamo sprendimo, ES valstybės narės, vadovaudamosi įmonei privalomomis taisyklėmis ir standartinėmis sutarties sąlygomis, gali išduoti leidimus teikti asmens duomenis JAV.

Paminėtina, kad didelę reikšmę aiškinant direktyvos nuostatas ir keliant kompetenciją asmens duomenų apsaugos srityje turi Direktyvos 29 str. darbo grupė[45]. Ši grupė, kurią sudaro visų nacionalinių duomenų apsaugos institucijų atstovai, EU institucijų atstovai ir Europos Komisijos atstovas, leidžia nuomones, rekomendacijas (kurios gali būti laikomos vadinamąja minkštąja teise (angl. *soft law*), be to, atlieka daugybę kitų svarbių funkcijų.

Bendrąją duomenų apsaugos direktyvą Lietuvoje įgyvendina Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas. Pirmoji šio įstatymo redakcija buvo priimta dar 1996 metais. Naujas įstatymo redakcijas Lietuvos Respublikos Seimas priėmė 2003 ir 2009 metais. Be naujų įstatymo redakcijų, dar buvo ir daugelis kitų įstatymo normų pakeitimų.

Bendrasis Įstatymo tikslas – ginti žmogaus privataus gyvenimo neliečiamumo teisę, kai tai susiję su asmens duomenų tvarkymu. Įstatymas reglamentuoja santykius, kurie atsiranda automatiškai tvarkant asmens duomenis, taip pat neautomatiniu būdu tvarkant asmens duomenų susistemintas rinkmenas: sąrašus, kartotekas, bylas, sąvadus ir kita.

Įgyvendindamas Bendrąją duomenų apsaugos direktyvą, įstatymas tam tikslui nustato panašius asmens duomenų teisėto tvarkymo kriterijus ir asmens duomenų tvarkymo principus.

2003 m. 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 papildomas naujomis sąvokomis – duomenų tvarkymas automatiniu būdu ir vieša duomenų rinkmena. Nėra privalomas raštiškas

[45] <http://ec.europa.eu/justice/data-protection/article-29/index_en.htm>.

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 įrodymų, kad duomenų subjektas davė aiškiai išreikštą sutikimą tvarkyti jo asmens duomenis. Įstatyme nustatyta, kad tvarkomi duomenys turi būti tapatūs, tinkami ir tik tokios apimties, kuri būtina jų rinkimo ir tolesnio tvarkymo tikslams. Jeigu duomenys yra nepilni (neišsamūs) arba netikslūs, palyginti su tikslais, dėl kurių buvo surinkti ar paskui tvarkomi, jie turi būti ištaisyti, papildyti, sunaikinti, sustabdytas jų tvarkymas. Įstatyme įtvirtinamas bendrasis principas, kad draudžiama tvarkyti ypatingus asmens duomenis, išskyrus įstatyme nustatytą baigtinį sąrašą atvejų, kai ypatingi asmens duomenys gali būti tvarkomi. Įstatyme įtvirtinama nuostata, susiaurinanti asmens kodo naudojimo sritį. Asmens kodą, neturint duomenų subjekto sutikimo, galima naudoti tik tada, jeigu 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 išplėstos duomenų subjekto teisės. Duomenų subjektui suteikta teisė reikalauti sustabdyti savo asmens duomenų tvarkymo veiksmus. Be to, įstatyme nustatyta papildoma duomenų valdytojo pareiga renkant asmens duomenis tiek tiesiogiai iš paties duomenų subjekto, tiek iš kitų šaltinių, informuoti duomenų subjektą apie jo teisę susipažinti su savo asmens duomenimis, reikalauti ištaisyti neteisingus, neišsamius, netikslius savo asmens duomenis, taip pat suteikti kitos papildomos informacijos (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 tokios informacijos jau turi. Įstatyme įtvirtinama 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 įtvirtinamos normos, reglamentuojančios išankstinę patikrą. Pateikiamas 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 ir teisės.

2009 m. naujos įstatymo redakcijos naujovės – įtvirtintos nuostatos, patikslinančios asmens kodo naudojimo reguliavimą, taip pat sureguliuotas asmens duomenų tvarkymas naudojant vaizdo stebėjimo priemones, patikslintas asmens mokumo vertinimo ir asmens duomenų tvarkymo tiesioginės rinkodaros tikslais reguliavimas, nustatyta skundų nagrinėjimo tvarka, sureguliuotas už duomenų apsaugą atsakingo asmens ar padalinio teisinis statusas, taip pat įtvirtintos nuostatos dėl Valstybinės duomenų apsaugos inspekcijos – Įstatymo priežiūrą vykdančios institucijos – nepriklausomumo.

Įstatymo 7 str. nustato asmens kodo naudojimo reikalavimus. Pagal minėtojo straipsnio 2 d., naudoti asmens kodą tvarkant asmens duomenis galima tik gavus duomenų subjekto sutikimą, o 3 d. nustatyti atvejai, kai asmens kodą galima naudoti be duomenų subjekto sutikimo:

- 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.

Dėl asmens kodo kaip privalomo elemento sutartyse su paslaugų teikėju, Lietuvos vyriausiasis administracinis teismas 2013 m. gegužės 23 d. administracinėje byloje Nr. A^{822}-1173/2013 yra patvirtinęs argumentus, kad remiantis sutartyse su pareiškėju pateikiama asmens duomenų visuma asmenį galima vienareikšmiškai identifikuoti ir tam nėra būtina naudoti asmens kodo. Remdamiesi šiuo teismo sprendimu, paslaugų teikėjai negali reikalauti sutartyse privalomai nurodyti asmens kodą.

Svarbu paminėti, kad asmens kodą pagal įstatymą draudžiama naudoti tiesioginės rinkodaros tikslams ar skelbti viešai. Dėl asmens kodo naudojimo tiesioginei rinkodarai, Vyriausiasis administracinis teismas vienoje byloje yra pasisakęs: Lietuvos vyriausiasis administracinis teismas konstatavo, kad asmens identifikavimas, kiek tai yra būtina duomenų valdytojui vykdant lojalumo programą, yra galimas ir pagal kitus duomenis. Lojalumo taškų skaičiavimas, nuolaidų teikimas, kortelių teikimas ir kiti veiksmai gali būti atliekami ir nežinant bei netvarkant lojalumo programoje dalyvaujančio kliento asmens kodo.

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

Įstatymas nustato specialius reikalavimus, jei asmens duomenys tvarkomi specialiems nustatytiems tikslams:

- socialinio draudimo ir socialinės globos tikslams (įstatymo 9 str.);
- sveikatos apsaugos tikslams (įstatymo 10 str.);
- rinkimų, referendumo, piliečių įstatymų leidybos iniciatyvos tikslams (įstatymo 11 str.);
- mokslinio tyrimo tikslams (įstatymo 12 str.);
- statistikos tikslams (įstatymo 13 str.);
- rinkodaros tikslams (įstatymo 14 str.);
- mokumui įvertinti ir įsiskolinimui valdyti (įstatymo 21 str.).

Labai aktuali asmens duomenų apsaugos sritis, susijusi su tiesiogine rinkodara. Neteisėta rinkodara, vykdoma elektroninių ryšių tinklais, dažnai vadinama nepageidaujama komercine informacija, elektroninėmis šiukšlėmis arba brukalu[46]. Pasitelkus brukalą komercinė reklama gali pasiekti milijonus žmonių minimaliomis sąnaudomis. Šis gali būti užsakomas už atlygį, daugiausia smulkiųjų verslo subjektų, kurie siekia kuo pigesnės ir tuo pačiu platesnės reklamos. Reikėtų paminėti, kad Lietuvoje yra ne vienas precedentas, kai nepageidaujamos komercinės informacijos arba brukalo siuntėjai buvo patraukti atsakomybėn. 2004 m. lapkričio 22 d. Valstybinėje duomenų apsaugos inspekcijoje gautas R. L. skundas dėl nepageidaujamo elektroninio pašto pranešimo. Tyrimo metu nustatyta, kad serveris, iš kurio siųstas nepageidaujamas elektroninio pašto pranešimas, priklauso UAB „Biuro sprendimų tinklas“. Minėtoji įmonė, atsakydama į Inspekcijos paklausimą, pranešė, kad už nustatyto serverio palaikymą jai moka ir už jį atsako UAB ,,Interprekyba“. Inspekcijos darbuotojai minėtojoje bendrovėje atliko asmens duomenų tvarkymo teisėtumo patikrinimą ir nustatė, kad iš UAB „Interprekyba“ pareiškėjui siųstas elektroninio pašto pranešimas tiesioginės rinkodaros tikslu be išankstinio abonento sutikimo pažeidžia ERĮ 68 str. 1 dalį.

Tiesioginė rinkodara e. erdvėje pastaruoju metu tampa vis aktualesnė, nes reklamos teikimo būdai iš tradicinių transformuojasi į elektroninius (pvz., elektroninio pašto, SMS ar kt., pasitelkus komunikacijos priemones, virtualiuose socialiniuose tinkluose ir pan.). Apibendrintai galima teigti, kad Lietuvoje tiesioginės rinkodaros atveju yra nustatytas OPT-IN principas,

[46] Angl. *spam* – nepageidaujama (nesant informacijos gavėjo sutikimo ar prašymo) ir (ar) nepageidautina (esant informacijos gavėjo prieštaravimui), plataus masto, dažniausiai reklaminiais komerciniais tikslais (visada siekiant gauti tam tikros naudos) elektroniniu paštu siunčiama įvairi informacija, apkraunanti informacines sistemas bei interneto vartotojų elektroninio pašto dėžutes ir daranti žalą fiziniams bei juridiniams asmenims.

kuris reiškia, kad tiesioginę rinkodarą galima vykdyti tik turint išankstinį asmens sutikimą. Beje, pagal Lietuvos vyriausiojo administracinio teismo praktiką, sutikimas turėtų būti gaunamas iš anksto, t. y. negalima tuo pat metu naudojant elektroninių ryšių priemones gauti ir sutikimą.

Dėl tiesioginės rinkodaros tik vieninteliu atveju yra nustatyta išimtis, kai, vadovaujantis OPTOUT principu, savo klientams galima reklamuoti savo prekes ir paslaugas be išankstinio sutikimo, jeigu nemokamai ir aiškiai informuojama, kaip atsisakyti tokios reklamos.

Gana didelę tiesioginės rinkodaros dalį sudaro skambučiai telefonu. Kadangi pagal nustatytą teisinį reguliavimą tokiems skambučiams reikia išankstinio vartotojo sutikimo, tokie sutikimai buvo pradėti rinkti telefonu, to paties skambučio metu siūlant prekes ar paslaugas. 2006 m. birželio 22 d. Lietuvos vyriausiasis administracinis teismas administracinėje byloje Nr. N3-733-06 išaiškino, kad abonento sutikimas naudoti elektroninio ryšio paslaugas tiesioginės rinkodaros tikslu, Elektroninių ryšių įstatymo 68 str. 1 dalies prasme turėtų būti gautas iš anksto, o ne tuo pačiu metu naudojant tiesiogines rinkodaros priemones.

2009 m. sausio 1 d. Lietuvoje įsigaliojus naujai Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo redakcijai, įvestas atskiras naujasis trečiasis skirsnis, reglamentuojantis vaizdo stebėjimą. Taip Lietuvoje buvo pašalinti vaizdo stebėjimo teisinio reguliavimo trūkumai. Neatsižvelgiant į naująjį vaizdo stebėjimo teisinį reguliavimą, praktikoje kartais pasitaiko atvejų, kai potencialūs pažeidėjai lieka nenubausti. Pavyzdžiui, 2009 m. Valstybinė duomenų apsaugos inspekcija surašė R. A. administracinio teisės pažeidimo protokolą už tai, kad ši, siekdama apsaugoti savo turtą, 2009 m. kovo mėn. name įrengė (ir eksploatuoja) vaizdo stebėjimo kameras, į kurių stebėjimo lauką patenka ne tik jai priklausanti žemės sklypo dalis, įėjimo į gyvenamąsias patalpas durys, ūkiniai pastatai ir bendras namo kiemas, bet ir J. M. gyvenamųjų patalpų langai bei ūkiniai pastatai. Vaizdo stebėjimas buvo atliekamas didesnėje teritorijoje ir renkama daugiau vaizdo duomenų, nei tai yra būtina. Tačiau, kilus teisminiams ginčams, Lietuvos vyriausiasis administracinis teismas 2010 m. spalio 29 d. nutartimi administracinėje byloje Nr. N-62-2622/2010 konstatavo, jog administracinė atsakomybė pagal Lietuvos Respublikos administracinių teisės pažeidimų kodeksą R. A. nekyla. R. A. visi jai inkriminuoti Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo pažeidimai netaikomi, nes Institucija neįrodė, kad R. A. yra duomenų tvarkytoja ar valdytoja, taip pat, kad ji tvarkė J. M. asmens duomenis ne asmeniniams poreikiams tenkinti.Tokiais atvejais kyla klausimų dėl administracinio teisės pažeidimo įforminimo.

Be to, teisės aktų reikalavimų dėl vaizdo stebėjimo Lietuvoje labai dažnai yra paprasčiausiai nesilaikoma. Dažniausiai pasitaikantis pažeidimas – duomenų valdytojai neinformuoja duomenų subjektų apie vykdomą vaizdo stebėjimą (nors pagal įstatymą stebėjimo vietose reikia pakabinti nustatyto turinio pranešimus) arba informuoja netinkamai. Pavyzdžiui, 2009 m. Valstybinė duomenų apsaugos inspekcija nustatė, kad viename grožio salone neteisėtai įrengtos slaptos vaizdo stebėjimo kameros. Be to, 2009 m. inspekcija paskelbė degalinių patikrinimo rezultatų apibendrinimą. Paaiškėjo, kad iš patikrintų 57 degalinių, kurios atlieka vaizdo stebėjimą, visose rasta pažeidimų. Tik dvi degalinės buvo pranešusios apie asmens vaizdo duomenų tvarkymą, 47 degalinės netinkamai informavo apie vaizdo stebėjimą. Vėlesniais metais atlikta ir daugiau patikrinimų, kurie irgi parodė, kad stebint vaizdą gana dažnai yra nesilaikoma nustatytų reikalavimų. Kadangi Valstybinės duomenų apsaugos inspekcijos pajėgumai prevenciškai tikrinti duomenų valdytojus dėl asmens duomenų tvarkymo teisėtumo yra riboti, piliečiai turėtų patys aktyviau stebėti neteisėto duomenų tvarkymo atvejus ir apie tai informuoti inspekciją. Svarbi ir asmens duomenų apsaugos reikalavimų viešinimo funkcija, kurią inspekcija turėtų vykdyti aktyviau. Ši prevencijos priemonė skatintų duomenų valdytojus tvarkyti asmens duomenis pagal nustatytus reikalavimus.

Vienuoliktasis įstatymo skirsnis skirtas atsakomybės klausimams reglamentuoti. Pagal įstatymo 53 str., duomenų valdytojams, duomenų tvarkytojams ir kitiems asmenims, pažeidusiems įstatymą, taikoma Lietuvos Respublikos įstatymų nustatyta atsakomybė. Šiuo metu už asmens duomenų apsugos reikalavimų pažeidimus nustatyta administracinė atsakomybė. Pagal Lietuvos Respublikos administracinių teisės pažeidimų kodekso 214^{14} str. „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 šios sankcijos: bauda iki 290 Eur, pakartotinai – bauda iki 580 Eur. Duomenų subjekto teisių, numatytų Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatyme, pažeidimas užtraukia administracinę atsakomybę pagal Lietuvos Respublikos administracinių teisės pažeidimų kodekso 214^{16} str., kur nustatytos tokio pat lygio baudos. Valstybinės duomenų apsaugos inspekcijos pareigūnų teisėtų nurodymų nevykdymas yra baudžiamas pagal Lietuvos Respublikos administracinių teisės pažeidimų kodekso 214^{17} str. ir užtraukia neproporcingai mažą baudą – iki 58 Eur. Šiame kodekse yra ir normų, nustatančių administracinę atsakomybę ir *lex specialis* asmens duomenų apsaugos teisės normų pažeidimo atveju – pvz., kodekso 214^{23} str. numato atsakomybę už neteisėtą asmens duomenų tvarkymą elektroninių ryšių srityje.

Įstatymą detalizuoja nemažai įstatymo įgyvendinamųjų teisės aktų. 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 ir patvirtinti asmens duomenų valdytojų valstybės registro nuostatai. Valstybinės duomenų apsaugos inspekcijos direktoriaus įsakymais taip pat yra patvirtinti:

- bendrieji reikalavimai, taikomi organizacinėms ir techninėms duomenų saugumo priemonėms,
- rekomenduojama pranešimo apie duomenų tvarkymą forma;
- duomenų apsaugos priemonių aprašo reikalavimai;
- pavyzdinė duomenų teikimo sutarties forma;
- Valstybinės duomenų apsaugos inspekcijos vykdomų patikrinimų atlikimo taisyklės;
- duomenų subjekto teisių įgyvendinimo Valstybinėje duomenų apsaugos inspekcijoje tvarka;
- išankstinės patikros taisyklės ir kt.

Valstybinė duomenų apsaugos inspekcija be privalomų įstatymo įgyvendinamųjų teisės aktų leidžia ir rekomendacijas (angl. *soft law*), kurios nėra privalomojo pobūdžio. Visos inspekcijos rekomendacijos ir kita aktuali informacija skelbiama inspekcijos tinklalapyje *http://www.ada.lt*.

3. ES duomenų apsaugos reforma

Atlikti tyrimai parodė, kad valstybės narės skirtingai įgyvendino 1995 m. duomenų apsaugos direktyvą. Vienas iš pavyzdžių – stambiosios įmonės, norinčios vykdyti veiklą visoje ES ar daugelyje ES valstybių, dėl to patiria didelių teisinių išlaidų, nes reikalavimai ES valstybėse narėse skiriasi. Pavyzdžiui, nors direktyvos tekstas siekia 12 psl., Vokietija įgyvendino direktyvą įstatyme, kurio apimtis – 60 puslapių. Šios ir kitos priežastys lėmė poreikį peržiūrėti ir atnaujinti teisinį duomenų apsaugos ES reguliavimą.

2012 m. sausio 25 d. Europos Komisija pasiūlė visapusišką 1995 m. ES asmens duomenų taisyklių reformą, kad sustiprintų teises į privatumą internete ir paskatintų Europos skaitmeninės ekonomikos plėtrą.

Dėl technologinės pažangos ir globalizacijos labai pasikeitė duomenų rinkimo, naudojimo ir susipažinimo su jais būdai. Be to, 27 ES valstybės

narės nevienodai įgyvendino 1995 m. taisykles, dėl to jos buvo taikomos skirtingai.

Komisijos siūlymais atnaujinami ir modernizuojami 1995 m. duomenų apsaugos direktyvoje įtvirtinti principai – ateityje užtikrinti teises į privatumą. Priimtas politinis komunikatas, kuriame nustatyti Komisijos tikslai, ir du teisėkūros pasiūlymai: reglamento, kuriuo nustatoma bendra ES duomenų apsaugos sistema ir direktyvos dėl asmens duomenų apsaugos, tuos duomenis tvarkant nusikalstamų veikų prevencijos, nustatymo, tyrimo ar traukimo baudžiamojon atsakomybėn už jas ir susijusios teisminės veiklos tikslams.

Pagrindiniai siūlomi pakeitimai:

- Visoje ES taikomos vienodos duomenų apsaugos taisyklės. Bus pašalinti nereikalingi administraciniai reikalavimai, pvz., įmonėms taikomi reikalavimai pranešimams apie duomenų tvarkymą. Dėl to jos sutaupys apie 2,3 mlrd. Eur per metus.
- Vietoj dabartinio įpareigojimo (kuris lėmė nereikalingą biurokratizmą ir įmonėms kainavo 130 mln. Eur per metus) visoms įmonėms pranešti duomenų apsaugos priežiūros pareigūnams apie visą su duomenų apsauga susijusią veiklą, reglamente numatyta didesnė asmens duomenis tvarkančiųjų atsakomybė ir atskaitomybė.
- Numatyta pareiga pranešti apie asmens duomenų saugumo pažeidimus. Pavyzdžiui, įmonės ir organizacijos privalo kuo greičiau (jeigu įmanoma, per 24 val.) pranešti nacionalinei priežiūros institucijai apie šiurkščius duomenų pažeidimus.
- Organizacijos turės bendrauti tik su viena nacionaline duomenų apsaugos institucija toje ES šalyje, kurioje yra pagrindinė organizacijos buveinė. Be to, asmenys galės kreiptis į savo šalies duomenų apsaugos instituciją net ir tada, kai jų duomenis tvarkys ES nepriklausančioje šalyje esanti įmonė. Aiškiai nustatoma, kad sutikimas tvarkyti duomenis, kai jo reikia, turi būti aiškus, o ne tariamas.
- Asmenys galės lengviau susipažinti su savo duomenimis ir juos perduoti iš vieno paslaugos teikėjo kitam (teisė į duomenų perkeliamumą). Dėl to pagerės paslaugos teikėjų tarpusavio konkurencija.
- „Teisė būti pamirštam“ padės žmonėms geriau valdyti interneto keliamas duomenų apsaugos grėsmes. Jie galės ištrinti savo duomenis, jeigu nebus teisinio pagrindo jų saugoti.
- ES taisyklės turi būti taikomos, jeigu asmens duomenis užsienyje tvarko ES rinkoje aktyviai veikiančios ir ES piliečiams savo paslaugas teikiančios įmonės.

– Nepriklausomos nacionalinės duomenų apsaugos institucijos bus sustiprintos, kad savo šalyje galėtų geriau užtikrinti ES taisyklių laikymąsi. Jos galės nubausti įmones, pažeidžiančias ES duomenų apsaugos taisykles. Baudos galės siekti iki 4 proc. visos įmonės metinės apyvartos.
– Pagal naująją direktyvą, bendri duomenų apsaugos principai ir taisyklės bus taikomi policijos ir teisminiam bendradarbiavimui baudžiamosiose bylose. Taisyklės bus taikomos ir šalyje, ir tarpvalstybiniu mastu perduodant duomenis.
– Šiuo metu Komisijos siūlymai pasiekė paskutinę svarstymo stadiją ir galutinio teksto dar nėra. Ypač daug diskusijų kelia Reglamento projektas. Teigiama, kad dėl šio projekto kilusios diskusijos yra didžiausios per visą ES teisės aktų priėmimo istoriją. Vieni iš aktyviausiai savo poziciją dėl reglamento reiškia privataus elektroninių ryšių sektoriaus atstovai. Be kitų klausimų, dažniausiai keliami šie:
– taikoma teisė (dėl „įsikūrimo“ tikslesnio apibrėžimo ir pan.);
– duomenų subjekto sutikimas (teigiama, kad ne visais atvejais turėtų būti privaloma gauti aktyvų asmens sutikimą tvarkyti jo duomenis, nes tai stabdytų verslo procesus ir nebūtų patogu pačiam vartotojui);
– sankcijos (teigiama, kad sankcijos yra per griežtos, be to, nepriklauso nuo padarinių ir pažeidimo tyčios);
– dokumentavimo įpareigojimas (teigiama, kad tai užkraus nereikalingą naštą verslui ir didins jo sąnaudas);
– duomenų saugumo pažeidimai (teigiama, kad nėra skiriami pavojingi ir kiti pažeidimai, o laikas, per kurį reikia pranešti apie pažeidimus, yra per trumpas. Be to, įpareigojimas dubliuojasi su įpareigojimu dėl duomenų saugumo pažeidimų, numatytų Privatumo direktyvoje).

Apskritai vertinant visą verslo sektorių, 2013 m. gegužės 14 d. nepriklausomo tyrimo rezultatai, paskelbti per Berlyne vykusią trečiąją ES duomenų apsaugos konferenciją, parodė, kad 40 proc. verslo bendrovių iki galo nesupranta, kokios pagrindinės nuostatos siūlomos reglamente. Net 87 proc. verslo bendrovių negali įvertinti reglamento finansinės įtakos jų verslui.

Duomenų apsaugos reglamentas ir direktyva turėtų įsigalioti po dvejų metų nuo jų priėmimo.

2 skirsnis. Privatumo ir asmens duomenų apsauga palaikant elektroninius ryšius

1. Pagrindiniai privatumo ir asmens duomenų apsaugos palaikant elektroninius ryšius ypatumai

Dėl elektroninių komunikacijų ir ryšio priemonių konvergencijos[47] pastaruoju metu vietoj telekomunikacinių naudojama elektroninių ryšių sąvoka. Elektroniniai ryšiai – signalų perdavimas laidinėmis, radijo, optinėmis ar kitomis elektromagnetinėmis priemonėmis, suteikia galimybę žmonėms bendrauti, neatsižvelgiant į jų fizinio buvimo vietą. Tačiau elektroniniai ryšiai turi ne tik neabejotinų pranašumų, bet ir kelia vis didesnę grėsmę privačiam žmogaus gyvenimui. Elektroninių ryšių paslaugų ir tinklų teikėjai, vykdydami savo veiklą, tvarko didžiulius kiekius duomenų, kurių dauguma priskirtina asmens duomenims. Elektroniniais ryšiais taip pat perduodama elektroninių ryšių paslaugų gavėjų siunčiama informacija (turinys). Todėl toks duomenų tvarkymas ir (ar) perdavimas neabejotinai turi (gali turėti) didelę įtaką elektroninių ryšių paslaugų gavėjų privatumui.

ES privatumo ir asmens duomenų apsaugos palaikant elektroninius ryšius reguliavimas pritaikytas išimtinai elektroninių ryšių sektoriui. Tam skirta 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių). Ši direktyva pakeitė senosios reguliavimo sistemos 1997 m. gruodžio 15 d. Europos Parlamento ir Tarybos direktyvą 97/66/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos telekomunikacijų srityje. Minimoji 2002/58/EB direktyva irgi papildo bendrąją duomenų apsaugos direktyvą 95/46/EB, kurios bendrieji duomenų apsaugos principai taip pat svarbūs elektroninių ryšių sektoriui. Vis dėlto 2002/585/EB direktyvos normos laikytinos *lex specialis,* o 2009 m. 2002/58/EB direktyvą pakeitė naujausia 2009/136/EB direktyva.

Viešųjų elektroninių ryšių paslaugų abonentai gali būti fiziniai arba juridiniai asmenys, tad 2002/58/EB direktyva (įskaitant ir ją pakeitusią 2009/136/EB direktyvą) siekiama apsaugoti fizinių asmenų teises, ypač jų teisę į privatumą, ir teisėtus juridinių asmenų interesus.

2002/58/EB direktyva (įskaitant ir ją pakeitusią 2009/136/EB direktyvą) Lietuvoje įgyvendinta Lietuvos Respublikos elektroninių ryšių įsta-

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

tymo IX skirsnyje ir, kaip jau buvo minėta, už šio skirsnio priežiūrą yra atsakinga Valstybinė duomenų apsaugos inspekcija. Atkreiptinas dėmesys, kad juridiniams asmenims apsauga taikoma tik tiesioginės rinkodaros ir abonentų sąrašų atvejais.

Privatumo ir asmens duomenų apsaugos palaikant elektroninius ryšius reguliavimą galima suskirstyti į šias pagrindines grupes:

1) viešųjų elektroninių ryšių paslaugų ir tinklų saugumas;
2) ryšio slaptumas;
3) duomenų srauto tvarkymas;
4) detaliosios sąskaitos;
5) abonentų sąrašai;
6) tiesioginė rinkodara;
7) ryšio linijos nustatymas;
8) slapukų naudojimas.

Toliau šios grupės bus aptariamos detaliau.

Viešųjų elektroninių ryšių paslaugų ir tinklų saugumas. Pagal Lietuvos Respublikos elektroninių ryšių įstatymo 62 str., viešųjų elektroninių ryšių paslaugų teikėjai privalo įgyvendinti tinkamas technines ir organizacines priemones savo teikiamų paslaugų saugumui užtikrinti, o prireikus – kartu su viešųjų ryšių tinklų teikėjais imtis tokių pat priemonių viešųjų ryšių tinklų saugumui užtikrinti. 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 apie tai informuoti abonentus net 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 (tokiu kaip internetas) teikiamoms elektroninių ryšių paslaugoms ir kitais atvejais. Paslaugų teikėjai, siūlantys viešai prieinamų elektroninių ryšių paslaugas internetu, turėtų informuoti naudotojus ir abonentus, kokias priemones jie galėtų taikyti savo pranešimams apsaugoti, pvz., specialią programinę įrangą ar šifravimo technologijas. Reikalavimas pranešti abonentams apie konkrečią saugumui kylančią riziką neatleidžia paslaugų teikėjo nuo įsipareigojimo savo lėšomis imtis tinkamų ir skubių priemonių bet kokiai naujai, nenumatytai saugumo rizikai pašalinti ir normaliam paslaugos saugumo lygiui atkurti. Informacija abonentui apie saugumo riziką turėtų būti teikiama nemokamai.

Papildomai paminėtina, kad Valstybinė duomenų apsaugos inspekcija yra priėmusi rekomendacinio pobūdžio akrą – 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.

2009/136/EB direktyva įvedė asmens duomenų saugumo pažeidimo institutą, įskaitant ir pareigą informuoti kompetentingą instituciją apie asmens duomenų saugumo pažeidimus. Pagal Lietuvos Respublikos elektroninių ryšių įstatymo 3 str. 4 p., asmens duomenų saugumo pažeidimas – pažeidimas, dėl kurio atsitiktinai arba neteisėtai sunaikinami, prarandami, pakeičiami, be asmens sutikimo atskleidžiami asmens duomenys arba sudaroma galimybė naudotis tais duomenimis, kai jie buvo perduodami, saugomi arba kitaip tvarkomi teikiant viešąsias elektroninių ryšių paslaugas. To paties įstatymo 62 str. 4 dalyje reglamentuojama, jog asmens duomenų saugumo pažeidimo atveju viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjas apie šį pažeidimą nedelsdamas privalo pranešti Valstybinei duomenų apsaugos inspekcijai. Tuo atveju, jeigu asmens duomenų saugumo pažeidimas gali turėti neigiamą poveikį abonento ar registruoto elektroninių ryšių paslaugų naudotojo arba kito asmens duomenų ar privatumo saugumui, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjas taip pat privalo apie tai pranešti abonentui ar registruotam elektroninių ryšių paslaugų naudotojui arba kitam asmeniui, išskyrus atvejus, kai viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjas Valstybinei duomenų apsaugos inspekcijai įrodo, kad naudojo tinkamas technines priemones, kurios buvo taikomos saugumo pažeidimo paveiktiems asmens duomenims. Šios priemonės turi užtikrinti, kad neįgaliotieji asmenys negalėtų susipažinti su asmens duomenimis.

Siekdama užtikrinti direktyvos nuostatos dėl duomenų saugumo pažeidimo tinkamą įgyvendinimą visose ES valstybėse narėse, Europos Komisija parengė „technines įgyvendinimo priemones“ – praktines taisykles, įgyvendinančias minėtąją nuostatą. Šios taisyklės, anot Europos Komisijos, padės užtikrinti, kad visose ES valstybėse duomenų saugumo pažeidimai bus taip traktuojami ir apie tokius pažeidimus bus pranešama tuo pačiu laiku. Tam tikslui Europos Komisija 2013 m. birželio 24 d. priėmė reglamentą (ES) Nr. 611/2013 dėl priemonių, kurios pagal Europos Parlamento ir Tarybos direktyvą 2002/58/EB dėl privatumo ir elektroninių ryšių taikomos pranešimams apie asmens duomenų saugumo pažeidimus.

Ryšio slaptumas. Lietuvos Respublikos elektroninių ryšių įstatymo 61 str. įtvirtina konfidencialumo apsaugą ir draudžia ne faktiniams elektroninių ryšių paslaugų naudotojams be 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 61 str. nuostatų pažeidimas gali užtraukti baudžiamąją atsakomybę pagal Lietuvos Respublikos baudžiamojo kodekso 166 str. „Neteisėtas susirašinėjimo, kitokių pranešimų, siuntų ar pokalbių telefonu slaptumo pažeidimas".

Srauto duomenų tvarkymas. Pagal Lietuvos Respublikos elektroninių ryšių įstatymo 3 str. 57 p., srauto duomenimis laikytini „duomenys, tvarkomi siekiant perduoti informaciją elektroninių ryšių tinklu ir (arba) tokio perdavimo apskaitai". ES direktyvos 2002/58/EB preambulės 15 p. 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 ir skambinančiojo telefono numerį, o elektroninio pašto atveju – siuntėjo *IP* adresas, elektroninio pašto adresas, elektroninio pašto žinutės dydis, elektroninio pašto žinutės pavadinimas, elektroninio pašto žinutės priedų dydis ir tipas.

Galima daryti išvadą, kad srauto duomenys yra itin jautrūs ir jie gali atskleisti daugybę asmeninio gyvenimo detalių, tokių kaip asmens įpročiai, pomėgiai, asmenų, su kuriais bendraujama, grupė ir pan. Tokie duomenys saugotini tiek, kiek jie reikalingi sąskaitoms pateikti bei sumokėti už tinklų sujungimus, ir tik ribotą laiko tarpą (pagal Lietuvos Respublikos elektroninių ryšių įstatymo 66 str. 6 d. – 6 mėnesius nuo ryšio datos[48]). Jeigu vėliau viešai prieinamų elektroninių ryšių paslaugų teikėjas pageidauja tvarkyti šiuos duomenis elektroninių ryšių paslaugų rinkodaros tikslams arba pridėtinės vertės paslaugai sukurti, tai leidžiama tik abonentui sutikus ir šis apsisprendžia remdamasis tikslia ir išsamia iš šio teikėjo gauta informacija

[48] Lietuvos Respublikos elektroninių ryšių įstatymo 77 str. numato, kad *jeigu šio Įstatymo 65 str. nurodyti duomenys reikalingi kriminalinės žvalgybos subjektams, žvalgybos institucijoms, ikiteisminio tyrimo įstaigoms, prokurorui, teismui ar teisėjui nusikalstamoms veikoms užkardyti, tirti, nustatyti, Vyriausybės įgaliotosios institucijos – kriminalinės žvalgybos subjekto, žvalgybos institucijų – nurodymu ūkio subjektai, teikiantys elektroninių ryšių tinklus ir (arba) paslaugas, turi tokią informaciją saugoti ilgiau, negu nurodyta šio Įstatymo 66 str. 4, 5 ir 6 d., bet ne ilgiau kaip 6 mėnesius papildomai*.

apie numatomus tolesnio duomenų tvarkymo būdus ir abonento teisę nesutikti arba panaikinti duotą sutikimą tvarkyti tokius duomenis. Suteikus ryšių rinkodaros arba pridėtinės vertės paslaugas, sunaikinami arba padaromi anoniminiai tokioms paslaugoms reikalingi srauto duomenys. Paslaugų teikėjai visada privalo informuoti abonentus, kokių tipų duomenis tvarko, kokiems tikslams ir kokį laiko tarpą.

Įsipareigojimas sunaikinti srauto duomenis arba padaryti juos anoniminiais, kai jų jau nereikia pranešimui perduoti, neprieštarauja šioms interneto procedūroms: *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. Be to, teikėjui leidžiama pateikiant sąskaitas naudotis srauto duomenimis, kai reikia nustatyti ir nutraukti sukčiavimą, pasireiškiantį tuo, kad nesumokama už suteiktas elektroninių ryšių paslaugas.

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

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

Valstybinė duomenų apsaugos inspekcija 2005 m. patvirtino detaliųjų sąskaitų reikalavimus, kurie nustato viešųjų elektroninių ryšių paslaugų teikėjų išduodamų 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 2002/22/EB 5 str., universaliųjų paslaugų operatoriai turi garantuoti viešųjų abonentų sąrašų buvimą. Į šiuos sąrašus yra įtraukiami visi abonentai, išskyrus tuos, kurie nesutinka būti įtraukiami. Fizinių asmenų teisė į privatumą ir juridinių asmenų teisėti interesai reikalauja, kad abonentas apsispręstų ne tik dėl to, ar jo asmens duomenys apskritai skelbtini sąraše, bet ir kokie duomenys gali būti skelbiami.

Pagal Lietuvos Respublikos elektroninių ryšių įstatymo 67 str., kai viešuoju abonentų sąrašu siekiama daugiau nei tik suteikti galimybę ieškoti abonentų kontaktinių duomenų pagal jų vardus (pavardes), kad abonento duomenys būtų įtraukti į tokį sąrašą, turi būti gautas atitinkamo abonento sutikimas.

Tiesioginė rinkodara. Direktyva 2002/58/EB skiria automatinę ir neautomatinę tiesioginę rinkodarą. Remiantis Direktyvos 2002/58/EB 13 str., „naudoti automatinio skambinimo sistemas be žmogaus įsiterpimo (skambinimo automatus), faksimilinius aparatus (faksus) ar elektroninį paštą tiesioginės rinkodaros tikslais gali būti leidžiama tik gavus išankstinį abonentų sutikimą“. Dėl kitų tiesioginės rinkodaros formų (pvz., neautomatinės tiesioginės rinkodaros), Direktyvos 2002/58/EB 13 str. suteikia valstybėms narėms pasirinkimo laisvę. Lietuvos įstatymų leidėjai nusprendė, kad abonentų sutikimas yra būtinas tiek esant automatinei, tiek ir neautomatinei tiesioginei rinkodarai. Taigi palaikant elektroninius ryšius tiesioginę rinkodarą galima naudoti tik laikantis vadinamojo OPT-IN principo.

Reikia paminėti, kad savo paties panašių prekių ar paslaugų rinkodarai Elektroninių ryšių įstatymas nustato OPT-OUT principą. Įstatymo 69 str. 2 d. nurodyta, jog asmuo, kuris teikdamas paslaugas ar parduodamas prekes Asmens duomenų teisinės apsaugos įstatymo nustatyta tvarka ir sąlygomis gauna iš savo klientų kontaktinius elektroninio pašto duomenis, gali naudoti šiuos kontaktinius duomenis savo paties panašių prekių ar paslaugų rinkodarai, jei klientams yra suteikiama aiški, nemokama ir lengvai įgyvendinama galimybė nesutikti arba atsisakyti tokio kontaktinių duomenų naudojimo pirmiau nurodytais tikslais, kai šie duomenys yra renkami ir, jei klientas iš pradžių neprieštaravo dėl tokio duomenų naudojimo, siunčiant kiekvieną žinutę.

Pagal Elektroninių ryšių įstatymo 69 str. 3 d., draudžiama tiesioginės rinkodaros tikslu siųsti elektroninio pašto pranešimus slepiant siuntėjo, kurio vardu informacija siunčiama, tapatybę arba nenurodant galiojančio adreso, kuriuo gavėjas galėtų pareikalauti nutraukti tokios informacijos siuntimą.

Ryšio linijos nustatymas. Kalbant apie ryšio linijos, iš kurios skambinama, nustatymą, būtina apsaugoti skambinančiosios šalies teisę neleisti nustatyti linijos, iš kurios skambinama, taip pat ir šalies, kuriai skambinama, teisę atsisakyti skambučių iš nenustatytų linijų. Elektroninių ryšių įstatymo 64 str. užtikrina šias svarbiausias teises:

- teisė skambinančiajam panaikinti galimybę nustatyti ryšio liniją, iš kurios skambinama;
- teisė abonentui, kuriam skambina, panaikinti galimybę nustatyti ryšio liniją, iš kurios skambinama;

– teisė atsisakyti skambučio iš nenustatytos linijos;
– teisė uždrausti nustatyti ryšio liniją, į kurią skambinama.

2003 m. Lietuvos Respublikos Vyriausybė nutarimu Nr. 212 patvirtino 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. Minėtieji atvejai susiję su erzinančiais ar piktybiniais skambučiais.

Slapukų naudojimas. Slapukas (angl. *cookies*) – tai mažas duomenų rinkinis (failas), įrašytas į naudotojo kompiuterį ar esantis kitame galiniame prisijungimo įrenginyje, jam lankantis interneto svetainėje. Slapuke kaupiama lankomos svetainės informacija. Kitą kartą lankantis toje pačioje interneto svetainėje, automatiškai išanalizuojama slapukuose esanti informacija. Slapukų teikiama informacija gali būti naudojama vertinant naudotojų elgesį internete ir teikiant jiems reklaminius siūlymus arba techninei interneto svetainės struktūrai ir turiniui atvaizduoti.

Slapuke gali būti saugomi individo tapatybę atskleidžiantys duomenys: prisijungimo *IP* adresas, specialiai tam asmeniui sukurtas unikalus naudotojo identifikatorius (unikalus žymuo) ir kt. Užsiregistravęs interneto svetainėje ir pateikęs paslaugoms teikti reikalingus duomenis, pvz., vardą, el. pašto adresą, darbo ar gyvenamosios vietos adresą, telefono numerį, naudotojas pats suteikia galimybę paslaugų teikėjui naudotis šiais duomenimis. Interneto svetainė gali gauti tik tą informaciją, kurią pateikia pats naudotojas, pvz., jeigu jis nenurodys savo el. pašto adreso, šis ir nebus atskleistas. Slapuke esantis unikalus žymuo nesuteikia prieigos prie naudotojo kompiuteryje saugomos informacijos, tačiau leidžia atsekti jo veiksmus netgi tada, kai naudojamas kintamas (dinaminis) *IP* adresas.

2011 m. rugpjūčio 1 d. įsigaliojo Elektroninių ryšių įstatymo pakeitimas (įgyvendinantis direktyvą 2009/136/EB), numatantis, kad saugoti informaciją arba suteikti galimybę naudotis jau saugoma informacija abonento ar faktinio elektroninių ryšių paslaugų naudotojo galiniame įrenginyje (pvz., naudoti slapukus leidžiama tik tuo atveju, jeigu naudotojas buvo aiškiai ir išsamiai informuotas apie slapukų naudojimo pobūdį, tikslą ir davė tam sutikimą. Ši tvarka numatyta ERĮ 61 str. 4 d.: „Saugoti informaciją arba suteikti galimybę naudotis jau saugoma informacija abonento ar faktinio elektroninių ryšių paslaugų naudotojo galiniame įrenginyje leidžiama tik su sąlyga, kad atitinkamam abonentui ar faktiniam elektroninių ryšių paslaugų naudotojui vadovaujantis Asmens duomenų teisinės apsaugos įstatymu suteikus aiškią ir išsamią informaciją, įskaitant informaciją apie tvarkymo tikslus, jis davė sutikimą. Atkreiptinas dėmesys,

kad minimame straipsnyje numatyta ir išimtis: Šios nuostatos nedraudžia techninio saugojimo ar naudojimosi duomenimis, kurio vienintelis tikslas yra perduoti informaciją elektroninių ryšių tinklu, taip pat būtinais atvejais teikti informacinės visuomenės paslaugas, kurias užsako abonentas ar faktinis elektroninių ryšių paslaugų naudotojas."

2011 m. *VDAI* parengė rekomendacijas duomenų valdytojams ir duomenų subjektams dėl slapukų naudojimo. Pagrindiniai šių rekomendacijų aspektai:

1) slapukai gali būti naudojami tik esant išankstiniam naudotojo sutikimui. Prieš duodamas tokį sutikimą, naudotojas privalo būti tinkamai informuotas. Be to, naudotojui turi būti suteikta galimybė bet kada atšaukti savo duotą sutikimą. Svetainių valdytojų patarimai, kaip nustatyti naršyklių parametrus norint nepriimti slapukų, dar nereiškia, kad naudotojas sutiko šiuos slapukus įrašyti į jo įrenginį;
2) sutikimas dėl slapukų nebūtinas, kai:
   - galimas techninis saugojimas (slapukai naudojami techninei interneto svetainės struktūrai ir turiniui atvaizduoti);
   - jeigu vienintelis tikslas – perduoti informaciją elektroninių ryšių tinklu;
   - būtinais atvejais teikti informacinės visuomenės paslaugas, kurias užsako naudotojas (jeigu slapukas naudojamas internetinės parduotuvės interneto svetainėje pirkėjo pasirinktų prekių krepšeliui formuoti, siekiant naudotojui suteikti jo prašomą paslaugą ir pan.);
   - nors šiuo atveju slapukams naudotojo sutikimo nereikia, naudotojai vis tiek apie tai turi būti informuojami (pvz., interneto svetainės privatumo politikoje);
3) naudotojo sutikimas dėl slapukų naudojimo turėtų galioti tam tikrą ribotą laiką, pvz., vienus metus. Asmuo, naudojantis slapukus, turi užtikrinti, kad pasibaigus šiam terminui slapukai, kuriems naudoti buvo reikalingas naudotojo sutikimas, būtų panaikinti. Norint naudoti slapukus toliau, turi būti gautas naujas naudotojo sutikimas;
4) pareiga informuoti naudotoją ir gauti jo sutikimą dėl slapukų naudojimo tenka asmenims, ketinantiems juos naudoti. Padėtis tampa sudėtingesnė, kai interneto svetainė sudaro sąlygas slapukus į „savo" naudotojų įrenginius įrašyti tretiesiems asmenims (pvz., reklamos tinklų operatoriams). Šiuo atveju siekiant užtikrinti, kad naudotojas galėtų duoti sutikimą, interneto svetainės valdytojas ir trečiasis asmuo privalo bendradarbiauti ir nuspręsti, kas informuos naudotoją ir gaus jo sutikimą bei kaip tai bus padaryta.

2. Privataus gyvenimo neliečiamumo ribojimas palaikant elektroninius ryšius nusikaltimų tyrimo tikslams

Elektroniniai ryšiai suteikia ne tik neabejotinų pranašumų, bet ir kelia vis didelę grėsmę privačiam žmogaus gyvenimui. Neabejotina, kad elektroninės komunikacijos, pasitelkus elektroninių ryšių tinklus, labiausiai gali veikti asmens santykių su kitais asmenimis aspektą. Būtent asmens susižinojimas ir pan. gali būti pažeidžiamas vykstant elektroninei komunikacijai, nors svarbūs ir kiti privataus gyvenimo aspektai.

Svarbu paminėti, 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 neliečiamumą, užtikrinimo. Lietuvos Respublikos Konstitucinis Teismas yra pabrėžęs, 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“.

Tiek Lietuvos Respublikos Konstitucijos 22 str., tiek Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos 8 str. 2 d. numato, kad ši teisė gali būti ribojama esant tam tikroms aplinkybėms. Pavyzdžiui, minima teisė gali būti ribojama, turint omenyje valstybės interesą gauti informaciją apie asmenį, pvz., padariusį nusikaltimą. Kaip jau minėta, Lietuvos Respublikos Konstitucijos 22 str. 3 d. teigiama, jog „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 str. 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. Šiuo atveju svarbi Europos žmogaus teisių teismo praktika. Bylose *Amann prieš Šveicariją, Armstrong prieš Jungtinę Karalystę, Khan prieš Jungtinę Karalystę* ir kt. Europos Žmogaus Teisių Teismas yra suformavęs šias pagrindines žmogaus teisių ribojimo sąlygas:

1) teisėtumo sąlyga, nurodanti, kad ribojimai gali būti nustatomi tik viešai paskelbtu ir aiškiai suformuluotu įstatymu;
2) būtinumo sąlyga, nurodanti, kad ribojimai gali būti nustatomi tik tada, kai tai reikalinga demokratinėje visuomenėje.

Žmogaus teisių ribojimo klausimu yra pasisakęs ir Lietuvos Respublikos Konstitucinis Teismas. 2002 m. rugsėjo 19 d. Lietuvos Respublikos Konstitucinio Teismo nutarime teigiama, jog pagal Konstituciją riboti konstitucines žmogaus teises ir laisves galima tada, kai 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.

Teisės į privatų gyvenimą ribojimas elektroniniuose ryšiuose[49] taip pat turėtų būti vykdomas vadovaujantis aukščiau išvardytais principais ir sąlygomis. Elektroninių ryšių kontrolę (plačiąja prasme), vykdomą operatyviniais ar kitais nusikaltimų tyrimo tikslams, galima skirstyti į dvi grupes:

1) buvusių elektroninių ryšių įvykių kontrolė – informacijos apie buvusius elektroninių ryšių įvykius (srauto duomenis) gavimas iš elektroninių ryšių paslaugų teikėjų;
2) elektroninių ryšių tinklais perduodamos informacijos kontrolė (kompetentingų teisėsaugos institucijų vykdoma elektroninių ryšių turinio ar kitos elektroninių ryšių tinklais perduodamos informacijos kontrolė).

Siekiant kiekvieną kontrolės grupę įgyvendinti praktikoje, teisės aktais nustatomi šiek tiek skirtingi reikalavimai. Toliau atskirai bus aptariamos abi aukščiau išvardytos elektroninių ryšių kontrolės grupės.

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 tele-

[49] Šis ribojimas dar gali būti vadinamas elektroninių ryšių kontrole.

komunikacijų įvykis apibūdinamas kaip „informacijos perdavimo, siuntimo, priėmimo telekomunikacijų tinklais faktas“. Pagal Lietuvos Respublikos elektroninių ryšių įstatymo 3 str. 57 p., 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 pan., o elektroninio pašto atveju srauto duomenimis gali būti laikomi šie duomenys: siuntėjo *IP* adresas ir elektroninio pašto adresas, elektroninio pašto žinutės dydis, elektroninio pašto žinutės pavadinimas[50], elektroninio pašto žinutės priedų dydis, tipas ir pan.

Pagal Lietuvos Respublikos elektroninių ryšių įstatymo 77 str. 1 d., „ūkio subjektai, teikiantys elektroninių ryšių tinklus ir (ar) paslaugas, privalo įstatymų nustatyta tvarka turimą ir nusikalstamoms veikoms užkardyti, tirti, nustatyti reikalingą informaciją pateikti operatyvinės veiklos subjektų pagrindinėms institucijoms, Vyriausybės nurodytoms ikiteisminio tyrimo įstaigoms, prokurorui, teismui ar teisėjui. Šią informaciją ūkio subjektai, teikiantys elektroninių ryšių tinklus ir (ar) paslaugas, neatlygintinai teikia operatyvinės veiklos subjektų pagrindinėms institucijoms, Vyriausybės nurodytoms ikiteisminio tyrimo įstaigoms pagal jų paklausimus elektroniniu būdu ir nedelsdami.“ Šiai informacijai priklauso ir informacija apie elektroninių ryšių įvykius, t. y. srauto duomenys.

Jeigu informacija renkama kriminalinės žvalgybos tikslams, pagal Lietuvos Respublikos kriminalinės žvalgybos įstatymo 9 str. yra būtina teismo nutartis. Pagal minėtojo įstatymo 9 str. 6 d., „siekiant gauti šio straipsnio 1 dalyje nurodytą informaciją, ūkio subjektams, teikiantiems elektroninių ryšių tinklus ir (ar) paslaugas, Lietuvos bankui, finansų įmonėms ir kredito įstaigoms ar kitiems juridiniams asmenims pateikiamas pranešimas, kuriame nurodomi teikimo numeris, nutarties priėmimo data, nutartį priėmęs teismas ir kokią informaciją prašoma pateikti, o neatidėliotinais atvejais, kai kriminalinės žvalgybos subjekto vadovas ar įgaliotas vadovo pavaduotojas priima nutarimą, pranešime nurodomi nutarimo numeris ir data, nutarimą priėmęs kriminalinės žvalgybos subjektas. Už šio pranešimo

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

turinio atitiktį teismo nutarčiai įstatymų nustatyta tvarka atsako pranešimą teikiantis pareigūnas. Šioje dalyje nurodyti subjektai šio pranešimo turinio negali atskleisti asmenims, dėl kurių pateiktas prašymas. Apie tai pažymima pranešime."

Pagal Lietuvos Respublikos baudžiamojo proceso kodekso 154 str., „kai pagal prokuroro prašymą yra priimta ikiteisminio tyrimo teisėjo nutartis, ikiteisminio tyrimo pareigūnas gali klausytis asmenų pokalbių, perduodamų elektroninių ryšių tinklais, daryti jų įrašus, kontroliuoti kitą elektroninių ryšių tinklais perduodamą informaciją ir ją fiksuoti bei kaupti, jeigu yra pagrindas manyti, kad tokiu būdu galima gauti duomenų apie rengiamą, daromą ar padarytą labai sunkų, sunkų ar apysunkį nusikaltimą arba apie nesunkius nusikaltimus, numatytus Lietuvos Respublikos baudžiamojo kodekso 170 straipsnyje, 182 str. 1 d., arba jeigu yra pavojus, kad nukentėjusiajam, liudytojui ar kitiems proceso dalyviams arba jų artimiesiems bus panaudotas smurtas, prievartavimas ar kitokios neteisėtos veikos." Ši teisės norma apima ir buvusių elektroninių ryšių įvykių kontrolę.

Lietuvos Respublikos elektroninių ryšių įstatymo 77 str. 1 d. nurodyta, kad „ūkio subjektai, teikiantys elektroninių ryšių tinklus ir (arba) paslaugas, privalo įstatymų nustatyta tvarka turimą ir nusikalstamoms veikoms užkardyti, tirti, nustatyti reikalingą informaciją pateikti kriminalinės žvalgybos pagrindinėms institucijoms, Vyriausybės nurodytoms ikiteisminio tyrimo įstaigoms, prokurorui, teismui ar teisėjui. Šią informaciją ūkio subjektai, teikiantys elektroninių ryšių tinklus ir (arba) paslaugas, neatlygintinai teikia kriminalinės žvalgybos pagrindinėms institucijoms, Vyriausybės nurodytoms ikiteisminio tyrimo įstaigoms pagal jų paklausimus elektroniniu būdu ir nedelsdami. Vyriausybės nurodytos ikiteisminio tyrimo įstaigos Vyriausybės nustatyta tvarka organizuoja ir sudaro galimybę gauti šią informaciją savo padaliniams ir (arba) kitoms ikiteisminio tyrimo įstaigoms. Visi asmenys, dalyvaujantys keičiantis duomenimis, Vyriausybės nustatyta tvarka ir sąlygomis imasi būtinų priemonių duomenų saugumui užtikrinti, o tam reikalinga papildoma įranga įsigyjama ir išlaikoma valstybės lėšomis." 2010 m. lapkričio 3 d. Lietuvos Respublikos Vyriausybės nutarimu Nr. 1569 „Dėl duomenų apie elektroninių ryšių įvykius viešuosiuose ryšių tinkluose teikimo Lietuvos Respublikos kompetentingoms institucijoms tvarkos aprašo patvirtinimo" buvo patvirtintas minėtų duomenų teikimo tvarkos aprašas. Šis aprašas reglamentuoja viešųjų ryšių tinklų ir (ar) viešųjų elektroninių ryšių paslaugų teikėjų saugomų duomenų, nurodytų Elektroninių ryšių įstatymo 65 str. (elektroninių ryšių įvykių duomenų), teikimo kompetentingoms institucijoms tvarką. Pagal šio aprašo 4 p., bendrą automatizuoto elektroninių ryšių įvykių duomenų

tvarkymo įrangą ir ryšio kanalus su teikėjų elektroninių ryšių duomenų bazėmis įdiegia ir eksploatuoja Lietuvos Respublikos valstybės saugumo departamentas.

Svarbu paminėti 2006 m. kovo 15 d. Europos Parlamento ir Tarybos direktyvą 2006/24/EB dėl duomenų, gautų arba tvarkomų teikiant viešai prieinamas elektroninių ryšių paslaugas arba viešuosius ryšių tinklus, saugojimo ir iš dalies keičianti direktyvą 2002/58/EB, kurioje informacijos apie srauto duomenis teikimo teisėsaugos institucijoms tikslais buvo numatyta pareiga elektroninių ryšių paslaugų teikėjams srauto duomenis privalomai kaupti ir saugoti nuo šešių mėn. iki dvejų metų nuo jų užfiksavimo. Kadangi, kaip parodė praktika, ūkinei veiklai užtikrinti informaciją apie srauto duomenis elektroninių ryšių paslaugų teikėjai kaupia ne daugiau nei kelis mėnesius, nustatant reikalavimą duomenis kaupti iki dvejų metų, duomenys, sudarantys privataus gyvenimo paslaptį, tam tikrą laikotarpį teisėsaugos tikslams būtų kaupiami be teismo leidimo. Kaip jau minėta, pagal Lietuvos Respublikos Konstitucijos 22 str., informacija apie privatų gyvenimą gali būti renkama tik motyvuotu teismo sprendimu ir tik pagal įstatymą. Apie tai yra užsiminęs ir Lietuvos Respublikos Konstitucinis Teismas. Todėl toks įpareigojimas be motyvuoto teismo sprendimo saugoti informaciją daugiau nei reikia ūkinei veiklai užtikrinti, taip įsiterpiant į žmogaus privatų gyvenimą, galbūt prieštarauja Konstitucijos 22 str. nuostatoms. Galimas direktyvos nuostatų, susijusių su duomenų saugojimo laikotarpiu, prieštaravimas žmogaus teises reglamentuojantiems tarptautinės teisės aktams, buvo aptariamas ir mokslinėje literatūroje. 2014 m. Europos Sąjungos Teisingumo Teismas duomenų saugojimo direktyvą bylose C-293/12 ir C-594/12 duomenų saugojimo direktyvą pripažino kaip pažeidžiančią proporcingumo principą ir negaliojančią. Pvz., direktyvoje buvo nustatytas nuo šešių iki dvidešimt keturių mėnesių duomenų saugojimo terminas, tačiau nepagrįstas jokiais kriterijais. Teismui priėmus šį sprendimą, kurį laiką vyko diskusijos, ką daryti atskiroms nacionalinėms valstybėms, kurios jau įgyvendino duomenų saugojimo direktyvą. Kai kuriose valstybėse tam tikri elektroninių ryšių paslaugų teikėjai apskritai buvo nutraukę duomenų apsaugą, tačiau tai buvo daugiau išimtys. Kitose valstybėse (pvz., Olandijoje) nacionaliniai teismai pripažino, kad esamos nuostatos dėl duomenų saugojimo šiukščiai pažeidžia žmogaus teises. Padėtis atskirose valstybėse tapo skirtinga ir pasigirdo raginimų Europos Komisijai inicijuoti naujos direktyvos siūlymą.

2015 m. Europos Komisija informavo, kad nesirengia inicijuoti naujos direktyvos ar naujų teisės aktų šioje srityje. Valstybės turi pačios spręsti šį klausimą, tačiau svarbu, kad nacionaliniai teisės aktai neprieštarautų

privatumo direktyvai. Paminėtina, kad Elektroninių ryšių įstatymo nuostatos, įgyvendinusios duomenų saugojimo direktyvą, iki šiol neperžiūrėtos, todėl dalis šių nuostatų galbūt prieštarauja teisinėje praktikoje ir ES dokumentuose įtvirtintiems privatumo apsaugos principams.

Elektroninių ryšių turinio ir srauto duomenų kontrolė realiuoju laiku. Kas yra elektroninių ryšių turinys ar kita elektroninių ryšių tinklais perduodama informacija? Teisės aktuose nėra nustatyta, kas laikoma turinio duomenimis. Tačiau teisės literatūroje nurodoma, kad turinio duomenimis (angl. *communication)* laikoma bet kokia informacija, kuria keičiasi šalys viešųjų elektroninių ryšių paslaugų teikimo atveju. Paprastai tariant, turinio duomenimis laikomas pokalbio telefonu ar susirašinėjimo elektroniniu paštu turinys. Kitai elektroniniais ryšiais perduodamai informacijai priskirtina informacija apie srauto duomenis ir pan.

Manoma, jog procesiniai reikalavimai, taikomi srauto ir turinio duomenims surinkti, turėtų skirtis, nes turinio duomenys atskleidžia komunikacijų turinį, ir neteisėtas jų atkleidimas daro didesnę žalą, palyginti su srauto duomenų neteisėtu atkleidimu. Todėl turinio duomenų kontrolės sankcionavimas turėtų būti griežtesnis. Tačiau reikėtų paminėti, jog nors tradicinėse telekomunikacijose sąlygiškai lengva atskirti turinio duomenis nuo srauto duomenų, kitos susižinojimo formos, pvz., internetas, kuris priskiriamas elektroniniams ryšiams, tokį atskyrimą padaro gana komplikuotą. Turinio ir srauto duomenų atskyrimas buvo lemtas 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 interneto atveju yra gana sudėtingas, jeigu išvis įmanomas. Neaišku, ar turinio duomenimis laikytinas visas elektroninių paketų turinys, ar srauto duomenys yra tik elektroninių paketų antraštės, ar srauto duomenimis laikytini angl. *clickstreams* ar *http* užklausos. Tokiu atveju užklausa „http:///searchengine/com/++aids++homosexuality++symptoms“ būtų laikoma srauto duomenimis, kai minėtoji užklausa yra susijusi su susižinojimo turiniu. Šis pavyzdys verčia atkreipti dėmesį į diskusijų sritį – minėtųjų dviejų kategorijų (turinio duomenų ir srauto duomenų) sujungimo, šias kategorijas kartu pavadinant komunikacijomis (elektroniniais ryšiais), problemą.

Reikia paminėti, jog skirtingai nuo informacijos apie buvusius elektroninių ryšių įvykius gavimo iš elektroninių ryšių paslaugų teikėjų, elektroniniais ryšiais perduodamos informacijos kontrolė realiu laiku atliekama pačių kontroliuojančių subjektų. Pagal Elektroninių ryšių įstatymo 77 str., „kai yra motyvuota teismo nutartis, ūkio subjektai, teikiantys elektroninių ryšių tinklus ir (arba) paslaugas, privalo sudaryti techninę galimybę

kriminalinės žvalgybos subjektams, žvalgybos institucijoms įstatymų nustatyta tvarka, o ikiteisminio tyrimo įstaigoms – Baudžiamojo proceso kodekso nustatyta tvarka, kontroliuoti elektroninių ryšių tinklais perduodamos informacijos turinį."

Elektroniniais ryšiais perduodamos informacijos kontrolė pagal Lietuvos Respublikos įstatymus gali būti atliekama kriminalinės žvalgybos ar baudžiamojo proceso metu.

Lietuvos Respublikos kriminalinės žvalgybos įstatymo 10 str. nurodyta, kad „Elektroninių ryšių tinklais perduodamos asmenų informacijos turinio kontrolė ir jos fiksavimas, net ir žinant apie tokią kontrolę vienam iš jų, reikalauja motyvuotos teismo nutarties, išskyrus atvejus, kai asmuo paprašo arba sutinka su tokia kontrole ar fiksavimu nesinaudojant ūkio subjektų, teikiančių elektroninių ryšių tinklus ir (ar) paslaugas, paslaugomis ir įrenginiais".

Lietuvos Respublikos baudžiamojo kodekso 154 str. nustatyta, jog „<...> ikiteisminio tyrimo pareigūnas gali klausytis telefoninių pokalbių, kontroliuoti kitą elektroninių ryšių tinklais perduodamą informaciją ar daryti įrašus <...>. To paties straipsnio 4 dalyje nurodyta, jog elektroninių ryšių operatoriai privalo sudaryti sąlygas klausytis telefoninių pokalbių ar kontroliuoti kitą telekomunikacijų tinklais perduodamą informaciją ar daryti įrašus."

Lietuvos Respublikos baudžiamojo proceso kodekse kitos nei turinio elektroniniais ryšiais perduodamos informacijos kontrolei nustatytos platesnės galimybės – šią informaciją galima kontroliuoti ir tais atvejais, „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.

3 skirsnis. Privatumas elektroninėje darbo vietoje

Šiuo metu vis labiau plinta darbdavio vykdoma darbuotojo elektroninės darbo vietos kontrolė. Darbdavys nori žinoti, ką darbo metu veikia darbuotojas. Tokiai kontrolei būdingas darbo internete, elektroninio pašto, darbo su programomis, kompiuteryje saugomos elektroninės informacijos tikrinimas. Pastaruoju metu ypač sparčiai plinta *IP* telefonija, todėl elektroninės darbo vietos kontrolė gali apimti ir darbuotojo pokalbių klausymą.

Darbdaviui kontroliuojant elektroninę darbuotojo darbo vietą, susiduria du priešingi interesai: darbuotojo ir darbdavio. Viena vertus,

darbuotojas kaip asmuo turi teisę į asmeninį gyvenimą ir tikisi, kad ši jo teisė nebus pažeista. Kita vertus, egzistuoja daugybė priežasčių, sąlygų ir aplinkybių, kurios verčia darbdavius elektroninėmis priemonėmis stebėti ir kontroliuoti darbuotojus darbo vietoje. Galima paminėti darbo tvarkos ir drausmės užtikrinimo, darbuotojų darbo našumo ir efektyvumo didinimo, darbdavio finansinių išteklių taupymo ir gero vardo išsaugojimo, kompiuterių sistemos apsaugos ir veiksmingumo poreikius ir kt. Visa tai sudaro teisėtą darbdavio verslo interesą.

Elektroninės darbo vietos kontrolės koncepcijos yra skirtingos. Verta pabrėžti, kad skirtingos teisės tradicijos darbdavio ir darbuotojo santykį, kai darbdavys kontroliuoja elektroninę darbuotojo darbo vietą, įtvirtina nevienodai.

JAV Konstitucija istoriškai labai silpnai saugo asmeninį darbuotojų gyvenimą elektroninėje darbo vietoje. JAV federaliniuose ir valstijų teisės aktuose darbuotojų privatumui užtikrinti irgi skiriama labai mažai dėmesio. Vienas iš pagrindinių JAV 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 poreikį, o darbdaviui suteikiama teisė tikrinti elektroninę darbuotojo darbo vietą:

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

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

Elektroninių komunikacijų privatumo įstatymas irgi įgalina darbdavį kontroliuoti elektroninę darbuotojo darbo vietą, remiantis įprastinės verslo eigos išimtimi, jei to reikia, pvz., apsaugoti įmonės teises ar turtą.

Sutikimo išimtis reiškia, kad darbuotojo sutikimas lėmė jo paties teisės į privatumą apribojimą ir suteikė darbdaviui besąlygišką teisę tikrinti jo elektroninę darbo vietą. Sutikimas gali būti išreikštas (pasirašytas) arba numanomas. Pavyzdžiui, preziumuojama, kad darbuotojas davė sutikimą tikrinti elektroninį paštą, jeigu jis, žinodamas apie egzistuojančią tokio 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

jų – *Bourke v. Nissan Corp*. Teismas šioje byloje konstatavo, kad darbdavys turėjo visą teisę tikrinti darbuotojo elektroninį paštą, nes darbuotojas buvo iš anksto informuotas apie tokio tikrinimo galimybę. Jokios įtakos nedarė ir tai, kad darbuotojas turėjo prisijungimo prie kompiuterio slaptažodį, nes jo privatumo tikėjimasis nebuvo objektyviai pagrįstas.

Tiek JAV federaliniai ir valstijų įstatymai, tiek teismo precedentai darbdavio interesams kontroliuoti elektroninę darbuotojo darbo vietą didžiąja dalimi suteikia pirmenybę prieš darbuotojo interesus. Teismų interpretacija daugiausia remiasi tuo, jog elektroninė darbo vieta priklauso darbdaviui, todėl šis pagrįstai reikalauja, kad tokia darbo vieta būtų tinkamai naudojama. Dėl šios priežasties darbdavys JAV turi plačias teises kontroliuoti elektroninę darbuotojo darbo vietą.

Europoje asmeniniam darbuotojų gyvenimui elektroninėje darbo vietoje saugoti skiriama daugiau dėmesio, palyginti su JAV. Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos 8 str. asmenims garantuoja teisę į asmeninį ir šeimos gyvenimą, buto neliečiamybę ir susirašinėjimo slaptumą.

Pagal ES bendrosios duomenų apsaugos direktyvos 95/46/EB 29 str. nuostatas suformuota duomenų apsaugos darbo grupė, kurią sudaro įvairių valstybių duomenų apsaugos institucijų atstovai (toliau – Duomenų apsaugos darbo grupė), pateikia tris elektroninei darbo vietai taikomus principus:

1) darbuotojai gali teisėtai tikėtis privatumo darbo vietoje, ir jis nėra panaikinamas fakto, kad jie naudoja darbdavio komunikacijos įrangą ar kitas verslo priemones. Tačiau tuo atveju, kai darbdavys suteikia tinkamos informacijos darbuotojui, šio teisėti lūkesčiai dėl privatumo gali būti sumažinti, t. y. privatumas elektroninėje darbo vietoje tam tikra prasme gali būti ribojamas;
2) bendrasis korespondencijos slaptumo principas apima komunikacijas darbo vietoje: elektroninį paštą ir su juo susijusius failus. Todėl darbdavys turi žinoti, kad elektroninis paštas irgi patenka į darbuotojo asmeninio gyvenimo sritį;
3) asmeninio gyvenimo gerbimas apima ir teisę kurti bei puoselėti santykius su kitais žmonėmis. Faktas, kad tokie santykiai gana dažnai plėtojami darbo vietoje (pvz., darbuotojas kompiuteriu siunčia elektroninę žinutę auklei norėdamas pasiteirauti, kaip sekasi prižiūrėti vaiką), apriboja teisėtą darbdavio poreikį naudoti sekimo priemones.

Šiuo metu svarbiausias ES 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 (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 specialiai neskirta elektroninei darbo vietos kontrolei reglamentuoti.

Kai kuriose ES valstybėse jau yra priimti teisės aktai, reguliuojantys elektroninės darbo vietos kontrolę. Pirmasis teisės aktas, nacionaliniu lygiu reglamentuojantis privatumą darbo vietoje – 2001 m. Suomijos privatumo apsaugos darbo veikloje įstatymas (nauja redakcija įsigaliojo 2004 m.). Pvz., 6-ame šio įstatymo skyriuje reglamentuojamas darbdaviui priklausančių elektroninių pašto žinučių perėmimas. Be to, nustatyta svarbiausia 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; e. žinutės gali būti atidaromos tik dalyvaujant serverio administratoriui ir kitiems asmenims).

Belgijoje pusiausvyrai tarp darbuotojų privatumo ir darbdavių interesų palaikyti 2002 m. darbuotojų ir darbdavių atstovų buvo pasirašyta Nacionalinė kolektyvinė sutartis Nr. 81, skirta privataus sektoriaus darbuotojų teisei į privatumą apsaugoti, kai renkami elektroninės komunikacijos duomenys darbuotojų kontrolės tikslams. Šioje kolektyvinėje sutartyje apibrėžtos priežastys, pateisinančios darbuotojų kontrolę, kontrolės būdai, kuriuos gali naudoti darbdaviai, ir teisėto surinktų duomenų tvarkymo reikalavimai. Kontrolę pateisinančiomis priežastimis laikoma: neteisėtų šmeižimo veiksmų, kuriais siekiama pažeminti kito asmens orumą, prevencija; darbdavio materialinių ar verslo interesų apsauga; efektyvaus įmonės kompiuterių sistemos veikimo apsauga; vidaus darbo taisyklių laikymasis. Duomenų, susijusių su darbuotojo aplankytais interneto tinklalapiais ar išsiųstų elektroninių laiškų apimtimi ir kiekiu, tvarkymas bus laikomas teisėtu, kol iš tų duomenų nebus įmanoma identifikuoti konkretaus darbuotojo. Galiausiai Belgijoje daugeliu atvejų turi būti gautas darbuotojo sutikimas jį kontroliuoti. Gali būti nustatytas reikalavimas prieš pradedant bet kokį elektroninį duomenų tvarkymą pirmiausia gauti profesinės sąjungos ar kitų kolektyvinių darbuotojų atstovų sutikimą.

Didžiojoje Britanijoje elektroninės darbo vietos kontrolės klausimai detaliai 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 darbo vietos kontrolei. Pabrėžtina, kad šis sąvadas yra rekomendacinio pobūdžio, tačiau papildo 1998 m. Jungtinės Karalystės duomenų apsaugos įstatymą, interpretuoja jo nuostatų taikymą elektroninei darbo kontrolei. Palaikant darbo santykius, praktinis duomenų apsaugos sąvadas

nedraudžia elektroninės darbo vietos kontrolės ir įvardija ją kaip pagrįstą darbo santykių komponentą. Kol darbdaviai laikysis sąvade įtvirtintų gairių, palaikančių balansą tarp darbuotojų privatumo ir darbdavių interesų, elektroninė kontrolė bus teisėta ir pagal Duomenų apsaugos įstatymą. Skaidrumas ir proporcingumas – du svarbiausi principai, kurių privalo laikytis darbdaviai, norintys vykdyti elektroninę kontrolę. Jie privalo informuoti darbuotojus ir kitus susijusius asmenis apie rengiamą ar vykdomą kontrolę (skaidrumas), be to, privalo nutraukti darbo santykiams nereikalingą ir neadekvatų asmens duomenų rinkimą (proporcingumas).

Panašių iniciatyvų esama ir kitose ES valstybėse. Specialūs privatumą elektroninėje darbo vietoje reglamentuojantys teisės aktai galioja Portugalijoje, Austrijoje, Prancūzijoje, Italijoje.

Galima paminėti ir vieną iš didžiausių atgarsių visuomenėje sukėlusių bylų – telekomunikacijų paslaugų teikimo įmonės „Sonera“ Saugos skyriaus darbuotojų privatumo pažeidimo bylą. Penki kaltinamieji – buvę minėtosios įmonės Saugos skyriaus darbuotojai, buvo nuteisti už tai, kad slapta neteisėtai kontroliavo darbuotojų pokalbius telefonu. Ši byla tapo pavyzdžiu kitiems darbdaviams, kad slaptas neteisėtas darbuotojų pokalbių telefonu klausymasis (kontrolė) yra baudžiami kaip kriminaliniai nusikaltimai.

Atskira sritis – darbuotojo pokalbių telefonu ar susirašinėjimo elektroniniu paštu kontrolė. Šios kontrolės metu darbdavys sužino darbuotojo susirašinėjimo su kitais asmenimis turinį.

Padėtis Lietuvoje. Lietuvos Respublikos Konstitucijos 22 str. 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, jog „privatus žmogaus gyvenimas – tai individo asmeninis gyvenimas: gyvenimo būdas, šeiminė 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 pabrėžė, kad teisinė asmeninio gyvenimo samprata siejama su asmens būsena, kai šis gali tikėtis privatumo, su jo teisėtais asmeninio gyvenimo lūkesčiais. Jeigu asmuo vykdo viešojo pobūdžio veikas (nors ir savo namuose ar kitose privačiose valdose) ir tą supranta arba turi ir gali suprasti, tokios viešojo pobūdžio veikos pagal Konstitucijos 22 ir Konvencijos 8 str. nebus apsaugos

objektas, ir asmuo negali tikėtis privatumo. Galima remtis ir Lietuvos Aukščiausiojo Teismo praktika. Byloje *J. Bartasiūnienė v. Viešoji įstaiga „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 turėtų būti gerbiama. Vis dėlto lieka neaišku, kokiais atvejais darbuotojas gali tikėtis privatumo darbo vietoje, o kokiais – ne.

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

Galima teigti, kad Lietuvoje trūksta bent minimalaus teisinio darbuotojo ir darbdavio santykių privatumo apsaugos prasme reglamentavimo. Toks reglamentavimas pageidautinas įstatymo lygmeniu ir jis padėtų išvengti dviprasmybių.

Lietuvos Respublikos Konstitucinis Teismas yra pabrėžęs, 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, kurią Lietuva yra ratifikavusi, 8 str. irgi 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, pvz., 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.

Manytina, kad privatumo ribos darbo vietoje turėtų baigtis ten, kur kėsinamasi padaryti teisės pažeidimą ar nusikaltimą, arba jis yra padaromas, nesilaikoma įstatymų ir darbo sutarties, kitų darbdavio ir darbuotojo susitarimų. Darbuotojui privatumas negali būti garantuojamas ir tuo atveju, kai pažeidžiamas teisėtas darbdavio verslo interesas arba kėsinamasi jį pažeisti. 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 laikomasi darbuotojo ir darbdavio interesų pusiausvyros. Kaip rodo bendrieji teisės principai, negalima teikti pirmenybės darbuotojo asmens privatumo vertybei ir visiškai ignoruoti darbdavio interesų ir, priešingai, turi būti rasta šių dviejų konfliktuojančių interesų pusiausvyra, todėl negalima teigti, kad darbuotojas turi visišką teisę į privatumą arba kad darbdavys turi besąlygišką teisę tikrinti elektroninę darbuotojo darbo vietą.

Svarbiausia, kad praktikoje nebūtų vadovaujamasi vien sutikimo principu. Pernelyg dažnai gali kilti abejonių, kad toks „sutikimas“ duotas laisva valia, nes darbuotojas pagrįstai bijo, kad gali patekti į nepalankią padėtį, jeigu tokio sutikimo neduos.

Svarbiausias principas, kurio turėtų laikytis darbdaviai – proporcingumo. Elektroninės darbo vietos kontrolė turi būti atliekama tada, kai tai neišvengiamai reikalinga. Kai norimas tikslas gali būti pasiektas mažiau privatumą pažeidžiančiomis priemonėmis, darbdavys turėtų apsvarstyti šią galimybę. Pavyzdžiui, darbuotojo kompiuterio kietajame diske saugomos elektroninės informacijos kasdienė įprasta kontrolė neturėtų būti leistina, išskyrus atvejus, kai turima konkrečių įrodymų apie darbuotojo platinamą nelegalią programinę įrangą ar vykdomą kitą neteisėtą veiklą. Darbuotojo susirašinėjimas iš elektroninio pašto dėžutės, priklausančios darbdaviui, galėtų būti kontroliuojamas tik tada, jeigu darbdavys yra nustatęs aiškias taisykles dėl elektroninio pašto naudojimo asmeniniams tikslams būdo ir laiko.

Proporcingos elektroninės darbo vietos kontrolės priemonės irgi turėtų būti aiškiai ir nedviprasmiškai įvardijamos darbo sutartyse ar jų įgyvendinamuosiuose vidiniuose norminiuose dokumentuose (pvz., darbo tvarkos taisyklėse), su kuriais darbuotojas yra supažindinamas.

Kitas svarbus principas – būtinybės. Vadinasi, prieš imdamasis bet kokios elektroninės darbo vietos kontrolės priemonės darbdavys pirmiausia turi įvertinti, ar ši priemonė yra būtina konkrečiam tikslui pasiekti.

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

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

Vadovaudamasis aukščiau išvardytais principais, darbdavys, norėdamas kontroliuoti darbuotojo el. paštą, turėtų nustatyti šiuos pagrindinius aspektus:

- ar darbuotojui leidžiama naudoti el. paštą asmeniniams tikslams;
- kada ir kokiais atvejais darbuotojui leidžiama naudotis asmenine el. pašto dėžute;
- kokiais atvejais yra daromos atsarginės el. pašto žinučių kopijos;
- informacija, kada el. pašto žinutės ištrinamos iš serverio.

Interneto prieigos stebėjimo atveju, kiek įmanoma dažniau, turėtų būti taikomos techninės prieigos kontrolės priemonės, tokios kaip darbdaviui nepriimtinų interneto tinklalapių lankymo uždraudimas. Be to, darbdavys turi nustatyti aiškias taisykles, kada darbuotojui leidžiama asmeniniais tikslais naršyti internete. Darbuotojai turi būti informuojami apie nustatomas technines prieigos kontrolės (apribojimo) priemones.

Lietuvoje jau pradėta plėtoti teismų praktika, kiek tai susiję su privatumu elektroninėje darbo vietoje. 2010 m. gegužės 6 d. Vilniaus apygardos teismas byloje *J. B. v. UAB „Turto administravimo grupė“* priėmė sprendimą, pagal kurį darbdavys turi teisę žinoti, kokiam tikslui darbuotojai naudoja kompiuterius ir kuo užsiima darbo metu, todėl yra teisėta, jeigu vadovas tikrina pavaldinio pokalbius programa *Skype*. Teismo sprendime pabrėžiama, kad darbdavys kompiuterį ir elektroninį ryšį ieškovei suteikė darbinėms pareigoms atlikti. Todėl teismas konstatavo, kad darbdavys turi teisę žinoti, kokiam tikslui yra naudojamos darbo priemonės ir kuo užsiima darbuotojas darbo metu <...> darbdavio pateikti duomenys yra susiję tik su ieškovės J. B. padarytais pažeidimais ir požiūriu į darbdavį, todėl apeliantės teisė į privataus gyvenimo neliečiamumą nepažeista. Šiuo atveju esama požymių, kad teismas mėgino remtis ir JAV teisės tradicija

dėl darbuotojo privatumo darbo vietoje bei joje įtvirtinta teise darbdaviui tikrinti elektroninę darbuotojo darbo vietą, remiantis tiekėjo (angl. *provider)* išimtimi. Vadinasi, jeigu darbdavys sudaro sąlygas darbuotojo darbinėms funkcijoms atlikti naudoti darbdaviui priklausančią el. pašto sistemą, šis turi teisę tikrinti elektroninę darbuotojo darbo vietą. Tačiau pagal ES teisę ir Europos Žmogaus Teisių Teismo jurisprudenciją bylose *Niemietz v. Germany, Halford v. United Kingdom* ir kitose precedentinėse bylose, darbuotojai gali teisėtai tikėtis privatumo elektroninėje darbo vietoje ir ši teisė gali būti ribojama tik remiantis tam tikrais principais. Tai pabrėžiama ir Bendrosios duomenų apsaugos direktyvos 95/46/EB 29 str. darbo grupės dokumentuose (WP55, WP118), kuriuose ir išdėstomi aptartieji principai. Atkreipiamas dėmesys, kad minėtuoju atveju teismas galėjo papildomai išnagrinėti, ar darbdavys buvo nustatęs kokius nors naudojimosi kompiuteriu darbo vietoje tvarkos apribojimus ir ar buvo įspėjęs darbuotojus apie galimybę tikrinti susirašinėjimą ir lankymąsi interneto tinklalapiuose. Todėl kyla abejonių, kad byla išnagrinėta neištyrus visų svarbių jai aplinkybių, ir teismo išvada, jog apeliantės teisė į privataus gyvenimo neliečiamumą nebuvo pažeista, gali būti diskutuotina.

Reikėtų paminėti ir kitą teismo sprendimą – Vilniaus apygardos teismas 2012-12-28 civilinėje byloje Nr. 2A-3217-781/2012 *R. J. v. UAB „Baltic Transport Group"* priėmė nutartį dėl neteisėto atleidimo iš darbo. Šioje nutartyje teismas konstatavo, kad nagrinėjamuoju atveju „darbdavys, suteikęs darbuotojai kompiuterį ir mobiliojo ryšio telefoną darbo funkcijoms atlikti, tačiau nenustatęs darbo priemonių naudojimosi tvarkos apribojimų (lokalinių teisės aktų), iš jų ir dėl draudimo programa *Skype* naudotis asmeniniams tikslams, neįspėjęs dėl to, kad susirašinėjimas ar lankymasis internetiniuose tinklalapiuose bus tikrinami, slapta nurašęs kompiuterio atmintyje esančius programos *Skype* ir lankytų internetinių svetainių adresų duomenis, pažeidė ieškovės privatumą, juolab kad ieškovei buvo leista kompiuteriu naudotis ir asmeniniais tikslais po darbo." Taigi šia nutartimi teismas pasisakė dėl konkrečių darbuotojo veiklos elektroninėje darbo vietoje kontrolės aspektų ir palaikė darbuotojo privatumo apsaugos elektroninėje darbo vietoje koncepciją (esant tam tikroms sąlygoms).

Manytina, kad Lietuvos teismų praktika šioje srityje dar tik pradedama plėtoti.

4 skirsnis. Privatumo ir asmens duomenų teisinės apsaugos aspektai teikiant nuotolinės kompiuterijos *(cloud computing)* paslaugas

1. Nuotolinės kompiuterijos samprata ir požymiai privatumo bei asmens duomenų apsaugos aspektu

Pastaraisiais metais nuotolinė kompiuterija plinta labai sparčiai. Jos paslaugomis naudojasi tiek verslas, tiek organizacijos, tiek privatūs asmenys. Minėtosios kompiuterijos atveju „debesyse“ gali būti saugomi didžiuliai kiekiai asmeninės informacijos: privatūs asmenys gali saugoti savo asmeninę informaciją, o įmonės ar organizacijos – privačių asmenų duomenis.

Kaip yra suprantama nuotolinė kompiuterija ir kokie pagrindiniai jos požymiai? Europos Komisijos nuomone, nuotolinė („debesų“) kompiuterija yra duomenų saugojimas, apdorojimas ir naudojimas toli esančiuose internetu pasiekiamuose kompiuteriuose.

Nuotolinės kompiuterijos samprata pateikiama ir duomenų apsaugos apžvalgoje. Tai – modelis, įgalinantis patogią, pagal vartotojo pareikalavimą galimą interneto prieigą prie konfigūruojamų kompiuterijos išteklių (tinklų, serverių, laikymo, aplikacijų ir paslaugų), kurie gali būti greitai peržiūrimi ir pakeičiami minimaliomis valdymo sąnaudomis arba minimaliu paslaugų teikėjo įsitraukimu. Nuotolinė kompiuterija M. H. Wittowo ir D. J. Bullerio apibrėžiama kaip užsakomosios paslaugos, atliekančios kompiuterijos ir duomenų saugojimo funkcijas, joms naudojama virtuali neribota įranga ir komunikacijos infrastruktūra, kuri yra valdoma trečiosios šalies paslaugų teikėjo.

95/46/EB direktyvos 29 str. darbo grupė nuotolinę kompiuteriją apibrėžia kaip visumą technologinių ar paslauginių modelių, kurie paremti interneto naudojimu, ir suteikia galimybę naudotis IT aplikacijomis, apdorojimo galimybėmis, saugojimu ar atminties vieta.

Anot Europos Komisijos pranešimo, daugelis žmonių šiandien naudojasi nuotoliniais kompiuteriais, apie tai nė negalvodami. Tokios paslaugos kaip el. pašto dėžutės žiniatinklyje ir socialiniai tinklai gali būti pagrįstos nuotoline kompiuterija. Profesionaliems IT vartotojams nuotolinė kompiuterija suteikia daug galimybių rinktis skaičiavimo galią. Pavyzdžiui, kai paslauga naudojamasi intensyviau, labai paprasta jai suteikti daugiau galios. Jeigu tokiam poreikiui patenkinti įmonė į savo duomenų centrą turėtų įdiegti naują įrenginį, tai užtruktų kur kas ilgiau.

Nuotolinės kompiuterijos atveju duomenys gali būti saugomi duomenų centre kur nors pasaulyje. Vartotojams nereikia pirkti programinės įrangos, išlaikyti brangių serverių ir rūpintis duomenų saugojimu. Taip

sutaupoma lėšų, patalpų erdvės, savo IT priežiūros personalo. Be to, vartotojai gali beveik neribotai rinktis vietos duomenims laikyti talpą ir naudojamas priemones. Apklausos rodo, kad 80 proc. įmonių, kurios naudojasi nuotoline kompiuterija, sutaupo bent 10–20 proc. IT skirtų išlaidų, o 20 proc. iš jų teigė sutaupančios 30 proc. ar net daugiau. Daugelis vartotojų jau naudojasi bazinėmis nuotolinės kompiuterijos paslaugomis, pvz., el. pašto paskyromis žiniatinklyje. Daugybė vietos duomenims saugoti nemokamai ar už labai mažą mokestį ir galimybė pasiekti juos iš bet kurios vietos, mažesnės sąnaudos – tik keli nuotolinės kompiuterijos pranašumai. Ši kompiuterija galėtų būti labai naudinga viešajam sektoriui, nes ja naudojantis taptų lengviau teikti integruotas, efektyvesnes ir pigesnes paslaugas. Jos naudojimas galėtų paskatinti mokslinius tyrimus (tyrimų institutai galėtų nuotolinių kompiuterių ištekliais sustiprinti turimas skaičiavimo infrastruktūras ir taip saugoti bei daug sparčiau apdoroti didelius duomenų kiekius) ir inovacijas, nes taptų lengviau ir pigiau išmėginti naujas IT produktų ar paslaugų idėjas.

2. Nuotolinės kompiuterijos privatumo ir asmens duomenų apsaugos rizikos ir jų teisinis reguliavimas

Šiuo metu svarbiausias ES dokumentas, reglamentuojantis nuotolinę kompiuteriją – 95/46/EB direktyva. Ši direktyva taikoma kiekvienu atveju, kai asmens duomenys yra apdorojami kaip nuotolinės kompiuterijos paslaugų teikimo rezultatas.

Kitas dokumentas – 2002/58/EB direktyva, kuri taikoma, kai apdorojami asmens duomenys teikiant viešąsias elektroninių ryšių paslaugas ir kai šios teikiamos paslaugos sudaro nuotolinės kompiuterijos sprendimą.

95/46/EB direktyvos 29 str. nuotolinės kompiuterijos atveju darbo grupė išskiria dvi pagrindines privatumui ir asmens duomenų apsaugai kylančių pavojų kategorijas:

1) kontrolės trūkumas duomenims, saugomiems nuotolinės kompiuterijos būdu.

Pateikiant asmens duomenis į sistemas, valdomas nuotolinės kompiuterijos paslaugų teikėjų, nuotolinės kompiuterijos paslaugų gavėjai (vartotojai) praranda šių duomenų kontrolę ir neturi jokio supratimo apie technines ir organizacines priemones, užtikrinančias asmens duomenų prieinamumą, integralumą ar konfidencialumą;

2) informacijos apie duomenų apdorojimo operacijas trūkumas.

Ši kategorija kelia riziką tiek duomenų valdytojams, tiek duomenų subjektams, nes jie gali nežinoti potencialių grėsmių bei rizikų ir dėl to

negali imtis atitinkamų priemonių. Pavyzdžiui, galimų rizikų gali kilti dėl to, kad duomenų valdytojas nežino šių dalykų:

- „grandininis“ tvarkymas apima daugialypę tvarkytojų ir subkontraktorių grandinę;
- asmens duomenys tvarkomi skirtingose geografinėse vietovėse. Tai tiesiogiai lemia taikomą teisę asmens duomenų apsaugos ginčams, kurie kyla tarp teikėjo ir vartotojo;
- asmens duomenys perduodami į trečiąsias šalis, kurios gali neužtikrinti tinkamo asmens duomenų apsaugos lygio, o pats duomenų perdavimas gali būti neapsaugotas reikiamomis priemonėmis ir būti neteisėtas.

Nuotolinės kompiuterijos atveju galimos ir kitos rizikos. Daug rizikų kyla palaikant nuotolinės kompiuterijos paslaugų teikėjo ir gavėjo santykius. Manytina, kad teikiant nuotolinės kompiuterijos paslaugas yra svarbus šių pagrindinių asmens duomenų apsaugos principų įgyvendinimas:

- *Skaidrumo* (Direktyvos 95/46/EC 10 str. įpareigoja nuotolinės kompiuterijos paslaugų teikėją arba jo atstovą informuoti nuotolinės kompiuterijos paslaugų gavėją, iš kurio renkami su juo susiję duomenys, suteikti informacijos apie duomenų valdytojo tapatybę ir tikslus, dėl kurių ketinama tvarkyti duomenis);
- *Tikslo nustatymo ir apribojimo* (Kaip nurodyta Direktyvos 95/46/EC 6 str. 1 d. b punkte, paskirties nurodymo ir apribojimo principas reikalauja, kad asmens duomenys privalo būti renkami tik įvardytiems, aiškiai apibrėžtiems ir teisėtiems tikslams, paskui tvarkomi su šiais tikslais suderintais būdais);
- *Duomenų sunaikinimo* (Kaip nurodyta Direktyvos 95/46/EC 6 str. 1 d. e punkte, asmens duomenys turi būti laikomi tokio pavidalo, kad duomenų subjektų tapatybes galima būtų nustatyti ne ilgiau, nei tai yra reikalinga tiems tikslams, dėl kurių duomenys buvo surinkti arba paskui tvarkomi);

Svarbūs ir šie principai:

- konfidencialumo;
- prieinamumo;
- integralumo;
- atsakomybės.

Autoriai D. Štitilis ir I. Malinauskaitė 2013 m. atliko tyrimą, kuriame minėtuosius principus ir jų veikimą nagrinėjo nuotolinės kompiuterijos paslaugų teikimo ir sąsajų su sutartiniais paslaugų teikėjų ir vartotojų

santykiais aspektu. Buvo nagrinėjama keturių pasirinktų pasaulinių nuotolinės kompiuterijos paslaugų teikėjų taikoma privatumo politika. Autoriai nustatė, kad daugeliu atvejų nuotolinės kompiuterijos paslaugų teikėjai neatsižvelgia į aukščiau minėtus principus ir prieita prie išvados, kad būtina atidžiau laikytis nuostatų, susijusių su privatumu ir asmens duomenų teisine apsauga.

5 skirsnis. Teisinė privatumo ir asmens duomenų apsauga virtualiuose socialiniuose tinkluose

Pastaruoju metu vis daugiau diskusijų kelia teisinė privatumo ir asmens duomenų apsauga virtualiuose socialiniuose tinkluose. Šie tinklai gali būti suprantami kaip socialinė struktūra, vienijanti tam tikras interesų grupes, kurių nariai (vartotojai) tarpusavyje susiję įvairiais ryšiais (draugyste, giminyste, ekonominiais santykiais, simpatija ar antipatija, seksualiniais ryšiais, religija, išsilavinimu, pomėgiais, socialine padėtimi), motyvuoti dalytis turima informacija, diskutuoti aktualiais klausimais, keistis muzika, vaizdo medžiaga, pristatyti save e. erdvėje ir viešai demonstruoti socialinį aktyvumą.

Svarbiausi virtualių socialinių tinklų elementai – asmeniniai vartotojų profiliai. Į juos kiekvienas asmuo įkelia savo svarbiausius duomenis. Individas, norėdamas tapti virtualaus socialinio tinklo nariu, turi susikurti savo asmeninį profilį, kuriame dažniausiai nurodomas asmens vardas, pavardė, amžius, gyvenamoji vieta, pomėgiai ir kita panaši informacija. Be to, dauguma socialinių tinklų svetainių leidžia vartotojams į savo asmeninį profilį įsikelti nuotraukas ir kitą vaizdinę medžiagą.

Prisijungę prie socialinių tinklų svetainių vartotojai yra skatinami konkrečioje sistemoje susirasti savo pažįstamus asmenis ir taip maksimaliai išplėsti savo virtualų socialinį tinklą. Viešas ryšių demonstravimas irgi yra svarbus socialinių tinklų svetainių elementas. Visiems matomas draugų sąrašas yra tarsi nuoroda į kiekvieno draugo asmeninį profilį, kuris kitiems vartotojams teikia galimybę plėsti savo socialinio tinklo svetainės draugų sąrašą.

Nepaisant internetinių socialinių tinklų teikiamų galimybių, vartotojams labai svarbu valdyti savo privatumą. Internetiniai socialiniai tinklai kaip socializacijos platformos privalo suteikti savo vartotojams galimybę patiems spręsti, kiek ir kokios informacijos padaryti prieinamos skirtingiems asmenims ar interesų grupėms. Tai daroma pasitelkiant techninės priemones, vadinamuosius privatumo nustatymus (angl. *Privacy settings)*. Tokie nustatymai, pateikiami daugelyje didžiausių internetinių socialinių tinklų, leidžia vartotojams reguliuoti savo profilio ar tam tikros informa-

cijos matomumą ir prieinamumą. Privatumo nustatymai dar leidžia nustatyti, kam bus prieinama tam tikrose skirtingose profilio dalyse esanti informacija, atsižvelgiant į galimą profilio stebėtojų auditorijos įvairovę. Pavyzdžiui, socialinio tinklo *Facebook* privatumo nustatymai leidžia reguliuoti informacijos prieinamumą ne tik viso profilio ar tam tikrų jo dalių lygiu, bet ir suteikia vartotojams galimybę nustatyti atskirus prieinamumo lygius kiekvienam įkeltam fotoalbumui, tam tikrai nuotraukai ar net atskirai žymai (angl. *Post)*. Viena iš 2011 m. pristatytų *Facebook* privatumo politikos naujovių yra susijusi su galimybe kontroliuoti, kokią informaciją galima matyti konkretaus kontakto atveju. Nemažiau svarbi ir tais pačiais metais suteikta galimybė vartotojams kontroliuoti savęs žymėjimą (angl. *Tagging)* kitų kontaktų sąraše, esančių asmenų įkeliamose vaizdo medžiagose ar nuotraukose.

Tačiau privatumo nustatymai neretai kritikuojami dėl to, kad vartotojams nėra sukuriamas paprastas jų valdymo mechanizmas. Norint suvokti, kaip naudotis privatumo nustatymais, dažniausiai reikalingas sudėtingas susipažinimo su tam tikromis galimybėmis procesas, kuris iš esmės yra naudingas internetinių socialinių tinklų paslaugų teikėjams, bet ne jų vartotojams. Problemų kelia ir didelės apimties ar sudėtingu stiliumi pateikiami privatumo politikų tekstai. Visa tai verčia susimąstyti, ar toks painumas, sukuriamas ne visada aiškių ir skaidrių privatumo nustatymų, ir nuolatinis internetinių socialinių tinklų privatumo politikos keitimas atitinka teisingumo principą ES duomenų apsaugos direktyvos prasme. Pavyzdžiui, net ir atlikus socialinio tinklo *Facebook* privatumo nustatymų patobulinimus, grindžiamus lengva navigacija ir draugiška vartotojui aplinka, įvairių privatumo apsaugos organizacijų (ir pačių vartotojų) kritikos lygmuo dėl naudojimosi privatumo nustatymais anaiptol nesumažėjo. Manytina, kad viena iš svarbiausių to priežasčių – labai didelis informacijos kiekis, kuriam taikant numatytuosius privatumo nustatymus suteikiamas viešo prieinamumo statusas.

Keblumų kelia ir tai, jog pati procedūra, leidžianti vartotojams atsisakyti leisti prieigą prie savo informacijos, yra gana sudėtinga. Privatumo nustatymai pateikiami ne vienoje vietoje, o išskirstomi į kelias dalis, į jas patenkama spaudžiant nuorodas, kurių tekstinio šrifto dydis paprastai yra gerokai mažesnis, palyginti su įprastai naudojamu visoje socialinio tinklalapio aplinkoje. Dėl šių priežasčių, net ir tiksliai žinant, kokį privatumo nustatymų elementą norima pakeisti, dažniausiai nepavyksta to tinkamai atlikti, nes neaišku, kaip tai padaryti.

Suprasti ir tinkamai reguliuoti privatumo nustatymus vartotojams dar labiau trukdo tai, kad tiek kai kurių privatumo nustatymų valdymo aplinka, tiek pati socialinio tinklo privatumo politika yra tik anglų kalba.

Vadinasi, prastai angliškai mokantys vartotojai neturi galimybės gimtąja kalba susipažinti su privatumo politika ir privatumo nustatymais, kad galėtų visaverčiai valdyti ir kontroliuoti savo pateikiamą asmeninę informaciją. Vis dėlto tokių galimybių interneto socialinių tinklų paslaugų teikėjai nėra linkę suteikti.

Vienas iš teisingumo (sąžiningumo) principo koncepcijos elementų yra interneto socialinių tinklų paslaugų teikėjų įsipareigojimas atsižvelgti į duomenų subjektų (vartotojų) interesus bei teisėtus lūkesčius jų asmeninių duomenų tvarkymo srityje. Kitaip tariant, tokių duomenų rinkimas bei tvarkymas turi būti atliekami taip, kad nebūtų nepagrįstai kišamasi į duomenų subjektų privatumą, ar nepagrįstai pažeidžiamas jų autonomiškumas bei teisė patiems kontroliuoti savo asmeninės informacijos naudojimą. Todėl staigūs ir vienašališki internetinių socialinių tinklų privatumo politikos pakeitimai, neretai didelį duomenų subjektų asmeninės informacijos kiekį padarantys viešai prieinamą pagal numatytuosius nustatymus, neabejotinai neatitinka vartotojų turimų saugumo ir asmeninio privatumo lūkesčių.

Aukščiau išvardytiems aspektams internetiniuose socialiniuose tinkluose sureguliuoti yra arba turi būti pasitelkiami teisės aktai.

Privatumas ir asmens duomenų apsauga virtualiuose socialiniuose tinkluose nereglamentuojami specialiomis teisės normomis. Todėl toliau virtualių socialinių tinklų aspektu bus nagrinėjamas bendrojo pobūdžio ES teisės aktas – 1995 m. Bendroji duomenų apsaugos direktyva.

Tuo metu, kai buvo priiminėjama Direktyva, interneto socialiniai tinklai dar nebuvo paplitę ir nekėlė privatumo bei asmens duomenų teisinės apsaugos problemų. Tačiau kai kurios Direktyvoje nurodomos kategorijos yra glaudžiai susijusios su internetiniais socialiniais tinklais. Viena iš jų – duomenų valdytojo institutas. Pagal Direktyvą, internetinių socialinių tinklų paslaugų teikėjai yra duomenų valdytojai. Jie teikia vartotojo duomenų tvarkymo priemones ir visas pagrindines paslaugas, susijusias su vartotojų valdymu (pvz., paskyrų registracija ir šalinimas).

Internetinių socialinių tinklų kontekste pabrėžiama, kad teisinė Direktyvos kalba, apibūdinanti duomenų valdytojo vaidmenį, gali paskatinti požiūrį, jog vartotojai, internete skelbiantys informaciją apie kitus vartotojus, ar asmenys, kurie internete rastą informaciją apie kitus duomenų subjektus skelbia turėdami tam tikrą tikslą, gali būti vertinami kaip duomenų valdytojai. Todėl ne tik internetinių socialinių tinklų bendrovės, bet ir atskiri vartotojai bei asmenys, kurie naudoja internetiniuose socialiniuose tinkluose skelbiamą informaciją, gali būti klasifikuojami kaip duomenų valdytojai ir tam tikrus reguliacinius reikalavimus pagal duomenų apsaugos direktyvą turintys atitikti subjektai.

Tarp organizacijų ir individualių asmenų kaip duomenų valdytojų (kalbant internetinių socialinių tinklų kontekste) esantis nemažas skirtumas galimybę griežtai ir vienodai taikyti Direktyvą abiem minėtosioms grupėms padaro gana sudėtingą. Nors reikalavimų, skirtų asmens duomenis tvarkantiems valdytojams, Direktyvoje yra daug ir įvairių, tačiau tam, kad būtų atskleistas galimybės vienodai juos taikyti ir individualiems asmenims (vartotojams) sudėtingumas, užtenka aptarti kelis iš jų. Visų pirma Direktyvos 6 str. 1 d. reikalauja, kad asmens duomenys būtų tvarkomi teisingai ir teisėtai. Organizacijoms kaip duomenų valdytojoms ši pareiga teikti nurodytą informaciją yra įprasta. Tuo metu reikalavimas kiekvienam vartotojui (kaip duomenų valdytojui) laikytis šios nuostatos internetinių socialinių tinklų aplinkoje atrodytų neįgyvendinamas. Sunku įsivaizduoti situaciją, kai kiekvienas vartotojas, prieš paskelbdamas tam tikrą informaciją internetinio socialinio tinklo aplinkoje, analizuotų atitinkamus Direktyvą įgyvendinančius vietos įstatymus ir atidžiai tikrintų, ar tokios informacijos skelbimas, tvarkant asmens duomenis, nepažeidžia teisinių teisingumo ir teisėtumo reikalavimų.

Net ir tuo atveju, jeigu vartotojai sugebėtų tinkamai laikytis minėtojo Direktyvos reikalavimo, valdžios institucijoms, atsakingoms už asmens duomenų apsaugą, dėl milžiniško internetinių socialinių tinklų vartotojų kiekio būtų labai sudėtinga kontroliuoti ir užtikrinti nuolatinį šios nuostatos laikymąsi.

Organizacijoms, kaip duomenų valdytojoms, pareiga teikti nurodytą informaciją yra įprasta. Tačiau daugumai internetinių socialinių tinklų vartotojų toks reikalavimas ne tik neįprastas, bet galbūt ir apskritai nežinomas. Pavyzdžiui, asmens duomenis tvarkanti organizacija, siekdama įgyti pasitikėjimą ir paskatinti vartotojus paskelbti savo asmenius duomenis, yra linkusi teikti tokią informaciją duomenų subjektams. Tuo metu individualiems vartotojams paprastai nereikia stengtis tokiu būdu skatinti asmenų aktyvumo, nes informacijos apie duomenų subjektus jie jau turi ir gali ja naudotis.

Be to, galimybė individualiam vartotojui nustatyti, kas bus paskelbtų duomenų gavėjas, yra beveik neįmanoma, nes daugeliu atvejų vartotojų skelbiamai informacijai taikomas prieinamumo statusas „visiems“, vadinasi, prie tokių asmens duomenų visame pasaulyje gali prieiti bet kas.

Antra, Direktyvos 6 str. nustato, jog asmens duomenys turi būti adekvatūs, susiję ir savo apimtimi neviršijantys tikslų, kuriems jie renkami, ir (arba) vėliau tvarkomi. Ši nuostata labiau taikytina organizacijoms, nes individualūs vartotojai patys nusprendžia, kokį asmeninės informacijos apie kitus asmenis kiekį atskleisti savo profilyje, ir tokių veiksmų tikslas kiekvieną kartą gali skirtis, tai priklauso nuo individualaus vartotojo ketinimų.

Trečia, Direktyva ne tik reikalauja, kad duomenų valdytojas gautų duomenų subjekto sutikimą tvarkyti jo asmeninę informaciją, bet ir įpareigoja tokį sutikimą gauti konkrečiam duomenų tvarkymo tikslui. Tokio reikalavimo nustatymas individualiam vartotojui būtų gana nepraktiškas, nes internetiniuose socialiniuose tinkluose skelbiant su kitu asmeniu susijusius duomenis (nuotraukas ar vaizdo medžiagą), nėra įprasta prieš tai atsiklausti minėtosiose laikmenose esančių asmenų ir gauti jų sutikimus.

Be to, konkretus internetinio socialinio tinklo vartotojas, savo paties profilyje skelbdamas tam tikro pobūdžio asmeninę informaciją, ir taip socialinio tinklo paslaugų teikėjui išreikšdamas sutikimą ją tvarkyti, nebūtinai pageidauja (sutinka), kad ji būtų tvarkoma kitų, draugų statusą turinčių, asmenų. Kitaip tariant, vartotojas, skelbdamas asmeninę informaciją, ir privatumo nustatymais nustatęs tokios informacijos prieinamumą uždarai vartotojų grupei, tam tikra prasme išreiškia nesutikimą, kad tokią informaciją gavę asmenys ja disponuotų kartu su kitais subjektais, įskaitant ir trečiuosius asmenis, darbdavius ar kitą platesnę asmenų grupę. Deja, užtikrinti, kad vartotojai nenaudotų tokios informacijos kitiems tikslams, yra labai sudėtinga, jeigu apskritai įmanoma.

Taigi galima apibendrintai teigti, jog galimybės prilyginti internetinių socialinių tinklų vartotojus duomenų valdytojų kategorijai ir griežtai jiems taikyti Direktyvoje esančius reikalavimus yra menkos ir sunkiai įgyvendinamos dėl pernelyg didelės vartotojų kaip socialinės grupės specifikos.

Kalbant apie internetinius socialinius tinklus, itin svarbus ir reikšmingas Direktyvos 29 str. pagrindu įkurtos duomenų apsaugos darbo grupės dokumentas – Nuomonė Nr. 5/2009 dėl socialinių tinklų internete (toliau – Nuomonė). Joje internetinių socialinių tinklų paslauga apibrėžiama kaip internetinės ryšių platformos, leidžiančios žmonėms susisiekti arba kurti tų pačių pažiūrų vartotojų tinklus. Be to, kaip apibrėžiama Direktyvos 98/34/EB, iš dalies pakeistos Direktyvos 98/48/EB 1 str. 2 d., teisiniu požiūriu internetiniai socialiniai tinklai yra informacinės visuomenės paslaugos.

Pabrėžtina, kad Nuomonėje išreiškiamas nemažas susirūpinimas dėl internetiniuose socialiniuose tinkluose naudojamų privatumo nustatymų. Tik nedidelė vartotojų dalis, registruodamiesi internetiniuose socialiniuose tinkluose, atlieka kokius nors numatytųjų nuostatų keitimus. Todėl, darbo grupės nuomone, internetinių socialinių tinklų paslaugų teikėjai privatumo atžvilgiu turėtų teikti patogias numatytąsias nuostatas, suteikiančias galimybę vartotojams laisvai ir aiškiai leisti kokią nors prieigą prie jų profilio turinio, nepasiekiamo jų pasirinktiems adresatams, ir taip sumažinti neteisėto trečiųjų šalių atliekamo duomenų tvarkymo pavojų. Konkrečių darbo siūlymų grupė nepateikė. Autorių nuomone, numatytųjų privatumo

nustatymų turinį prioritetiškai derėtų sieti ne su internetinių socialinių tinklų paslaugų teikėjais, bet su pačiais vartotojais. Tai būtų įmanoma padaryti sukuriant naujų vartotojų registracijos vartus, kur dar prieš pradedant naudotis socialinio tinklo paslaugomis būtų galima atskirai pažymėti kiekvieno elemento privatumo lygį ir nustatyti atitinkamus apribojimus.

Be to, Nuomonėje minimas ir visuomenėje nemažai kritikos sulaukiantis su neaktyviais socialinių tinklų vartotojų profiliais susijęs klausimas. Iš pirmo žvilgsnio gali atrodyti, kad tokių profilių buvimas nekelia didelių pavojų, tačiau atkreiptinas dėmesys, jog vartotojui, tam tikrą laikotarpį nesinaudojančiam internetinio socialinio tinklo paslaugomis, turėtų būti nustatyta, kad profilis yra neaktyvus, t. y. jo daugiau nemato kiti vartotojai arba išorinis pasaulis, o dar po kurio laiko nenaudojamos paskyros duomenys turėtų būti išvis pašalinami. Autorių nuomone, tokios priemonės irgi padėtų išvengti didelio kiekio internetinių platformų „šiukšlių“, o tam tikrais atvejais – išreikšti pagarbą mirusiam vartotojui.

Ypatingas dėmesys darbo grupės Nuomonėje skiriamas vaikų ir nepilnamečių privatumo apsaugos klausimams. Prioritetas teikiamas sąmoningumui ugdyti ir švietimui apie galimus pavojus skatinti. Darbo grupė mano, kad įvairiapusė strategija būtų tinkama sprendžiant vaikų duomenų apsaugos klausimus socialinių tinklų paslaugų srityje. Tokia strategija galėtų būti grindžiama sąmoningumo ugdymo iniciatyvomis, paslaugų teikėjų vykdomu savireguliavimu ir diegiant privatumo didinimo technologijas, įgyvendinant *ad hoc* teisėkūros priemones ir pan.

Galiausiai darbo grupė, apibendrindama Nuomonėje išdėstytą medžiagą, internetinių socialinių tinklų paslaugų teikėjams nurodo savotiškų gairių:

- internetinių socialinių tinklų paslaugų teikėjai turėtų pranešti vartotojams apie savo tapatybę ir suteikti išsamios bei aiškios informacijos apie tikslus, dėl kurių jie ketina tvarkyti asmens duomenis, ir būdus, kaip jie ketina tai daryti;
- internetinių socialinių tinklų paslaugų teikėjai turėtų teikti privatumo atžvilgiu patogias numatytąsias nuostatas;
- vartotojams turėtų būti suteikiama informacijos ir tinkamai įspėjama apie privatumui kylančius pavojus, kai jie įkelia duomenis į socialinių tinklų svetaines;
- vartotojams turėtų būti patariama, kad kitų asmenų nuotraukos arba informacija apie juos gali būti įkelta tik gavus to asmens sutikimą;
- internetinių socialinių tinklų paslaugų teikėjų pradžios tinklalapyje

turėtų būti bendra nuoroda, kur nariai ir ne nariai galėtų pateikti skundų dėl duomenų apsaugos;

- rinkodaros veikla turi atitikti duomenų apsaugos ir e. privatumo direktyvose išdėstytas taisykles;
- internetinių socialinių tinklų paslaugų teikėjai privalo nustatyti maksimalius duomenų arba neaktyvių vartotojų paskyrų saugojimo laikotarpius. Nenaudojamos paskyros turėtų būti šalinamos;
- dėl nepilnamečių internetinių socialinių tinklų paslaugų teikėjai turėtų imtis atitinkamų veiksmų, kad sumažintų pavojų tikimybę.

Nors 29 str. duomenų apsaugos darbo grupės pateikiama nuomonė nėra teisiškai įpareigojanti, reikėtų pabrėžti, kad turint tikslą ateityje sukurti atskirą internetinių socialinių tinklų teisinį reguliavimą, jos indėlis neabejotinai ryškus. Teisiniam reguliavimui tenka nuolat vytis technologijų progresą ir galbūt apskritai neįmanoma spėti laiku reaguoti į dideliu tempu vykstančius pokyčius, tačiau duomenų apsaugos darbo grupės vykdomi pokyčiai yra svarbūs ir, tikėtina, bus sėkmingai tęsiami.

Žinių įtvirtinimo klausimai

1. Ar teisę į privatų gyvenimą galima tapatinti su asmens duomenų apsauga?
2. Kuo skiriasi duomenų valdytojas nuo duomenų tvarkytojo? Ar duomenų valdytojas ir duomenų tvarkytojas gali būti tas pats asmuo?
3. Koks asmens duomenų apsaugos e. erdvėje modelis taikomas Lietuvoje?
4. Kokie yra pagrindiniai asmens duomenų apsaugos e. erdvėje principai?
5. Koks principas – OPT-IN ar OPT-OUT yra nustatytas Lietuvoje tiesioginės rinkodaros atveju?
6. Kokius pagrindinius klausimus reglamentuoja Direktyva dėl privatumo ir asmens duomenų apsaugos elektroniniuose ryšiuose 2002/58/EB?
7. Kiek laiko elektroninių ryšių paslaugų teikėjai gali saugoti elektroninių ryšių srauto duomenis?
8. Kokie reikalavimai taikomi teisėsaugos institucijų vykdomai elektroninių ryšių turinio kontrolei?
9. Kokios yra pagrindinės darbdavio vykdomos elektroninės darbo vietos kontrolės koncepcijos?
10. Kokiais principais turėtų vadovautis Lietuvos darbdavys, siekdamas kontroliuoti elektroninę darbo vietą?

/*VIII*/ *skyrius*

Teisinis asmens identifikavimo elektroninėje erdvėje reguliavimas

/ 379–400 / *puslapiai*

1 skirsnis. Teisinis asmens identifikavimo reguliavimas

1. Tapatybė ir asmens identifikavimas

Tapatybę galima suvokti skirtingai, gali būti tautinė, regioninė, profesinė ar asmens tapatybė, tačiau tai daugiau ne teisinio pobūdžio sąvokos. Tokia tapatybė apima asmens savęs suvokimą per sąsają su kita grupe ar grupėmis. Tokią tapatybę galima pavadinti socialine. Ši tapatybė apima savęs identifikavimą kolektyve ar grupėje, priklausymą tautai, klasei, nusako priklausomumą etninei ar religinei grupėms, tokiai tapatybei priskiriamas ir kultūrinis identitetas.

Moksliniuose šaltiniuose išskiriama kita svarbi sąvoka – medicininė asmens tapatybė. Ji yra pati tiksliausia, su asmeniu vienareikšmiškai susieta tapatybė. Ją galima apibūdinti kaip asmens duomenis ir informaciją, kuri naudojama asmens tapatybei nustatyti, tokia kaip asmens atvaizdas, pirštų atspaudai, išsamus asmens aprašymas (kūno, veido), *DNR* duomenys, kiti ypatingi kūno požymiai (apsigimimai ar turimos fizinės negalios pateikiami kaip papildomi identifikatoriai).

Aktuali asmens tapatybė būtų ta, kurią asmeniui patvirtina valstybė. Tokia tapatybė išreiškiama įrašais į atitinkamus registrus. Valstybės registruose kaupiama ir saugoma informacija apie asmenį gali būti vadinama teisine asmens tapatybe, nes ji sukuriama vadovaujantis konkrečiai teisės normose įtvirtinta tvarka, suteikiant asmeniui skaitinius kodus (asmens kodai, socialinio draudimo numeriai, asmenį identifikuojantys kodai ir kt.) ir valstybės registruose darant įrašus, tiesiogiai susijusius su asmeniu (vardas, pavardė, gimimo data ir kt.). Galima teigti, kad tokią tapatybę kuria tik valstybė, ji gali skirtis nuo socialinės asmens tapatybės. Dabar valstybė, kurdama asmens tapatybę, taiko ne tik aptartąjį įrašų darymo metodą, bet ir modernų medicininį – biometrinį, kuris leidžia išvengti klaidų ir klastočių, nes pasisavinti medicininę asmens tapatybę yra beveik neįmanoma. Gali egzistuoti ir egzistuoja valstybės nekuriama, tačiau jos pripažįstama tapatybė (pvz., saugus identifikavimas per banko sistemą, naudojamas Valstybinės mokesčių inspekcijos paslaugoms gauti ir valdyti).

Be to, galima ir vadinamoji sutartinė tapatybė, kai asmuo identifikuojamas remiantis ne valstybės patvirtintais, o sutartiniais identifikavimo metodais ir priemonėmis. Tokia tapatybė nėra detaliai teisiškai sureguliuota ir todėl gali būti nepatikima, tačiau neretai tokie identifikavimo metodai tinka abiem šalims.

Taigi duomenų, naudojamų asmeniui identifikuoti, visuma ir sudaro mūsų tapatybę. „Tarptautinių žodžių žodyne“ tapatybė lyginama su identitetu – tapatybe, ko nors apibrėžtumu ar individualumu. „Dabartinės

lietuvių kalbos žodyne“ tapatybė – nurodanti objekto lygybę pačiam sau arba kitam objektui, tolygumą, vienodumą.

Detaliau nagrinėjant elektroninės tapatybės sukūrimo ir nustatymo būdus, galima teigti, kad šie būdai skirtingose valstybėse apibrėžiami nevienodai. JAV elektroninė tapatybė – unikalus individualaus asmens pavadinimas. Kadangi asmenų pavadinimai nebūtinai yra unikalūs, elektroninė asmens tapatybė turi suteikti pakankamai papildomos informacijos, kad būtų sukurta visiškai unikali elektroninė tapatybė. Kiek kitokį elektroninės tapatybės apibrėžimą pateikia Naujosios Zelandijos institucijos: elektroninė tapatybė – nustatyta grupė požymių ir (ar) duomenų, susijusių su konkrečiu asmeniu. Tačiau nenurodoma, ar tokia tapatybė gali būti prilyginama teisinei (išskyrus atvejus, kai naudojamos atitinkamos e. parašo technologijos ir sprendimai) ir kokie duomenys turi būti naudojami norint sukurti unikalią elektroninę asmens tapatybę. Taigi dėl elektroninės asmens tapatybės kyla daug klausimų, į kuriuos galima atsakyti išnagrinėjus e. identifikavimą ir teisinį reguliavimą.

Taigi, kaip tapatybė reglamentuojama fizinėje ir elektroninėje erdvėse?

2. Asmens identifikavimo sąvoka ir samprata

Asmens tapatumas, identitetas (lot. *identitas* (buvimas) – tai subjektyvus savęs kaip individo supratimas. Jis nusako žmogaus arba daikto savybių visumą, pagal kurią mes atskiriame jį nuo kitų.

„Tarptautinių žodžių žodyne“ asmens identifikavimas (angl. *Personal identity)* suprantamas kaip asmens tapatybės nustatymas. Kitais žodžiais tariant, identifikavimas – asmens pripažinimas juo pačiu. Plintant elektroninių ryšių naudojimui, identifikavimas perkeliamas ir į e. erdvę.

Identifikacija informacinėse sistemose gali būti suvokiama kaip identifikatoriaus paskyrimas subjektams ir objektams arba identifikatoriaus ir priskirto identifikatoriaus sąrašo palyginimas, pvz., identifikavimas naudojant brūkšninį kodą. Asmens tapatybė gali būti nustatoma naudojant biometrinius, rašytinius ar finansinius identifikatorius. Kartais identifikavimas kaip vartotojų tapatybės nustatymas gali būti klaidinamai aiškinamas vietoj sąvokų „autentifikacija“ arba „autorizacija“. Identifikacija ir autentifikacija – tai sampratos, kurios mūsų gyvenime visada egzistuoja viena šalia kitos. „Tarptautinių žodžių žodyne“ žodis „autentifikavimas“ suprantamas kaip nustatymas ar atitinkantis originalą. Kitais žodžiais tariant, autentifikacija – tai procesas, kurio metu vartotojo įvesti duomenys yra palyginami su duomenų bazėje apie šį vartotoją esančia informacija.

Kai kalbame apie asmens identifikavimą, neišvengiamai susiduriame su „asmens duomenų“ sąvoka.

Asmens duomenys – bet kokia informacija apie fizinį asmenį, leidžianti tiesiogiai ar netiesiogiai nustatyti jo tapatybę – šiuolaikiniame virtualiame pasaulyje yra itin vertinga prekė. Tapatybė gali būti tiesiogiai ar netiesiogiai nustatoma naudojantis tokiais duomenimis kaip asmens kodas, vienas arba keli asmeniui būdingi fizinio, fiziologinio, ekonominio, kultūrinio ar socialinio pobūdžio požymiai.

Minėtųjų teisės normų analizė leidžia daryti išvadą, kad asmens duomenų sąvoka yra labai plati ir apima daug duomenų, kurie *prima facie* turi menką ryšį su konkrečiu asmeniu, ir jais remiantis gali būti nustatoma tapatybė. Taigi asmens tapatybė – individo atitikimo nustatymas, naudojant pakankamą duomenų ir priemonių asmeniui identifikuoti visumą.

3. Asmens identifikavimas fizinėje erdvėje

Palyginimui trumpai aprašytinas asmens identifikavimas fizinėje erdvėje, jis vykdomas naudojant vieną iš jam privalomų priemonių – tinkamą asmens dokumentą. Toks identifikavimas, naudojant oficialius valstybės išduotus dokumentus, gali būti vadinamas oficialiuoju. Galimas ir kitoks identifikavimo fizinėje erdvėje būdas – naudojant ne valstybės, o kitų subjektų išduotus dokumentus (pvz., darbuotojo pažymėjimą), tačiau šis identifikavimas yra lokalus ir nebus nagrinėjamas šiame moksliniame straipsnyje.

Reikėtų paminėti, kad identifikavimas fizinėje erdvėje vyksta tik tam tikromis numatytomis aplinkybėmis (pvz., kai valstybė įsakmiai nurodo identifikavimo būtinybę), o daugumai santykių jis apskritai nebūtinas. Galima pateikti paprastos parduotuvės atvejį, kai nereikalaujama identifikuoti perkančiojo prekę asmens, nes vyksta momentinis sandoris ir atsiskaitoma iš karto, t. y. prekės pirkimo metu.

Vis dėlto, kai reikia identifikuoti asmenį, dažniausiai naudojami oficialūs valstybės patvirtinti dokumentai. Galima teigti, kad oficialiuose asmens dokumentuose patvirtinti duomenys ir formuoja asmens tapatybę fizinėje erdvėje. Tačiau kaip atsiranda tapatybė fizinėje erdvėje ir kas tą tapatybę patvirtina?

Fizinės asmens tapatybės suteikimo procesas prasideda asmeniui tik gimus. Lietuvoje apie vaiko gimimą turi būti pranešta, ir šis civilinės metrikacijos įstaigoje turi būti užregistruotas per tris mėnesius nuo jo gimimo dienos. Registruojant gimimą, turi būti pateiktas sveikatos priežiūros įstaigos arba gydytojų konsultacinės komisijos išduotas vaiko gimimo pažymėjimas, būtent juo ir yra patvirtinamas vaiko gimimo faktas bei laikas[51]. Šis vaiko gimimo pažymėjimas yra pirmieji fiksuoti asmens duomenys, kurie vėliau naudojami įrašant gimimo įrašą ir išduodant gimimo liudijimą.

[51] Būtent nuo šio momento ir atsiranda asmens tapatybė.

Asmeniui gimus, civilinės metrikacijos įstaiga suformuoja naują įrašą pagrindinėje Lietuvos Respublikos gyventojų duomenų bazėje – Gyventojų registre. Institucija, kuriai pavesta rinkti, kaupti, apdoroti ir saugoti asmens duomenis (apie Lietuvos Respublikos piliečius, asmenis be pilietybės ir kitų valstybių piliečius, deklaruojančius gyvenamąją vietą Lietuvoje ar registruojančius asmens civilinės būklės pasikeitimus Lietuvos Respublikos institucijose), teikti šiuos duomenis Lietuvos Respublikos valdžios ir valdymo institucijoms, vietos savivaldos institucijoms, valstybės registrams bei kitiems juridiniams ir fiziniams asmenims įstatymų ir kitų teisės aktų nustatyta tvarka – Gyventojų registro tarnyba prie Lietuvos Respublikos vidaus reikalų ministerijos. Ši institucija valdo Gyventojų registrą.

Gyventojų registro tarnyba operuoja svarbiausiais identifikuoti skirtais asmens tapatybės duomenimis, šiai vienintelei institucijai pavesta funkcija kaupti visus duomenis, kuriuos pasitelkus gali būti formuojama asmens tapatybė.

Gyventojų registre kaupiami asmens duomenys sudaro tapatybės turinį (elementus), tačiau visų šių duomenų neprireikia kasdienėje asmens veikloje. Šie Gyventojų registre kaupiami asmens duomenys naudojami asmenims išduodant atitinkamus oficialius dokumentus, kuriais fizinėje erdvėje gali būti identifikuojamas fizinis asmuo.

Asmens tapatybę patvirtinantys dokumentai gali būti: gimimo liudijimas, asmens tapatybės kortelė, pasas, naujojo pavyzdžio vairuotojo pažymėjimas – svarbiausi, teisiškai pripažįstami dokumentai, kurie patvirtina asmens tapatybę fizinėje erdvėje. Tokius dokumentus išduoda tik valstybės įgaliotosios institucijos, ir jie yra vienintelė teisėta tapatybės nustatymo priemonė Lietuvoje. Kiekvienas iš šių dokumentų skirtas tam tikram konkrečiam tikslui, todėl jie nesidubliuoja[52], be to, šiuose dokumentuose nurodoma tiek asmens duomenų, kiek būtina konkrečiam teisiniam santykiui.

Gimimo liudijimas – pirmasis svarbiausias vaiko dokumentas, kuris patvirtina jo tapatybę ir kilmę. Kaip vienintelis dokumentas gimimo liudijimas išlieka, kol vaikas sulaukia atitinkamo amžiaus (pilnametystės) ir gauna asmens tapatybės kortelę arba pasą. Lietuvos Respublikos pilietis nuo šešiolikos metų privalo turėti asmens tapatybės kortelę, jeigu jis neturi galiojančio Lietuvos Respublikos išduoto paso. Verta pabrėžti, kad asmens tapatybės kortelė yra Lietuvos Respublikos piliečio asmens dokumentas, patvirtinantis jo asmens tapatybę bei pilietybę, ir skirtas naudoti Lietuvos Respublikoje. O pasas yra Lietuvos Respublikos piliečio asmens dokumentas, patvirtinantis jo asmens tapatybę bei pilietybę, ir skirtas vykti į užsienio

[52] Išskyrus paso ir kortelės atvejį.

valstybes arba naudoti Lietuvos Respublikoje. Taigi Lietuvos Respublikos teisės aktai nustato, kad šešiolikos metų sulaukęs Lietuvos pilietis privalo turėti pasą arba asmens tapatybės kortelę kaip asmens tapatybę patvirtinantį dokumentą. Į šiuos abu dokumentus yra įrašoma: vardas, pavardė, lytis, gimimo data, asmens kodas ir pilietybė. Pase papildomai dar nurodoma vieta, kur asmuo gimė, dėl to šie du dokumentai vienas nuo kito šiek tiek skiriasi. Šis skirtumas susijęs su paso paskirtimi identifikuoti į užsienio valstybes vykstantį asmenį.

Vairuotojo pažymėjimas – teisės aktų nustatyta tvarka išduotas dokumentas, kuriuo patvirtinama asmens teisė vairuoti tam tikros kategorijos motorinę transporto priemonę (priemones) ir nurodomos vairavimo sąlygos. Iš šio apibrėžimo matyti, kad vairuotojo pažymėjimas Lietuvos Respublikoje nėra laikomas asmens tapatybę patvirtinančiu dokumentu, nors ES valstybėse ir JAV tokiu jau pripažįstamas.

Duomenys, kurie įrašomi į vairuotojo pažymėjimus, atitinka duomenis, esančius teisėtai pripažintuose asmens tapatybę patvirtinančiuose dokumentuose. Remiantis Lietuvos Respublikos gyventojų registro duomenų centrine baze, į asmens tapatybės kortelę įrašoma: piliečio vardas, pavardė, lytis, gimimo data, asmens kodas, pilietybė, veido atvaizdas ir parašas. Šiuos duomenis kaip būtinus vairuotojo pažymėjimo elementus nustato ir 2006 m. gruodžio 20 d. Europos Parlamento ir Tarybos direktyvos 2006/126/EB II priedas.

Taigi nustatyti asmens tapatybę fizinėje erdvėje gana paprasta – tereikia paprašyti jo tapatybę patvirtinančio dokumento ir įsitikinti, kad dokumentas nėra suklastotas ar naudojamas neteisėtiems tikslams.

4. Asmens identifikavimas elektroninėje erdvėje

Valstybėms, plėtojančioms e. paslaugas, iškilo poreikis identifikuoti asmenis ne tik fizinėje, bet ir e. erdvėje. Tapatybės turinys fizinėje erdvėje, neatsižvelgiant į naudojamą asmens tapatybę patvirtinantį dokumentą, yra panašus. Tuo metu e. erdvėje neįmanoma pateikti oficialaus tradicinio asmens tapatybę nustatančio ne elektroninio dokumento, tačiau asmenims labai dažnai prireikia patvirtinti savo tapatybę ir šioje terpėje.

Reikėtų paminėti, kad, palyginti su fizine erdve, identifikavimo atvejų e. erdvėje kiekis sąlygiškai didesnis. Taigi e. erdvėje gerokai dažniau prireikia naudoti asmeninę informaciją, ir vien tai, anot H. E. Higginso, lemia daugiau tapatybės vagysčių atvejų *(Higgins G. E.*, 2010).

Elektroninė erdvė identifikavimo aspektu pasižymi tam tikra specifika, ir norint joje identifikuotis nereikia fiziškai būti atitinkamoje geografinėje vietoje – efektyvius veiksmus galima atlikti per atstumą. Tokie veiksmai

gali būti: e. informacijos perdavimas, kaupimas, apdorojimas ar naudojimas, dėl to asmenims nereikia būti konkrečioje vietoje, jeigu jie nori pasinaudoti tokia informacija arba atlikti efektyvų veiksmą.

Tad kyla klausimas, kokios tapatybės patvirtinimo priemonės naudojamos e. erdvėje? Ir kokie oficialūs valstybės patvirtinti identifikavimo metodai?

Didžioji dalis elektroninių paslaugų sistemų naudoja panašias asmens identifikavimo priemones. Apibendrinus ir sugrupavus, galima išskirti šiuos svarbiausius asmens identifikavimo e. erdvėje elementus:

– identifikavimas pagal tai, ką vartotojas žino;
– identifikavimas pagal tai, ką vartotojas turi;
– identifikavimas pagal tai, kas vartotojas yra;
– kiti identifikavimo e. erdvėje metodai.

Identifikavimas pagal tai, ką vartotojas žino

Asmuo e. erdvėje gali būti identifikuojamas pagal unikalų pavadinimą (vardą) ir slaptažodį. Fizinėje erdvėje asmenų vardai gali kartotis, tačiau toje pačioje e. sistemoje asmens tapatybė turi būti nustatoma naudojant unikalų identifikatorių. Tai lemia pačių sistemų specifika – negali būti tokių pačių vardų, žyminčių skirtingus asmenis. Pasirinktas slaptažodis paprastai būna sudarytas iš ženklų eilutės. Tokio metodo patikimumas priklauso nuo informacinės sistemos apsaugos lygio. Trumpi slaptažodžiai yra nesaugūs, o ilgus ir sudėtingus sunku įsiminti. Tokių sistemų saugumas priklauso nuo pačių vartotojų. Jeigu vartotojai nesaugiai naudos savo identifikavimo elementus, tokią tapatybę bus galima lengvai pasisavinti. Šiuo identifikavimo principu naudojasi didžioji dalis žinomų elektroninių paslaugų teikėjų:

- komunikacijos paslaugos: el. paštas, elektroninės konferencijos, ryšio paslaugos *VoIP* ir kt.;
- elektroninė komercija: e. parduotuvės, kiti subjektai, teikiantys elektronines paslaugas, alternatyvūs elektroniniai atsiskaitymai ir kt.;
- socialiniai tinklai, virtualios bendruomenės ir kt.

Jeigu tokius pat socialinius santykius analizuotume fizinėje erdvėje, matytume, kad identifikavimas panašiais atvejais gali išvis neįvykti, be to, rastume daug atvejų, kai fizinio asmens tapatybė išvis nereikšminga (pvz., svarbu, kad būtų sumokamas atlygis). Tuo metu e. erdvėje momentinių sandorių beveik nebūna, tad net dėl menkiausios operacijos reikalinga identifikuoti asmenį. Ir, kaip matome, toks identifikavimas dažnai būna sutartinis.

Identifikavimas pagal tai, ką vartotojas turi

Šiuo principu grindžiamas kliento atpažinimas pagal turimas priemones: e. parašas (patvirtintas e. sertifikatu), kodų generatoriai ir lentelės. Palyginti su fizine erdve, tai yra būtent valstybės reguliuojama (ar pripažįstama) tapatybė.

Elektroniniu parašu duomenys pasirašomi, naudojant jo formavimo duomenis, o patikrinami juos atitinkančiais elektroninio parašo tikrinimo duomenimis. Elektroninio parašo pagrindų direktyvoje apibrėžiama, jog vykstant šiam procesui identifikavimo kriterijus užtikrinamas pasitelkiant trečiąjį asmenį – sertifikavimo paslaugų teikėją, kuris per išduodamą sertifikatą susieja pasirašančiojo asmens tapatybę su parašo formavimo ir tikrinimo duomenimis bei suteikia galimybę bet kam susipažinti su sertifikatu ir pagal šiame įrašytus tikrinimo duomenis įsitikinti, kad pasirašęs asmuo yra tas pats, kokiu save nurodo.

Elektroninis asmens sertifikatas sukurtas remiantis matematiniais algoritmais, jo patikimumas yra garantuojamas patvirtintų standartų. Toks sertifikatas teoriškai yra saugesnis už bet kokį asmens dokumentą. Tačiau jo saugumas priklauso ir nuo jį turinčio asmens, nes pats sertifikatas yra apsaugotas slaptažodžiu, o šį praradus kyla rizika, kad kas nors gali pasinaudoti elektroniniu sertifikatu ir identifikuoti save kaip kitą asmenį. Rizika dar labiau padidėja dėl fizinio kontakto nebuvimo, galimybės pamesti sertifikato laikmeną.

Aptartoji sertifikatais paremta elektroninė tapatybė šiuo metu plačiai naudojama asmenų, siekiančių gauti valstybės institucijų teikiamas e. paslaugas. Institucijos identifikuoja asmenis pagal jų elektroninius sertifikatus ir ne tik juos. Viešojo administravimo institucijų informacinių sistemų interoperabilumo sistemos funkcionavimo taisyklėse nurodyta, kad jungiantis prie viešojo administravimo institucijų informacinių sistemų asmens tapatybė gali būti nustatoma naudojant e. parašą, patvirtintą kvalifikuotu sertifikatu, bei elektroninės bankininkystės sistemas.

Be to, galima ir valstybės pripažįstama elektroninė tapatybė. Elektroninės bankininkystės paslaugos naudoja savo identifikavimo sistemą, kuri susieja du identifikavimo e. erdvėje elementus: „Tai ką žino“ ir „Tai ką turi“, ir kurią pripažįsta valstybė.

Banko naudojamos apsaugos priemonės klientams identifikuoti:[53]

1) atpažinimo kodas – unikali skaitmenų seka, naudojama asmens tapatybei nustatyti registruojantis sistemoje;

[53] Parengta vadovaujantis Lietuvoje veikiančių komercinių bankų paslaugų teikimo sutartimis.

2) slaptažodis – unikali skaitmenų seka, naudojama asmens tapatybei patvirtinti registruojantis sistemoje, slaptažodį bankas rekomenduoja sudaryti iš raidžių, skaičių ar simbolių ir reguliariai jį keisti.

Banko naudojamos atpažinimo priemonės klientams identifikuoti:

- slaptažodžių kortelė, kurioje nurodyti sunumeruoti slaptažodžiai, įvedami į sistemą ryšio seanso pradžioje arba patvirtinant operacijas;
- slaptažodžių generatorius, kuris pagal specialų algoritmą kiekvieną kartą registruojantis sistemoje sudaro unikalų slaptažodį – skaitmenų seką.

Klientas savo nuožiūra pasirenka vartotojui suteikiamą atpažinimo priemonę. Vartotojas turi žinoti savo unikalų numerį sistemoje ir slaptažodį, kurį jis nuolat keičia, bei turėti vieną iš atpažinimo priemonių. Pasirinktų slaptažodžių generatorių gaunamos skaitinės išraiškos niekada nesikartoja, priešingai nei slaptažodžių kortelėje.

Vartotojo autentiškumas laikomas patvirtintas, jeigu šis ryšio seanso pradžioje teisingai panaudojo banko suteiktas atpažinimo ir apsaugos priemones, o bankas gavo vartotojo informaciją apie jo registravimąsi sistemoje. Bankas pripažįsta ir laiko vartotojo pasirašytais bei patvirtintais banko sistema gautus pranešimus apie kliento sąskaitose esančių lėšų naudojimą, sutarčių sudarymą, sutarties sąlygų pakeitimą, papildymą, termino pratęsimą arba sutarties nutraukimą ir kitą informaciją, jeigu ryšio seanso pradžioje buvo nurodytos teisingos atpažinimo ir apsaugos priemonės, kitaip tariant, bankas pripažįsta šią identifikavimo sistemą kaip elektroninį sertifikatą ir visus patvirtintus dokumentus laiko lygiaverčiais rašytiniams.

Šiuo metodu vykdomas identifikavimas atitinka tikrąją – formalią – asmens tapatybę, tai užtikrina institucijos, išduodančios elektroninius sertifikatus, ir bankai, vadovaudamiesi svarbiausiu principu – tinkamu kliento identifikavimu.

2009 m. sausį Lietuvoje atsirado dar viena asmens identifikavimo galimybė – elektroninė asmens tapatybės kortelė. Minėtoji kortelė (toliau – *eID*) yra asmens tapatybę ir Lietuvos Respublikos pilietybę patvirtinantis dokumentas. *eID* suteikia galimybę pasirašyti e. dokumentus saugiu e. parašu, o informacinėms sistemoms ir kitiems paslaugų teikėjams – identifikuoti asmenį, kuris, siųsdamas duomenis internetu, jungiasi prie informacinių sistemų ir registrų. *eID* kortelių teikiama asmens atpažinimo e. erdvėje galimybe galima naudotis tik tuo atveju, jeigu tokią galimybę aiškiai deklaruoja elektroninės paslaugos ar interneto portalai, kurie turi įgyvendintą reikiamą bei saugią sąsają vartotojui atpažinti sertifikatu. Identifikavimo dokumentas e. aplinkoje reikalingas asmenų santykiams su

valstybe, privačiomis struktūromis ar tarp pačių asmenų palaikyti. Tačiau norint naudotis elektronine asmens tapatybės kortele pirmiausia reikia pasirūpinti lustinės kortelės skaitytuvu, t. y. įsigyti vidinį (esantį klaviatūroje) arba išorinį (prijungiamą prie kompiuterio) kortelės skaitytuvą (angl. *smart card reader)*. Asmens tapatybės kortelės gali būti naudojamos kaip e. dokumentų pasirašymo ir asmens atpažinimo e. erdvėje priemonė jungiantis prie elektronines paslaugas teikiančių interneto portalų, pvz., elektroninės valdžios portalo *www.epaslaugos.lt*. Suteikiama galimybė prisijungti prie VĮ „Regitra“, VĮ Registrų centro, Lietuvos darbo biržos e. paslaugų, Valstybinės mokesčių inspekcijos e. deklaravimo sistemos, „Sodros“ elektroninės gyventojų aptarnavimo sistemos (*EGAS*) ir kt. Siekiama, kad elektroninę asmens tapatybės kortelę naudotų ir finansines paslaugas teikiančios organizacijos.

Identifikavimas pagal tai, kas yra vartotojas

Šiuo atveju naudojami biometriniai tapatybės elementai leidžia identifikuoti asmenį pagal jo specifines fiziologines arba elgesio charakteristikas. Naudojamos nekintančios asmeninės charakteristikos reikalauja specialios įrangos. Dažniausiai naudojami: pirštų antspaudai, akies tinklainės ar rainelės skenavimas. Ne tokie patikimi metodai: veido atvaizdavimas, rankos geometrija, parašo ar balso atpažinimas. Tokios technologijos turi daug pranašumų:

- biometrinės charakteristikos negali būti perduotos kitam žmogui;
- biometrinės technikos neleidžia atsirasti klaidoms, susijusioms su netiksliu vertinimu, atsirandančiu dėl išankstinės nuomonės, išsiblaškymo ar nuovargio;
- žmogui nereikia nešiotis jokių papildomų daiktų (paso, mokėjimo kortelės) ar prisiminti kokių nors slaptažodžių ir kodų.

Taigi biometrija – unikali, išmatuojama asmens charakteristika, skirta automatiniam identifikavimui ar patikrinimui. Biometriniai duomenys naudojami siekiant greitai automatiškai nustatyti asmens tapatybę, t. y. realiu laiku. Identifikavimas per biometrines technologijas reiškia, kad lyginamas anksčiau įvestas biometrinis pavyzdys su naujai įvestais biometriniais duomenimis. Jeigu kalbėtume apie identifikavimą, sistema mėgina išsiaiškinti, kam priklauso nurodytasis pavyzdys, lyginant jį su turima duomenų baze ir siekiant rasti atitikmenį.

Nors ši technologija iš aptartųjų pati saugiausia, jos kaina ir integravimo sudėtingumas verčia rinktis kitas (pigesnes) asmens identifikavimo priemones.

Kiti identifikavimo elektroninėje erdvėje metodai

Slapukai – pats populiariausias identifikacijos internete metodas, tai maži duomenų paketai, sukuriami interneto puslapio serverio ir laikomi vartotojo kietajame diske. Slapukai buvo sukurti siekiant padėti klientui naudotis serveriu bei rinkti duomenis ir jie gali būti serverio vertinami dabartinio ar vėlesnio apsilankymo tinklalapyje metu.

Svetainės naudoja slapukus, kad galėtų vartotojams pasiūlyti personalizuotą naudojimo patirtį ir surinkti informaciją apie svetainės lankomumą. Slapukas gali pagerinti patikimos svetainės darbą, leisdamas sužinoti prioritetus. Tačiau kai kurie iš jų gali kelti grėsmę privatumui ir sekti lankomas svetaines. Kadangi slapuke gali būti individo tapatybę atskleidžiantys duomenys: prisijungimo *IP* adresas, specialiai tam asmeniui sukurtas unikalus naudotojo identifikatorius (unikalus žymuo) ir kt. Užsiregistravęs interneto svetainėje ir pateikęs paslaugoms teikti reikalingus duomenis, pvz., vardą, el. pašto adresą, darbo ar gyvenamosios vietos adresą, telefono numerį, vartotojas pats suteikia galimybę paslaugų teikėjui naudotis šiais duomenimis.

IP adreso svarba. *IP* adresas yra unikalus kiekvieno kompiuterio adresas internete, kuris leidžia identifikuoti jo buvimo vietą tam tikru momentu. Viešai prieinama informacija yra tik apie šalį, miestą ir interneto prieigos teikėją arba organizaciją, kuriai priklauso tas *IP* adresas.

Nors *IP* adresas neskirtas pačiam kompiuteriui ar jo vartotojui identifikuoti, nes jis gali būti nepastovus, be to, *IP* adresu gali naudotis daug vartotojų ar dėl kitų priežasčių. Tačiau pasitaiko atvejų, kai siekiant identifikuoti interneto abonentą ar naudotoją leidžiama įpareigoti interneto prieigos paslaugų teikėją atskleisti abonento, kuriam suteiktas *IP* adresas, tapatybę (2012 m. balandžio 19 d. Teisingumo Teismo byla C461/10). Interneto paslaugų teikėjo vidinių duomenų bazių įrašai leidžia vienareikšmiškai nustatyti fizinį ar juridinį asmenį, kuriam tam tikru momentu buvo suteiktas atitinkamas *IP* adresas.

Darbo grupė 29 str. norėtų akcentuoti, kad interneto vartotojams priskirti *IP* adresai yra asmens duomenys ir jie yra saugomi ES direktyvų 95/46 ir 97/66. Kaip apibrėžiama Direktyvos 95/46 26 konstatuojamoje dalyje, duomenys laikomi asmens duomenimis, kai juos pasitelkęs duomenų valdytojas ar bet kuris kitas asmuo, naudodamas deramas priemones, nustato duomenų subjekto tapatybę (šiuo atveju *IP* adreso vartotojo). *IP* adresų atveju, *ISP* visada gali nustatyti ryšį tarp vartotojo tapatybės ir *IP* adresų, kaip ir kitos šalys, pvz., pasinaudojusios prieinamu *IP* adresų registru ar kitomis egzistuojančiomis techninėmis priemonėmis.

Ši darbo grupė dar nurodė, kad jeigu unikalus identifikatorius (sąsajos identifikatorius, pvz., kurio pagrindas yra unikalus *MAC* adresas tinklo plokštėje) yra integruotas į vartotojo kiekvieno elektroninės komunikacijos prietaiso *IP* adresą, tokiu atveju visi vartotojo pranešimai gali būti susieti tarpusavyje daug lengviau negu naudojant dabar egzistuojančius slapukus. Taigi reikėtų pabrėžti, jog laikui bėgant *IP* ir *MAC* adresas taps vis svarbesnis kaip tapatybės nustatymo priemonė.

MAC adresas – tai unikalus serijos numeris, suteikiamas kiekvienam prie tinklo prijungiamam įrenginiui, siekiant jį identifikuoti tinkle. *MAC* adresas yra šešių baitų (48 bitų) apimties, paprastai užrašomas šešioliktainiais, pvz., 00:34:56:78:90:AB. *MAC* adresą sudaro ženklai: 0-9, A-F. Detalesnė *MAC* adreso struktūra nustatoma tarptautiniame standarte ISO/IEC 10039. Jis gamintojo tvirtai „įsiuvamas“ į tinklo plokštes ir yra nepakeičiamas. Tokiu būdu pasaulyje negali būti dviejų vienodų *MAC* adresų, tai užtikrina tikslų informacijos pateikimą nuo jos ištakų iki gavėjo. *MAC* adreso supažindinimo vadove nurodoma, kad galiniai įrenginiai naudoja dviejų tipų adresus: vienas generuojamas adresas remiasi unikaliu *MAC* adresu ir yra naudojamas ryšiui užmegzti (pvz., terminalas visada pasiekiamas, naudojant nuolatinį adresą) ir kitas generuojamas adresas, kuris remiasi atsitiktiniu (pseudo) pagrindu, naudojamas terminalo išeinamiesiems ryšiams. Taigi kai terminalas (ir vartotojas už jo) yra atsakingas už ryšį, jis negali būti identifikuojamas, naudojantis jo *MAC* adresu.

Taigi identifikacija naudojant *MAC* adresą gali užtikrinti aukštą patikimumo lygį nustatant adresato „tapatybę“. Jis pasitelkiamas per keitimosi informacija procesą tik kaip papildoma apsaugos priemonė, siekiant patikrinti, iš kokio prietaiso informacija buvo perduota ir kokiu prietaisu gauta. Norėdama tai padaryti, viena šalis turi žinoti kitos *MAC* adresą. Tokia apsauga naudojama, kai prisijungia keletas interneto paslaugų teikėjų, tačiau svarbi būna ir prisijungiant prie *Wi-Fi* tinklo, kai reikalaujama susieti konkrečius *MAC* adresus, kad būtų galima vienareikšmiškai identifikuoti nereikalaujant slaptažodžių. Šis metodas naudojamas kuriant privačius tinklus.

5. Elektroninė asmens tapatybė ir jos teisinis reguliavimas

Vienas iš svarbiausių klausimų, susijusių su elektroninės tapatybės teisiniu reguliavimu, yra tokios tapatybės sukūrimas[54]. Kaip jau minėta, e. erdvėje tapatybė nustatoma dažniausiai pagal tai, ką vartotojas turi (patvirtinta tapatybė), tačiau per pastaruosius kelerius metus e. erdvėje atsirado kitų,

[54] Pirmoji iniciatyva – ES šalyse vykdomas projektas STORK (angl. *Secure idenTity acrOss boRders linKed)*. Prieiga per internetą: <www.eid-stork.eu>.

vartotojo pasirinktų, tapatybių, kurios skirstomos pagal profilius, sukuriamus oficialioje arba asmeninėje aplinkoje.

5.1. Identifikavimo elektroninėje erdvėje pagal tai, ką vartotojas turi žinoti, teisinis reguliavimas

Paminėtina, kad šio identifikavimo būdo valstybė nereglamentuoja. Vadinasi, toks identifikavimo mechanizmas – paslaugos teikėjo ir kliento reikalas. Praktikoje asmenų pasirinkti unikalūs vardai dažniausiai neturi nieko bendra su tikrosiomis tapatybėmis. Vartotojai, registruodamiesi tokiose sistemose, nėra įpareigoti patvirtinti savo tikrąją tapatybę, bet tokia sukurta tapatybė tampa asmens duomenimis, kurių apsaugą užtikrina teisės aktai. Elektroninio pašto adresas neretai tampa vienu iš svarbiausių tapatybę identifikuojančių elementų e. erdvėje. Tačiau elektroninio pašto paslaugų teikėjai netikrina asmens tapatybių jiems registruojantis, taip sudarydami palankias sąlygas tapatybės klastotojams. Elektroninio pašto identifikavimo sistemų sąlygiškas paprastumas, galimybė pasisavinti vartotojų vardus ir slaptažodžius kelia rimtą problemą – elektroninės tapatybės praradimą.

Problemų kyla ir dėl sparčiai internete plintančių socialinių tinklų. Jie įgalina savo tapatybę ir socialinius ryšius perkelti į e. erdvę. Socialiniai tinklai tampa ne tik bendravimo priemone, bet ir verslo vykdymo, darbinių santykių plėtojimo terpe, kur kiekviena elektroninė tapatybė asocijuojasi su tikrąja – egzistuojančiu asmeniu. Asmenys registruojasi, į tokius tinklus perkelia savo asmens duomenis, tačiau neturi garantijų, kad jų tapatybės kas nors nepasisavins. Registruojantis į tokius socialinius tinklus naudojamasi el. paštu, būtent šis ir pasirinktas slaptažodis tampa elektronine tapatybe. Tačiau patikimų identifikavimo priemonių netaikymas ir sąlygiškai paprastas registravimosi būdas didina riziką, kad socialiniai tinklai bus naudojami nusikalstamai veikai. 2010 m. rugsėjį nusikaltėliai pasisavino Interpolo vadovo socialinio tinklo *Facebook* tapatybę. Jo vardu buvo sukurti du netikri profiliai, nusikaltėliai juos naudojo siekdami gauti informacijos apie tarptautinės policijos agentūros atliekamas operacijas. Socialinių tinklų saugumas dėl registravimosi paprastumo tampa pasauline problema.

5.2. Identifikavimo elektroninėje erdvėje pagal tai, ką vartotojas turi, reglamentavimas

Šią elektroninę tapatybę ir jos kūrimo tvarką valstybė imperatyviai reguliuoja. Teisiškai pripažįstamas ir reguliuojamas asmens identifikavimo būdas e. erdvėje – e. sertifikatas ir e. parašas. Elektroninis sertifikatas – tai elektroninis liudijimas, kuris susieja parašo tikrinimo duomenis su pasirašančiuoju asmeniu ir patvirtina arba leidžia nustatyti šio tapatybę.

Elektroninis parašas – duomenys, kurie įterpiami, prijungiami ar logiškai susiejami su kitais duomenimis pastarųjų autentiškumui patvirtinti ir (ar) pasirašančiajam asmeniui identifikuoti. Detaliau e. sertifikatą kaip asmens tapatybės patvirtinimo e. erdvėje būdą apibrėžia Tapatybės kortelės įstatymas: „Asmens atpažinimo elektroninėje erdvėje sertifikatas – elektroninis liudijimas su įrašytais, nurodytais ir vidaus reikalų ministro nustatytais techniniais duomenimis ir patvirtinantis arba leidžiantis nustatyti asmens tapatybę elektroninėje erdvėje.“ Aiškiai nurodoma jo paskirtis – nustatyti asmens tapatybę, o į sertifikatą įrašomi asmens duomenys atitinka tapatybės kortelės duomenis: vardas (vardai), pavardė, lytis, gimimo data, asmens kodas, pilietybė.

Paminėtina administracinė byla Nr. A-143-2740-12 dėl asmens kodo naudojimo e. parašo sertifikate. Bylos priešistorė ta, kad Valstybinė duomenų apsaugos inspekcija, pagal asmens pranešime pateiktą informaciją atlikusi patikrinimą VĮ Registrų centre, nustatė, kad Elektroninio parašo įstatymas nenustato imperatyvios teisės normos, t. y. neįtvirtina asmens kodo kaip privalomo duomens naudojimo kvalifikuotame sertifikate, skirtame e. dokumentams pasirašyti, todėl, vadovaujantis ADTAĮ 3 str. 1 d. 4 p., asmens kodo naudojimas, pasirašant e. dokumentus, laikytinas pertekliniu asmens duomeniu. Valstybinės duomenų apsaugos inspekcijos nuomone, VĮ Registrų centras, sudarydamas sertifikatą ir į jį įrašydamas asmens kodą kaip perteklinį asmens duomenį, pažeidžia ADTAĮ 3 str. 1 d. 4 punktą. VDAI 2011 m. lapkritį VĮ Registrų centrui pateikė nurodymą atsisakyti asmens kodo naudojimo kvalifikuotame sertifikate, skirtame e. dokumentams ir e. laiškams pasirašyti. Registrų centras šį nurodymą apskundė Vilniaus apygardos administraciniam teismui ir šis minėtąjį nurodymą panaikino. Teismas nustatė, kad asmens kodas gali būti laikomas kvalifikuotame sertifikate nurodomu specialiu atributu pagal Elektroninio parašo įstatymo 2 str. 15 d. 4 p., jeigu jis reikalingas atsižvelgiant į sertifikato naudojimo tikslus. Be to, nurodė, kad įstatymų leidėjas nesuteikia teisės VDAI uždrausti trečiajam asmeniui leisti naudoti asmens kodą jo sutikimu (dėl asmens kodo naudojimo asmuo pasirašo sutikimą). Teismas konstatavo, kad Inspekcijos nurodymas yra neteisėtas ir nepagrįstas. VDAI pateikė apeliacinį skundą LVAT ir paprašė panaikinti pirmosios instancijos teismo sprendimą. LVAT 2012-12-18 sprendimu Inspekcijos apeliacinį skundą patenkino. Teismas nurodė, kad, sprendžiant šį klausimą, specialiuoju įstatymu laikytinas ne Elektroninio parašo įstatymas, o Asmens duomenų teisinės apsaugos įstatymas (ADTAĮ). Anot LVAT, Asmens duomenų teisinės apsaugos įstatymo 7 str. 4 d. nustatytas asmens kodo naudojimo būdas – jo viešas paskelbimas – yra imperatyviai draudžiamas. Aiškindama šią teisės

normą lingvistiniu teisės aiškinimo metodu, kolegija pabrėžia, kad, pagal „Dabartinės lietuvių kalbos žodyną“, viena iš žodžio „viešas“ reikšmių yra atviras, neslaptas, o žodžio „skelbti“ – skleisti žinias (Dabartinės lietuvių kalbos žodynas, Lietuvių kalbos institutas, Vilnius, 2000, 701, 931 psl.). Aptartoji situacija dėl asmens kodo atskleidimo – e. parašu pasirašyto e. dokumento persiuntimo šio asmens požiūriu neapibrėžtam asmenų kiekiui, kolegijos manymu, iš esmės atitinka nurodytas žodžių „skelbti viešai“ reikšmes. Tai leidžia kolegijai daryti išvadą, kad byloje nagrinėjamoje situacijoje įžvelgtinas ir Asmens duomenų teisinės apsaugos įstatymo 7 str. 4 d. nustatyto draudimo pažeidimas. Taigi pareiškėjo VĮ Registrų centro skundas buvo pripažintas nepagrįstu, o pirmosios instancijos teismo sprendimas panaikintas. Po šio sprendimo VĮ Registrų centras turėtų koreguoti asmens kodų naudojimo politiką, ir asmens kodus elektroniniuose sertifikatuose naudoti tik turėdamas duomenų subjekto sutikimą.

Lietuvoje yra trys e. sertifikatų ir kvalifikuotų e. parašų paslaugų teikėjai.[55] Visi jie turi teisę sukurti galiojančią ir patvirtintą asmens elektroninę tapatybę[56], kuri teisiškai yra lygiavertė fizinei, patvirtintai galiojančiais asmens dokumentais. Tačiau aptartuosius asmens dokumentus turi teisę išduoti tik valstybinės institucijos, kurios garantuoja tokių dokumentų autentiškumą ir tikrumą. Tuo metu elektroninę asmens tapatybę gali kurti ir nevalstybinės įstaigos. Žinoma, neturėtų būti formuojama nuomonė, kad tai nėra saugu, tačiau jeigu valstybė yra atsakinga už asmenų tapatybės turinio formavimą ir tokių duomenų kaupimą bei saugojimą, ar nederėtų tokio pat mechanizmo taikyti ir kuriant e. tapatybę?

Valstybės pripažįstamos tapatybės atveju ši e. tapatybė turi teisinę galią, nes remiasi Lietuvos Respublikos elektroninio parašo įstatymo 8 str. 3 d. nuostata: „Elektroninis parašas visais atvejais turi šio straipsnio 1 dalyje įtvirtintą teisinę galią, jeigu parašų naudotojai tarpusavyje dėl to susitaria“. LR Vyriausybės nutarime „Dėl kliento tapatybės nustatymo bei informacijos apie operacijas pinigais pateikimo tvarkos“ nustatyta, kad kreditų įstaigos ir kiti subjektai, privalantys nustatyti kliento tapatybę, reikalauja iš kliento jo tapatybę identifikuojančių galiojančių dokumentų. Banko ir kliento susitarimas, kad tam tikra banko sistema atitinka saugios sistemos požymius, minima įstatymo teisės norma bei identifikavimas remiantis šia sistema ir lemia faktą, jog minėtoji identifikavimo sistema yra pripažįstama valstybės.

[55] UAB Skaitmeninio sertifikavimo centras, VĮ Registrų centras, Gyventojų registro tarnyba prie Lietuvos Respublikos vidaus reikalų ministerijos.

[56] Paminėtina, kad elektroninį parašą galima turėti ne vieną (paremtą skirtingomis sistemomis), skirtingai nei fizinėje erdvėje, teisėtai niekada negalima turėti dviejų to paties dokumento originalų.

Teisinis elektroninės asmens tapatybės kortelės reguliavimas. Nuostatos dėl elektroninės asmens tapatybės kortelės naudojimo yra įtvirtintos Asmens tapatybės kortelės įstatyme. Šio įstatymo 2 str. 3 d. nustatyta, jog nuo 2009 m. gaminama asmens tapatybės kortelė gali būti naudojama asmens tapatybei e. erdvėje patvirtinti ar nustatyti ir e. duomenims pasirašyti. Asmens tapatybės kortelėje, be kitų duomenų, elektroniniu būdu fiksuojami piliečio veido atvaizdas ir pirštų antspaudai, asmens atpažinimo e. erdvėje sertifikatas[57] ir kvalifikuotas sertifikatas.

5.3. Identifikavimo elektroninėje erdvėje pagal tai, kas yra vartotojas, reglamentavimas

Kadangi vadovaujantis proporcingumo principu tam, kad būtų pasiektas svarbiausias tikslas – įvesti bendrus apsaugos standartus ir sąveikius biometrinius identifikatorius, yra būtina ir tikslinga visoms valstybėms narėms nustatyti vienodas taisykles. Tai Reglamento (EB) Nr. 2252/2004 dėl valstybių narių išduodamų pasų ir kelionės dokumentų apsauginių savybių ir biometrikos standartų 1 str. 2 d. nustato skaitmeninį veido atvaizdą ir pirštų antspaudus kaip privalomas ES pasų biometrines savybes. Duomenys turi būti apsaugoti, o laikmena – pakankamos talpos ir galios, kad būtų garantuotas duomenų integralumas, autentiškumas ir konfidencialumas. Biometriniai duomenys į pasą ar kelionės dokumentą integruojami siekiant sukurti patikimą sąsają tarp dokumento ir tikrojo jo savininko.

Galima teigti, kad biometrinio identifikavimo reglamentavimo srityje yra žengti tik pirmieji žingsniai, nes teisinis reglamentavimas apima tik asmens duomenų įtvirtinimą pasuose, vizose ir leidimuose. ES priimti privalomojo pobūdžio teisės aktai nustato tik pirštų antspaudų ir veido atvaizdo naudojimą nurodytuose asmens tapatybę patvirtinančiuose dokumentuose. Visą kitą informaciją, kaip šie identifikatoriai turėtų būti naudojami, randame rekomendacinio pobūdžio dokumentuose ir *ISO* standartuose.

Teisės aktai iš principo šio identifikavimo būdo nereglamentuoja, išskyrus tik biometrinių duomenų, saugomų tapatybės kortelėje, reguliavimą.

5.4. Kiti asmens identifikavimo elektroninėje erdvėje metodai ir jų teisinis reguliavimas

Jeigu tokie įtaisai kaip „sausainėliai“ naudojami teisėtiems tikslams, juos naudoti leidžiama tik su sąlyga, kad vartotojai aiškiai ir tiksliai pagal Direktyvą 95/46/EB informuojami apie jų naudojimo tikslus tam, kad žinotų, kokia informacija pateikiama į jų naudojamą galinį įrenginį. Vartotojams

[57] Asmens atpažinimo e. sertifikatas leidžia nustatyti asmens tapatybę e. erdvėje.

turėtų būti suteikiama galimybė atsisakyti „sausainėlio“. Tai ypač svarbu tada, kai kiti vartotojai prieina prie pagrindinio vartotojo galinio įrenginio, taigi ir prie jame saugomų privačių duomenų. Informacija, kaip tokie įtaisai bus naudojami, vartotojui pateikiama kartu su teise jų atsisakyti prieš įrengiant jo galiniame įrenginyje grupę tokių įtaisų vienu prijungimu, kartu nurodant, kaip jie galės būti naudojami po vėlesnių prijungimų. Informacija pateikiama, atsisakymo teisė primenama arba vartotojo sutikimo prašoma jam patogiais būdais.

Lietuvoje įgyvendinus Europos Parlamento ir Tarybos privatumo elektroniniuose ryšiuose direktyvą, 2011 m. rugpjūčio 1 d. įsigaliojo Elektroninių ryšių įstatymo pakeitimai, įtvirtinantys reikalavimą, kad paslaugų vartotojo galiniuose įrenginiuose (kompiuteriuose, išmaniuosiuose telefonuose ir kt.) slapukai gali būti išsaugomi tik turint išankstinį šio asmens sutikimą. Išimtis, kai vartotojo sutikimo nereikia, yra taikoma tik tiems slapukams, kurie yra būtini tam, kad vartotojas gautų tik tas informacinės visuomenės paslaugas, kurias užsisakė (Elektroninių ryšių įstatymo 61 str. 4 d.). Vadinasi, prieš įrašydamas slapukus į vartotojo kompiuterį ir vėliau juos naudodamas, informacinės visuomenės paslaugų teikėjas turės gauti vartotojo sutikimą.

Tuo metu minėtoji direktyva numato: „svarbiausia, kad paslaugų gavėjai, užsiimdami veikla, dėl kurios jų įrenginyje gali būti saugoma informacija arba jie gali suteikti minėtą prieigą, gautų aiškią ir išsamią informaciją apie tai.“

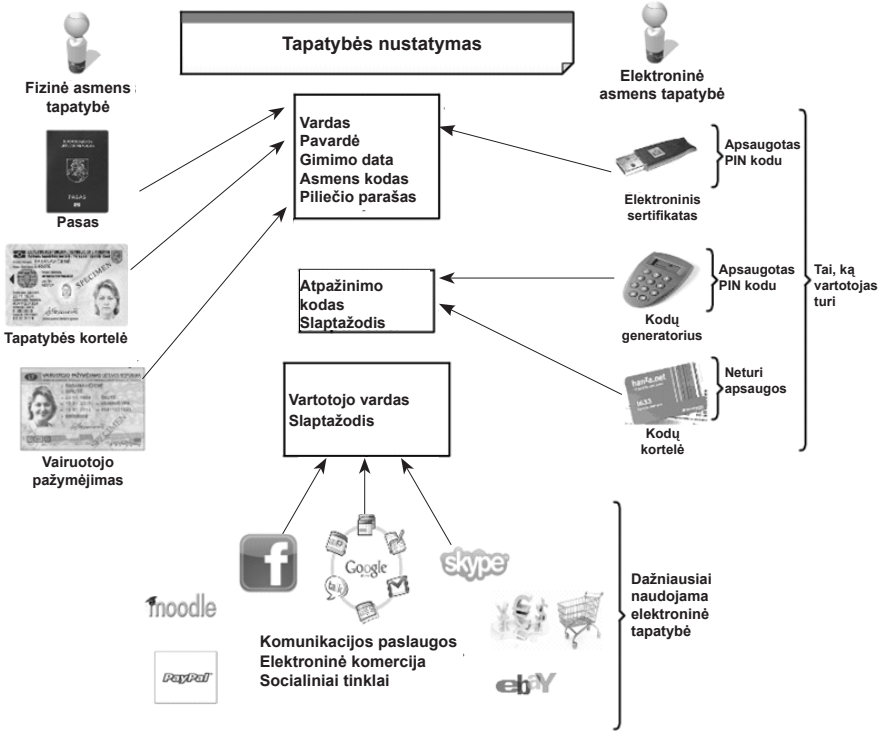
Kartais tinklalapiuose yra numatoma slapukų naudojimo politika, tai atitinka Parlamento ir Tarybos privatumo palaikant e. ryšius direktyvą ir joje nustatytą visuomenės informavimo principą. Taigi slapukų naudojimo politikoje deklaruojama, kad administratoriai juos naudos atpažindami asmenį kaip ankstesnį svetainės lankytoją ir rinkdami svetainės lankomumo statistiką. Jie suteikia galimybę bet kada peržiūrėti, kokia informacija buvo įrašyta, leidžia atšaukti duotą sutikimą ištrindami įrašytus slapukus ar palieka teisę nesutikti, kad slapukai būtų įrašomi į vartotojo kompiuterį (įrenginį), tačiau tokiu atveju kai kurios svetainės funkcijos gali tapti neprieinamos (privatumo politika).

MAC ir *IP* adresai yra reglamentuoti teisės aktuose – kaip technologija, t. y. reglamentuota *MAC, IP* sandara. *IP* adresų naudojimas bei identifikavimo teisinė galia yra nustatyta keliose ESTT bylose, kuriose pabrėžiama, kad *IP* adresas identifikuoja tik įrenginį, kuriuo buvo pasinaudota tam tikram veiksmui atlikti, o ne asmenį, kuris tai padarė. Tačiau *IP* adresas priskiriamas prie asmens duomenų ir jam būtina teisinė asmens duomenų apsauga. Dėl slapukų naudojimo galime taikyti platesnį reglamentavimą

tiek tarptautiniu, tiek nacionaliniu lygmeniu. Be to, daugelis interneto svetainių, naudojančių slapukus, turi sukūrusios savo slapukų naudojimo politiką, su kuria vartotojas gali lengvai susipažinti ir sutikti ar nesutikti naudotis šia paslauga.

6. Minimalių identifikavimo reikalavimų elektroninėje erdvėje nustatymo prielaidos

Elektroninių identifikavimo būdų ir priemonių naudojimą bei santykį su realiu asmeniu galima pavaizduoti grafiškai (žr. 8 paveikslą, kur pateikiama apibendrinta informacija dėl asmens tapatybės nustatymo tiek fizinėje, tiek elektroninėje erdvėje priemonių). Kairėje paveikslo pusėje pavaizduotos asmens tapatybės nustatymo fizinėje erdvėje priemonės. Dešinėje – nurodytos patvirtintos elektroninės tapatybės priemonės, kai asmuo gali būti vienareikšmiškai nustatytas, o paveikslo apačioje pateikiamos dažniausiai naudojamos nepatvirtintos tapatybės priemonės.



8 pav. Asmens tapatybės nustatymas
(Štitilis, Pakutinskas, Dauparaitė, Laurinaitis, 2011).

Tuo atveju, kai tapatybė nepatvirtinta, dažniausiai remiamasi vienu rodikliu, o šie yra lengviau suklastojami ir ne tokie saugūs. Tapatybės vagysčių atvejai patys dažniausi būtent tokio tipo sistemose. Elektroninėje erdvėje dažniausiai naudojama pačių vartotojų sukurta tapatybė, kurią pasisavinti nėra sudėtinga.

Asmeninėje aplinkoje naudojamas identifikavimas sukuria daugiau problemų, išplečia ir papildo tapatumo nustatymo būdus, nes vartotojai skirtingose sistemose naudoja įvairius tapatybės nustatymo būdus. Taip susiklosto situacijos, kai vienas asmuo turi 20, 30 ir daugiau elektroninių identifikavimo priemonių. Šios identifikavimo priemonės dažnai pamirštamos, dėl to daugėja elektroninių tapatybių šiukšlių.

Gali kilti klausimas, ar reikia garantuoti teisę turėti teisingą, neiškreiptą elektroninę tapatybę. Ši teisė apima sąlygiškai naujus teisinius santykius, kai subjektas pagrįstai tikisi, kad jo elektroninė tapatybė tinkamai jį identifikuos ir niekas kitas tokios tapatybės negalės turėti. Ši teisė yra glaudžiai susijusi su kontekstinės vientisumo tapatybės idėja, ji apsaugo nuo neteisingo identifikavimo. Paminėtinas ir vartotojų teisių apsaugos aspektas, kuriuo remdamasi valstybė turėtų imtis tam tikrų priemonių ir pašalinti lengvai prieinamus būdus pasisavinti atitinkamo vartotojo tapatybę (dėl to atitinkamam vartotojui padaryti vienokios ar kitokios žalos).

Dažnai akcentuojama vartotojų pasirinkimo laisvė kuriant elektroninę tapatybę, bet tai kartais verčia rinktis pigesnes identifikavimo sistemas. Vartotojai susiduria su daugybe identifikavimo sistemų ir metodų, kurie susieja skirtingus tapatybės elementus, taiko nevienodus standartus ir techninius procesus. Sunku suprasti, kaip kiekviena sistema veikia, ir jas naudoti. Reikia spręsti švietimo ir sąmoningumo problemas taip, kad vartotojai galėtų tinkamai valdyti savo elektronines tapatybes. Švietimas yra svarbus kuriant pasitikėjimą ir mažinant vartotojų susirūpinimą. Pagrindinis informatyvumo didinimo elementas – atskaitomybė ir aukštas skaidrumo lygis. Tačiau klausimų dėl daugybės sudėtingų sistemų kyla vis daugiau. Atsižvelgiant į tai, turėtų būti parengtos priemonės, kuriomis bus siekiama gilinti piliečių žinias ir apsvarstyti būdus, kaip pareikalauti didesnio elektroninės tapatybės paslaugų teikėjų atskaitingumo.

Kitas klausimas, ar galima verslui privalomai nurodyti, kaip sukurti saugias ir valstybės pripažįstamas tapatybes. Viena vertus, kištis į verslą yra nevykusi praktika. Kita vertus, siekiant užtikrinti vartotojų teisių apsaugą, tam tikri valstybės privalomi nurodymai netgi pageidautini.

Manytina, kad optimaliausias variantas – pati rinka turėtų nuspręsti, kokias konkrečias identifikavimo priemones naudoti, tačiau tai daryti turėtų paskatinti valstybė (naudodama teisinį reguliavimą). Valstybė turėtų

nustatyti minimalius identifikavimo e. erdvėje reikalavimus. Reikėtų nurodyti, kurie duomenys ir tapatybės elementai turi būti vienodi skirtingose sektoriuose, identifikuojant asmenį e. erdvėje. Derėtų sutarti ir perimti atitinkamą praktiką iš valstybės, kai tapatybei kurti e. erdvėje naudojami tie patys asmens duomenys kaip ir fizinėje erdvėje.

Dar siūlytina teisės normose numatyti, kad jeigu naudojamos nepatikimos identifikavimo priemonės (nepripažįstamos valstybės), paslaugos teikėjas yra atsakingas[58] už neteisėtais veiksmais sukeltus padarinius. Todėl manytina, kad toks reguliavimas paskatintų rinką pradėti naudoti patikimas identifikavimo priemones (paremtas tuo, ką vartotojas turi). Ir rinka, remdamasi technologijų neutralumo principu, pati galėtų pasirinkti naudotiną technologiją.

Be to, paminėtina, kad egzistuoja atitinkamos problemos, kurios užkerta kelią e. tapatybės plėtrai. Su elektronine asmens tapatybe susijusių sąvokų nebuvimas: „pilnas“, „dalinis tapatumo identifikatorius“, „virtuali tapatybė“, „interneto vartotojų profiliai“, šiuo metu tai nėra teisiškai apibrėžta. Aiškių bendrų sąvokų nebuvimas iškreipia vertinimą, trukdo pasiekti bendrą teisinį sutarimą minėtojo apibrėžimo klausimu. Be to, nėra bendros terminijos skirtinguose teisės šaltiniuose. Konkrečių apibrėžimų būtinumas atsiranda dėl santykių e. erdvėje ir jų paplitimo. Įvairių paslaugų teikimas elektroniniu būdu reikalauja nustatyti šalis, jų teises ir pareigas, numatyti būdus, kuriais subjektai identifikuojami (vardas, pavardė, numeris, organizacija, įstaiga), tokio identifikatoriaus atsekamumą, šalių autentifikaciją, ir, be viso to, subjektas dar turi žinoti ir paslaugų teikėjo tapatybę.

2012 m. ES kilo viena iš svarbesnių teisinio reguliavimo iniciatyvų, kiek tai susiję su asmens identifikavimu: paskelbtas pasiūlymas Europos Parlamento ir Tarybos reglamentui dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje[59]. Šio siūlymo pagrindu 2014 m. buvo priimtas Europos Parlamento ir Tarybos reglamentas (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB. Nors reglamentas įsigaliojo 2014 m. rugsėjo 17 d., didžioji dalis nuostatų bus pradėtos taikyti nuo 2016 m. liepos 1 dienos. Iki to laiko planuojama atlikti reikiamus teisės aktų pakeitimus. Reglamento reguliavimo apimtis išplečiama ir apima elektroninę atpažintį, elektroninius dokumentus ir patikimumo užtikrinimo paslaugas.

[58] Prievolė atlyginti atsiradusius nuostolius.

[59] Pasiūlymas Europos Parlamento ir Tarybos reglamentui dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, Briuselis, 2012-06-04, COM(2012)238final.

Šio reglamento tikslas – užtikrinti, kad naudojantis valstybių narių siūlomomis tarpvalstybinėmis internetinėmis paslaugomis būtų galima užtikrinti saugią elektroninę atpažintį ir tapatumo nustatymą. Vienas šio reglamento uždavinių – pašalinti esamas valstybėse narėse naudojamų elektroninės atpažinties priemonių, reikalingų tapatybei nustatyti bent siekiant pasinaudoti viešosiomis paslaugomis, tarpvalstybinio naudojimo kliūtis. Šiuo reglamentu nesiekiama kištis į valstybėse narėse įdiegtas elektroninės atpažinties valdymo sistemas ir su jomis susijusias infrastruktūras.

Reglamente valstybėms narėms paliekama laisvė elektroninės atpažinties tikslams diegti priemones, reikalingas norint naudotis internetinėmis paslaugomis. Be to, joms suteikiama galimybė spręsti, ar į tų priemonių užtikrinimą įtraukti privatųjį sektorių. Valstybės narės neįpareigojamos pranešti Komisijai apie savo elektroninės atpažinties schemas. Valstybės narės turės pačios spręsti, ar pranešti Komisijai apie visas elektroninės atpažinties schemas, nacionaliniu lygiu taikomas tam, kad būtų galima pasinaudoti bent viešosiomis internetinėmis paslaugomis arba tam tikromis paslaugomis, ar pranešti tik apie kai kurias schemas, ar išvis apie jas nepranešti.

Reglamente nustatytos tam tikros sąlygos, numatančios, kurios elektroninės atpažinties priemonės turi būti pripažįstamos ir kokiu būdu turėtų būti pranešama apie elektroninės atpažinties schemas. Tos sąlygos turėtų padėti valstybėms narėms įgyti būtiną pasitikėjimą viena kitos elektroninės atpažinties schemomis ir abipusiai pripažinti elektroninės atpažinties priemones, kurioms taikomos schemos, apie kurias pranešta. Abipusio pripažinimo principas turėtų būti taikomas, jeigu pranešančiosios valstybės narės elektroninės atpažinties schema laikomasi pranešimo sąlygų ir jeigu pranešimas buvo paskelbtas Europos Sąjungos oficialiajame leidinyje.

Taigi šiuo reglamentu valstybės narės neįpareigojamos diegti elektroninės atpažinties schemų ar apie jas pranešti, tačiau jos įpareigojamos pripažinti ir priimti elektroninės atpažinties schemas, apie kurias pranešta ir kurios skirtos toms virtualioms paslaugoms, kuriomis norint pasinaudoti nacionaliniu lygmeniu būtina elektroninė atpažintis. Galimas masto ekonomijos efekto stiprėjimas dėl pranešime nurodytų tarpvalstybinio elektroninės atpažinties priemonių naudojimo ir tapatumo nustatymo sistemų taikymo gali paskatinti valstybes nares pranešti apie savo elektroninės atpažinties schemas. Reglamento siūlymo 6–7 str. nustatytos abipusio pripažinimo ir pranešimo apie elektroninės atpažinties schemas sąlygos.

Valstybės narės gali pranešti apie elektroninės atpažinties schemas, kurias jos pripažįsta savo jurisdikcijoje, kai norint pasinaudoti viešosiomis paslaugomis būtina elektroninė atpažintis. Be to, keliamas reikalavimas, kad atitinkamos elektroninės atpažinties priemonės turi būti išduodamos

apie schemą pranešančios valstybės narės vardu arba bent jau jos atsakomybe. Valstybės narės privalo užtikrinti vienareikšmį elektroninės atpažinties duomenų ryšį su atitinkamu asmeniu. Šis įpareigojimas nereiškia, kad asmuo negali turėti kelių elektroninės atpažinties priemonių, tačiau visos jos turi būti susietos su tuo pačiu asmeniu.

Valstybės narės privalo prisiimti įsipareigojimą dėl ryšio vienareikšmiškumo (dėl to, kad su asmeniu susiję atpažinties duomenys nebūtų susieti su kitu asmeniu) ir dėl tapatumo nustatymo galimybės (ar galima patvirtinti elektroninės atpažinties duomenis). Valstybių narių įsipareigojimas neapima kitų atpažinties proceso arba operacijos, kuriems reikalinga atpažintis, aspektų.

Žinių įtvirtinimo klausimai

1. Kaip apibrėžiama ir identifikuojama asmens tapatybė?
2. Kokie yra asmens identifikavimo fizinėje ir elektroninėje erdvėje skirtumai?
3. Kokie išskirtini svarbiausi asmens identifikavimo elektroninėje erdvėje elementai?
4. Kaip yra reguliuojamas asmens identifikavimas elektroninėje erdvėje?
5. Kokie motyvai naudojami argumentuojant, kad elektroninėje erdvėje reikėtų nustatyti minimalius asmens identifikavimo reikalavimus?
6. Kas nustatoma 2014 m. elektroninės atpažinties reglamente Nr. 910/2014?

/IX/ *skyrius*

Elektroniniai nusikaltimai

1 skirsnis. Elektroninio nusikaltimo samprata

Daugelyje žmogaus veiklos sričių sparčiai plinta šiuolaikinės informacinės technologijos, kuriomis naudojantis tampa prieinama e. erdvė. Todėl neišvengiamai susiduriama ir su didėjančiu nusikalstamų veikų, susijusių su šios erdvės naudojimu, kiekiu. Elektroninė erdvė suteikia naujų galimybių daryti nusikaltimus, sudaro sąlygas naujiems nusikaltimų būdams atsirasti ir vykdyti naujas veikas, iki tol nežinomas teisinėje praktikoje.

Elektroninis nusikalstamumas tapo pasauliniu reiškiniu, darančiu vis daugiau žalos atskiriems piliečiams, organizacijoms, visai visuomenei ir valstybei. Dauguma pasaulio valstybių elektroninius nusikaltimus pagal jų pavojingumą ir pelningumą netgi prilygina tokioms nusikalstamoms veikoms kaip terorizmas ir prekyba narkotikais.

Elektroninių nusikaltimų istorija siekia jau ne vieną dešimtmetį, tačiau dėl bendros elektroninių nusikaltimų sampratos iki šiol vyksta mokslininkų ir praktikų diskusijos. Nors teisinės problemos, susijusios su pavojingomis veikomis naudojant kompiuterius, pradėtos nagrinėti jau prieš kelis dešimtmečius, iki šiol nėra suformuota bendra 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 (toliau – Konvencija), vis dažniau vartojama „elektroninio nusikaltimo“ sąvoka. Tačiau kelis dešimtmečius labai aktyviai buvo vartojama „kompiuterinio nusikaltimo“ sąvoka.

Literatūroje nurodoma, kad „kompiuterinio nusikaltimo“ terminas buvo vartojamas jau septintajame dešimtmetyje, kai mokslinėje literatūroje pasirodė straipsnių šia tema. Vienas iš pirmųjų šia problema susidomėjo JAV mokslininkas D. Parkeris, jis taip apibrėžė kompiuterinio nusikaltimo sąvoką: „visos tyčinės veikos, vienu ar kitu būdu susijusios su kompiuteriais, dėl kurių nukentėjęs patyrė ar galėjo patirti žalą, o nusikaltimo subjektas turėjo ar 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 vertinama 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. EBPO 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 duomenų elektronine forma apdorojimu ir siuntimu. Tačiau šiame apibrėžime nepaminėta, kokios teisės šakos atžvilgiu minėtasis elgesys yra neteisėtas.

Tai tik pirmieji mėginimai apibrėžti kompiuterinius nusikaltimus. Per daugelį metų įvairios institucijos, mokslininkai bandė apibrėžti kompiuterinius nusikaltimus, tačiau prie bendros nuomonės dėl kompiuterinių nusikaltimų sampratos nebuvo prieita. Netgi paminėtina, kad įvairios tarptautinės organizacijos sąmoningai neapbrėžia kompiuterinio nusikaltimo, nes mano, kad nuolat keičiantis technologijoms toks apibrėžimas greitai taptų nebeaktualus.

Vis dėlto, 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 vykstant informacijos apdorojimo procesui) 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 kompiuterinėje sistemoje, o kompiuteris yra nusikaltimo įrankis. Šių nusikaltimų objektas skiriasi. Todėl prie tokių veikų priskiriamos ir šios: sukčiavimas naudojant kompiuterius, autorių teisių pažeidimas, naudojant kompiuterius ir kt. Paminėtina, jog kartais šios veikos vadinamos su kompiuteriais susijusiais nusikaltimais (*angl. computer-related crime)*, nors pastarasis terminas turėtų apimti daugiau pavojingų veikų (pvz., šmeižtą naudojant elektroninę erdvę).

Tačiau pastaruoju metu, 2001 m., priėmus Konvenciją dėl elektroninių nusikaltimų, „kompiuterinių nusikaltimų“ terminą pakeitė „elektroninių nusikaltimų“ (angl. *cybercrime)* terminas.

Visų pirma reikėtų atkreipti dėmesį į patį terminą „elektroninis nusikaltimas“. Tai nėra tiksliausia sąvoka, apibūdinanti nusikaltimus, vykdomus naudojant e. erdvę. Šie nusikaltimai būdingi ne elektronikos sričiai ar

elektronikos mokslui, o informatikos inžinerijai ir kompiuterijos mokslams. Elektronika, elektroniniai signalai, elektroniniai įtaisai plačiai naudojami televizijoje, radiofonijoje, automobiliuose, pramonėje ir pasižymi analogine signalų forma, o termino *cybercrime* skiriamasis požymis – nusikaltimų dalykas – duomenys, informacija kompiuterine, įskaitmeninta (angl. *digital)*, elektronine forma. Terminas *cybercrime* simbolizuoja globaliai stipriai kompiuterizuotai interneto visuomenei būdingas nusikalstamas veikas. Jis kilęs iš termino *Cyber space*, kuris verčiamas kaip „elektroninė erdvė". Tačiau reikėtų paminėti, kad Lietuva ratifikavo Konvenciją dėl elektroninių nusikaltimų ir tokiu būdu *de jure* buvo įteisintas „elektroninio nusikaltimo" terminas.

Reikėtų pabrėžti, kad iki šiol užsienio literatūroje elektroninio nusikaltimo samprata nėra išsamiai analizuota. Kai kurie autoriai nurodo, kad 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 kompiuterinės sistemos, neteisėtas kompiuterinės informacijos perėmimas, neteisėto turinio medžiagos siuntimas ir kt. Manoma, kad kaip elektroniniai nusikaltimai suprantami įvairūs veiksmai, tokie kaip poveikis kompiuterinei sistemai, su turiniu susiję pažeidimai (neteisėto ir žalingo turinio medžiagos naudojimas) ir kiti.

Mokslininkas George'as Higginsas skiria kompiuterinius ir elektroninius nusikaltimus. Kompiuteriniai nusikaltimai yra veikos, kurioms vykdyti naudojamas kompiuteris ir kurios uždraustos baudžiamųjų įstatymų. Kompiuteriniai nusikaltimai gali būti skirstomi į tris grupes (*Higgins*, 2010):

1) kai kompiuteris naudojamas kaip nusikaltimo padarymo įrankis (pvz., neteisėtas garso failų siuntimasis);
2) kai kompiuteris yra kaip nusikaltimo objektas (pvz., neteisėtos prieigos atveju);
3) kai kompiuteris naudojamas kaip nelegalaus turinio saugykla (pvz., kai naudojamas vaikų pornografijos medžiagai saugoti).

Elektroniniais nusikaltimais autorius laiko tuos, kurie daromi per internetą (naudojant bet kokios rūšies prieigą).

Pabrėžtina, kad Konvencijoje dėl elektroninių nusikaltimų nėra pateikiama „elektroninio nusikaltimo" sąvoka. Tačiau, atsižvelgiant į Konvencijoje dėl elektroninių nusikaltimų kriminalizuotinas veikas, apibrėžiant elektroninius nusikaltimus, ne tik reikėtų laikytis kompiuterinių nusikaltimų sampratos plačiąja prasme krypties, bet ir tokias veikas galima būtų laikyti susijusiomis su kompiuterių naudojimu (angl. *computer-related crime)*, kurios apima gana platų nusikalstamų veikų spektrą. Galima konstatuoti, kad Konvencijoje dėl elektroninių nusikaltimų minimos veikos yra labai

skirtingos (objekto skirtumai ir pan.), dėl to pateikti bendrą tokių veikų sampratą yra problemiška.

Nepaisant to, kad konvencijoje nebuvo ryžtasi apibrėžti elektroninių nusikaltimų, – paminėtina ES kibernetinio saugumo strategija[60]. Šios strategijos vienoje iš išnašų nurodyta, jog elektroniniai nusikaltimai – tai plataus spektro nusikalstamos veikos, kai kompiuteriai ar informacinės sistemos naudojamos kaip įrankis ar kaip taikinys. Nors šis apibrėžimas buvo sukritikuotas Europos duomenų apsaugos pareigūno išvadoje dėl kibernetinio saugumo kaip per daug platus, vis dėlto – tai vienas iš pirmųjų mėginimų oficialiai (oficialiuosiuose dokumentuose) apibrėžti elektroninius nusikaltimus.

2 skirsnis. Elektroninių nusikaltimų žala ir latentiškumas

Pagal statistiką, 2015 m. birželio 30 d. pasaulyje buvo 3.27 mlrd. interneto vartotojų. Prognozuojama, kad 2017 m. mobiliojo plačiajuosčio ryšio vartotojų bus apie 70 proc. viso pasaulio populiacijos, o mobiliųjų įrenginių 2020 m. turėtų būti 6:1, t. y. šeši įrenginiai vienam vartotojui. Šie skaičiai rodo kibernetinių incidentų ir elektroninius nusikaltimų didėjimo tikimybę.

Reikėtų pabrėžti, kad nusikalstamos veikos, vykdomos pasitelkiant e. erdvę, yra ypač pavojingos, nes oficiali teisėsaugos organų statistika neatspindi tikrosios padėties. FBI nacionalinės kompiuterinių nusikaltimų tyrimų grupės teigimu, 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 procentų. Dar 1995 m. JAV gynybos departamento finansuoti tyrimai parodė, kad mėginant įsibrauti į 8 932 informacines sistemas, kurios dalyvavo tyrime, 7 860 atvejai buvo sėkmingi. Tik 390 sistemų administratorių (iš 7 860) užfiksavo įsibrovimą, vos devyniolika iš jų apie tai pranešė oficialioms instancijoms. Pastarųjų metų tyrimai dėl latentiškumo pateikia gana skirtingus duomenis, tačiau visi jie rodo bendrą rodiklį – visais atvejais latentiškumas labai didelis. Pagal kai kuriuos tyrimus, apie du trečdalius visų interneto vartotojų yra tapę elektroninių nusikaltimų aukomis, tik dauguma to nė nežino. Taigi elektroniniai nusikaltimai yra vieni latentiškiausių iš visų nusikalstamumo rūšių. Tokį didelį elektroninių nusikaltimų latentiškumą lemia keli faktoriai:

1. Kompiuterių vartotojai dažnai neturi pakankamai žinių tokiems nusikaltimams pastebėti.

[60] Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions. Cybersecurity strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN/2013/1 final.

2. Aukos vengia informuoti apie aptiktus elektroninius nusikaltimus. Verslo srityje šis nenoras susijęs su dviem dalykais:
   - vienos aukos nenori atskleisti informacijos apie savo darbą, bijodamos viešumo arba prarasti gerą vardą;
   - kitos aukos bijo prarasti investuotoją ar visuomenės pasitikėjimą.

Elektroniniai nusikaltimai kelia susirūpinimą ir dėl savo plitimo tempų. Įvairi statistika liudija, kad elektroninių nusikaltimų skaičius vis dar didėja. Literatūroje teigiama, kad yra glaudus ryšys tarp elektroninių nusikaltimų skaičiaus ir interneto paplitimo. Taigi valstybėse, kuriose interneto, ypač plačiajuosčio ryšio, penetracija yra didžiausia, elektroninių nusikaltimų skaičius taip pat turėtų būti gana didelis. Paminėtina, kad Lietuva šiuo metu šviesolaidį internetą diegia sparčiausiai Europoje.

Vis dėlto reikėtų pabrėžti, kad dėl elektroninių nusikaltimų nėra patikimos statistikos, nes vieni statistiniai duomenys skiriasi nuo kitų. Todėl galima vertinti tik atitinkamus statistinės informacijos pavyzdžius, kurie, tikėtina, turės didesnę ar mažesnę paklaidą. Pavyzdžiui, pagal Didžiosios Britanijos elektroninio saugumo ir informacijos aprūpinimo tarnybos duomenis (studiją), 2010 m. Jungtinėje Karalystėje dėl elektroninių nusikaltimų buvo patirta 43,5 mln. dolerių žala. Pagal Nacionalinės sukčiavimo agentūros (angl. *National Fraud Authority)* duomenis, 2012 m. Jungtinėje Karalystėje dėl sukčiavimo e. erdvėje patirti nuostoliai siekė 73 mln. FS. Pasauliniu mastu, pagal *Symantec* 2012 m. elektroninių nusikaltimų ataskaitą, kasmetiniai nuostoliai dėl elektroninių nusikaltimų sudaro 110 mlrd. JAV dolerių. 2015 m. kituose šaltiniuose ši suma įvardijama jau 266 mlrd. JAV dolerių. Prognozuojama, kad elektroninių nusikaltimų daroma žala 2019 m. viršys du trilijonus JAV dolerių.

Vienas iš žymesnių dar 1998 m. įvykusių precedentų – R. T. Morriso byla, susijusi su vadinamuoju internetiniu kirminu. Dvidešimt trejų metų studentas R. T. Morrisas nebuvo tipinis sistemlaužys. Šio studento tėvas dirbo kompiuterinio saugumo ekspertu Nacionaliniame kompiuterinio saugumo centre. Tačiau, remiantis CFAA, R. T. Morrisas buvo nuteistas trejiems metams lygtinai, 10 000 USD bauda ir 400 val. viešųjų darbų. Bausmė jam buvo skirta už kompiuterių programos – kirmino – sukūrimą ir naudojimą. Ši programa, anot R. T. Morriso, buvo skirta rinkti informacijai apie kompiuterius, įjungtus į pasaulinį kompiuterių tinklą, bei šių kompiuterių apsaugos priemones. Programa buvo sukurta 1998 m., ja buvo siekiama atlikti jokios žalos nedarantį eksperimentą kompiuterių mokslo srityje. Tačiau, R. T. Morrisui nežinant, padaryta programinė klaida lėmė, kad programa pradėjo daugintis didžiuliais tempais. Programai

patekus į internetą, po keleto valandų buvo užkrėsta apie 2 000 kompiuterių (buvo sutrikdytas kompiuterių ir jų tinklų darbas), dėl to vien JAV padaryta 150 000 JAV dolerių žalos. Reikia paminėti, kad vertinimai, susiję su padaryta žala, skiriasi. J. McAfee, Kompiuterių virusų asociacijos pirmininkas, yra pareiškęs, kad R. T. Morriso kirmino padaryta žala siekia 96 mln. JAV dolerių.

Vienu iš didžiausią finansinę žalą sukėlusių nusikalstamų veikų istorijoje, 2015 m. duomenimis, laikoma vagystė iš bankų, kai nelegalia kenkiamąja programine įranga užkrėtus viso pasaulio finansinių institucijų elektronines sistemas buvo pasisavinta apie 650 mln. JAV dolerių. Tai tik vieni iš daugelio precedentų, iškilusių į viešumą. Reikėtų paminėti, kad elektroninių nusikaltimų daroma žala gali pasireikšti ne tik kaip finansinė. Grėsmė gali kilti žmogaus sveikatai, gyvybei, reputacijai ar net pačiai valstybei ir jos saugumui bei viešųjų ir privačių paslaugų funkcionavimui. Vis labiau plintant daiktų internetui, nuotolinei debesijai, e. sveikatos paslaugoms, tiek žalos pasireiškimo spektras, tiek apimtis vis didės.

3 skirsnis. Pagrindinės elektroninių nusikaltimų rūšys

Viena iš pirmųjų elektroninių nusikaltimų klasifikacijų pateikta 1989 metais. Šiais metais Europos Tarybos ministrų kabinetas priėmė rekomendaciją R89(9) ES šalių vyriausybėms, kurioje siūloma peržiūrint ar kuriant įstatymus atsižvelgti į Europos Komiteto nusikaltimų problemoms tirti skirtą pranešimą apie su kompiuteriais susijusius nusikaltimus. Šiame pranešime pateikiami du sąrašai veikų, susijusių su tokiais nusikaltimais. ES šalims leidžiama savarankiškai spręsti, kaip ir kiek pasinaudoti šiuo pasiūlymu. „Minimaliame sąraše“ išvardytos aštuonios pavojingesnės veikos, susijusios su kompiuterinėmis technologijomis. Papildomas sąrašas apima keturias ne tokias pavojingas veikas, kurios įtraukiamos į įstatymų leidybą, bet nėra privalomos. Šie sąrašai reikalingi suvienodinant ES šalių teisines sistemas kompiuterių nusikaltimų atžvilgiu. Šios veikos nėra kompiuteriniai nusikaltimai teisine prasme, o tik veikos, kurias valstybėms rekomenduojama fiksuoti savo nacionaliniuose teisiniuose aktuose kaip pažeidimus ir nebūtinai kaip kriminalines veikas.

Minimalus sąrašas:

1) sukčiavimas naudojant kompiuterį (angl. *computer-related fraud)*;
2) klastojimas naudojant kompiuterį (angl. *computer forgery)*;
3) elektroninių duomenų ar programų sunaikinimas ar sugadinimas (angl. *damage to computer data or computer programs)*;

4) sabotažas naudojant kompiuterį (angl. *computer sabotage)*;
5) neteisėta prieiga prie kompiuterinių sistemų (angl. *unauthorised access)*;
6) neteisėtas informacijos perėmimas kompiuterinėse sistemose (angl. *unauthorised interception)*;
7) neteisėtas apsaugotų kompiuterių programų dauginimas ir platinimas (angl. *unauthorised reproduction of a protected computer program)*;
8) neteisėtas kompiuterių lustų (mikroschemų) topografijų dauginimas ir platinimas (angl. *unauthorised reproduction of a topography)*.

Neprivalomas sąrašas:

1) kompiuterių duomenų ar programų pakeitimas (angl. *iteration of computer data or computer programs)*;
2) špionažas naudojant kompiuterį (angl. *computer espionage)*;
3) neteisėtas kompiuterio naudojimas (laiko vagystė) (angl. *unauthorised use of computer)*;
4) neteisėtas apsaugotų kompiuterių programų naudojimas (angl. *unauthorised use of a protected computer program)*.

1995 m. Interpolo rekomendacijose „Computers and crime“ (čia pateikiamas tik minimalus sąrašas), Europos Tarybos rekomendacijose pateiktos šios pavojingos veikos, naudojant kompiuterį (kurios aiškinamos toliau):

1. *Sukčiavimas naudojant kompiuterį*. Kompiuterių duomenų ar programų įvedimas, pakeitimas, ištrynimas ar kitoks trukdymas duomenų apdorojimo procesui, kas paveikia šio proceso galutinį rezultatą, padarydamas žalos kito asmens nuosavybei, norint neteisėtai gauti materialinės naudos sau ar kitam asmeniui.
2. *Klastojimas naudojant kompiuterį*. Kompiuterių duomenų ar programų įvedimas, pakeitimas, ištrynimas ar kitoks trukdymas duomenų apdorojimo procesui, kai šių veiksmų tikslas yra toks pats, kaip ir įstatymuose, numatančiuose atsakomybę už klastojimą.
3. *Kompiuterių duomenų sunaikinimas arba sugadinimas*. Kompiuterių duomenų ar programų ištrynimas, sunaikinimas, sugadinimas, neturint tam teisės.
4. *Sabotažas naudojant kompiuterį*. Kompiuterių duomenų ar programų įvedimas, pakeitimas, ištrynimas ar įsikišimas, trukdymas kompiuterių sistemoms, norint surikdyti kompiuterių ar telekomunikacijų sistemos darbą.
5. *Neteisėta prieiga prie kompiuterių sistemų*. Priėjimas, neturint teisės, prie kompiuterių sistemos ar tinklo, pažeidžiant saugumo priemones.

6. *Neteisėtas informacijos perėmimas kompiuterių sistemose.* Perėmimas, atliktas techniškai, legaliai nenumatytais būdais, kompiuterių tinklo viduje ar iš išorės.

Jungtinių Tautų tarptautinėje kriminalinės policijos kompiuterinių nusikaltimų apžvalgoje pateikiama tokia kompiuterinių nusikaltimų klasifikacija:

1) manipuliavimas naudojant kompiuterį (kompiuterinis sukčiavimas);
2) klastojimas naudojant kompiuterį;
3) kompiuterių duomenų ir programų sunaikinimas ir modifikavimas (sabotažas);
4) neteisėta prieiga prie kompiuterių duomenų;
5) neteisėtas kompiuterių programų platinimas.

1. Manipuliavimas naudojant kompiuterį (kompiuterinis sukčiavimas)

Tai manipuliavimas įvedimu, išvedimu ar įvedimas kompiuterių programų, kurios tampa duomenų praradimo ar sugadinimo priežastimi, siekiant materialinės naudos sau, dėl ko patiriama ekonominių nuostolių.

Manipuliavimas įvedimu yra dažniausiai pasitaikantis, nes tai lengva padaryti ir sunku susekti. Šiuo būdu į kompiuterių sistemą gali būti įvesti neteisingi duomenys. Tam nereikia ypatingų kompiuterinių žinių ir tai gali padaryti bet kas, turintis prieigą prie kompiuterių sistemų duomenų apdorojimo funkcijų.

Manipuliacija programomis, kurią sunku aptikti, reikalauja specialių kompiuterinių žinių. Šiems nusikaltimams priskiriamas kompiuterių sistemoje esančių programų pakeitimas arba naujų įvedimas. Dažniausiai naudojamas asmenų, turinčių specialių kompiuterinių žinių, metodas yra Trojos arklys, kompiuterinės instrukcijos, slaptai įvedamos į kompiuterių programą. Trojos arklys gali būti užprogramuotas pats save sunaikinti, nepaliekant jokių egzistavimo požymių, išskyrus padarytą žalą.

Manipuliavimas išvedimu yra vykdomas paveikiant kompiuterių sistemų išvedimo procedūras. Aiškus pavyzdys yra grynųjų pinigų automato apgavimas, atliekamas įvestimis falsifikuojant komandas kompiuteriui. Dažniausiai šiai apgavystei naudojamos vogtos bankų kortelės. Pasitaiko ir tam tikrų sukčiavimo atvejų, kurių metu vykdomos manipuliacijos, kai gaunama naudos iš automatizuotų kompiuterinių procedūrų pakartojimo. Tokios manipuliacijos vadinamos Salami technika, kai labai nedidelė finansinio pervedimo dalis pervedama į kitą sąskaitą.

2. Klastojimas naudojant kompiuterį

Tai kompiuterine forma saugomų duomenų pakeitimas, sugadinimas ar sunaikinimas. Vykdymo motyvai ir tikslai gali būti įvairūs. Nuo sukčiavimo skiriasi tuo, kad šiuo atveju nesiekiama tiesioginės materialinės naudos. Prie šio tipo nusikaltimų gali būti priskirtina ir neteisėta (nesąžininga) konkurencija. Vykdant kompiuterinius klastojimus organizacijose, kurių apskaita kompiuterizuota, gali būti slepiami mokesčiai.

Naujoji apgavikų klastotojų karta pasirodė, kai atsirado galimybė daryti spalvotas lazerines kopijas. Lazeriniai spausdintuvai turi puikios kokybės kopijavimo galimybių, gali išspausdinti pakeistus ar net naujai sukurtus dokumentus, kuriuos atskirti nuo originalų be eksperto pagalbos gana sunku.

3. Kompiuterių duomenų ir programų sunaikinimas ar modifikavimas (kompiuterinis sabotažas)

Tai kompiuterių programų, duomenų, kompiuterinės technikos sugadinimas ar sunaikinimas bei techninio personalo veiklos apribojimas, trukdant jiems dirbti su kompiuterių ištekliais. Programų, skirtų sugadinti ar sunaikinti kitoms kompiuterių programoms ir duomenims (kompiuterių virusų, loginių bombų ir pan.) kūrimas, platinimas bei įvedimas.

Kompiuterinio sabotažo tikslas – sugadinti kompiuterių programas, sunaikinti duomenis. Nusikaltimas gali būti vykdomas dėl karinių, politinių motyvų, konkurencinėje kovoje, kerštaujant arba iš chuliganiškų paskatų. Duomenis per labai trumpą laiką galima sugadinti, naudojant kompiuterių programas (standartines ir specialiai sukurtas), arba pasitelkus elektromagnetines bangas ar radiaciją.

Šios kategorijos kriminalinės veikos apima ir tiesioginę, ir slaptą neteisėtą prieigą prie kompiuterių sistemos, įvedant naujas programas, žinomas kaip virusus, logines bombas, kirminus. Neteisėtas duomenų modifikavimas ar sunaikinimas per internetą, kuris sutrikdo normalų kompiuterių sistemos darbą, dažniausiai minimas kaip kompiuterinis sabotažas. Pavyzdžiui, 1987 m. Londone atskleistas nesėkmingas vienos firmos darbuotojo mėginimas sužlugdyti firmos kompiuterių sistemą, įvedant į programą vadinamąją loginę bombą, kuri po tam tikro laiko visiškai ją sunaikintų.

4. Neteisėta prieiga prie kompiuterių duomenų

Neteisėta prieiga funkciškai yra nuosavybės ribų peržengimo analogas. Tai prieiga prie kompiuterių duomenų, prie kurių neturima teisės prieiti, įveikiant apsaugos sistemas, kai yra pažeidžiamas kompiuterinės informacijos slaptumas. Prieigos prie kompiuterių duomenų šiuo atveju nereikėtų

suprasti kaip fizinės. Motyvai gauti neteisėtą prieigą gali būti įvairūs, pvz., programišių noras pasirodyti ir kt. Neteisėta prieiga prie duomenų, kurie yra valstybės ar firmos komercinė paslaptis, visose valstybėse yra baudžiama. Žmogaus, neturinčio įgaliojimų prieiti prie kompiuterių sistemos, tyčinė ir nepateisinama prieiga dažnai vertinama kaip kriminalinis elgesys. Neteisėta prieiga suteikia galimybę padaryti žalos duomenims, sutrikdyti kompiuterių sistemos darbą. Neteisėtai prieiti prie duomenų galima pasitelkus kompiuterių tinklus. Norint gauti prieigą, gali būti pasinaudota silpnomis apsaugos vietomis. Dažniausiai programišiai apsimeta teisėtais vartotojais. Tai gali atsitikti ten, kur naudojamasi bendraisiais slaptažodžiais.

Slaptažodis dažnai minimas kaip priemonė, užkertanti kelią neteisėtai prieigai. Tačiau šiuolaikinis programišius, naudodamasis tam tikrais metodais, gali lengvai apeiti šią apsaugą. Jeigu jis sugeba nulaužti prieigos leidimo slaptažodį, gali įvesti Trojos arklį, kad „sugautų“ kitų teisėtų vartotojų slaptažodžius. Šią programą sunku aptikti. Vėliau per nuotolinę prieigą programišius gali gauti daugumą slaptažodžių. Šių apsaugą galima apeiti ir kitais būdais, pvz., naudojant slaptažodžių nulaužimo programas. Nulaužimo programomis programišiai keičiasi internetu.

5. Neteisėtas kompiuterių programų platinimas

Tai programinės įrangos, kurią gali naudoti tik ją sukūrusi ar įsigijusi organizacija, pasisavinimas ir platinimas. Ši veika gali padaryti ekonominės žalos teisėtiems savininkams. Programinės įrangos piratavimas yra labai paplitęs Rytų Europos ir buvusios Sovietų Sąjungos šalyse.

Paminėtina prof. U. Sieberio 1988 m. pateikta elektroninių nusikaltimų (tuo metu – kompiuterinių nusikaltimų, su kompiuteriais susijusių nusikaltimų) formų klasifikacija (*Sieber*, 1988):

- privatumo pažeidimai;
- ekonominiai pažeidimai (įsilaužimas į kompiuterį; špionažas naudojant kompiuterį; neteisėtas programinės įrangos kopijavimas; sabotažas naudojant kompiuterį; sukčiavimas naudojant kompiuterį);
- pažeidimai, susiję su neteisėtu ir žalingu turiniu (medžiagos, susijusios su pornografija, platinimas ar pan.);
- kiti pažeidimai.

Šios klasifikacijos pateiktos jau prieš kurį laiką ir gali atrodyti pasenusios, tačiau nors ir atsirado naujų elektroninių nusikaltimų, šios klasifikacijos iš esmės išlaiko savo aktualumą ir dabartiniu metu.

Skirstant elektroninius nusikaltimus, galima pasiremti sąlygiška klasifikacija, pateikta Konvencijoje dėl elektroninių nusikaltimų – elektroniniai nusikaltimai pagal įstatymo saugomą interesą skirstomi į:

– nusikaltimus, pažeidžiančius kompiuterinės informacijos ir kompiuterių sistemų konfidencialumą, vientisumą bei prieinamumą (neteisėta prieiga, neteisėtas perėmimas, įsikišimas į duomenų apdorojimo procesą ir kompiuterių sistemos darbą);
– nusikaltimus, susijusius su kompiuterių naudojimu (klastojimas naudojant kompiuterius; sukčiavimas naudojant kompiuterius);
– nusikaltimus, susijusius su turiniu (medžiagos su vaikų pornografija naudojimas);
– pažeidimus, susijusius su autorių teisėmis ar gretutinėmis teisėmis.

Šios elektroninių nusikaltimų rūšys atitinkamai skirstomos ir į tam tikrus porūšius:

6. Nusikaltimai, pažeidžiantys kompiuterinės informacijos ir kompiuterių sistemų konfidencialumą, vientisumą ir prieinamumą

Viena iš žinomiausių veikų – neteisėta prieiga (angl. *hacking)*. Tokia prieiga prie kompiuterių programų ar duomenų elektronine forma laikytina tokia veika, kuri pažeidžia laikomos informacijos slaptumą bei konfidencialumą (kyla realios žalos grėsmė), o dėl neteisėtos prieigos vykdomas špionažas, neteisėtai kopijuojami autorių teisėmis apsaugoti kūriniai, sabotažas, sukčiavimas naudojant kompiuterius 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 finansų institucijų kompiuterių sistemas, tačiau nepadarė jokios žalos. Apie šiuos veiksmus buvo pranešta Vienos teisėsaugos institucijoms. Tačiau tyrimas buvo sustabdytas, nes nebuvo padaryta jokios žalos, o studento motyvacija buvo pavadinta „intelektualiu iššūkiu“. Byloje *R. v. Gold* taip pat buvo parodyta baudžiamųjų įstatymų nuostatų, susijusių su neteisėta prieiga, būtinybė. Jungtinėje Karalystėje tyrimas prasidėjo dėl to, kad sistemlaužiai be leidimo įsilaužė į „British Telecom“ kompiuterių tinklą ir pakeitė tam tikrus duomenis. Kaltinamieji teigė, kad buvo įsilaužta turint tikslą „British Telecom“ kompiuterių sistemoje „išryškinti saugumo skyles“. Sistemlaužiai buvo apkaltinti remiantis 1981 m. Klastojimo įstatymu, nes buvo sudarytas klaidingas dokumentas, vėliau buvo nuteisti. Tačiau apeliacinėje instancijoje teismo sprendimas buvo panaikintas teigiant, kad šių asmenų veiksmuose nebuvo jokio nusikaltimo sudėties. Tokiu būdu buvo pademonstruotas egzistuojančių įstatymų netobulumas.

Įsikišimą į kompiuterinės informacijos apdorojimo procesą galima vadinti neteisėtos prieigos tąsa. Tokia veika gali pasireikšti neteisėtu

kompiuterinės informacijos ištrynimu, sunaikinimu, sugadinimu ar pakeitimu. Manoma, jog kompiuterių programos ir kompiuterinė informacija turi būti apsaugota nuo tokio kėsinimosi, kaip ir materialūs objektai, siekiant užtikrinti kompiuterinės informacijos integralumą bei kompiuterių programų ar kompiuterinės informacijos tinkamą naudojimą (funkcionavimą). Kompiuterinės informacijos vagystę (tam tikra dalimi sietiną su šnipinėjimu naudojant kompiuterį) galima įvardyti kaip neteisėtos prieigos tąsą. Šiandienės informacinės technologijos, ypač kompiuterių tinklai, suteikia didžiulių galimybių akimirksniu nukopijuoti bet kokį informacijos kiekį. 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 e. erdve. Prieš keletą metų perėmimo (angl. *Interception*) veika dažniausiai buvo tapatinama su telefoninių pokalbių perėmimu. Tačiau M. Mohrenschlageris teigia, kad plėtojantis technologijoms ir komunikacijoms, telekomunikacijoms ir kompiuterių sistemoms susiliejant į bendrą visumą, apsaugos reikalauja ir kiti kompiuterinės informacijos tipai, siunčiami e. erdve.

Sabotažu naudojant kompiuterius vadinama veika, kai į kompiuterių sistemą įvedant kenkimo programas (ar padarant kompiuterių programose pakeitimų) neteisėtai sunaikinama, pakeičiama ar ištrinama kompiuterinė informacija, siekiant sutrikdyti kompiuterių sistemos darbą. Duomenų, saugomų elektronine forma, koncentruotumas, įmonių, organizacijų bei fizinių asmenų priklausomumas nuo informacijos, laikomos elektronine forma, sabotažą naudojant kompiuterius daro labai pavojinga veika. Visuomenė įvairiose gyvenimo srityse (medicinos tarnybų, transporto veikla ir pan.) tampa vis labiau priklausoma nuo kompiuterių sistemų, kurios dažnai sujungtos su kompiuterių tinklais (e. erdve). Todėl net nedidelis šių sistemų funkcionavimo sutrikimas, atsiradęs dėl veikos naudojant e. erdvę, gali sukelti pavojų žmonių sveikatai ar gyvybei. Atsiradus e. erdvei, populiariausi žalos padarymo metodai – specialių programų, kurios gali ištrinti didelius duomenų kiekius per trumpą laiką, naudojimas. Tokios programos gali būti kompiuterių virusai, Trojos arkliai ir kt. Daugiausia problemų kelia kompiuterių virusų ir kirminų paplitimas. Kompiuterių virusai – tai programos, kurios savaime platinasi e. erdvėje bei kompiuterių sistemose ir tik po tam tikro laiko padaro žalos.

Pastaruoju metu akcentuojamas *kompiuterių sistemos darbo sutrikdymas*, kai kompiuterių sistema internetu „užverčiama“ dideliu kiekiu žinučių (angl. *a distributed denial of service (DDoS) attack*). Šiuo būdu sutrikdomas kompiuterių sistemos darbas, nors neteisėta prieiga prie sistemos ir

neatliekama. Literatūroje *DDoS* atakos suprantamos kaip kruopščiai atlikti veiksmai, kuriais siekiama teisėtus vartotojus atkirsti nuo tinklo išteklių. *DDoS* atakos dažnai neatsiejamos nuo botnetų[61] panaudojimo. Tokiais veiksmais buvo sutrikdytas CNN, „Yahoo!“, „E-Bay“ ir kitų interneto svetainių darbas, dėl to buvo patirta milžiniškų finansinių nuostolių. Teisminėje praktikoje yra ne viena byla, kai buvo nuteisti tokias veikas įvykdę asmenys. Pavyzdžiui, 2002 m. pradžioje, remiantis Federaliniu sukčiavimo bei piktnaudžiavimo panaudojant kompiuterį įstatymu, buvo nuteistas B. McDanelis. Šis asmuo buvo pripažintas kaltu, nes piktavališkai siuntė tūkstančius elektroninių žinučių į centrinį kompiuterį, kurio operatorius buvo „Tornado Development“. Tokiu būdu šis centrinis kompiuteris buvo perpildytas, dėl to sutriko jo darbas. B. McDanelis buvo nuteistas laisvės atėmimu penkeriems metams.

Kaip viena iš didžiausių *DDoS* atakų paminėtini 2007 m. Estijos įvykiai, kai botnetas, kurį sudarė apie milijoną kompiuterių, buvo panaudotas Estijos kompiuteriams ir kompiuterių tinklams atakuoti, dėl to buvo sutrikdytas šalies valstybinių institucijų, parlamento bei daugumos bankų darbas. Estija manė, kad Rusija pradėjo elektroninį karą. Tačiau pakankamai įrodymų tam nėra iki šiol. Beje, kai kurie autoriai Estijos įvykius pristato vadovaudamiesi elektroninio terorizmo samprata. Kituose šaltiniuose minima, kad ši ataka laikytina pavojingiausia ir koordinuota kibernetine ataka prieš savarankišką valstybę per visą istoriją.

Paminėti ir Gruzijos 2008 m. įvykiai. Masinės kibernetinės atakos buvo vykdomos prieš šios šalies vyriausybinius tinklalapius ir komunikacijų tinklus. Šios atakos buvo pradėtos tą pačią dieną, kai Gruzija pradėjo karinius veiksmus Pietų Osetijoje.

Vienas iš žinomesnių precedentų įvyko Lietuvoje 2013 m. gegužę. Didžiausias elektroninis žinių portalas „Delfi“ buvo pradėtas atakuoti po to, kai paskelbė, kad per „Eurovizijos“ dainų konkursą Lietuvoje buvo organizuotai pirkti balsai už Rusijos atstovę. Iki atakų pradžios „Delfi“ redakciją pasiekė elektroninis laiškas rusų kalba, kuriame buvo grasinta imtis „radikalių veiksmų“, jeigu nebus pašalinta informacija apie perkamus balsus. Jau po valandos „Delfi“ portalas trims valandoms tapo neprieinamas dėl masinių *DDoS* atakų. Atakos tęsėsi keletą dienų. Teisėsaugos institucijos pradėjo ikiteisminį tyrimą pabal Lietuvos Respublikos baudžiamojo kodekso 197 str. 1 dalį. Vėliau buvo pradėta atakuoti ir „Delfi“ prieglobos paslaugų teikėją UAB „Hostex“, kurios vadovas šią ataką įvertino kaip didžiausią kibernetinę Lietuvos istorijoje (pagal trukmę ir apimtį).

[61] Pasitelkus virusus iš išorės, neteisėtiems tikslams valdomi kompiuterių tinklai (grupė atskirų kompiuterių).

Politikai šią ataką prieš žiniasklaidos priemonę įvertino kaip ataką prieš valstybę bei įžvelgė viešojo intereso gynimo būtinybę.

2015 m. pabaigoje ilgiausiai DDoS ataka truko 320 val., t. y. beveik dvi savaites. Norint įvykdyti DDoS ataką, nereikia turėti specialių techninių žinių. Tokią ataką galima užsisakyti, sumokėjus atitinkamą pinigų sumą, priklausančią nuo atakos laiko, dydžio ir kitų parametrų.

Minėtųjų DDoS veikų vykdymas dažniausiai susijęs su tam tikrų įrankių ar priemonių turėjimu. M. Mohrenschlageris nurodo, kad praktikoje egzistuoja ištisos nelegalios slaptažodžių ir prieigos kodų rinkos e. erdvėje. Todėl viena iš įvardijamų internetinių nusikaltimų rūšių – neteisėtos prieigos priemonių ir įrenginių platinimas, gaminimas ir kt. Šio tipo veikų pavojingumas buvo pabrėžtas jau 1994 m. Kriminalinės policijos tarptautinėje apžvalgoje dėl kompiuterinių nusikaltimų, kur nurodyta, jog veikos pavojingumas sietinas su galimybe padaryti žalą.

Kenkimo programų sukūrimas, naudojimas ir platinimas irgi laikomas pavojinga veika. Literatūroje nurodoma, kad kenkimo programų sukūrimo, naudojimo bei platinimo pavojingumas visuomenei pasireiškia tuo, kad tokios programos gali pačiu netikėčiausiu momentu sutrikdyti kompiuterių sistemos darbą, dėl ko gali kilti žalingų padarinių. Atsiradus e. erdvei, kenkiamųjų programų grėsmė padidėjo, nes, pvz., paskleidus virusą internete, dėl šio tinklo globalumo jis gali padaryti daug žalos. Kenkiamosiomis programomis laikomos kompiuterių programos, turinčios virusų (kompiuterių virusai), ar tam tikrų nurodymų (pvz., loginės bombos, Trojos arkliai, asinchroninės atakos, liukai), ar turinčios specifinių savybių įvykdyti neteisėtus arba nusikalstamus veiksmus (grobti pinigus iš bankų sąskaitų ir kt.). Šios programos turi savybę persikelti kompiuterių tinklu iš vienos kompiuterių sistemos į kitą, patekti į kompiuterių sistemą ir daugintis kaip virusinės ligos.

7. Su kompiuterių naudojimu susiję nusikaltimai

Technologinė revoliucija padidino galimybes vykdyti tokius ekonominius nusikaltimus kaip sukčiavimas. Šiandien daugelis didelių įmonių prijungtos prie interneto ar kitų kompiuterių tinklų, o jų kompiuterių sistemose esančios ir administruojamos vertybės tapo dažnu taikiniu. Sukčiavimas naudojant kompiuterį apibrėžiamas kaip piniginių lėšų ar kito turto grobimas. Ši veika apima nurodymus kompiuteriui pervesti pinigus į banko sąskaitą ar pan. 2012 m. JAV grupė programišių per keletą valandų iš dviejų užsienio bankų pagrobė 45 mln. JAV dolerių. Pinigai buvo gryninami per 27 užsienio valstybių bankomatus. Išaiškinus nusikaltimą, JAV buvo sulaikyti septyni programišiai.

Veikas atliekant sukčiavimą, susijusį su kompiuteriais, galima suskirstyti į dvi pagrindines grupes: sukčiavimą, susijusį su duomenimis, ir sukčiavimą, susijusį su kompiuterių programomis. Literatūroje nurodoma, kad terminas „sukčiavimas panaudojant kompiuterį“ tam tikrais atvejais gali būti klaidinantis, nes juo 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 ar paslaugų gavimu apgaule ir kt. U. Sieberis nurodo, kad pastaruoju metu sukčiavimas naudojant kompiuterius apima įvairias veikas ekonominių nusikaltimų srityje bei tai, kad elektroninė erdvė suteikia ypač dideles galimybes vykdyti tokio tipo nusikaltimus *(Sieber*, 1988). Taigi keliamas tikslas kriminalizuoti sukčiavimo veikas e. erdvėje, manipuliuojant kompiuterine informacija ar kompiuterių programomis, siekiant materialinės naudos.

Elektroninės erdvės atsiradimas atvėrė kelią ir klastojimo veikoms. Kompiuterinės informacijos klastojimas gali turėti tokių pačių padarinių, kaip ir tradicinis, kuris yra susijęs su kompiuteriais ir apima neteisėtą kompiuterinės informacijos sukūrimą ar jau sukurtos pakeitimą, dėl to ši informacija įgyja kitokią reikšmę. Todėl turi būti užtikrintas kompiuterinės informacijos patikimumas ir saugumas, siekiant užkirsti kelią neigiamiems teisinių asmenų santykių padariniams.

8. Nusikaltimai, susiję su turiniu

Interneto plėtra paskatino neteisėto ir žalingo turinio medžiagos plitimą e. erdvėje. Literatūroje nurodoma, kad tai yra labiausiai besiplėtojanti nusikaltimų e. erdvėje sritis. Teigiama, kad internetas ne tik sudarė geresnes sąlygas platinti pornografinį turinį, bet ir sukūrė naujų būdų, kad šis turinys pasiektų kuo didesnę auditoriją.

Pornografinio turinio medžiagos internete platinimas, rasistinių nuostatų skleidimas kelia klausimų dėl baudžiamosios teisės vaidmens vertinant šias veikas. U. Sieberis mini ir problemas, susijusias su rasistinėmis nuostatomis, šmeižtu ar grasinimais e. erdvėje *(Sieber*, 1988). Paminėtina, kad pavojingos veikos, susijusios su pornografinio turinio medžiagos naudojimu, rasistinėmis nuostatomis, šmeižtu ar grasinimais e. erdvėje, kelia teisinės atsakomybės problemas daugiau dėl įvairių valstybių teisinių ir kultūrinių tradicijų skirtumų, todėl šiame darbe minimos problemos nebus nagrinėjamos. Šiuo metu didžiausias dėmesys yra skiriamas vaikų pornografijos e. erdvėje problemai. Įstatymų, susijusių su vaikų pornografija, kūrimo problemą akcentuoja ir Europos Komisija. Tokiu būdu siekiama apsaugoti vaikus nuo seksualinio išnaudojimo. Dėl interneto paplitimo šiuo metu

e. erdvė tapo pagrindine tokio pobūdžio medžiagos platinimo priemone. Todėl ši nauja pavojingos veikos forma turi būti nurodyta baudžiamuosiuose įstatymuose.

9. Pažeidimai, susiję su autorių teisėmis ir gretutinėmis teisėmis

Intelektualios nuosavybės teisių, 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, kad šiandien dėl interneto įtakos dažniausiai neteisėtai platinamos kompiuterių programos ir kiti autorių teisėmis apsaugoti kūriniai. Tokiais apsaugotais darbais laikomi literatūros, fotografijos, muzikos, garso ir vaizdo kūriniai ir kiti, kurie gali būti platinami naudojant P2P tinklus, FTP serverius, socialinius tinklus, elektroninį paštą ir kt. Didžiulės darbų kopijavimo ir platinimo galimybės, kurias suteikia e. erdvė, verčia įstatymo leidėjus baudžiamuosiuose įstatymuose nustatyti normas, uždraudžiančias tokias veikas. Trumpai paminėtina, kokios autorių teisės gali būti pažeidžiamos e. erdvėje. Internete gali būti pažeidžiamos net kelios autoriaus teisės: autoriaus teisė viešai demonstruoti, atgaminti kūrinį ir kt. Be to, pavojingos veikos gali pasireikšti informacijos apie autorių teisių valdymą sunaikinimu ar pakeitimu, autorių teisių techninių apsaugos priemonių pašalinimu ir pan.

Pastaruoju metu dideliais tempais plinta nauja nusikalstama veika – tapatybės vagystė elektroninėje erdvėje. Asmens tapatybės vagystė e. erdvėje yra sąlygiškai naujas socialinis ir teisinis reiškinys, susijęs su vartotojų teisių, informacijos saugumo, privatumo, taisyklių, reglamentuojančių nepageidaujamos informacijos gavimą, ir kitais pažeidimais.

Globalus e. erdvės pobūdis ir specifinės jos savybės leidžia teisės pažeidėjams veikti gana saugioje aplinkoje, nukreipti savo veiksmus bet kuria linkme ir veikti bet kurioje vietoje ar vykdyti labai plačios apimties veikas, visiškai nepaisant valstybių sienų ir jurisdikcijos. Todėl ir tapatybės vagystė e. erdvėje yra globali problema. Mokslinėje literatūroje nurodoma, jog tapatybės vagystės e. erdvėje padariniai gali apimti daugelį visuomenės aspektų – nuo ekonomikos iki nacionalinio saugumo.

D. Štitilis, P. Pakutinskas, I. Dauparaitė ir M. Laurinaitis tapatybės vagystę e. erdvėje apibrėžia taip: „tapatybės vagystė – tai bet kokie neteisėti veiksmai su kito asmens duomenimis ir (ar) asmenine informacija, leidžiančia identifikuoti kitą asmenį (tokių duomenų ir (ar) asmeninės informacijos perėmimas, įgijimas, laikymas, naudojimas, paskleidimas, disponavimas ar kitokių veiksmų atlikimas), turint tikslą apsimesti tuo asmeniu, iš kurio buvo

gautos jį identifikuojančios priemonės, tam, kad būtų galima atlikti teisės pažeidimus ir (ar) nusikalstamas veikas. Tuo metu tapatybės vagystė elektroninėje erdvėje galėtų būti suprantama kaip tapatybės vagystės rūšis, kai tapatybės vagystė atliekama per atstumą, t. y. naudojantis informacinėmis ir ryšio technologijomis" *(Štitilis, Pakutinskas, Dauparaitė, Laurinaitis,* 2011).

Tapatybės vagystė e. erdvėje dažniausiai prasideda nuo asmeninės informacijos pasisavinimo. Pagal 2012 m. statistiką, jeigu pasisavinami asmens duomenys, kyla 25 proc. tikimybė, kad jie bus naudojami sukčiavimui.

Pastaraisiais metais Lietuvoje priimti pirmieji precedentiniai teismo sprendimai dėl tapatybės vagystės, tiesa, įvykdytos tradiciniu būdu, o ne e. erdvėje. Vis dėlto tai patvirtina, kad tapatybės vagystė yra reali grėsmė, nes apsimesti kitu asmeniu e. erdvėje yra kur kas lengviau. Šie teismo sprendimai paminėtini detaliau:

1. 2009 m. birželio 30 d. *LAT* priėmė nutartį byloje Nr. 2A-11/2009. Jis pabrėžė, kad nagrinėjamoje byloje atnaujinus ikiteisminį tyrimą, kaip liudytojos apklaustos kaltinamosios, įrodė, kad jos odinio sijono iš parduotuvės nevogė, o jų pavardėmis prisistatė jų pusseserės, nes šios kurį laiką pas jas gyveno. Pareiškus įtarimų minėtosioms pusseserėms, abi prisipažino įvykdžiusios vagystę iš parduotuvės, be to, patvirtino, kad vežamos į policijos komisariatą tarpusavyje susitarė pasivadinti kaltinamųjų vardais ir pavardėmis. Kadangi šios aplinkybės nebuvo ir negalėjo būti žinomos teismui priimant nuosprendį, baudžiamoji byla atnaujintina ir perduotina tirti iš naujo.
2. 2009 m. liepos 14 d. *LAT* priėmė nutartį byloje Nr. 2A-12/2009. LAT pabrėžė, kad iš tyrimo medžiagos ir išvadoje išdėstytų aplinkybių akivaizdžiai matyti, jog 2005 m. sausio 26-28 d. apkaltintoji nebuvo Lietuvoje ir negalėjo pasikėsinti padaryti baudžiamojo nusižengimo, už kurį ji nepagrįstai nuteista pirmosios instancijos teismo nuosprendžiu. Byloje esantys naujai paaiškėję duomenys apie kitą asmenį (galbūt pasinaudojo panašumu į apkaltintąją ir nurodė jos anketinius duomenis), kuris (kuri) 2005-01-26 16.45 val. pasikėsino pagrobti nedidelės vertės svetimą turtą iš parduotuvės, turėtų būti įvertinti naujo ikiteisminio tyrimo metu atskleidžiant visas šios nusikalstamos veikos padarymo aplinkybes, įvertinant procesines galimybes patraukti šį asmenį baudžiamojon atsakomybėn ir priimant atitinkamą BPK numatytą sprendimą. Todėl teismo apkaltinamasis nuosprendis naikintinas, o byla perduotina tirti iš naujo.

Teismų praktika liudija, kad tapatybės vagystei jau dabar turėtų būti skiriama kur kas daugiau dėmesio.

4 skirsnis. Asmenys, darantys elektroninius nusikaltimus

Informacinės technologijos suteikia unikalių galimybių žmonėms, turintiems kriminalinių tikslų. Formuojasi organizuotos elektroninių nusikaltėlių grupės, kurias sudaro nariai iš viso pasaulio.

Elektroniniai nusikaltėliai, beje, yra pelnę didesnį visuomenės palankumą negu tradiciniai. Nuomonė, kad elektroninis nusikaltėlis yra ne toks pavojingas, neteisinga. Manoma, kad ateities grėsmė bus beveik proporcinga informacinių technologijų teikiamiems pranašumams.

Kodėl reikia žinoti, kas yra elektroninių nusikaltimų subjektai? Atskirų kategorijų tipinių nusikaltimų išskyrimas, šių žmonių pagrindinių bruožų žinojimas leidžia optimaliai išskirti grupę žmonių, tarp kurių reikėtų ieškoti nusikaltėlio, ir nustatyti konkretaus nusikaltėlio išaiškinimo būdus.

Daugelis elektroninių nusikaltimų tyrinėtojų šios rūšies nusikaltimų atsiradimą sieja su programišių, vadinamųjų hakerių, atsiradimu. Tačiau programišius – ne vienintelis elektroninio nusikaltėlio tipas. Nors į elektroninius nusikaltėlius reikėtų žiūrėti kaip į bendrą visumą, pagal tam tikrus požymius galima išskirti kai kurias jų rūšis. Kaip matyti iš istorijos, elektroninius nusikaltimus vykdo įvairūs žmonės: studentai, mėgėjai, teroristai, nusikalstamų grupuočių nariai. Tačiau skiriasi jų padarytų nusikaltimų pobūdis. Asmuo, kuris patenka į kompiuterį neturėdamas nusikalstamų ketinimų, skiriasi nuo finansų institucijos darbuotojo, vagiančio pinigus iš klientų sąskaitų. Labai prieštaringai vertinami tipiški elektroninių nusikaltėlių įgūdžiai.

Elektroniniai nusikaltėliai priklauso skirtingiems visuomenės sluoksniams. Jų amžius vidutininškai svyruoja nuo šešių ar septynių iki šešiadešimties ir daugiau metų, įgūdžių lygis – nuo naujoko iki profesionalo.

Nors ankstesni tyrimai atskleidė, kad didžiausią grėsmę kelia darbuotojai (vidiniai nusikaltėliai), vėlesnės tendencijos rodo, kad labai padaugėjo išorės nusikaltėlių. Todėl elektroniniai nusikaltimai jau nebegali būti taip dažnai vadinami vidiniais nusikaltimais. Manytina, kad išorinių nusikaltimų skaičiaus didėjimą, palyginti su bendru elektroninių nusikaltimų skaičiumi, lėmė sparti interneto plėtra ir penetracija. Ir nors įvairių tyrimų, koks procentas elektroninių nusikaltimų įvykdomi iš vidaus ir iš išorės, rezultatai skiriasi, manytina, kad tokie skirtingi duomenys yra dėl elektroninių nusikaltimų latentiškumo.

Egzistuoja daug tyčinių elektroninių nusikaltėlių skirstymo būdų. Pateiktinas prof. S. Brennerio siūlomas elektroninių nusikaltėlių skirstymas. Nusikaltėlių, vykdančių elektroninius nusikaltimus, rūšys pateikiamos atsižvelgiant į dažniausiai daromus elektroninius nusikaltimus (pvz., neteisėtą

prieigą, sukčiavimą). Prof. Brenneris elektroninius nusikaltėlius skirsto į šias grupes (*Brenner*, 2010):

1) programišius;
2) vidinius nusikaltėlius;
3) sukčiautojus;
4) persekiotojus (angl. *stalkers)*.

Programišius – nauja kategorija, atsiradusi XX amžiuje. Dažnas nusikaltimas e. erdvėje prasideda nuo neteisėtos prieigos. Pirmuosius programišius galima net pavadinti „sportininkais-studentais", nes jie neteisėtą prieigą vertino kaip intelektualų iššūkį. Taigi pirmieji programišiai į kompiuterių sistemas įsilauždavo norėdami pasilinksminti, bet ne dėl finansinės naudos. Šiuo metu šio tipo nusikaltėlių mažėja (dėl tos priežasties, kad vis mažiau įsilaužimų į kompiuterių sistemas vykdoma vien dėl sportinio intereso).

Vidinės atakos tapo labai didele grėsme kompiuterių saugumui. Mokslininkai vidinius nusikaltėlius apibūdina kaip individus, kurie būdami autorizuoti informacinių sistemų vartotojai (ar tokie buvę) netikėtai padaro žalos. Tyrimai rodo, kad yra tam tikrų skirtumų tarp vidinių nusikaltėlių bankų ir finansų sektoriuje ir nusikaltėlių, dirbančių su kritine infrastruktūra. Pirmuoju atveju tokių nusikaltėlių daromi elektroniniai nusikaltimai nėra labai sudėtingi ir kompleksiniai, dažniausiai naudojamos netechninės pažeidžiamos vietos (organizacijos politika ir kt.). Svarbiausias tokių nusikaltėlių tikslas dažniausiai būna finansinė nauda, bet ne žala organizacijai. Tuo metu kritinės infrastruktūros atveju, kaip rodo tyrimai, 86 proc. elektroninių nusikaltimų padaro techniniai darbuotojai (sistemos administratoriai ir pan.). 84 proc. atvejų pagrindinis tokių nusikaltėlių motyvas – kerštas. Šie nusikaltėliai organizacijai paprastai padaro labai daug žalos.

Sukčiavimas – vienas iš tų nusikaltimų, kurie atsiradus e. erdvei gali būti įvykdomi ją pasitelkus. Tokie nusikaltėliai dažnai veikia iš kitos valstybės (pvz., Nigerijos sukčiavimo atvejai). Elektroninė erdvė suteikia galimybių tokiems nusikaltėliams savo aukas pasiekti beveik visame pasaulyje (ten, kur veikia interneto ryšys). Tarptautinis nusikaltimų pobūdis gerokai pasunkina tokių nusikaltėlių išaiškinimą.

Elektroninės erdvės persekiotojai elektroninius nusikaltimus vykdo veikiami labai įvairių motyvų. Vieni iš dažniausių elektroninio persekiojimo atvejų, kai persekiojamas buvęs partneris. Nors dažni atvejai, kai persekiotojas savo aukos gali ir nepažinoti.

Knygoje „Computer crime: A Crimefighter`s Handbook" *(Icove D., 1995)* nusikaltėliai skirstomi į šias grupes[62]:

[62] Šis skirstymas aktualus ir šiandien.

1) programišius;
2) tipinius nusikaltėlius;
3) vandalus.

Šios kategorijos tam tikrais atvejais susiduria. Geriausia juos atskirti pagal motyvus. Programišiai dažniausiai nori tik patekti į kompiuterių sistemą, šių nusikaltėlių pagrindinis motyvas – nauda ir pinigai, o vandalai dažniausiai nori padaryti kokios nors žalos.

1. Programišiai

Šie žmonės labai gerai išmano kompiuterių programų ir kompiuterių tinklų kūrimo procesus bei jų spragas. Labai didelė jų dalis yra kompiuterių technikos fanatikai, nuolat ieškantys silpnų kompiuterių įrangos vietų, kurių nežino net patys įrangos kūrėjai. Dėl šios priežasties tokie nusikaltimai vadinami baltųjų apykaklių nusikaltimais. Šio tipo nusikaltimams nereikia įspūdingų raumenų ar galingų ginklų, jie daromi pasitelkus intelektą: įsibrauti į banką per atstumą gali asmuo, neturintis kojų, tačiau gerai išmanantis kompiuterių techniką ir turintis prieigą prie kompiuterių tinklo.

Bet kokios kategorijos nusikaltėliai gali padaryti tą patį, ką ir programišiai, tačiau šių grupė yra unikali. Istoriškai savo „profesija“ jie susiviliojo iš nuobodulio arba norėdami pademonstruoti intelektualinius gebėjimus. Jie gali veikti ištisą naktį, nes dieną dažniausiai būna mokykloje arba darbe.

Dauguma šių nusikaltėlių yra paaugliai. Nors šie žmonės dar labai jauni, jie jau gali sėkmingai įsiveržti į bet kokio tipo kompiuterių sistemas: bankų, įmonių, gamyklų ar karines. 1989 m. keturiolikmetis, naudodamas asmeninį kompiuterį, įsilaužė į JAV karinių pajėgų navigacinę palydovų sistemą. Vėliau tiriant bylą buvo išsiaiškinta, kad įsilaužėlio karjerą jis pradėjo aštuonerių.

Kai kurie programišiai veikia grupėmis, bet yra ir vienišių. Nors ir turi neeilinių protinių gebėjimų, dauguma iš jų prastai mokosi mokykloje arba jos išvis nelanko. Kai kurie be bičiulių programišių, su kuriais dažniausiai bendrauja ne būdami kartu, o per kompiuterių ar socialinius tinklus, turi mažai draugų. Susikūrusios programišių grupės siekia būti neformalios.

Programišius (angl. *hacker)* – reiškia juvelyrą, žmogų, kuris kruopščiai atlieka savo darbą. Analogiškai kompiuterių programišius – tai žmogus, juvelyriškai dirbantis kompiuteriu. Kitais žodžiais tariant, jis gali padaryti tai, ko nesugebėtų paprastas vartotojas.

Pagal priklausomybę programišius galima skirstyti į dvi grupes:

- vidinius darbuotojus;
- „svetimšalius“.

Programišiai pagal profesionalumą skirstomi į dar dvi pagrindines grupes:

- diletantus;
- profesionalus.

Diletantai paprastai būna jauni žmonės (17–25 m.), besimėgaujantys kompiuteriais, savo intelektualinėmis galimybėmis, padedančiomis įveikti kliūtis, kurios neįveikiamos paprastiems vartotojams.

Programišius diletantas paprastai siekia šių tikslų:

1) įsibrauti į sistemą ir nustatyti jos paskirtį;
2) gauti prieigą prie žaidimų;
3) pakeisti ar ištrinti duomenis ir tyčia palikti savo pėdsakų.

Dauguma diletantų nepavojingi 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 rasti programos klaidų ir jas ištaisyti, sumaniai pasinaudoti tokiomis klaidomis ar šalutiniais programos darbo poveikiais. Tikėtina, kad jie yra didelės dalies virusų ir Trojos arklių kūrėjai.

Dažnai vien dėl malonumo ir asmeninio pasitenkinimo tokie prog-ramišiai įsiskverbia į įvairių operacinių sistemų, turinčių daugiapakopę apsaugą, apsaugos sistemas. Šių programišių motyvai paprasti: jie arba nori gauti prieigą prie žaidimų, arba parodyti savo gebėjimus. Pastarasis variantas kur kas rimtesnis, nes programišiai sistemoje gali padaryti įsilaužimo žymių, sugadinti kokius nors failus arba paprasčiausiai palikti žinučių. Pavojingi bet kokie įsilaužimai į kompiuterių sistemą. Įsilaužėlis gauna prieigą prie vartotojų failų, kuriuose gali būti saugoma konfidenciali informacija. Kiekvienas gana kvalifikuotas programišius supranta, kad jį sugauti labai sunku. Patrauktas atsakomybėn, toks asmuo neretai atsiperka nedidelėmis baudomis.

Gerokai pavojingesni profesionalūs programišiai, kurie aktyviai naudoja savo žinias, kad padarytų žalos kitiems ar gautų asmeninės naudos. Veikti jie gali savo iniciatyva, taip pat kaip nusikalstamos grupuotės nariai arba vykdydami nurodymus. Dažniausiai profesionalūs programišiai nusitaiko į bankus, draudimo bendroves ar įvairias firmas.

Profesionalūs programišiai skirstomi į šias grupes:

1) nusikaltėlių grupuotes, siekiančias politinių tikslų;
2) asmenis, besistengiančius gauti informacijos pramoninio šnipinėjimo tikslais;
3) asmenų grupuotes, susiformavusias pasipelnymo tikslais.

Dvi paskutinės grupės beveik nesiskiria nuo tipinių nusikaltėlių. Profesionalūs programišiai – tai pereinamoji grandis tarp programišių ir tipinių

nusikaltėlių. Kai pagrindinė programišiaus veikla susijusi su naudos gavimu, jis tampa nusikaltėliu.

Tam, kad programišiai pasiektų savo tikslus, jiems reikalingas betarpiškas priėjimas arba prieiga per kompiuterių tinklus. Betarpiškas priėjimas prie kompiuterių sistemos įmanomas tada, kai tam tikras pastatas yra prastai saugomas. Kai kurių darbuotojų, paliekančių savo kompiuterius be priežiūros, nerūpestingumas labai palengvina įsilaužėlių darbą. Gerai pasiruošusiam programišiui nereikia daug laiko, kad įsibrautų į kompiuterių sistemą: nuo penkiolikos iki dvidešimties minučių (labai gerai po darbo) gali užtekti įsiskverbti į kompiuterių sistemą, saugomą daugiapakope apsauga. Pirmojo įsibrovimo metu gautų duomenų pakanka, kad nusikaltėliai išsiaiškintų, per kiek laiko galima įsiskverbti į kompiuterių sistemą bet kuriuo metu.

Profesionalūs nusikaltėliai visada stengiasi kuo labiau sumažinti riziką. Nusikaltimų darymas pasitelkus kompiuterių tinklą leido jiems tapti beveik nesugaunamiems. Neretai kartu su jais dirba ir firmos darbuotojai arba neseniai iš darbo atleisti asmenys. Tokių buvusių darbuotojų pagalbos profesionalūs nusikaltėliai ypač siekia tais atvejais, kai firmos kompiuterių tinklas yra gerai saugomas.

2. Tipiniai nusikaltėliai

Tai dažniausiai būna suaugę žmonės. Jie koncentruojasi į dvi pagrindines veikas: šnipinėjimą ir sukčiavimą bei piktnaudžiavimą.

Šnipinėjimas. Ši elektroninių nusikaltėlių kategorija – tai asmenys, kurie vagia slaptą informaciją iš strategiškai svarbių ir kitų objektų. Į šią kategoriją įeina ir nusikaltėliai, vagiantys informaciją iš teisėsaugos kompiuterių; industrinio šnipinėjimo agentai, dirbantys konkurentų firmoms ar užsienio vyriausybėms, pasirengusioms mokėti už vogtą informaciją.

Sukčiavimas ir piktnaudžiavimas. Apgavysčių ir piktnaudžiavimo naudojant kompiuterius atvejų sparčiai daugėja. Kriminalinės grupuotės – tiek vietinės, tiek tarptautinės – į elektroninius nusikaltimus įsitraukia kaip į tiesioginį nelegalių pajamų šaltinį. Nusikaltėliai supranta, kad vykdydami kompiuterinį sukčiavimą jie gali uždirbti daugiau pinigų ir kur kas saugiau, nei darydami kitus įprastus nusikaltimus. Bankai visada traukė kompiuterinius nusikaltėlius. 1988 m. septynių įsilaužėlių grupė atliko operaciją, nukreiptą į vieną iš stambiausių Vakarų bankų. 70 mln. dolerių, kurie priklausė trims bendrovėms, jie pirmiausia neteisėtai pervedė į vieną iš Niujorko bankų, paskui – 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 vieno iš bendrininkų namus. Kai pinigai buvo pervesti, trys bendrovės susisiekė su banku, kad išsiaiškintų, kas įvyko. Prasidėjo tyrimas, ir telefono numeris, kuriuo buvo atliekami kontroliniai skambučiai, padėjo rasti nusikaltėlių pėdsakus.

3. Vandalai

Šios kategorijos nusikaltėliai dažniausiai nedaro nusikaltimų tam, kad parodytų savo intelektualinius gebėjimus (kaip programišiai) ar finansiniais, politiniais sumetimais (kaip elektroniniai nusikaltėliai). Vandalizmo motyvas dažnai būna kerštas už realų ar išgalvotą įžeidimą. Dažniausiai šios kategorijos žmonės būna pikti, paprastai pyksta ant konkrečios organizacijos, bet kartais būna tiesiog apskritai nusivylę gyvenimu. Vandalus apytikriai galima suskirstyti į dvi grupes, kurias būtų galima pavadinti naudotojais ir svetimšaliais. Naudotojai yra tie, kurie piktnaudžiauja teisėta prieiga prie kompiuterių sistemos. Svetimšaliai teisėtos prieigos prie sistemos neturi.

Pagal alternatyvų elektroninių nusikaltėlių skirstymą, egzistuoja hakeriai ir krakeriai. Remiantis naujuoju hakerių žodynu, krakeris apibrėžiamas taip: tas, kuris pralaužia kompiuterių sistemos apsaugą. Hakeris apibrėžiamas kaip asmuo, kuris mėgaujasi programinėmis sistemomis, kad išlavintų savo gebėjimus, dirba iš entuziazmo. Ir hakeriai, ir krakeriai įsilaužia į kompiuterių sistemas, bet jų įsilaužimo motyvai skiriasi. Hakeriai įsilaužia tam, kad patikrintų savo intelektualinius gebėjimus, o krakeriai yra piktavališkesni ir padaro žalos kompiuterių sistemoms. Dažniausi motyvai – naudos siekimas arba kerštas.

Naujausioje literatūroje hakeriai skirstomi į „baltąsias skrybėles“, „pilkąsias skrybėles“ ir „juodąsias skrybėles“. Pirmoji grupė dažniausiai klientų užsakymu testuoja sistemas, turėdami tikslą rasti silpnų vietų ir taip stiprinti kibernetinį saugumą. Antroji grupė žmonių naudoja savo įgūdžius tam, kad kovodami su įvairiais „kenkėjais“ užtikrinų e. erdvės saugumą. Tačiau jų pačių veikla gana dažnai peržengia įstatymo ribas ir daugeliu atvejų gali būti kvalifikuojama kaip nusikaltimai. Ši grupė savo veiklą dažniausiai pateisina ginama didesne vertybe. Tuo metu trečioji grupė savo žinias ir įgūdžius naudoja siekdama tiesioginės naudos, pradedant asmeninės hakerio „reputacijos“ didinimu ir baigiant informacijos pasisavinimu turint tikslą tokią informaciją parduoti ir gauti finansinės naudos.

Reikėtų paminėti ir elektroninių nusikaltėlių klasifikaciją, paplitusią Rusijoje. Šioje šalyje elektroninių nusikaltimų subjektai skirstomi į tris grupes:

1. Pirmajai elektroninių nusikaltėlių grupei priklauso kompiuterių technikos profesionalai, programavimo žinovai. Jiems dar būdingas

tam tikras fanatizmas ir išradingumas. Kai kurių autorių manymu, šie subjektai kompiuterių technikos priemones vertina kaip tam tikrą iššūkį jų profesionalioms žinioms. Būtent tai ir yra pagrindinis stimulas vykdyti veikas, kurių dauguma yra nusikalstamos. Reikia paminėti dar vieną minėtosios grupės požymį – šie nusikaltėliai neturi jokių konkrečių tikslų pažeisti įstatymo. Beveik visus veiksmus jie atlieka norėdami pademonstruoti savo intelektualinius ir profesinius gebėjimus. Šios grupės atstovai yra gana smalsūs, aukšto intelekto ir turi tam tikro „sportinio azarto". Jie bet kokiomis priemonėmis nori įrodyti savo pranašumą prieš kompiuterius. Paprastai tai ir paskatina juos padaryti nusikaltimą.

Kartais laikui bėgant šios kategorijos žmonės ne tik įgyja patirties, bet ir keičiasi jų interesai. Iš savo veiklos jie siekia gauti materialinės naudos. Tokiu būdu programuotojas mėgėjas virsta profesionaliu nusikaltėliu.

Taigi galima išskirti tokius nagrinėtosios grupės požymius:

- nėra tam tikro išankstinio pasiruošimo padaryti konkretų nusikaltimą;
- nusikaltimo padarymo būdas turi būti originalus;
- nusikaltimui naudojamos buitinės kompiuterių technikos priemonės;
- nusikaltimo pėdsakai neslepiami.

2. Šiai grupei artima ir kita nusikaltėlių grupė, serganti naujosiomis psichikos ligomis, t. y. informacinėmis ligomis ir kompiuterinėmis fobijomis.

Minėtųjų negalavimų atsiranda žmogui sistemingai pažeidžiant informacinį režimą: arba dėl informacijos bado, arba dėl jos perkrovos. Šių klausimų tyrimu užsiima gana nauja medicinos šaka – informacinė medicina. Žiūrint iš šios srities pozicijų, žmogus suprantamas kaip universali, save reguliuojanti informacinė sistema, turinti nustatytą biologinės informacijos balansą. Šį pažeidus dėl vidinių ar išorinių destabilizuojančių faktorių susergama įvairiomis informacinėmis ligomis, iš jų labiausiai paplitusios informacinės neurozės. Kitais žodžiais tariant, žmogui reikia vienodos kiek fizinės, tiek informacinės apkrovos. Kai jos trūksta, prasideda informacinis badas, kai per daug – žmogus kenčia nuo informacinės perkrovos (pasireiškia įvairūs stresai ir emociniai protrūkiai). Visa tai gali peraugti į informacinę ligą. Esant dabartiniam darbo kompiuterizavimui, daugelis darbuotojų patenka į stresines situacijas, kai kada tai baigiasi kompiuterine fobija. Tai ne kas kita, kaip profesinė liga. Jos simptomai yra tokie: greitas nuovargis, staigūs kraujo spaudimo šuoliai, naudojantis kompiuteriu fiziškai ir jo garso bei vaizdo galimybėmis, galvos svaigimas ir skausmas, galūnių drebėjimas ir t. t. Iš esmės atsiranda baimė prarasti savikontrolę.

Taigi elektroninius nusikaltimus gali daryti žmonės, sergantys minėtosiomis psichikos ligomis. Tiriant tokį elektroninį nusikaltimą, būtina skirti teismo psichiatrinę ekspertizę, kad būtų nustatyta kaltinamojo psichikos būklė nusikaltimo padarymo metu (ar tai nebuvo afekto būsena arba nepakaltinamumas).

Dažniausiai šios grupės nusikaltėliai iš dalies arba visiškai praradę kontrolę, fiziškai naikina kompiuterius (be nusikalstamų ketinimų).

3. Trečiąją grupę sudaro profesionalūs elektroniniai nusikaltėliai. Į šią grupę įeina žmonės, kurių nusikalstami ketinimai yra aiškiai išreikšti. Skirtingai nei pirmųjų dviejų grupių, jų veikos nebūna vienkartinės. Dažniausiai jie slepia savo nusikaltimus. Paprastai šie žmonės būna gerai organizuotų grupių, aprūpintų specialia technika (neretai operatyvine), nariai. Tai kvalifikuoti specialistai, turintys techninį, aukštąjį juridinį ar ekonominį išsilavinimą. Būtent ši grupė kelia didžiausią grėsmę visuomenei. Pavyzdžiui, 79 proc. pinigų grobimų stambiu mastu įvykdo būtent šie asmenys.

Galimos ir kitokios elektroninių nusikaltėlių pagal elektroninių nusikaltimų įvykdymo būdus klasifikacijos, vienos iš jų pavyzdys:

1) krekeriai[63] (angl. *cracker)* – asmenys, vykdantys įsilaužimus (įskaitant duomenų modifikavimą, blokavimą ar sunaikinimą) į įstatymo saugomas informacines sistemas;
2) frekeriai (angl. *phreacker)* – asmenys, kurie vykdo elektroninius nusikaltimus naudodami elektroninius ryšius, kai pasitelkus specialias priemones slapta perimama konfidenciali informacija;
3) karderiai (angl. *card)* – asmenys, vykdantys elektroninius nusikaltimus, susijusius su mokėjimo kortelių apyvarta.

Kaip matyti, elektroninių nusikaltėlių klasifikacijų yra daug ir įvairių. Tai tik parodo šios nusikaltimų grupės subjektų įvairovę ir neteisėtos veiklos mastą bei spektrą.

5 skirsnis. Teisiniai elektroninių nusikaltimų aspektai

Pastaraisiais dešimtmečiais matoma sparti informacinių technologijų sklaida ir tiek gerokai padidėjusi elektroninės informacijos vertė bei reikšmė socialiniame gyvenime, tiek didžiuliais tempais didėjanti elektroninių ryšių tinklų skverbtis, tiek ir didėjantis prie tinklo prijungtų įrenginių skaičius, o kartu ir tolesnis elektroninių nusikaltimų atvejų daugėjimas. Tai

[63] Nors, kita vertus, krekeriais dažnai vadinami asmenys, nulaužinėjantys kompiuterių programų ar garso ir vaizdo turinio failų techninę apsaugą.

lemia būtinybę įstatymų leidėjui imtis priemonių, padedančių apsaugoti elektroninę erdvę ir kovoti su pavojingomis veikomis internete.

1. Tarptautiniai ir ES dokumentai dėl elektroninių nusikaltimų

Tarptautiniu mastu elektroninių nusikaltimų sritį reguliuoja (teisines priemones koordinuoja) šios organizacijos: EBPO, Europos Taryba, Jungtinių Tautų Organizacija, Pasaulio prekybos organizacija, Europos Komisija ir kt. Toliau aptartini pagrindiniai dokumentai, susiję su elektroniniais nusikaltimais.

1.1. Konvencija dėl elektroninių nusikaltimų

Svarbiausias tarptautinės teisės aktas elektroninių nusikaltimų srityje – 2001 m. Konvencija dėl elektroninių nusikaltimų CETS Nr. 185. Šis teisės aktas mokslinėje literatūroje laikomas vienu iš sistemingiausių tarptautinių teisės aktų, reguliuojančių „žalingas“ ir kriminalines veikas, naudojant elektroninius įrenginius ir elektroninę erdvę.

Atsižvelgiant į tai, kad elektroninėje erdvėje vykdomos veikos yra pavojingos visuomenei, nusikaltėlio buvimo ir nusikaltimo padarymo vieta dažnai nesutampa, atskirų valstybių įstatymai yra apriboti jų teritorija, elektroninė erdvė leidžia atlikti naujo tipo pavojingas veikas, bei 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. 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 nusikalstamų veikų kompiuterių tinkluose problemoms spręsti. 2001 m. lapkričio 8 d. Konvencijai dėl elektroninių nusikaltimų pritarė užsienio reikalų ministrai, o Europos Tarybos šalys narės ją pasirašė 2001 m. lapkričio 23 dieną. Konvencijos įsigaliojimo sąlyga – penkios ratifikacijos (iš jų – bent trys Europos Tarybos valstybių narių). Ši sąlyga buvo įvykdyta, ir Konvencija įsigaliojo 2004 m. liepos 1 dieną. Lietuva Konvenciją pasirašė 2003 m. birželio 23 d., o ratifikavo 2004 m. kovo 18 dieną.

2015 m. pabaigoje Konvenciją buvo ratifikavusios 47 valstybės. Kadangi iš viso yra 195 valstybės[64], Konvencija ne mažiau nei tikėtasi veikia globalią kovą su elektroniniais nusikaltimais. Esama nuomonių, kad

[64] Pagal skirtingus vertinimus, šis skaičius gali skirtis.

Konvencija iki galo nepasiekė užsibrėžtų tikslų, todėl jos neratifikavusios valstybės vis dar raginamos tai padaryti.

Konvencijos struktūra ir turinys aptartini detaliau. Ją sudaro trys pagrindiniai skyriai: I. Sąvokos; II. Priemonės, kurių reikia imtis nacionaliniu lygiu, bei III. Tarptautinis bendradarbiavimas. Pirmojo skyriaus 1 skirsnyje (Konvencijos 2–11 str.) 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 kompiuterių, srauto duomenis, juos atskleisti ar pateikti, surinkti srauto duomenis realiuoju laiku, įrašyti tokius duomenis ir pan. Pastarųjų proceso veiksmų atlikimas susijęs su pagrindinėmis žmogaus teisėmis ir laisvėmis bei jų apsauga. Todėl pati Konvencija numato, kad minėtųjų veiksmų atlikimas turi būti suderinamas su pagrindiniais tarptautiniais žmogaus teisių ir laisvių apsaugos dokumentais. Trečiajame skyriuje Konvencija įtvirtina nuostatas, skirtas ekstradicijai ir savitarpio pagalbai reglamentuoti. Visos Konvencijos 2–11 str. 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 ar nagrinėjant baudžiamąsias bylas dėl elektroninių nusikaltimų. Tam tikslui Konvencijos 35 str. įpareigoja susitariančiąsias šalis skirti dvidešimt keturias valandas per parą ir septynias dienas per savaitę veikiančią instituciją, kuri galėtų teikti technines konsultacijas ir atlikti Konvencijoje nurodytus veiksmus.

1.2. Konvencijos dėl elektroninių nusikaltimų nuostatos dėl materialinės teisės

Konvencijos pirmojo skyriaus pirmajame skirsnyje, kuris susijęs su materialine teise, siūloma nustatyti teisinės atsakomybės pagrindus už šias pavojingų veikų rūšis:

- konfidencialumo, duomenų vientisumo, kompiuterių duomenų ir sistemų pažeidimus (neteisėta prieiga ir perėmimas, įsikišimas į duomenų apdorojimo ir kompiuterių sistemų darbo procesą, piktnaudžiavimas kompiuteriniais įrenginiais);
- su kompiuteriais susijusius pažeidimus (sukčiavimas, susijęs su kompiuteriais; klastojimas, susijęs su kompiuteriais);
- pažeidimus, susijusius su turiniu (pažeidimai, susiję su vaikų pornografija);
- pažeidimus, susijusius su autorių teisėmis ar gretutinėmis teisėmis.

Konvencijos nuostatos, susijusios su materialine teise (teisinės atsakomybės pagrindų už pavojingas veikas e. erdvėje nustatymu):

1) *konfidencialumo, duomenų vientisumo, kompiuterių duomenų ir sistemų pažeidimai*

Neteisėta prieiga. Konvencijos 2 str. 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 kompiuterių sistemų ir duomenų saugumui (konfidencialumui, integruotumui ir prieinamumui), t. y. angliškai vadinamas *Hacking, Cracking*, *Computer trespass*. Tame pačiame Konvencijos straipsnyje nurodoma, kad nustatant baudžiamosios atsakomybės pagrindus gali būti reikalaujama, jog nusikaltimas būtų padaromas pažeidžiant saugumo priemones, siekiant gauti kompiuterinės informacijos arba turint nesąžiningą tikslą, arba kai veika yra susijusi su kompiuterių sistema, kuri sujungta su kita kompiuterių sistema. Anksčiau paminėta formuluotė valstybėms narėms palieka tam tikrą veikimo laisvę nustatant baudžiamosios atsakomybės pagrindus už neteisėtą prieigą. Galima konstatuoti, jog Konvencijoje laikomasi nuostatos, kad tyčinė prieiga prie kompiuterių sistemos neturint tam teisės turi būti įvardijama kaip neteisėta veika.

Neteisėtas perėmimas. Konvencijos 3 str. nurodyta, jog „turi būti priimtos teisės normos, nustatančios baudžiamosios atsakomybės pagrindus už tyčinį informacijos perėmimą, neturint tam teisės, kai tai padaroma pasinaudojus techninėmis priemonėmis bei informacija, perimama neviešai siunčiant kompiuterinę informaciją į, iš ar viduje kompiuterių sistemos (įskaitant ir elektromagnetinį kompiuterio sistemos spinduliavimą).“ Šia nuostata siekiama apsaugoti duomenų komunikacijų privatumą, kuris saugomas Europos žmogaus teisių konvencijos 8 straipsniu. Paminėta veika gali būti vykdoma neteisėtai perimant kompiuterinę informaciją, siunčiant ją elektroniniu paštu, persiunčiant failus (sauginius) ir kt. Anksčiau paminėtos nuostatos tekstas praktiškai buvo perkeltas iš Rekomendacijos (89)9. Reikia pabrėžti, kad remiantis Konvencijos komentaru, sąvoka „neviešas“ turėtų būti vartojama kalbant apie informacijos perdavimo, o ne pačios perduodamos informacijos neviešumą. Tame pačiame Konvencijos straipsnyje nurodyta, jog nustatant baudžiamosios atsakomybės už minėtąją veiką pagrindus, gali būti reikalaujama nesąžiningo tikslo ar kad veika būtų susijusi su kompiuterių sistema, kuri 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, kad 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 str. nustatyta, jog „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 ar kompiuterių programų naudojimą. Konvencijoje taip pat nurodoma, jog nustatant baudžiamosios atsakomybės pagrindus už minėtąją veiką gali būti reikalaujama didelio žalos atlyginimo. Taigi ši Konvencijos formuluotė valstybėms narėms palieka tam tikrą veikimo laisvę.

Įsikišimas į kompiuterių sistemos darbo procesą. Konvencijos 5 str. nustatyta, jog „turi būti priimtos teisės normos, nustatančios baudžiamosios atsakomybės pagrindus už tyčinį pavojingą kompiuterių 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 ar darant įtaką kompiuterinei informacijai. Šiame Konvencijos straipsnyje, nustatant baudžiamosios atsakomybės pagrindus už minėtąją veiką, nesiūloma įvesti jokių papildomų požymių. Pabrėžtina, kad Konvencijos formuluotė valstybėms narėms nepalieka veikimo laisvės nustatant baudžiamosios atsakomybės pagrindus už neteisėtą įsikišimą į duomenų apdorojimo procesą.

Piktnaudžiavimas įrenginiais (angl. *Misuse devices)*. Konvencijos 6 str. nustatyta, jog „turi būti priimtos teisės normos, nustatančios baudžiamosios atsakomybės pagrindus už tyčinį:

a) įrenginio (priemonės), įskaitant kompiuterio programą, sukurto ar pritaikyto bet kuriam iš pažeidimų, nurodytų Konvencijos 2–5 str., padaryti, taip pat kompiuterinio slaptažodžio, prieigos kodo ar panašių duomenų, kuriais naudojantis galima prieiti prie kompiuterių sistemos, gaminimą, pardavimą, parūpinimą, importą, platinimą ar kitu būdu padarymą prieinamais;
b) įrenginio (priemonės), įskaitant kompiuterio programą, sukurto ar pritaikyto bet kokiam iš pažeidimų, nurodytų Konvencijos 2–5 straipsniuose, padaryti, laikymą.“ Tačiau Konvencijoje nurodyta, jog galima nustatyti, kad baudžiamoji atsakomybė taikoma tik tuo atveju, jeigu laikoma keletas tokių įrenginių (priemonių), tokiu būdu valstybėms narėms paliekama tam tikra pasirinkimo laisvė.

Ši nuostata skirta kaip atskirą nusikaltimą įvardyti tyčinį specifinių neteisėtų veikų, susijusių su įrenginiais (priemonėmis) ar prieigos informacija, padarymą, siekiant įvykdyti kitus Konvencijoje paminėtus nusikaltimus pažeidžiant kompiuterių sistemų ar duomenų konfidencialumą, integruotumą ar prieinamumą. Reikia paminėti, jog Konvencijoje paliekama teisė išvis nenumatyti baudžiamosios atsakomybės pagrindų už kompiuterinio slaptažodžio, prieigos kodo ar panašių duomenų, kuriais naudojantis galima prieiti prie kompiuterių sistemos, pardavimą, platinimą ar kitu būdu padarymą prieinamais. Paminėtina, jog siekiant atriboti pavojingas veikas, įvestas svarbus požymis – tikslas įvykdyti pažeidimus, susijusius su kompiuterių naudojimu. Tokiomis nuostatomis aiškiai įvardijama, kad priemonės, skirtos teisėtai testuoti kompiuterių sistemas, nepatenka į teisinės atsakomybės pagrindų veikimo sritį.

2) *Su kompiuteriais susiję pažeidimai*

Klastojimas, susijęs su kompiuteriais. Konvencijos 7 str. nustatyta, jog „turi būti priimtos teisės normos, nustatančios baudžiamosios atsakomybės pagrindus už tyčinį (taip pat neturint tam teisės) kompiuterių duomenų įvedimą, pakeitimą, ištrynimą, dėl to gaunami neautentiški duomenys (informacija), siekiant, jog jie būtų laikomi autentiškais.“ Šios nuostatos tikslas – nustatyti lygiagrečią atsakomybę, kaip ir atsakomybę už materialių dokumentų klastojimą, t. y. pašalinti baudžiamųjų įstatymų spragas, susijusias su atsakomybės pagrindų nustatymu už tradicinį klastojimą, kai atitinkami įstatymai netaikomi elektroniniams duomenims. Kadangi vis daugiau sandorių sudaroma elektronine forma, vis daugiau žmonių veiklos perkeliama į elektroninę erdvę, tad minėtoji nuostata yra gana svarbi. Be to, reikėtų paminėti, kad šiame straipsnyje valstybėms narėms palikta pasirinkimo laisvė, nustatant baudžiamosios atsakomybės pagrindus už minėtąją veiką, reikalauti tikslo apgauti ar kito nesąžiningo tikslo.

Sukčiavimas, susijęs su kompiuteriais. Konvencijos 8 str. nustatyta, jog „turi būti priimtos teisės normos, nustatančios baudžiamosios atsakomybės pagrindus už tyčinį (taip pat neturint tam teisės):

a) kompiuterinės informacijos įvedimą ar ištrynimą;

b) bet kokį įsikišimą į kompiuterių sistemos funkcionavimą,

dėl to padaroma žala, turint apgavikišką ar nesąžiningą tikslą gauti materialinės naudos sau ar kitam.“ Ši nuostata susijusi su nauja technologine revoliucija, dėl kurios atsirado unikalių galimybių daryti ekonominius nusikaltimus elektroninėje erdvėje. Kadangi kompiuterių sistemose apdorojama informacija (pvz., susijusi su pinigais) pasidarė labai vertinga, kai kuriais atvejais netgi vertingesnė už nekilnojamąjį turtą, šios nuostatos

įgyvendinimas tapo būtinas. Reikia paminėti, jog šiame straipsnyje nepaliekama jokios veikimo laisvės nustatant baudžiamosios atsakomybės pagrindus už nurodytą veiką.

3) *Pažeidimai, susiję su turiniu*

Pažeidimai, susiję su medžiaga su vaikų pornografija. Konvencijos 9 str. nustatyta, jog turi būti priimtos teisės normos, kaip nusikalstamas įvardijančios tyčines (taip pat neturint tam teisės) veikas:

a) medžiagos 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 ar siuntimą per kompiuterių sistemą;
d) medžiagos, susijusios su vaikų pornografija, siuntimą per kompiuterių sistemą sau ar kitam;
e) medžiagos, susijusios su vaikų pornografija, turėjimą kompiuterių sistemoje ar įrenginyje, galinčiame saugoti kompiuterinę informaciją.

Šiomis nuostatomis siekiama sustiprinti vaikų teisines apsaugos priemones, įskaitant jų apsaugą nuo seksualinio išnaudojimo, modernizuojant baudžiamosios teisės normas, siekiant kovoti su veikomis, kai naudojant kompiuterių sistemas ir tinklus padaroma seksualinių nusikaltimų vaikams. Konvencijos komentare pabrėžiama, jog nors daugelis valstybių yra kriminalizavusios tradicines veikas, susijusias su vaikų pornografijos naudojimu ir platinimu, nauja tokios nelegalios veiklos forma (pvz., vykdant per internetą) taip pat turėtų būti numatyta baudžiamuosiuose įstatymuose. Šiame straipsnyje nustatyta pasirinkimo laisvė nenustatyti baudžiamosios atsakomybės už išvardytas veikas, nurodytas d) ir e).

4) *Pažeidimai, susiję su autorių teisėmis ar gretutinėmis teisėmis*

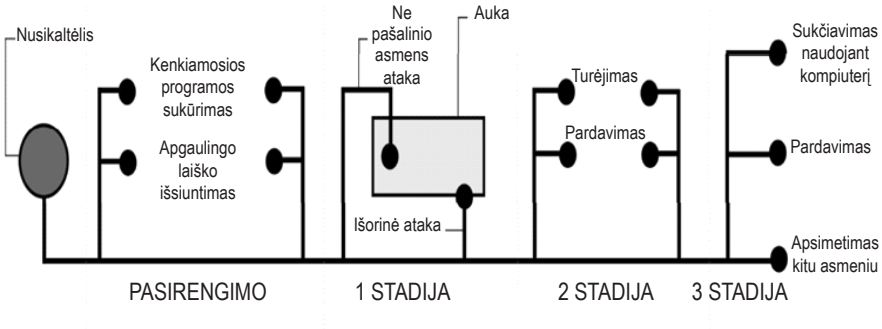
Konvencijos 10 str. nustatyta, jog „turi būti priimtos teisės normos, nustatančios baudžiamosios atsakomybės pagrindus už autorių teisių ir gretutinių teisių pažeidimą (pagal įstatymus, priimtus remiantis tarptautiniais dokumentais: (Berno konvencija dėl literatūros ir meno kūrinių apsaugos ir kiti)), padarytą naudojant kompiuterių sistemą, esant komerciškam tikslui.“ Tačiau tame pačiame straipsnyje nustatoma, jog už tokias veikas baudžiamoji atsakomybė gali būti ir nenumatyta, jeigu 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 labai pakeičia tarptautinę intelektualios nuosavybės apsaugą, ypač susijusią su apsaugotos medžiagos padarymu prieinama per internetą „pagal pareikalavimą“. Pavyzdžiui, 1996 m. PINO autorių teisių sutarties 6 str. platinimo teisė apibrėžiama taip: literatūros ir meno kūrinių autoriai turi išimtinę teisę suteikti leidimą padaryti jų kūrinių originalus ar jų kopijas viešai prieinamus, juos parduodant ar kitaip perduodant nuosavybėn.

S. Schjolbergas teigia, kad Konvencija remiasi nusikalstamomis veikomis, kurios egzistavo 1990 metais. Tačiau nuo to laiko atsirado naujų nusikaltimų metodų, kuriuos turėtų apimti baudžiamoji teisė, pvz., „slaptažodžio žvejyba“ (angl. *phishing)*, botnetų naudojimas, tapatybės vagystė ir kt.

Išskirtina tapatybės vagystės elektroninėje erdvėje kriminalizavimo problema. Pastaruoju metu pasauliniu mastu vyksta diskusijos, ar ši pavojinga veika turėtų būti kriminalizuota ir ar tokios veikos sudėties įtraukimas į valstybių baudžiamuosius įstatymus padėtų efektyviau kovoti su šiuo reiškiniu. Išsiskiria dvi konfrontuojančios pozicijos: vieni teigia, jog tapatybės vagystė turėtų būti kvalifikuojama kaip atskira, savo sudėtį turinti nusikalstama veika, t. y. siūlo šią veiką kriminalizuoti, argumentuodami, jog tais atvejais, kai užsienio valstybė neturi įstatymų, kriminalizuojančių tapatybės vagystę elektroninėje erdvėje kaip atskirą veiką, varžomos informaciją renkančios valstybės galimybės rinkti tapatybės vagystės elektroninėje erdvėje įrodymus atitinkamoje užsienio valstybėje. Tokiu atveju teisėsaugos institucijoms nėra suteikiama pakankamai įgaliojimų veiksmingai kovoti su tokio pobūdžio veikomis, pasunkinamas tokių veikų susekimas, tyrimas ir baudžiamasis persekiojimas nacionaliniu bei tarptautiniu lygiu. Tinkamai neįvertinus tapatybės vagystės, pasyviai laukiama kitų, dažnai sudėtingai ištiriamų, tarptautinių nusikaltimų padarinių ir tik tada pradedamos tirti kriminalizuotos veikos. Šios pozicijos oponentai tapatybės vagystę traktuoja kaip priemonę teisės pažeidimams ir (ar) nusikalstamoms veikoms vykdyti ir teigia, jog ši veika patenka į jau kriminalizuotas veikas reglamentuojančių straipsnių veikimo sritį, todėl tapatybės vagystės elektroninėje erdvėje nebūtina kriminalizuoti kaip savarankiškos veikos.

Nagrinėjant baudžiamosios atsakomybės už tapatybės vagystės elektroninėje erdvėje elementus, galima vadovautis M. Gercke'io sukurtu modeliu, kuriame pavaizduotos tapatybės vagystės elektroninėje erdvėje stadijos. Skiriamos trys tapatybės vagystės stadijos: pirmoji stadija – su tapatybe susijusios informacijos gavimas, antroji stadija – sąveika su tapatybe susijusia informacija, trečioji stadija – su tapatybe susijusios informacijos naudojimas siekiant padaryti nusikaltimą *(Gercke*, 2007).



9 pav. Trijų stadijų tapatybės vagystės modelis (Gercke, 2007).

Kai kurie autoriai laikosi pozicijos, jog yra tik dvi tapatybės vagystės stadijos: pirmoji stadija – su tapatybe susijusios informacijos gavimas, antroji stadija – neteisėtas su tapatybe susijusios informacijos naudojimas, tačiau šiame vadovėlyje laikomasi naujausioje literatūroje siūlomo tapatybės vagystės skirstymo į tris stadijas.

Nors šiuo metu kai kuriuos tapatybės vagystės elektroninėje erdvėje stadijų elementus Konvencija siūlo kriminalizuoti, vis dėlto kaip savarankiška veika tapatybės vagystė elektroninėje erdvėje neapibrėžta.

Pabrėžtina, kad tapatybės vagystės elektroninėje erdvėje veikos pavojingumas nekelia abejonių. Šia veika kėsinamasi į vienas svarbiausių vertybių: asmens teisę į privatumą ir teisinius nuosavybės santykius. Gali kilti klausimas, gal tapatybės vagystę elektroninėje erdvėje kaip savarankišką veiką užtektų pripažinti ne nusikaltimu, o kitu teisės pažeidimu (pavyzdžiui, asministracinės teisės pažeidimu)? Anot V. Piesliako, nusikaltimai nuo kitų teisės pažeidimų iš principo skiriasi didesniu pavojingumu. Nusikaltimo statusas suteikiamas pavojingiausioms žmogaus elgesio formoms. Nusikaltimai ir kiti teisės pažeidimai atskiriami vadovaujantis panašiais kriterijais kaip ir atskiriant nusikaltimus ir baudžiamuosius nusižengimus, t. y. pagal tam tikrus nusikalstamos veikos sudėties požymius. Vienas iš tokių požymių, dažnai naudojamas įstatymo leidėjo, yra nusikalstamos veikos dalykas, materiali jo vertė ar kiti dalyko požymiai. Autorių nuomone, tapatybės vagystės elektroninėje erdvėje atveju labai svarbūs kiti dalyko požymiai: grėsmė ir tikslas atlikti kitas nusikalstamas veikas. Pavyzdžiui, su asmens tapatybe susijusios informacijos laikymas yra būtina sąlyga įvykdyti kitus nusikaltimus, pvz., lėšų grobimą. Kaip pavyzdį galima paminėti ir LR BK 309 str. 2 d., kurioje kriminalizuotas pornografinės medžiagos apie vaikus laikymas, kuris kelia pavojų, kad nusikaltėlis, laikydamas tokią medžiagą, realybėje imsis neteisėtų veiksmų prieš vaikus.

Atsižvelgiant į tai, svarstytinas klausimas dėl Konvencijos papildymo nauja nusikalstama veika – tapatybės vagyste elektroninėje erdvėje.

1.3. 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 rimtų kliūčių minėtiesiems nusikaltimams tirti. Viena iš didžiausių kovos su elektroniniais nusikaltimais problemų – nusikaltimo subjekto identifikavimas, taip pat nusikalstamos veikos masto ar poveikio įvertinimas. Iššūkį kelia ir elektroninės informacijos, kuri gali tapti nusikalstamos veikos įrodymu, pažeidžiamumas, galimybė ją pakeisti ar sunaikinti. Užsienio valstybių praktika rodo, kad dažnai neužtenka galiojančių procesinių normų, kurios istoriškai pritaikytos tradiciniams nusikaltimams tirti (pvz., kratos išplėtimo kompiuterių tinkluose problema).

Atskiras Konvencijos skirsnis skirtas valstybių nacionalinių įstatymų proceso normoms suvienodinti. Šiuo 2 skirsniu siekiama tradicines procesines priemones, tokias kaip kratą ir poėmį, pritaikyti elektroninei aplinkai. Be to, tradicines įrodymų rinkimo priemones, pvz., kratą ir poėmį siekiant padaryti efektyvias besikeičiančioje elektroninėje aplinkoje, nustatomos tokios naujos priemonės kaip operatyvus laikomųjų kompiuterių duomenų išsaugojimas ir pan. Išskirtinos šios toliau nagrinėtinos pagrindinės proceso teisės skirsnio nuostatos dėl procesinių priemonių: operatyvus laikomųjų kompiuterių duomenų išsaugojimas, laikomųjų kompiuterių duomenų paieška ir poėmis bei kompiuterių duomenų surinkimas realiuoju laiku.

Konvencijos apžvalgoje teigiama, kad Lietuva, siekdama įgyvendinti Konvencijos nuostatas, pakeitė Lietuvos Respublikos baudžiamojo proceso kodeksą. Prisidėjus prie Konvencijos, Lietuvos Respublikos baudžiamojo proceso kodeksas buvo papildytas ir pakeistas (pvz., kodekso 154 str. papildymas antrąja dalimi). Tačiau ar įstatymo leidėjas identifikavo visas su elektroniniais nusikaltimais susijusias procesines problemas, kurias mėginama spręsti pasitelkus Konvencijos proceso teisės skirsnį?

Operatyvus laikomųjų kompiuterių duomenų išsaugojimas

Konvencijoje dėl elektroninių nusikaltimų teigiama, kad „kiekviena šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti įgalinant jos kompetentingas institucijas nurodyti arba panašiai pasirūpinti operatyviu konkrečių kompiuterių duomenų, įskaitant srauto duomenis, laikomus kompiuterių sistemoje, išsaugojimu, ypač, kai yra pagrindo manyti, jog tie kompiuterių duomenys gali būti nesunkiai prarasti arba pakeisti.“

Konvencijos 17 str. irgi reglamentuojamas minėtųjų išsaugotų duomenų atskleidimo galimybės užtikrinimas, o 18 str. – nurodymas dėl duomenų pateikimo.

Poreikis išsaugoti kompiuterių duomenis gali atsirasti tais atvejais, kai tyrimo nustatyta, jog tam tikri kompiuterių duomenys kitų duomenų srauto sudėtyje yra laikomi atitinkamo paslaugų teikėjo serveryje, kur teikėjas verslo tikslams kaupia ši srautą už tam tikrą laikotarpį. Tam, kad reikiama informacija iš duomenų srauto būtų išskirta bei išimama, reikalinga laikina duomenų apsauga. Tai įmanoma įgyvendinti tik tuo atveju, jei tyrimo organai turės atitinkamas teises įpareigoti paslaugų teikėją išsaugoti saugomus kompiuterių duomenis.

Ši priemonė taikytina tuo atveju, kai kompiuterių duomenys jau išsaugoti. Tačiau tyrimui svarbūs kompiuterių duomenys, nors ir išsaugoti, per trumpą laiką gali būti ištrinami. Pavyzdžiui, praktikoje galima situacija, kai paslaugos teikėjo užfiksuoti kompiuterių duomenys kompiuterių sistemoje saugomi ne ilgiau nei kelias valandas ar paras. Laikomų duomenų sunaikinimą gali lemti teisės aktų reikalavimai. Tuo atveju, kai kompiuterių duomenys laikytini asmens duomenimis, asmens duomenų apsaugą reglamentuojantys teisės aktai reikalauja tokius duomenis sunaikinti (arba padaryti anonimiškus) iš karto po to, kai šie duomenys tampa nereikalingi ūkinei veiklai užtikrinti.

Pabrėžtina, jog, Konvencijos rengėjų nuomone, tokia teisė įpareigoti subjektą išsaugoti laikomuosius kompiuterių duomenis nacionalinėje teisėje turi būti įtvirtinta ir siekiant suteikti galimybę pagelbėti kitai valstybei tarptautiniu lygiu, aktualius kompiuterių duomenis išsaugant savo teritorijoje. Taip būtų užtikrinta, kad svarbūs kompiuterių duomenys nebūtų prarasti iki to laiko, kol nustatyta tvarka bus gautas teisinės pagalbos prašymas suteikti informaciją. Atsižvelgiant į tai, kad per nusikaltimo tyrimo procesą skirtingų valstybių teisėsaugos institucijos privalo viena su kita bendradarbiauti tiek oficialiai, tiek ir neoficialiai, gali kilti tam tikrų problemų. Jeigu vienos iš valstybių teisės normos nenustato konkrečių įgalinimų rinkti elektroninę informaciją, tokia valstybė iš esmės gali būti nepajėgi adekvačiai reaguoti į prašymą suteikti pagalbą.

Laikomųjų kompiuterių duomenų paieška ir poėmis

Konvencijoje dėl elektroninių nusikaltimų teigiama, „jog kiekviena šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti, įgalinant jos kompetentingas institucijas apieškoti ar panašiai ištirti:

a) kompiuterių sistemą arba jos dalį ir joje laikomus kompiuterių duomenis;

b) kompiuterių duomenų atmeniąją terpę, kurioje tos Šalies teritorijoje gali būti laikomi kompiuterių duomenys.“

Kaip nurodyta Konvencijos 19 str. 2 d., „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 ar panašų tyrimą į kitą sistemą.“

Vienas iš pagrindinių aukščiau minėtų Konvencijos normų tikslų – kad elektroninės informacijos paėmimas iš apieškomos vietos nebūtų diskriminuojamas kitų materialių daiktų ar dokumentų atžvilgiu. Kitaip tariant, krata turi būti vienodai efektyvi tiek dėl materialių, tiek nematerialių objektų.

Labai aktuali nuostatų dėl kratos „išplėtimo“ įgyvendinimo problema. Konvencija nenurodo mechanizmo, kaip kratos „išplėtimas“ turi būti vykdomas. Tai paliekama nacionaliniam reguliavimui.

Šiuo metu nesiginčijama, jog tyrėjas turi turėti teises, norėdamas betarpiškai išplėsti paiešką į kitas sujungtas kompiuterių sistemas. Tačiau kaip tai turi būti įgyvendinama? Konvencijos rengėjų nuomone, nacionalinėje teisėje svarstytini keli kratos į kitą kompiuterių sistemą išplėtimo variantai:

1) išduota sankcija yra papildoma ją išdavusios institucijos, t. y. „išplečiama“ apimant ir kompiuterių sistemą, kurioje esanti informacija, prieinama iš tiriamosios kompiuterių sistemos;
2) suteikiami įgaliojimai sankciją gavusiai institucijai (pareigūnui) ją papildyti.

Nors pirmuoju atveju nereikėtų kreiptis dėl naujos sankcijos, šio varianto neigiama pusė būtų ta, jog tyrėjui, prieš „išplečiant“ kratos veiksmus į kitą kompiuterių sistemą, reikėtų kreiptis dėl sankcijos papildymo[65]. Turint omenyje kitoje kompiuterių sistemoje saugomos informacijos pažeidžiamumą ir tai, jog sankcijos papildymas negali būti atliekamas betarpiškai (t. y. tyrėjas turėtų atlikti veiksmus, kurie, laiko sąnaudų prasme, prilygintini naujos sankcijos gavimui) būnant kratos vietoje, šis būdas yra diskutuotinas.

Antruoju atveju tyrėjas nesikreiptų dėl sankcijos papildymo, o būtų traktuojama, jog išduota sankcija įgalina tyrėją savarankiškai „išplėsti“ paiešką į su tiriamąja kompiuterių sistema sujungtą kompiuterių sistemą,

[65] Tokio procesinio veiksmo galimybė Lietuvos Respublikos baudžiamojo proceso kodekse išvis nenumatyta.

esančią Lietuvos Respublikos teritorijoje, jei būtų manoma, kad toje kompiuterių sistemoje laikoma tyrimui svarbi informacija. Šiuo atveju būtų betarpiškai „išplečiama“ krata ir iki minimumo sumažinama galimybė pakeisti informaciją ar ją ištrinti iš atitinkamos kompiuterių sistemos, kol bus gauta nauja sankcija ar esamos sankcijos papildymas.

Paminėtina, jog Konvencijos aiškinamajame rašte įvardijama, kad kratos „išplėtimo“ galimybė nebūtinai turi būti reglamentuojama naujais teisės aktais pagal nacionalinę teisę. Jeigu egzistuojantys teisės aktai suteikia galimybę „išplėsti“ kratą, nėra būtinybės priimti naujų teisės normų, reglamentuojančių kratos „išplėtimą“.

Kompiuterių duomenų surinkimas realiuoju laiku

Konvencijoje numatyta, „jog kiekviena šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti, įgalinant 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.).

Kai kalbama apie kompiuterių duomenų surinkimą realiuoju laiku, turima omenyje įrodymų rinkimą iš esamu metu vykdomų komunikacijų, kurios generuoja tam tikrus duomenis. Reikėtų atskirti, jog šiuo atveju galimi dviejų tipų duomenys: srauto duomenys[66] bei turinio duomenys[67].

[66] 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. 2002-09-19 Konstitucinio Teismo nutarime telekomunikacijų įvykis apibūdinamas kaip „informacijos perdavimo, siuntimo, priėmimo telekomunikacijų tinklais faktas“. Pvz., srauto duomenimis laikytina informacija apie sujungimo laiką, trukmę, naudotus protokolus ir pan.

[67] Nei Konvencijoje, nei Lietuvos Respublikos 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) str., „pranešimas“ – tai informacija, kuria apsikeičiama arba kuri perduodama tarp baigtinio skaičiaus šalių, naudojantis viešai prieinamomis elektroninių ryšių paslaugomis. Kitaip tariant, turinio duomenimis laikytinas pokalbio telefonu ar elektroninio pašto žinutės turinys.

Manoma, jog procesiniai srauto ir turinio duomenų surinkimo reikalavimai turėtų skirtis, nes turinio duomenys atskleidžia komunikacijų turinį ir neteisėtas jų atskleidimas daro didesnę žalą, palyginti su neteisėtu srauto duomenų atskleidimu. Todėl turinio duomenų kontrolės sankcionavimas turėtų būti griežtesnis.

Vis dėlto net ir valstybėse narėse įgyvendinus šias Konvencijos nuostatas dėl proceso teisės, lieka neišspręstos kai kurios aktualios problemos. Viena iš jų – problema dėl įpareigojimų operatoriams užtikrinti technines *IP* telefonijos kontrolės galimybes.

1.4. Kitos Konvencijos dėl elektroninių nusikaltimų nuostatos

Svarbios konvencijos nuostatos dėl jurisdikcijos. Henrikas W. W. Kaspersenas jurisdikcijos problemą įvardija kaip opią, jis teigia, kad egzistuoja tiek taikomos jurisdikcijos nustatymo, tiek jurisdikcijų konfliktų problema elektroninėje erdvėje, kadangi elektroninė erdvė yra bendra, neapribota nacionalinių valstybių sienomis. Konvencijos 22 str. yra nustatyti teritorijos, pilietybės ir kiti principai, taikytini Konvencijoje numatytų veikų įvykdymo elektroninėje erdvėje atveju.

Konvencija taip pat įtvirtina nuostatas, skirtas ekstradicijos bei savitarpio pagalbos reglamentavimui. Visos Konvencijos 2-11 str. 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 ar nagrinėjant baudžiamąsias bylas dėl elektroninių nusikaltimų. Tuo tikslu Konvencijos 35 str. įpareigoja Susitariančiąsias Šalis skirti dvidešimt keturias valandas per parą ir septynias dienas per savaitę veikiančią instituciją, kuri galėtų teikti technines konsultacijas ir atlikti Konvencijoje nurodytus veiksmus.

1.5. Papildomasis Konvencijos dėl elektroninių nusikaltimų protokolas

Konvencijos dėl elektroninių nusikaltimų Papildomasis protokolas dėl rasistinio ir ksenofobinio pobūdžio veikų, padarytų naudojantis kompiuterių sistemomis, kriminalizavimo priimtas 2003 m. sausio 28 d. Strasbūre. 2011 m. balandžio mėnesį protokolą buvo ratifikavusios aštuoniolika valstybių. Lietuva šį protokolą ratifikavo 2006 m. birželio 8 d. įstatymu Nr. X-674.

Papildomojo protokolo tikslas – papildyti 2001 m. Konvencijos dėl elektroninių nusikaltimų nuostatas įpareigojimais valstybėms, ratifikavusioms Protokolą, kriminalizuoti rasistinio ir ksenofobinio pobūdžio veikas, padarytas naudojantis kompiuterių sistemomis, įpareigoti valstybes tarpusavyje bendradarbiauti tiriant tokius nusikaltimus.

Protokole pateikiama rasistinės ir ksenofobinės medžiagos sąvoka – tai bet kuri rašytinė medžiaga, bet kuris vaizdas arba bet kuris kitoks idėjų ar teorijų pateikimas, propaguojantis, skatinantis arba kurstantis neapykantą, diskriminavimą ar smurtą, nukreiptą prieš asmenį arba asmenų grupę dėl rasės, odos spalvos, kilmės arba tautinės ar etninės kilmės, taip pat religijos, jeigu tai naudojama kaip pretekstas kuriam nors iš šių veiksnių.

Dėl rasistinės ir ksenofobinės medžiagos skleidimo naudojantis kompiuterių sistemomis, protokole numatyta, jog kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti pagal jos vidaus teisę nustatyti baudžiamąją atsakomybę už tokią sąmoningą ir neteisėtą veiką: rasistinės ir ksenofobinės medžiagos platinimą ar kitokį skleidimą visuomenei naudojantis kompiuterių sistema.

Dėl rasistiniais ir ksenofobiniais ketinimais grindžiamo grasinimo protokole numatyta, jog Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti pagal jos vidaus teisę nustatyti baudžiamąją atsakomybę už tokią sąmoningą ir neteisėtą veiką: grasinimą, naudojantis kompiuterių sistema, padaryti sunkų nusikaltimą, kaip apibūdinama pagal jos vidaus teisę, i) asmenims dėl to, kad jie priklauso grupei, kuri yra kitokia dėl rasės, odos spalvos, kilmės arba tautinės ar etninės kilmės, taip pat religijos, jeigu tai naudojama kaip pretekstas kuriam nors iš šių veiksnių, arba ii) asmenų grupei, kuri yra kitokia dėl kurio nors iš šių požymių.

Dėl rasistiniais ir ksenofobiniais ketinimais grindžiamo įžeidimo protokole numatyta, jog Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti pagal jos vidaus teisę nustatyti baudžiamąją atsakomybę už tokią sąmoningą ir neteisėtą veiką: viešą įžeidimą, naudojantis kompiuterių sistema, i) asmenų dėl to, kad jie priklauso grupei, kuri yra kitokia dėl rasės, odos spalvos, kilmės arba tautinės ar etninės kilmės, taip pat religijos, jeigu tai naudojama kaip pretekstas kuriam nors iš šių veiksnių; arba ii) asmenų grupės, kuri yra kitokia dėl kurio nors iš šių požymių.

Protokole taip pat siūloma nustatyti baudžiamąją atsakomybę už genocido arba nusikaltimų žmoniškumui neigimą, pritarimą jiems arba pateisinimą, šiurkštų menkinimą.

Kitas Papildomojo protokolo (8 str. 2 d.) įpareigojimas – išplėsti Konvencijos 14–21 ir 23–25 str. apibūdintų priemonių taikymą Papildomojo protokolo atžvilgiu. Minėtieji Konvencijos straipsniai nustato valstybių procesinėms teisės normoms keliamus reikalavimus, įpareigoja imtis priemonių, būtinų operatyviai išsaugoti laikomus kompiuterių, srauto duomenis, juos atskleisti ar pateikti, surinkti srauto duomenis realiuoju laiku, juos įrašyti ir pan.

1.6. Tarptautinių organizacijų ir ES dokumentai dėl elektroninių nusikaltimų

Dėmesys elektroninių nusikaltimų problemai tarptautiniu mastu buvo parodytas jau 1983 metais. 1983–1985 m. EBPO paskirti ekspertai atliko tyrimą dėl baudžiamųjų įstatymų, susijusių su nusikaltimais, susietais su kompiuteriais, derinimo. Atlikus tyrimą, valstybėms narėms buvo pateiktas minimalus pavojingų veikų, susijusių su kompiuteriais, sąrašas. Prie tokių veikų buvo priskirta:

- tyčinis kompiuterių duomenų ir (arba) programų įvedimas, pakeitimas, ištrynimas ir (arba) slopinimas, siekiant nelegaliai pasisavinti lėšas ar kitas vertybes;
- tyčinis kompiuterių duomenų ir (arba) programų įvedimas, pakeitimas, ištrynimas ir (arba) slopinimas klastojimo tikslais;
- tyčinis kompiuterių duomenų ir (arba) kompiuterių programų įvedimas, pakeitimas, ištrynimas ir (arba) slopinimas ar kitoks kišimasis į kompiuterių sistemos darbą, siekiant trukdyti kompiuterių ir (arba) telekomunikacijų sistemos funkcionavimą;
- išskirtinės savininko teisės į saugomą kompiuterių programą pažeidimas, siekiant naudoti ją komerciniams tikslams 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 jų baudžiamieji įstatymai būtų pataisyti pagal išvardytą veikų sąrašą. Dauguma Informacijos, kompiuterių ir ryšių politikos komiteto narių taip pat buvo už tai, jog baudžiamosiomis normomis turėtų būti uždraustos ir kitos veikų rūšys, pvz., neteisėtas kompiuterių sistemų naudojimas ir kt.

Detaliau aptartina Europos Tarybos veikla, koordinuojant teisines priemones, kuriomis siekiama užkirsti kelią plisti elektroniniams nusikaltimams. Verta paminėti Europos Tarybos rekomendacijas. Nuo 1985 iki 1989 m. Europos Tarybos su kompiuteriais susijusių nusikaltimų ekspertų komitetas analizavo teisines kompiuterinių nusikaltimų problemas. Europos Tarybos Ministrų komitetas 1989 m. priėmė Rekomendaciją Nr. R(89)9, kuria ET šalių narių vyriausybes kviečia atsižvelgti į ekspertų komiteto parengtą ataskaitą kuriant įstatymus, susijusius su kompiuteriniais nusikaltimais. Šią ataskaitą sudaro penkios dalys. Pirmoji dalis aprašo kompiuterinio nusikaltimo fenomeną. Antrojoje 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. Paskutinėje dalyje kalbama apie kompiuterinių nusikaltimų prevenciją, latentiškumo mažinimą ir kt.

Kaip jau minėta, pranešime pateikiami du veikų, susijusių su tokiais nusikaltimais, sąrašai. ES šalims leidžiama savarankiškai spręsti, kaip ir kiek naudotis šiuo siūlymu. Minimaliame sąraše išvardytos aštuonios pavojingesnės veikos, susijusios su kompiuterių technologijomis. Papildomas sąrašas apima keturias ne tokias pavojingas veikas, kurios įtraukiamos į įstatymų leidybą, bet nėra privalomos. Šie sąrašai reikalingi siekiant suvienodinti ES šalių teisines sistemas dėl kompiuterinių nusikaltimų.

Pasiūlytas minimalus sąrašas:

- sukčiavimas, susijęs su kompiuteriu (kompiuterių duomenų ar programų įvedimas, ištrynimas, pakeitimas ar paslėpimas, ar kitoks įsikišimas į duomenų apdorojimo procesą, dėl to padaroma žalos kitam asmeniui, turint tikslą gauti materialinės naudos sau ar kitam asmeniui);
- klastojimas naudojant kompiuterį (kompiuterių duomenų ar programų įvedimas, ištrynimas, pakeitimas ar paslėpimas, ar kitoks įsikišimas į duomenų apdorojimo procesą, dėl to įvykdomas tradicinis klastojimas);
- kompiuterių duomenų ar programų sunaikinimas ar sugadinimas (kompiuterių duomenų ar programų ištrynimas, sunaikinimas, sugadinimas, neturint tam teisės);
- sabotažas naudojant kompiuterį (kompiuterių duomenų ar programų įvedimas, ištrynimas, pakeitimas ar paslėpimas, ar kitoks įsikišimas į duomenų apdorojimo procesą, siekiant sutrikdyti kompiuterio ar telekomunikacijų sistemos darbą);
- neteisėta prieiga prie kompiuterių sistemos (prieiga prie kompiuterių sistemos ar tinklo, neturint tam teisės ir pažeidžiant saugumo priemones);
- neteisėtas informacijos perėmimas kompiuterių sistemoje (neteisėtas susirašinėjimo perėmimas, atliktas techninėmis priemonėmis);
- neteisėtas saugomų kompiuterių programų dauginimas ir platinimas;
- neteisėtas kompiuterių lustų (mikroschemų) topografijų dauginimas ir platinimas.

Pasiūlytas neprivalomas sąrašas: kompiuterių duomenų ar programų pakeitimas, kompiuterinis šnipinėjimas, neteisėtas kompiuterio naudojimas (laiko vagystė), neteisėtas apsaugotų kompiuterių programų naudojimas.

Dar 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 suteikti galimybę „išplėsti" kratą ar poėmį į kitas kompiuterių sistemas, sujungtas per kompiuterių tinklą;
- *telekomunikacijų kontrolė*. Procesiniai įstatymai turi būti peržiūrėti, turint tikslą teisėsaugos institucijoms, tiriančioms sunkius nusikaltimus, suteikti galimybę kontroliuoti telekomunikacijų srauto duomenis ar 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, pateikiamiems 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 užtektinai patirties;
- *tarptautinis bendradarbiavimas*. Valstybių sienos neturi trukdyti atlikti numatytų tyrimo veiksmų, pvz., kratos ar poėmio, siekiant surinkti reikiamą informaciją elektronine forma.

Dalis aukščiau minėtųjų principų jau yra įgyvendinta, tačiau po rekomendacijos priėmimo praėjus daugiau nei dešimtmečiui kelios didžiausios problemos liko neišspręstos: efektyvaus tarptautinio bendradarbiavimo, elektroninių įrodymų ir pan.

Per pastarąjį dešimtmetį elektroninių nusikaltimų srityje savo veiklą suaktyvino ES institucijos, ypač Europos Komisija. Per šį laikotarpį priimta keletas, daugiausia neprivalomų, dokumentų. Šie dokumentai aptartini detaliau.

Vienas iš pirmųjų ES komunikatų dėl elektroninių nusikaltimų – 2001 m. sausio 26 d. komunikatas „Saugesnės informacinės visuomenės kūrimas, gerinant informacinių infrastruktūrų saugą ir kovą su nusikaltimais,

susijusiais su kompiuteriais“ KOM(2000)890 galutinis. Komunikate nurodyta, jog nusikaltimai, susiję su kompiuteriais, vykdomi visoje elektroninėje erdvėje ir negali būti sustabdyti prie sutartinių valstybių sienų. Tačiau nacionaliniu lygiu dažniausiai trūksta atsvaros naujiems tinklų saugumo iššūkiams ir naujai kompiuterinių nusikaltimų grėsmei. Daugelis valstybių į kompiuterinius nusikaltimus reaguoja pasitelkdamos nacionalinę teisę (ypač baudžiamąją), tačiau trūksta alternatyvių prevencijos priemonių.

Skiriasi ne tik nacionalinių valstybių baudžiamosios materialinės teisės normos, bet ir tyrimo struktūrų procesinės teisės – visa tai sunkina kovą su kompiuteriniais nusikaltimais.

Komunikate nurodoma, kokiu aspektu pateikiamas terminas „su kompiuteriais susiję nusikaltimai“ (angl. *computer-related crime)*. Ši kategorija suprantama plačiąja prasme, kaip bet koks nusikaltimas, kai vienu ar kitu būdu nusikaltimui padaryti naudojamos informacinės technologijos. Tačiau pabrėžiama, kad egzistuoja skirtingos nuomonės, kas priskiriama „su kompiuteriais susijusiems nusikaltimams“. Komunikate nurodoma, kad terminai „kompiuterinis nusikaltimas“, „su kompiuteriais susijęs nusikaltimas“, „aukštų technologijų nusikaltimas“ ir „elektroninis nusikaltimas“ dažnai vartojami kaip sinonimai. Vis dėlto, anot komunikato, skirtumas yra tarp specialių kompiuterinių (angl. *Computer specific crime)* ir tradicinių nusikaltimų, kurie padaromi naudojantis kompiuterinėmis technologijomis.

Be to, komunikate nurodoma, kad teisės aktai, susiję su specialiais kompiuteriniais nusikaltimais, ES gali būti priskirti kelioms tokių pažeidimų grupėms:

1) *privatumo pažeidimai*. Daugelis valstybių nusikaltimu laiko neteisėtą asmens duomenų rinkimą, saugojimą, modifikavimą, atskleidimą ar platinimą[68];
2) *su turiniu susiję pažeidimai*. Tokiems pažeidimams priskiriamas su vaikų pornografija susijusios medžiagos ar rasistinio pobūdžio informacijos platinimas internetu;
3) *ekonominiai pažeidimai, neteisėta prieiga ir sabotažas*. Šių nusikaltimų objektas dažniausiai yra nematerialus, pvz., elektroniniai pinigai ar kompiuterių programos;
4) *pažeidimai, susiję su intelektine nuosavybe*.

Taigi komunikate dar mėginama pateikti su kompiuteriais susijusių nusikaltimų rūšių klasifikaciją.

[68] Reikia paminėti, kad šiuo metu asmens duomenų teisinės apsaugos pažeidimai dažniausiai traktuojami kaip administraciniai pažeidimai arba kaip baudžiamieji nusižengimai (jeigu atitinkamoje valstybėje nėra administracinių pažeidimų). Tuo metu tik privatumo pažeidimai, kai pažeidžiamas komunikacinis privatumas, laikomi nusikaltimais.

Reikėtų atkreipti dėmesį į komunikato nurodymą, jog kovojant su kompiuteriniais nusikaltimais atitinkamose valstybėse reikia imtis šių priemonių:

I. Materialinės teisės aspektai.

Pabrėžiama, kad nacionalinės baudžiamosios teisės pritaikymas prie aukštųjų technologijų nusikaltimų srityje padėtų užtikrinti minimalią potencialių elektroninių nusikaltimų aukų apsaugą. Būtent šiame komunikate pirmą kartą paminėta Konvencija dėl elektroninių nusikaltimų, kuri galėtų prisidėti prie nacionalinės baudžiamosios teisės taikymo tiriant elektroninius nusikaltimus.

II. Proceso teisės aspektai.

Proceso teisės vienodinimas galėtų pagerinti potencialių elektroninių nusikaltimų aukų apsaugą ir užtikrinti tyrimo institucijų procesines teises tiriant elektroninius nusikaltimus. Komunikate išskiriamos šios proceso teisės vienodinimo sritys:

- komunikacijų perėmimas;
- srauto duomenų saugojimas;
- anoniminė prieiga ir naudojimas;
- praktinis bendradarbiavimas tarptautiniu lygiu;
- procesinės teisės ir jurisdikcija;
- įrodomoji kompiuterinių duomenų vertė.

Komunikate dar akcentuojamos ir neteisinės kovos su elektroniniais nusikaltimais priemonės. Pvz., bendradarbiavimo su vartotojų organizacijomis gerinimas, elektroninės informacijos saugos priemonių kūrimo skatinimas ir kt.

2005 m. Europos Taryba, turėdama tikslą gerinti bendradarbiavimą tarp teisminių ir kitų kompetentingų institucijų (įskaitant ir policijos struktūras) vienodinant ES valstybių narių baudžiamuosius įstatymus atakų prieš informacines sistemas srityje, priėmė pamatinį sprendimą „Dėl atakų prieš informacines sistemas“ Nr. 2005/222/JHA. Šiuo sprendimu buvo ypač pabrėžiama teroristinių atakų prieš informacines sistemas ir kritinę infrastruktūrą grėsmė. Be to, buvo konstatuota, kad baudžiamosios teisės srityje reikia imtis skubių veiksmų dėl transnacionalinio ir besienio elektroninių nusikaltimų pobūdžio.

Visų pirma siekiama unifikuoti tam tikras sąvokas atakų prieš informacines sistemas srityje. Sprendime pateikiamos „informacinės sistemos“, „kompiuterių duomenų“, „juridinio asmens“ ir „be teisės“ sąvokos. Sprendimu iš principo ketinta unifikuoti ES valstybių narių baudžiamąją teisę dėl trijų veikų:

1) neteisėtos prieigos prie informacinės sistemos;

2) neteisėto įsikišimo į informacinės sistemos funkcionavimą;

3) neteisėto įsikišimo į elektroninių duomenų apdorojimą.

Visais atvejais minimos veikos turi būti įvykdytos tyčia.

Sprendimu taip pat numatyta, kad baudžiamoji atsakomybė turėtų būti taikoma ir už rengimąsi ar pasikėsinimą įvykdyti šias tris aprašytąsias veikas. Be to, reglamentuojama, kad sankcijos už numatytas nusikalstamas veikas turėtų būti efektyvios, proporcingos ir atgrasančios nuo kitų nusikaltimų.

Sprendimas reglamentuoja ir juridinių asmenų atsakomybę už minėtąsias pavojingas veikas elektroninėje erdvėje (laikinas veiklos apribojimas ir kt.) bei jurisdikcijos klausimus. Nustatant jurisdikciją, siūloma naudoti teritorinį, pilietybės ir universalųjį jurisdikcijos principus.

Šis pamatinis sprendimas ES valstybėse narėse turėjo būti įgyvendintas iki 2007 m. kovo 16 dienos. Nors valstybės narės iš esmės įgyvendino Pamatinio sprendimo nuostatas, dėl vis aktyvėjančios nusikalstamos veikos (kibernetinių atakų) Sprendimas pasirodė turintis tam tikrų trūkumų. Minėtuoju sprendimu suderinamos tik ribotą nusikalstamų veikų skaičių reglamentuojančios nuostatos, tačiau nėra visapusiškai sprendžiama didelio masto atakų visuomenei keliamos potencialios grėsmės problema, be to, neatsižvelgiama į nusikaltimų sunkumą ir už juos taikomas sankcijas.

2007 m. gegužės 22 d. buvo priimtas EK komunikatas „Link bendros politikos kovojant su elektroniniais nusikaltimais“ KOM(2007)267 galutinis. Komunikato įvade nagrinėjama, kas yra elektroninis nusikaltimas (angl. *cyber crime)*. Nurodoma, jog šiai neteisėtai ir nusikalstamai veikai apibrėžti vartojama nemažai terminų, kurie yra sinonimai. Išskiriama, kad praktikoje terminas „elektroninis nusikaltimas“ vartojamas apibūdinant tris kriminalinių veikų kategorijas:

1) tradiciniai nusikaltimai, tokie kaip klastojimas ar sukčiavimas, elektroninių nusikaltimų atveju vykdomi naudojant elektroninių ryšių tinklus ir informacines sistemas;
2) neteisėto turinio nusikaltimai naudojant elektroninę žiniasklaidą, pvz., platinama vaikų pornografija;
3) elektroniniams tinklams būdingi nusikaltimai, pvz., atakos prieš informacines sistemas, *DDoS* atakos ar neteisėta prieiga (angl. *Hacking)*.

Apie pastarojo meto padėtį komunikate užsimenama, kad elektroninių nusikaltimų vis daugėja, o nusikalstamos veikos rūšys tampa vis sudėtingesnės ir įgyja tarptautinį pobūdį. Be to, pabrėžiama, kad elektroninių nusikaltimų srityje daugėja organizuoto nusikalstamumo ir beveik negerėja skirtingų valstybių teisėsaugos institucijų bendradarbiavimas.

Dėl to komunikate nurodomas svarbiausias tikslas – dėl nuolat kintančios aplinkos būtina kuo skubiau imtis priemonių – tiek nacionaliniu, tiek ir ES lygiu – prieš visų formų elektroninius nusikaltimus, kurie kelia vis didesnę grėsmę kritinei infrastruktūrai, visuomenei, verslui ir piliečiams. Apibendrinant tai, kas pasakyta, šį tikslą galima išskirti į tris svarbiausius potikslius:

1) gerinti koordinaciją ir bendradarbiavimą tarp elektroninių nusikaltimų padalinių, kitų kompetentingų institucijų ir ekspertų ES;
2) bendradarbiaujant su ES valstybėmis narėmis, tarptautinėmis organizacijomis ir kitais dalyviais, plėtoti ES kovos su elektroniniais nusikaltimais politiką;
3) skatinti švietimą, susijusį su elektroninių nusikaltimų daroma žala ir pavojingumu.

Komunikate išskiriamos šios kovos su elektroniniais nusikaltimais priemonės:

1) teisėsaugos bendradarbiavimo gerinimas ir mokymai;
2) dialogo su verslu skatinimas;
3) teisės aktų leidyba. Šioje srityje pabrėžiama, kad nacionalinės baudžiamosios teisės suderinamumas vis dar nėra tinkamas. Kaip pavyzdį galima paminėti tapatybės vagystę elektroninėje erdvėje. Ši veika (kai neteisėtai naudojami asmeniniai duomenys turint tikslą padaryti nusikaltimą) dar nekriminalizuota daugelio ES nacionalinių valstybių baudžiamuosiuose įstatymuose. Pagal šių valstybių įstatymus kaltasis asmuo būtų baudžiamas už sukčiavimą ar kitą nusikaltimą, tačiau ne už tapatybės vagystę. Kriminalizuoti tapatybės vagystę elektroninėje erdvėje kaip savarankišką nusikaltimą siūloma dėl to, kad ją įrodyti kur kas lengviau nei sukčiavimą. Dėl tapatybės vagystės kriminalizavimo pagerėtų teisėsaugos institucijų bendradarbiavimas;
4) statistinių duomenų kaupimas.

Naujausias EK komunikatas priimtas susirūpinus dėl kritinės infrastruktūros apsaugos. 2009 m. kovo 30 d. buvo priimtas Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui bei Regionų komitetui dėl ypatingos svarbos informacinės infrastruktūros apsaugos „Europos apsauga nuo didelio masto kibernetinių antpuolių ir veiklos sutrukdymo – geresnė parengtis, didesnis saugumas ir atsparumas“ KOM(2009)149 galutinis.

Komunikate teigiama, jog kasdienis gyvenimas vis labiau susijęs su informacinėmis ir komunikacinėmis technologijomis (*IKT*). Europos

ekonomikai ir visuomenei gyvybiškai svarbios kai kurios iš tų *IKT* sistemų, paslaugų, tinklų ir infrastruktūros objektų (trumpai tariant, IKT infrastruktūros objektų), nes jos naudojamos būtiniausioms prekėms ir paslaugoms teikti arba yra kitų ypatingos svarbos infrastruktūros objektų laikančioji konstrukcija. Paprastai jos laikomos ypatingos svarbos informacinės infrastruktūros objektais, nes jų sugadinimas ar sunaikinimas turėtų neigiamų padarinių gyvybiškai svarbioms visuomenės funkcijoms. Naujausi pavyzdžiai: 2007 m. didelio masto kibernetiniai Estijos antpuoliai, 2008 m. įvykę incidentai, kai buvo nutraukti tarpžemyniniai kabeliai.

2008 m. Pasaulio ekonomikos forume apskaičiuota, kad ypatingos svarbos informacinės infrastruktūros avarijos, kuri pasaulio ūkiui kainuotų apie 250 mlrd. JAV dolerių, tikimybė per artimiausią dešimtmetį yra nuo dešimties iki dvidešimties procentų.

Šiame komunikate daugiausia dėmesio skiriama prevencijai, parengčiai ir informavimui, be to, sudarytas neatidėliotinų veiksmų planas, kaip didinti ypatingos svarbos informacinės infrastruktūros objektų saugumą ir atsparumą. Tokie tikslai dera su Tarybos ir Europos Parlamento prašymu pradėta diskusija, kuria siekiama išnagrinėti sudėtingus tinklų ir informacijos saugumo politikos uždavinius bei prioritetus ir nutarti, kokių priemonių dėl tų uždavinių ir prioritetų reikia imtis ES. Be to, pasiūlytais veiksmais papildomi veiksmai, kuriais siekiama užkirsti kelią prieš ypatingos svarbos informacinės infrastruktūros objektus nukreiptai nusikalstamai ir teroristinei veiklai, su ja kovoti ir už ją persekioti baudžiamąja tvarka, taip pat užtikrinama sąveika su dabartinėmis bei būsimomis tinklų ir informacijos saugumo ES mokslinių tyrimų pastangomis ir su tarptautinėmis šios srities iniciatyvomis.

Apie ypatingos svarbos informacinės infrastruktūros objektams kylančias grėsmes komunikatas nurodo, jog „dėl piktavalių antpuolių, gaivalinių nelaimių arba techninių gedimų kylanti grėsmė dažnai nėra aiškiai suprantama ir (arba) pakankamai išnagrinėjama“. Todėl suinteresuotosios šalys nepakankamai informuotos, kad pritaikytų veiksmingas apsaugos ir atoveikio priemones. Kibernetiniai antpuoliai tapo kaip niekad sudėtingi. Paprasti eksperimentai perauga į konkrečius veiksmus, vykdomus siekiant pelno arba politinių tikslų. Neseniai įvykdyti didelio masto kibernetiniai Estijos, Lietuvos ir Gruzijos antpuoliai – tai plačiausiai nušviesti bendrosios tendencijos pavyzdžiai. Problemos sudėtingumą rodo daugybė virusų, kirminų (savaime plintančių kenkiamųjų programų) ir kitos kenkimui skirtos programinės įrangos, kenkiamuoju programiniu kodu užkrėstų kompiuterių tinklų, be to, nuolat daugėja nepageidaujamų el. pašto laiškų.

Atsižvelgiant į didelį priklausomumą nuo ypatingos svarbos informacinės infrastruktūros objektų, jų tarpvalstybinius sujungimus ir tarpusavio priklausomumą nuo kitos infrastruktūros objektų, taip pat į jų pažeidžiamumą ir jiems kylančias grėsmes, apsisaugoti nuo gedimų ir gintis nuo antpuolių reikėtų pirmiausia sistemingai sprendžiant ypatingos svarbos informacinės infrastruktūros objektų saugumo ir atsparumo klausimus.

Komunikate įvardijami tokie Europos uždaviniai:

1. Nevienodi ir nesuderinti nacionaliniai metodai.

Nors sudėtingi uždaviniai ir problemos, su kuriomis susiduriama, turi bendrumų, valstybėse narėse skiriasi ypatingos svarbos informacinės infrastruktūros objektų saugumo ir atsparumo užtikrinimo priemonės bei tvarka, profesinė kompetencija ir parengties lygis.

Šioms problemoms įveikti reikia visos Europos pastangų, kad nacionalinei politikai ir programoms būtų suteikta papildomos vertės, puoselėjant sąmoningumo ugdymą ir bendrą sudėtingų uždavinių supratimą, skatinant bendrų politikos uždavinių ir prioritetų priėmimą, stiprinant valstybių narių bendradarbiavimą ir integruojant nacionalines politikos kryptis labiau Europoje ir pasaulyje.

2. Ypatingos svarbos informacinės infrastruktūros objektams reikia Europos valdymo modelio.

Nacionaliniu lygmeniu kaip bazinis modelis skatinama viešojo ir privataus sektorių partnerystė šiai valdymo problemai spręsti. Nors ir sutariama, kad viešojo ir privataus sektorių partnerystė būtų naudinga ir Europos lygmeniu, tačiau tokiu mastu dar nebendradarbiaujama. Privatųjį sektorių dalyvauti nustatant viešosios politikos tikslus bei veiklos prioritetus ir priemones būtų galima paskatinti daugelio Europos mastu suinteresuotų šalių dalyvavimu grindžiama valdymo sistema, kurioje gali būti numatytas aktyvesnis ENISA vaidmuo. Tokia sistema leistų panaikinti atotrūkį tarp nacionalinės politikos formavimo ir praktinės veiklos tikrovės.

1. Ribotos Europos ankstyvojo atpažinimo ir reagavimo į incidentus išgalės.

Išgalės anksti atpažinti pavojus ir tinkamai reaguoti į incidentus Europoje turi būti pagrįstos sklandžiai dirbančiomis nacionalinėmis (valstybinėmis) kompiuterinių incidentų tyrimo grupėmis (angl. *National/Governmental Computer Emergency Response Teams*, *CERT)*, t. y. būtina turėti bendras pagrindines išgales. Šios įstaigos valstybėse turi skatinti suinteresuotųjų šalių domėjimąsi ir gebėjimą vykdyti viešosios politikos veiklą (įskaitant veiklą, susijusią su piliečius ir mažąsias bei vidutines įmones apimančiomis informacijos mainų ir įspėjimo sistemomis) bei užsiimti efektyviu

tarpvalstybiniu bendradarbiavimu ir informacijos mainais, galbūt maksimaliai naudodamosi esamomis organizacijomis, pvz., Europos vyriausybinių *CERT* grupe (angl. *European Governmental CERTs Group*, *EGC)*.

4. Tarptautinis bendradarbiavimas.

Internetas – pasaulinis, labai plačiai paskirstytas tinklų tinklas, kurio valdymo centrai savo veiklą dažniausiai vykdo neatsižvelgdami į nacionalines sienas. Norint užtikrinti interneto atsparumą ir stabilumą, būtinas specialus tikslinis metodas, pagrįstas dviem viena kitą papildančiomis priemonėmis. Pirma, atsižvelgiant į viešąją politiką ir praktinį diegimą, būtina susitarti, kokie interneto atsparumo ir stabilumo Europos prioritetai. Antra, remiantis mūsų strateginiu dialogu ir bendradarbiavimu su trečiosiomis šalimis bei tarptautinėmis organizacijomis, būtina atsižvelgti į svarbiausias Europos vertybes ir kartu su pasauline bendruomene nustatyti interneto atsparumo ir stabilumo principus. Ši veikla būtų pagrįsta Pasaulio aukščiausiojo lygio susitikimo informacinės visuomenės klausimais pripažinimu, kad interneto stabilumas yra svarbiausias dalykas.

Komunikate numatytas ir atitinkamas veiksmų planas, kurio reikėtų laikytis įgyvendinant minėtuosius uždavinius.

Jau 2008 m. liepos 14 d. Europos Komisija paskelbė Pamatinio sprendimo įgyvendinimo ataskaitą, kurios išvadose nurodyta, kad daugelis valstybių narių padarė didelę pažangą ir gana gerai įgyvendina sprendimą, tačiau kai kurios valstybės narės šio įsipareigojimo dar nebaigė vykdyti. Be to, ataskaitoje nurodyta, kad „po to, kai priimtas Sprendimas, visoje Europoje įvykdytos atakos parodė, kad kyla naujų pavojų: vienu metu įvykdytos itin didelio masto atakos prieš informacines sistemas ir padidėjo vadinamųjų „zombių“ tinklų naudojimas nusikalstamiems tikslams.“ Priimant sprendimą, šioms atakoms nebuvo skirta daug dėmesio.

Dėl to 2010 m. Europos Komisija parengė siūlymą dėl Europos Parlamento ir Tarybos direktyvos dėl atakų prieš informacines sistemas ir dėl Tarybos pamatinio sprendimo 2005/222/TVR panaikinimo. Siūlyme akcentuojama, kad svarbiausia elektroninių nusikaltimų priežastis – pažeidžiamumas, kurį lemia įvairūs veiksniai. Minėtieji reiškiniai nepašalinami ir dėl nepakankamo atsako taikant teisėsaugos mechanizmus, sunkumų irgi daugėja, nes tam tikros nusikalstamos veikos yra tarpvalstybinio pobūdžio.

Dažnai apie tokio pobūdžio nusikaltimus iš dalies nepranešama ir dėl to, kad kai kurie iš jų lieka nepastebėti, o kartais nukentėjusieji (ūkinės veiklos vykdytojai ir įmonės) apie nusikalstamą veiką nepraneša baimindamiesi blogos reputacijos ar nenorėdami pakenkti įmonės ateities perspektyvoms, jeigu būtų paviešinta informacija apie jos pažeidžiamumą. Be to, dėl valstybių baudžiamosios teisės sistemos ir procedūrų skirtumų tokių

nusikaltimų tyrimo ir traukimo baudžiamojon atsakomybėn tvarka gali skirtis, todėl kovoti su tokiais nusikaltimais gali tekti skirtingomis priemonėmis. Dėl informacinių technologijų raidos problemų dar padaugėjo, nes vis lengviau kuriamos ir platinamos priemonės (kenkiamoji programinė įranga ir botnetai), kaltininkai gali išlikti anonimiški, o atsakomybė spręsti klausimus priklauso skirtingoms jurisdikcijoms. Dėl sunkumų, kylančių baudžiamojo persekiojimo srityje, organizuoti nusikaltėliai gali daug uždirbti mažai rizikuodami. Šiame siūlyme atsižvelgiama į naujus elektroninių nusikaltimų metodus, visų pirma botnetų naudojimą. Sąvoka „botnetas“ reiškia kompiuterių, į kuriuos įdiegta kenkiamoji programinė įranga (kompiuterio virusai), tinklą. Toks užkrėstų kompiuterių („zombių“) tinklas gali būti naudojamas konkretiems veiksmams atlikti, pavyzdžiui, atakoms prieš informacines sistemas (kibernetinėms atakoms) rengti. Šie „zombiai“ gali būti kontroliuojami iš kito kompiuterio, o užkrėstų kompiuterių vartotojai apie tai dažniausiai nieko nežino. Šis kontroliuojantis kompiuteris dar vadinamas komandų ir kontrolės centru. Šį centrą kontroliuojantys asmenys yra pažeidėjai, nes jie naudojasi užkrėstais kompiuteriais atakoms prieš informacines sistemas rengti. Nusikaltėlius susekti labai sunku, nes botnetui priklausantys kompiuteriai, naudojami atakoms rengti, gali būti visai kitoje vietoje nei pažeidėjas. Naudojant botnetą surengtos atakos dažniausiai būna didelio masto – tokios, kurios rengiamos pasitelkiant priemones, dėl kurių nukenčia daug informacinių sistemų (kompiuterių), arba tokios atakos, dėl kurių patiriama didelė žala, pvz., dėl sutrikusių sistemos paslaugų, finansinių išlaidų, prarastų asmens duomenų ir t. t. Šiame kontekste didelis botnetas yra laikomas tinklu, galinčiu padaryti daug žalos. Sunku nustatyti botnetų dydį, tačiau apskaičiuota, kad prisijungimų prie didžiausių nustatytų botnetų (užkrėstų kompiuterių) skaičius buvo nuo 40 iki 100 tūkst. per 24 valandas.

2013 m. buvo priimta direktyva 2013/40/EB dėl atakų prieš informacines sistemas, keičianti pamatinį sprendimą 2005/222/JHA. Šia direktyva nustatomos būtiniausios taisyklės, susijusios su nusikalstamų veikų apibrėžtimi, ir sankcijos, taikomos atakoms prieš informacines sistemas. Ja siekiama sudaryti palankesnes tokių nusikalstamų veikų prevencijos sąlygas ir pagerinti teisminių bei kitų kompetentingų institucijų bendradarbiavimą. Šia direktyva siekiama iš dalies pakeisti ir išplėsti 2005 m. vasario 24 d. Tarybos pamatinio sprendimo 2005/222/TVR dėl atakų prieš informacines sistemas nuostatas.

Be kitų pakeitimų, direktyvoje dar buvo papildomai išskirtos dvi nusikalstamos veikos. Visas direktyvos nusikalstamų veikų sąrašas yra toks:

– neteisėta prieiga prie informacinių duomenų;

– neteisėtas įsikišimas į sistemą;
– neteisėtas įsikišimas į duomenis;
– neteisėtas duomenų perėmimas;
– priemonės, naudojamos nusikalstamoms veikoms vykdyti.

Ši direktyva valstybių narių teisės aktuose turėjo būti įgyvendinta iki 2015 m. rugsėjo 4 dienos.

2. Veikų elektroninėje erdvėje kriminalizavimas Lietuvoje

Vienas iš pagrindinių nacionalinių valstybių įstatymų leidėjų uždavinių kovojant su elektroniniais nusikaltimais – uždrausti šias pavojingas veikas nacionaliniuose baudžiamuosiuose įstatymuose.

Lietuvos Respublikos prisijungimas prie Konvencijos dėl elektroninių nusikaltimų gerokai paveikė Lietuvos nacionalinę baudžiamąją teisę, kiek tai susiję su veikomis elektroninėje erdvėje. Nors dar iki Konvencijos pasirašymo į naujai priimtą BK jau buvo įvestas atskiras skyrius „Nusikaltimai informatikai“[69], kuriame nustatyta atsakomybė už nusikaltimus, keliančius grėsmę saugiai apdoroti kompiuterinę informaciją, svarbūs BK papildymai buvo atlikti 2004 m. pradžioje. Įgyvendinant Konvenciją, nuo 2004 m. vasario 14 d. įsigaliojo nauji BK papildymai, kuriais į minėtąjį skyrių įvestos dvi naujos veikos: neteisėtas prisijungimas prie kompiuterio ar kompiuterių tinklo (198[1] str.) ir neteisėtas disponavimas įrenginiais, kompiuterių programomis, slaptažodžiais, prisijungimo kodais bei kitais duomenimis, skirtais nusikaltimams daryti (198[2] str.). Buvo papildyti ir kiti „tradiciniai“ straipsniai, pvz., 309 str., nustatantis atsakomybę už disponavimą pornografinio turinio informacija.

Šiuo metu BK 30 skyriaus pavadinimas yra toks: „Nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui“. Pastarąjį kartą šios skyriaus nuostatos buvo keičiamos 2015 m. birželio 11 d. įgyvendinant ES direktyvą 2013/40/EB dėl atakų prieš informacines sistemas. Atkreiptinas dėmesys, kad kartu su šios direktyvos įgyvendinimu į kai kurių straipsnių kvalifikuojančias sudėtis įvestos nuostatos „arba pasinaudodamas svetimais asmens duomenimis“. Tokiu būdu buvo kriminalizuoti kai kurie tapatybės vagystės elektroninėje erdvėje elementai. Tačiau įstatymo leidėjas tapatybės vagystės elektroninėje erdvėje kaip savarankiškos nusikalstamos veikos

[69] Iki 2004 m. vasario šį skirsnį sudarė trys straipsniai, numatantys baudžiamąją atsakomybę už kompiuterinės informacijos sunaikinimą ar pakeitimą (196 str.), kompiuterių programos sunaikinimą ar pakeitimą ir kompiuterių tinklo, duomenų banko ar informacinės sistemos darbo sutrikdymą (197 str.) bei kompiuterinės informacijos pasisavinimą ar skleidimą (198 str.).

BK vis dėlto nekriminalizavo. Reikėtų paminėti, kad atsakomybei už pavojingas veikas elektroninėje erdvėje BK skirtas ne tik minėtasis skyrius, bet ir kiti kodekso straipsniai.

BK saugo elektroninių ryšių privatumą – pavojingos šios srities veikos kriminalizuotos 166 str. „Neteisėtas susirašinėjimo, kitokių pranešimų, siuntų ar pokalbių telefonu slaptumo pažeidimas“. Šio straipsnio, iš esmės garantuojančio laisvą socialinį žmonių bendravimą, 1 d. nurodyta, jog 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 daryti prielaidą, jog ši nuostata taikoma apsikeitimams informacija elektroniniu paštu ar kitais būdais.

Baudžiamosios teisės normomis Lietuvoje saugoma formali elektroninių duomenų ir informacinių sistemų integralumo sritis, nustatant baudžiamąją atsakomybę BK 196 ir 197 straipsniuose. Šioms veikoms vykdyti gali būti naudojamos tokios kenkiamosios programos kaip Trojos arkliai, virusai, kirminai ir kt. Beje, 2004 m. papildžius BK 196 str., buvo kriminalizuotos ir vadinamosios *DoS* atakos.

Pagal BK 196 str. 1 d., baudžiamas tas asmuo, kuris neteisėtai sunaikino, sugadino, pašalino ar pakeitė elektroninius duomenis arba techninę, programinę įrangą ar kitais būdais apribojo naudojimąsi tokiais duomenimis padarydamas žalos, o šio straipsnio 2 d. numatyta baudžiamoji atsakomybė už tą pačią veiką, jeigu ji buvo padaryta daugelio informacinių sistemų elektroniniams duomenims arba strateginę reikšmę nacionaliniam saugumui ar didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinčios informacinės sistemos elektroniniams duomenims, arba pasinaudojus svetimais asmens duomenimis, arba padarant didelę žalą.

Atkreiptinas dėmesys, kad įstatymo leidėjas nėra pateikęs išaiškinimo, kokia žala jau yra laikoma didele. Todėl kiekvienu konkrečiu atveju teismui paliekama teisė pačiam spęsti, ar padarytoji žala yra didelė, taigi bendrieji didelės žalos nustatymo principai ir jos vertinimo kriterijai turėtų susiformuoti iš teismų praktikos. Remiantis teismų praktika galima teigti, kad iki šiol nagrinėtose bylose, susijusiose su pavojingomis BK 196 str. aprašytomis veikomis, padaroma didelė žala gali būti tiek turtinė, tiek ir neturtinė (moralinė, socialinė ir pan.).

Pabrėžtina, kad skaitant mokslinę literatūrą ir nagrinėjant teismų praktiką vis dažniau galima matyti, kad elektroninius nusikaltimus padaro darbuotojai, naudodamiesi savo tarnybine padėtimi ir padarydami žalos būtent tai įstaigai, bankui ar kitai institucijai, kurioje dirba. Pavyzdžiui,

Panevėžio miesto apylinkės teismas, nagrinėdamas baudžiamąją bylą Nr. 1-187-389/2011, nustatė, kad *R. Š., dirbdama vadybininke ir būdama atsakinga už UAB „D“ degalinės Nr. 3 materialinius ir piniginius likučius, jų judėjimą ir ataskaitų sudarymą, laikotarpiu nuo 2007 m. gruodžio 12 d. iki 2008 m. vasario 1 d., kad 2000 litrų dyzelino trūkumas nepasimatytų mėnesio pabaigoje pildomose ataskaitose, neteisėtai pakeitė kompiuteryje esančius elektroninius duomenis, tai yra informacinę sistemą papildė naujais neegzistuojančiais elektroniniais duomenimis, o būtent: 2007 m. gruodžio 12 d., pagal krovinio važtaraštį Nr. 0002393 į degalinę Nr. 3 atvežtus 13 293 litrus dyzelino 12:40:05 val. įvedė į kompiuterinę programą, po to, 09:13:54 val., suformavo neegzistuojantį dokumentą Nr. 00001, kuriuo iš programos išminusavo 3000 litrų dyzelino, 2007 m. gruodžio 14 d., 15:29:46 val., suformavo neegzistuojantį dokumentą DID Nr. 1111, kuriuo į programą įvedė 1000 litrų dyzelino, 2007 m. gruodžio 31 d., 23:25:02 val., suformavo neegzistuojantį dokumentą Nr. 00000345, kuriuo į programą įvedė 2000 litrų dyzelino, 2008 m. sausio 1 d., 01:31:35 val., suformavo neegzistuojantį dokumentą Nr. 00000345, kuriuo iš programos išminusavo 2000 litrų dyzelino, 2008 m. sausio 31 d., 20:43:38 val., suformavo neegzistuojantį dokumentą Nr. 002, kuriuo į programą įvedė 2000 litrų dyzelino, 2008 m. vasario 1 d., 06:09:29 val., suformavo neegzistuojantį dokumentą Nr.01/002, kuriuo iš programos išminusavo 2000 litrų dyzelino ir tokiu būdu iššvaistė jai patikėtą svetimą, UAB „D“ priklausantį turtą – 2000 litrų dyzelino bendros 5957,40 Lt vertės, perleisdama jį nenustatytiems asmenims, ir tuo padarydama UAB „D“ didelės žalos* (Vilniaus miesto 1 apylinkės teismo 2011 m. gruodžio 6 d. nuosprendis baudžiamojoje byloje Nr. 1-1430-276/2011).

BK 197 str. nustatyti ir baudžiamosios atsakomybės pagrindai už vadinamąsias sabotažo naudojant kompiuterį veikas. Pagal BK 197 str. 1 d., baudžiamas tas asmuo, kuris neteisėtai sutrikdė ar nutraukė informacinės sistemos darbą padarydamas žalos, o šio straipsnio 2 d. numatyta baudžiamoji atsakomybė, jeigu ta pati veika padaryta daugeliui informacinių sistemų arba strateginę reikšmę nacionaliniam saugumui ar didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinčiai informacinei sistemai, arba pasinaudojus svetimais asmens duomenimis, arba padarant didelės žalos. Nagrinėjant bylas pagal BK 197 str., teismų praktika dar tik formuojasi, todėl akivaizdu, kad turės praeiti gana nemažai laiko, kol bus suformuota bendra praktika, kuria galės remtis tiek ikiteisminio tyrimo pareigūnai, tiek kiti teismai, nagrinėjantys panašaus pobūdžio bylas.

Baudžiamoji atsakomybė už neteisėtą elektroninių duomenų perėmimą Lietuvoje gali kilti pagal LR BK 198 str. „Neteisėtas elektroninių duomenų perėmimas ir panaudojimas“. Pagal BK 198 str. 1 d., baudžiamas tas,

kas neteisėtai stebėjo, fiksavo, perėmė, įgijo, laikė, pasisavino, paskleidė ar kitaip panaudojo neviešus elektroninius duomenis, o, pagal LR BK 198 str. 2 d., tas, kas neteisėtai stebėjo, fiksavo, perėmė, įgijo, laikė, pasisavino, paskleidė ar kitaip panaudojo strateginę reikšmę nacionaliniam saugumui arba didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinčius neviešus elektroninius duomenis. Šie duomenys turėtų būti suprantami kaip viešai naudoti neskirti elektroniniai duomenys, kai jiems viešinti, remiantis konfidencialumu ar kitais pagrindais, taikoma tam tikrų ribojimų.

Vilniaus apygardos teismas, nagrinėdamas baudžiamąją bylą (Vilniaus apygardos teismo 2011 m. gruodžio 23 d. nuosprendis baudžiamojoje byloje Nr. 1A-977/2011) pagal nuteistojo T. S. ir Vilniaus miesto apylinkės prokuratūros prokuroro apeliacinius skundus dėl Vilniaus miesto antrojo apylinkės teismo 2011 m. liepos 1 d. nuosprendžio pabrėžė, kad „kitoks elektroninių duomenų panaudojimas yra tokių duomenų pritaikymas, pavartojimas kokiam nors tikslui. Tai gali būti tiek kaltininko, tiek kitų asmenų chuliganiškiems, savanaudiškiems ar kitokiems interesams tenkinti. Neteisėto elektroninių duomenų perėmimo ir panaudojimo objektyvieji požymiai įstatymo dispozicijoje suformuluoti kaip alternatyvūs, todėl baudžiamajai atsakomybei kilti pakanka, kad būtų padaryta bent viena iš šių veikų."

Kėsinantis į įstatymo saugomas vertybes, gali būti ne tik padaroma realios žalos, bet ir kilti tokios žalos grėsmė. Tais atvejais, kai realios žalos nepadaroma, o yra tiktai tokios žalos grėsmė, objektui irgi padaroma tam tikrų pakeitimų. Pavojingumo pobūdį paprastai apibūdina objekto, į kurį kėsinamasi, vertingumas. Nusikaltimo objekto, į kurį kėsinamasi naudojant neteisėtą prieigą – visuomeninių santykių saugant, apdorojant kompiuterinę informaciją vertingumą yra pabrėžęs ne vienas mokslininkas. Tokio objekto apsaugos baudžiamosiomis normomis praktika (kai nepadaroma realios žalos) nustatoma vis daugiau valstybių. Be to, kriminalizuoti neteisėtą prieigą, kai nepadaroma realios žalos, rekomenduojama ir tarptautiniuose norminiuose aktuose. Iki 2004 m. Lietuvoje neteisėta prieiga, turinti formalią sudėtį, išvis nebuvo kriminalizuota, tačiau ši teisės spraga buvo panaikinta. 2004 m. sausio 29 d. įstatymu Nr. IX-1992 BK buvo papildytas nauju 198^1 straipsniu „Neteisėtas prisijungimas prie kompiuterio ar kompiuterių tinklo" (šiuo metu straipsnio pavadinimas toks: „Neteisėtas prisijungimas prie informacinės sistemos").

Pagal BK 198^1 str. 1 d., baudžiamas tas, kas neteisėtai prisijungė prie informacinės sistemos ar jos dalies pažeisdamas informacinės sistemos apsaugos priemones, o pagal BK 198^1 str. 2 d. – tas, kas neteisėtai prisijungė prie strateginę reikšmę nacionaliniam saugumui ar didelę reikšmę valstybės

valdymui, ūkiui ar finansų sistemai turinčios informacinės sistemos ar jos dalies.

Kaip matyti iš straipsnio dispozicijos, tokio pobūdžio veika pripažįstama nusikalstama, jeigu ją vykdant tenkinamos dvi esminės sąlygos:

1) prie informacinės sistemos prisijungiama neteisėtai, t. y. neturint jos savininko ar teisėto valdytojo leidimo tokiems veiksmams atlikti;
2) nusikalstama veika įvykdoma ne bet kaip, o konkrečiu straipsnio dispozicijoje numatytu būdu – prie informacinės sistemos prisijungiama pažeidžiant jos apsaugos priemones.

Tai, kad šios dvi esminės sąlygos turi būti įvykdytos, patvirtina ir teismų praktika. Vilniaus miesto pirmasis apylinkės teismas konstatavo, jog yra visiškai įrodyta, kad T. Č. įvykdė nusikalstamą veiką, numatytą BK 198 str. 1 d., nes T. Č. laikotarpiu nuo 2010 m. spalio 13 d. iki 2010 m. gruodžio 8 d., AB SEB banko patalpose, per jo darbo vietoje esantį kompiuterį „DELL Optiplex 745“, nenustatyta programine įranga, nustatęs ir vėliau (ikiteisminio tyrimo nenustatytu laiku) savavališkai pakeitęs prisijungimo prie AB SEB banko tarnybinėse stotyse administruojamos neviešos informacinės sistemos administratoriaus slaptažodį, 2011 m. balandžio 13 d. 12 val. 01 min. neteisėtai, t. *y. neturėdamas šios informacinės sistemos savininko ar teisėto valdytojo leidimo jungtis prie šios informacinės sistemos, tyčia, pažeisdamas šios sistemos apsaugos priemones, prisijungė prie šios banko informacinės sistemos kaip neribotą prieigos teisę turintis vartotojas*.

Gali kilti klausimas, ką laikyti informacinės sistemos apsaugos priemonėmis. Nors teismų praktika šias priemones vertina siaurąja prasme, t. y. tik technologiniu aspektu (kaip techninių apsaugos priemonių pažeidimą), klausimas yra diskusinis. Neatmestinas variantas, kad informacinės sistemos apsaugos priemonės gali būti vertinamos ir plačiąja prasme, kaip apimančios ir organizacinių apsaugos priemonių pažeidimus.

Pavojingos veikos, kai tyčia atliekami tam tikri neteisėti su įrenginiais ar prieigos duomenimis susiję veiksmai, turint tikslą padaryti kitų kompiuterinių nusikaltimų, buvo kriminalizuotos 2004 m. sausio 29 d., BK papildžius 198^2 str. „Neteisėtas disponavimas įrenginiais, kompiuterių programomis, slaptažodžiais, prisijungimo kodais ir kitokiais duomenimis, skirtais nusikaltimams daryti“. Tai yra veikos, kai kuriami, platinami, naudojami ir t. t. neteisėti įrenginiai ir (ar) prieigos duomenys (slaptažodžių nulaužimo programos, neteisėtu būdu gauti slaptažodžiai ar pan.), skirti kompiuterių sistemų ar duomenų konfidencialumo, integruotumo ir prieinamumo pažeidimams įvykdyti.

Baudžiamoji atsakomybė už netinkamą įtaisų naudojimą Lietuvoje yra nustatyta BK 198[2] str. „Neteisėtas disponavimas įrenginiais, programine įranga, slaptažodžiais, prisijungimo kodais ir kitokiais duomenimis“. Pagal BK 198[2] str. 1 d., baudžiamas tas, kas nusikalstamais tikslais ar kitaip neteisėtai gamino, gabeno, importavo, pardavė, suteikė prieigą ar kitaip platino, įgijo ar laikė įrenginius ar programinę įrangą, tiesiogiai skirtus ar pritaikytus nusikalstamoms veikoms vykdyti, taip pat slaptažodžius, kodus ar kitokius panašius duomenis, skirtus prisijungti prie informacinės sistemos ar jos dalies.

Atkreiptinas dėmesys, kad pagal šį straipsnį nebūtina, jog, pasitelkus tokius įrenginius ar programinę įrangą, būtų realiai įvykdytos nusikalstamos veikos arba dėl tokių nusikalstamų veikų kiltų kokių nors neigiamų socialinių ar materialinių padarinių. Be to, nebūtina, kad atitinkamus įrenginius ar programinę įrangą pagaminęs asmuo, pasitelkęs šiuos įrenginius ar įrangą, pats vykdytų nusikalstamą veiką. Baudžiamajai atsakomybei kilti užtenka vien neteisėto įrenginių ar programinės įrangos, įskaitant slaptažodžius, prisijungimo kodus, tiesiogiai skirtų nusikalstamoms veikoms vykdyti, disponavimo fakto.

Vilniaus miesto apylinkės teismas (Vilniaus miesto pirmojo apylinkės teismo 2009 m. rugsėjo 14 d. baudžiamasis įsakymas baudžiamojoje byloje N1-1470-88/2009) pripažino J. P. kaltu pagal BK 198[2] str. 1 d. ir skyrė jam 10 MGL (1300 Lt) dydžio baudą už tai, kad jis asmeniniu kompiuteriu sukūrė netikrą AB bankas „X“ internetinės bankininkystės paslaugos „X.net“ puslapį, skirtą šio banko klientų prisijungimų prie elektroninės bankininkystės paslaugos tarnybinės stoties kodams ir slaptažodžiams fiksuoti, o vėliau juos persiųsti internetu į sukurtas elektroninio pašto dėžutes, ir taip pagamino programinę įrangą, reikalingą nusikaltimams daryti, būtent vykdyti toms nusikalstamoms veikoms, kurios numatytos BK 198[1], 214, 215 ir 182 straipsniais. Vėliau jis minėtąjį netikrą AB bankas „X“ interneto puslapį elektroniniu būdu persiuntė M. J. ir taip neteisėtai jam perdavė programinę įrangą, skirtą nusikaltimams daryti. Taigi, nors J. P., naudodamasis savo neteisėtai sukurta programine įranga, pats ir nevykdė jokios nusikalstamos veikos, vien už tokios įrangos pagaminimą ir perdavimą kitam asmeniui jo veikla yra kvalifikuojama pagal BK 198[2] straipsnį.

LAT Baudžiamųjų bylų skyriaus 2015 m. gegužės 12 d. nutartyje baudžiamojoje byloje Nr. 2K-188-489/2015 teisėjų kolegija, atsižvelgdama į skirtingus informacinės sistemos saugumo pažeidimo būdus (atakas), nurodė, kad BK 198[2] str. 1 d. nurodytos priemonės, tinkamos nusikalstamoms veikoms vykdyti, gali būti pagamintos ir turint teisėtą tikslą. Tačiau siekiant išvengti nepagrįsto baudžiamosios atsakomybės

taikymo, kai tokios priemonės yra pagamintos ir pateiktos vartotojams teisėtiems tikslams (pvz., skirtos informacinių technologijų produktų patikimumui ir saugumui testuoti), būtina nustatyti tiesioginį ketinimą panaudoti tokias priemones nusikalstamai veikai vykdyti. Toks aiškinimas atitiktų ir būtinos įgyvendinti 2013 m. rugpjūčio 12 d. Europos Parlamento ir Tarybos direktyvos 2013/40/ES dėl atakų prieš informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR (toliau – Direktyva 2013/40/ES) (OL 213 L 218, p. 8), preambulės 16 punktą. Taigi pagal nustatytas aplinkybes teisėjų kolegija sprendžia, kad BK 198-2 str. 1 d. nurodyto dalyko požymius šioje byloje atitinka ir dvejopo naudojimo priemonės (angl. *dual-use)*, kurios gali būti naudotojamos tiek teisėtiems, tiek ir nusikalstamiems tikslams.

Įstatymo leidėjas yra pasirinkęs veikų, susijusių su vaikų pornografijos platinimu internetu, kriminalizavimo „tradiciniais“ straipsniais variantą. Pagal BK 309 str. 1 d., baudžiamas tas, kas, turėdamas tikslą platinti, pagamino ar įsigijo arba platino pornografinio turinio dalykus, o pagal 2 d. – tas, kas pagamino, įgijo, laikė, demonstravo, reklamavo, siūlė arba platino pornografinio turinio dalykus, kuriuose vaizduojamas vaikas arba asmuo pateikiamas kaip vaikas, arba pasinaudodamas informacinėmis ir ryšių technologijomis ar kitomis priemonėmis įgijo ar suteikė prieigą prie pornografinio turinio dalykų, kuriuose vaizduojamas vaikas arba asmuo pateikiamas kaip vaikas. Beje, šiuo straipsniu kriminalizuotos ir veikos, įvykdytos platinant vadinamąsias pseudofotografijas, kuriose tam tikras asmuo pateikiamas kaip vaikas.

Bylų dėl vaikų pornografijos, susijusios su elektronine erdve, Lietuvoje kol kas nėra daug. Pavyzdžiui, 2011 m. Vilniaus apskrities vyriausiojo policijos komisariato Nusikaltimų tyrimo valdybos Ypatingų nusikaltimų tyrimo ir veiklos organizavimo skyriuje baigta didelės apimties ikiteisminio tyrimo byla dėl disponavimo pornografinio turinio dalykais, kuriuose vaizduojami vaikai arba asmenys, pateikiami kaip vaikai. Byla buvo pradėta nagrinėti 2009 m. rugpjūčio 17 dieną. Ikiteisminio tyrimo metu, atlikus daugybę ikiteisminio tyrimo veiksmų ir sudėtingų objektų tyrimų, buvo nustatyti aštuoni asmenys, įtariami disponavę pornografinio turinio dalykais. Dėl jų buvo atlikti aštuoni ikiteisminiai tyrimai, kurie prokuroro sprendimu perduoti teismui supaprastinto proceso tvarka (baudžiamasis įsakymas). Per trylika kratų rasta ir paimta kompiuterinių laikmenų, o atlikus kompiuterių laikmenų tyrimus aptikta, kaip įtariama, pornografinio turinio dalykų, kuriuose vaizduojami galbūt vaikai arba asmenys pateikiami kaip vaikai, arba galbūt pornografinio turinio dalykų, prieinamų iš tyrimui pateiktų tirti objektų kitiems interneto tinklo vartotojams. Pareigūnai

kreipėsi į Žurnalistų etikos inspektoriaus tarnybą, kad nustatytų, kokie kompiuterinėse laikmenose aptikti failai pripažįstami kaip pornografinio turinio dalykai, ir į Valstybinę teismo medicinos tarnybą, kad nustatytų, kurioje pornografinio turinio vaizdo medžiagoje vaizduojami vaikai.

LAT kol kas nenagrinėjo bylų, susijusių su BK 309 str. taikymu vaikų pornografijos platinimo, naudojant elektroninę erdvę, bylose.

Lietuvos įstatymo leidėjas BK sukčiavimo ir klastojimo veikas, vykdomas naudojantis elektronine erdve, kriminalizuoja „tradicinėmis" teisės normomis. Baudžiamoji atsakomybė už sukčiavimą nurodyta BK 182 straipsnyje. Šio straipsnio 1 dalyje nurodoma, kad baudžiamojon atsakomybėn traukiamas tas, kas apgaule savo ar kitų naudai įgijo svetimo turto ar turtinę teisę, išvengė turtinės prievolės ar ją panaikino. Pagal to paties straipsnio 2 d., baudžiamas tas, kas apgaule savo ar kitų naudai įgijo didelės vertės svetimą turtą ar turtinę teisę arba didelės mokslinės, istorinės ar kultūrinės reikšmės turinčių vertybių arba išvengė didelės vertės turtinės prievolės, arba ją panaikino, arba sukčiavo dalyvaudamas organizuotos grupės veikloje. Kaip matome, sudėtyse elektroninė erdvė neminima, vadinasi, sukčiaujama gali būti įvairiais būdais, įskaitant ir elektroninį. Atskirai elektroninio sukčiavimo būdo išskirti nebūtina.

BK baudžiamoji atsakomybė už klastojimą nurodyta 43 skyriuje „Nusikaltimai ir baudžiamieji nusižengimai valdymo tvarkai, susiję su dokumentų ar matavimo prietaisų klastojimu". Baudžiamoji atsakomybė už dokumento klastojimą nustatyta BK 300 str., kur nurodoma, jog baudžiamas yra tas, kas pagamino netikrą dokumentą, suklastojo tikrą dokumentą arba žinomai netikrą ar žinomai suklastotą tikrą dokumentą laikė, gabeno, siuntė, panaudojo ar realizavo. Straipsnyje numatytos ir kvalifikuotos sudėtys. Dokumento kategorija turėtų apimti ir elektroninius dokumentus, kurie neturėtų būti diskriminuojami, atsižvelgiant vien tik į dokumento formą.

Autorių teisių ir gretutinių teisių pažeidimo elektroninėje erdvėje veikas galima kvalifikuoti pagal BK XXIX skyriaus „Nusikaltimai intelektinei ir pramoninei nuosavybei" straipsnius. Šiame skyriuje kaip nusikaltimas įvardytas autorystės pasisavinimas (191 str.); literatūros, mokslo, meno ar kitokio kūrinio neteisėtas atgaminimas, neteisėtų kopijų platinimas, gabenimas ar laikymas (192 str.); informacijos apie autorių teisių ar gretutinių teisių valdymą sunaikinimas arba pakeitimas (193 str.) bei neteisėtas autorių teisių ar gretutinių teisių techninių apsaugos priemonių pašalinimas (194 str.). BK 192 str. nurodyta, kad baudžiamas tas, kas neteisėtai atgamino literatūros, mokslo ar meno kūrinį (įskaitant kompiuterių programas ir duomenų bazes) ar gretutinių teisių objektą arba jų dalį komercijos tikslais arba platino, gabeno ar laikė komercijos tikslais neteisėtas jų kopijas, jeigu

kopijų bendra vertė pagal teisėtų kopijų, o kai jų nėra, pagal atgamintų kūrinių originalų kainas viršijo 100 MGL dydžio sumą. LAT 2004 m. spalio 7 d. konsultacijoje Nr. B3-103 buvo aptarta komercinių tikslų sąvoka: pagal šią sąvoką tikslai laikytini komerciniais ne tik tais atvejais, kai vykdant veiklą, numatytą BK 192 str. 1 d., siekiama gauti tiesioginės ekonominės ar komercinės naudos, bet ir tada, kai ši veika vykdoma ir siekiant gauti netiesioginės ekonominės ar komercinės naudos. Kita vertus, įstatyme paminėti veiksmai nelaikomi nusikalstamais, jeigu tai daroma asmeninio naudojimo tikslams ar tam tikrų pelno nesiekiančių įstaigų, pvz., švietimo, mokslinio tyrimo, viešųjų bibliotekų, archyvų ir kt. labui.

Paminėtina ir jau anksčiau aptarta tapatybės vagystės elektroninėje erdvėje problema. Tapatybės vagystės elektroninėje erdvėje kaip savarankiškos pavojingos veikos kriminalizavimas, kaip rodo kai kurių tarptautinių organizacijų ir užsienio valstybių praktika, yra diskusijų objektas. Atkreiptinas dėmesys, kad Lietuvoje tapatybės vagystė elektroninėje erdvėje nėra kriminalizuota kaip savarankiškas nusikaltimas, nors, kaip jau minėta, kai kurie elementai, atlikus pastaruosius BK pakeitimus, yra įtraukti į tam tikrų veikų kvalifikuojančias sudėtis (kai pasinaudojama svetimais asmens duomenimis).

Žinių įtvirtinimo klausimai

1. Kuo skiriasi sampratos „elektroninis nusikaltimas“ ir „kompiuterinis nusikaltimas“?
2. Kokios yra pagrindinės elektroninių nusikaltimų latentiškumo priežastys?
3. Išvardykite pagrindinius elektroninių nusikaltėlių (hakerių) požymius.
4. Kokie yra pagrindiniai elektroninių nusikaltimų požymiai, skiriantys juos 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 baudžiamoji atsakomybė už elektroninius nusikaltimus yra numatyta Lietuvoje?

/X/ *skyrius*

Kibernetinis saugumas

1 skirsnis. Kibernetinio saugumo samprata

Internetas (arba elektroninė erdvė) daro vis daugiau įtakos kasdieniam gyvenimui, taip pat ir globaliai ekonomikai. Vidiniai šiuolaikinių organizacijų valdymo procesai yra neįmanomi ir neįsivaizduojami be informacinių technologijų ir sistemų, o informacinių technologijų atsiradimas yra neatsiejamas nuo informacijos saugumo ir apsaugos. Komercijos srityje vis daugėja komercinių sandorių, sudaromų elektroninėje erdvėje, viešųjų paslaugų vartojamumas irgi didėja didžiuliu tempu.

Nors suteikia daug galimybių, internetas kelia ir naujų, nuolat didėjančių grėsmių. Kadangi internetas yra globalus, labai sunku sekti jame vykdomas neteisėtas veikas. Informacija internete, anot P. Rosenzweigo, keičiamasi fiziniame pasaulyje beprecedenčiais greičiais ir būdais. Paprasti vartotojai arba įmonės ar organizacijos internete pajunta vis daugiau grėsmių. Plinta ir įvairi nusikalstama veika (visame pasaulyje elektroninių nusikaltimų aukomis kasdien tampa daugiau kaip milijonas žmonių). Su elektronine erdve susijusi nusikalstama veika gali būti labai įvairi: vogtos kreditinės kortelės parduodamos vos už vieną eurą, vykdomos tapatybės vagystės ir seksualinė prievarta prieš vaikus, rengiamos rimtos kibernetinės atakos prieš institucijas ir infrastruktūros objektus (COM/2012/140, 2012). Šių laikų nusikaltėliai vis labiau domisi informacinėmis technologijomis ir informacija, kuri gali būti naudojama neteisėtai veikai vykdyti.

Keletas faktų apie kibernetinį saugumą[70]:

- Apskaičiuota, kad nuolat sklando 150 tūkst. kompiuterinių virusų, kurie kasdien paveikia 148 tūkst. kompiuterių.
- Pasaulio ekonomikos forumo duomenimis, yra tikimybė, kad per ateinantį dešimtmetį ypatingos svarbos informacinės infrastruktūros objektai patirs didelių gedimų, kurių nuostoliai galėtų siekti apie 250 mlrd. JAV dolerių.
- Elektroniniai nusikaltimai sudaro nemažą kibernetinio saugumo incidentų dalį. „Symantec“ apskaičiavo, kad elektroninių nusikaltimų aukos visame pasaulyje kasmet praranda maždaug 290 mlrd. Eur, o „McAfee“ tyrimas atskleidė, kad elektroniniai nusikaltėliai kasmet gauna 750 mlrd. Eur pelno.
- 2014 m. „Eurobarometrui“ atlikus apklausą apie kibernetinį saugumą paaiškėjo, jog 85 proc. ES interneto vartotojų pripažįsta, kad rizika tapti elektroninio nusikaltimo auka nuolat didėja (atitinkamai 2013 m. tokia tikimybė siekė 76 proc.). 80 proc. interneto vartotojų

[70] Pabrėžtina, kad tokio pobūdžio informacija labai greitai keičiasi.

ES išreiškė susirūpinimą dėl interneto naudojimo tokiems dalykams kaip bankininkystė ar prekių pirkimas internetu (atitinkamai 2013 m. tokie vartotojai sudarė 75 proc.).

- Rengiant viešąsias konsultacijas dėl tinklų ir informacinių sistemų saugumo, 56,8 proc. respondentų nurodė, kad pernai teko patirti tinklų ir informacinių sistemų saugumo incidentų, kurie turėjo rimtų padarinių jų veiklai.
- Eurostato duomenys rodo, kad iki 2012 m. sausio tik 26 proc. ES įmonių turėjo oficialiai vykdomą IRT saugumo politiką.

Nuolat didėjanti rizika verčia labai rimtai susirūpinti dėl kibernetinio saugumo. Šiandieniame globaliame pasaulyje kibernetinis saugumas šiuolaikinei žinių ir informacijos visuomenei tampa vienu aktualiausių dalykų politiniu, socialiniu, ekonominiu, techniniu ir teisiniu aspektais.

Dar prieš keletą metų tiek teorijoje, tiek praktikoje buvo labiau paplitęs elektroninių duomenų saugumo (elektroninės informacijos saugos) terminas. Informacijos saugumas (sauga) buvo suprantama kaip informacijos ir sistemos infrastruktūros apsauga nuo atsitiktinio ar tyčinio, natūralaus ar dirbtinio poveikio, galinčio padaryti žalos informacijos ar sistemos infrastruktūros savininkams ir vartotojams. Praktikoje išskiriami trys pagrindiniai elektroninės informacijos saugos aspektai:

- prieinamumas – galimybė tam tikrą laiką gauti reikalingos informacijos;
- vientisumas – informacijos svarbumas ir nepriekaištingumas bei apsauga nuo sunaikinimo ir neteisėto pakeitimo;
- slaptumas – apsauga nuo neteisėto nuskaitymo.

Šios trys kategorijos kaip elektroninės informacijos saugos pagrindas išlieka iki šių dienų.

Pastaruoju metu vietoj minėtųjų terminų vis dažniau vartojamas kibernetinio saugumo terminas, tačiau tam tikrais atvejais išlieka ir elektroninės informacijos saugos kategorija. Kibernetinio saugumo termino ištakos susijusios su grėsmėmis, kylančiomis internete. Kadangi šiandieniame pasaulyje dauguma informacinių sistemų vienaip ar kitaip susijusios su internetu (debesų kompiuterija, socialiniai tinklai, internetinė televizija ir pan.), galima teigti, kad kibernetinio saugumo terminas geriau atspindi šiandienę padėtį. Nors žodis „kibernetinis“ yra diskutuotinas, vis dėlto „kibernetinio saugumo“ terminas jau yra įtvirtintas ir Lietuvos Respublikos teisės akuose.

Įvairių autorių ir organizacijų kibernetinis saugumas apibrėžiamas labai įvairiai. J. P. Trachtmanas kibernetinį saugumą apibūdina kaip apsaugą nuo

netinkamo interneto infrastruktūros naudojimo ir piktnaudžiavimo (žlugdymo). Anot autoriaus, kibernetinis saugumas apima apsaugą nuo elektroninių nusikaltimų (įskaitant sukčiavimą, informacijos vagystę ir pan.).

Tarptautinė telekomunikacijų sąjunga kibernetinį saugumą apibrėžia kur kas detaliau: kibernetinis saugumas – priemonių, politikų, saugumo koncepcijų ir jo užtikrinimo priemonių, rekomendacijų, rizikos valdymo požiūrių, veiksmų, mokymų, geriausių praktikų ir technologijų sistema, kuri naudojama siekiant apsaugoti elektroninę erdvę, organizacijas ir vartotojus.

Pagal D. Shoemakerį ir A. Conkliną, kibernetinis saugumas apima procesus, susijusius su kylančių kibernetinių grėsmių identifikavimu bei sąnaudomis pagrįstų kontrpriemonių taikymu, kūrimu ir palaikymu *(Shoemaker, Conklin*, 2012).

ES kibernetinio saugumo strategijoje (JOIN/2013/1 final, 2013) kibernetinis saugumas apibrėžiamas kaip: priemonės ir veiksmai, naudojami turint tikslą apsaugoti kibernetinę platformą, apimant civilinę ir karinę sritis, nuo grėsmių, kurios gali padaryti žalos elektroninių ryšių tinklams ar informacinei infrastruktūrai. Tai vienas iš pirmųjų bandymų oficialiuose dokumentuose apibrėžti kibernetinį saugumą.

Lietuvos Respublikos kibernetinio saugumo įstatyme kibernetinis saugumas apibrėžiamas kaip „visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, skirtų kibernetiniams incidentams išvengti, aptikti, analizuoti ir reaguoti į juos, taip pat įprastinei elektroninių ryšių tinklų, informacinių sistemų ar pramoninių procesų valdymo sistemų veiklai, įvykus šiems incidentams, atkurti."

Galima teigti, kad kibernetinio saugumo sąvoka gali būti vartojama skirtingai ir dar nėra galutinai nusistovėjusi.

2 skirsnis. Kibernetinio saugumo principai

Istoriškai elektroninės informacijos sauga buvo paremta tam tikrais svarbiausiais principais, kurių aktualumas išlieka iki šiol:

1. *Suvokimo principas*. Siekiant užtikrinti elektroninės informacijos saugą, reikia suvokti apsisaugojimo nuo galimos grėsmės elektroninei informacijai priemonių naudojimo būtinybę.
2. *Atsakomybės principas*. Kiekvienas elektroninės informacijos vartotojas turi suvokti savo atsakomybę ir funkcijas saugant elektroninę informaciją. Šios informacijos saugą informacinėse sistemose turi užtikrinti valstybės institucijos vadovas, o ją įgyvendinti – saugos įgaliotiniai.

3. *Reagavimo principas*. Elektroninei informacijai kyla įvairi grėsmė, todėl būtina laiku aptikti saugos incidentus ir užkirsti jiems kelią, be to, valstybės institucijos viduje ir su kitomis valstybės institucijomis nuolat keistis informacija apie elektroninei informacijai kylančią grėsmę ir kovos su ja priemones.
4. *Demokratiškumo principas*. Elektroninės informacijos sauga turi būti įgyvendinama ir suderinama su esminėmis demokratinės visuomenės vertybėmis (pvz., laisve skleisti informaciją ir ją gauti).
5. *Rizikos įvertinimo principas*. Siekiant nustatyti esamą elektroninės informacijos saugos lygį ir parinkti būtinas elektroninės informacijos saugos priemones, būtina periodiškai atlikti elektroninės informacijos saugos rizikos įvertinimą informacinėse sistemose.
6. *Elektroninės informacijos saugos kultūros kėlimo principas*. Siekiant užtikrinti elektroninės informacijos saugą, būtina ypač daug dėmesio skirti nuolatiniams šios informacijos vartotojų mokymams elektroninės informacijos saugos srityje ir taip kelti elektroninės informacijos saugos kultūrą valstybės institucijose.
7. *Elektroninės informacijos saugos priemonių projektavimo ir diegimo principas*. Elektroninės informacijos sauga turi būti užtikrinama kuriant informacinę sistemą. Minėtoji sauga turi būti pamatinis visų informacinės sistemos paslaugų elementas, kuriam būtina garantuoti nuolatinį lėšų, neviršijančių pačios elektroninės informacijos vertės, skyrimą.

Pastaruoju metu išskiriami šie svarbiausi kibernetinio saugumo principai[71]:

1. *Pagrindinių žmogaus teisių, raiškos laisvės, privatumo ir asmens duomenų apsauga.*

Kibernetinis saugumas gali būti efektyvus tik tuo atveju, jeigu paremtas pagrindinių teisių ir laisvių apsauga bei pagrįstas svarbiausiomis ES vertybėmis. Individų teisės atitinkamai negali būti užtikrinamos nesant saugių tinklų ir sistemų. Bet koks dalijimasis informacija siekiant kibernetinio saugumo tikslų, kai įtraukiami asmens duomenys, turi būti vykdomas vadovaujantis ES duomenų apsaugos reguliavimu ir užtikrinant visapusišką individų teisių apsaugą šioje srityje.

[71] Šie principai išskiriami 2003 m. ES kibernetinio saugumo strategijoje. Reikia paminėti, kad nacionalinėse ES valstybių strategijose kibernetinio saugumo principai pateikiami labai skirtingai, pradedant nuo proporcingumo ir baigiant individualia atsakomybe ar bendradarbiavimu.

2. *Prieiga visiems.*

Dėl ribotos prieigos prie interneto ar tokios prieigos nebuvimo piliečiams kyla nepatogumų. Kiekvienas turi turėti prieigą prie interneto ir informacijos. Interneto integralumas ir saugumas turi būti garantuojami siekiant visiems užtikrinti saugią prieigą.

3. *Demokratinis ir efektyvus valdymas.*

Skaitmeninis pasaulis nėra kontroliuojamas vienos struktūros (bendrovės). Šiuo metu yra keletas „žaidėjų“, daugelis iš jų yra komerciniai arba nevyriausybiniai dariniai, įsitraukę į kasdienį interneto išteklių valdymą, interneto protokolų ir standartų kūrimą. Būtina pabrėžti tokių „žaidėjų“ svarbą dabartiniam interneto valdymo modeliui ir paramą šiam daugialypio valdymo požiūriui.

4. *Bendra atsakomybė užtikrinant saugumą.*

Dėl didėjančios priklausomybės nuo informacijos ir komunikacijų technologijų atsirado silpnų vietų, kurios turi būti aptiktos, sustiprintos ir apgintos. Tiek viešasis sektorius, tiek privačios įmonės, tiek individualūs vartotojai turi pripažinti šią bendrą atsakomybę, imtis apsaugos priemonių ir, jeigu reikia – užtikrinti koordinuotus veiksmus kibernetiniam saugumui sustiprinti.

Pagal Lietuvos Respublikos kibernetinio saugumo įstatymą, „kibernetinis saugumas grindžiamas bendraisiais teisės principais, elektroninių ryšių veiklos reguliavimo principais ir šiais kibernetinio saugumo principais:

1) kibernetinės erdvės nediskriminavimo – įstatymų ir kitų teisės aktų nuostatos ir saugomi gėriai vienodai taikomi tiek fizinėje, tiek kibernetinėje erdvėje;
2) kibernetinio saugumo proporcingumo – taikomos kibernetinio saugumo užtikrinimo priemonės negali būti griežtesnės, negu būtina kibernetiniam saugumui užtikrinti, o taikomi teisiniai, organizaciniai ir techniniai kibernetinio saugumo reikalavimai neturi apriboti kibernetinio saugumo dalyvių veiklos kibernetinėje erdvėje labiau, nei tai būtina;
3) viešojo intereso viršenybės – naudojamos kibernetinio saugumo užtikrinimo priemonės pirmiausia turi užtikrinti visuomenės viešojo intereso apsaugą, tačiau neturi iš esmės pažeisti atskirų vartotojų teisių ar neproporcingai apriboti jų laisvės kibernetinėje erdvėje.“

Manytina, kad kibernetinio saugumo principai nėra iki galo nusistovėję, jie dar tik formuojasi.

3 skirsnis. ES kibernetinio saugumo strategija

Prieš analizuojant ES kibernetinio saugumo strategiją, reikėtų paminėti ir tai, jog tarptautiniu mastu ši sritis nėra reguliuojama. Vienintelis dokumentas – 2002 m. EBPO patvirtintos Informacinių sistemų saugos gairės. Tai tik rekomendacinio pobūdžio dokumentas, kuriuo įtvirtinti minėtieji elektroninės informacijos saugos principai, tačiau jis neturi privalomos teisinės galios.

Elektroninės informacijos sauga (kibernetinis saugumas) akcentuojama ne viename ES dokumente. Jau 2001 m. ES teisės aktuose yra nurodoma, kad informacinės ir telekomunikacinės technologijos tapo šiuolaikinės visuomenės gyvenimo kamienu ir nuo jų vis labiau tampa priklausomi socialiniai ir ekonominiai visuomenės gerovės aspektai (COM/2001/298, 2001), o 2006 m. atkreiptas ypatingas dėmesys į saugios Europos kibernetinės erdvės sukūrimą pasitelkiant visus socialinius valdžios partnerius (COM/2006/251, 2006). Didžiuliai informacijos kiekiai yra saugomi privačių įmonių duomenų centruose, valstybės institucijų duomenų saugyklose ir informacinių sistemų duomenų bazėse. Dėl tokios informacijos paviešinimo, nesavalaikio panaudojimo ar sugadinimo gali kilti daug problemų, o verslo organizacijos ar viešojo administravimo subjektai patirti didelių piniginių nuostolių.

ES valstybės atkreipia ypatingą dėmesį, kad reikalingas glaudesnis sąjungos valstybių narių bendradarbiavimas kovojant su nusikaltimais elektroninėje erdvėje ir užtikrinant kibernetinės erdvės bei „ypatingos svarbos informacinės infrastruktūros“ apsaugą nuo kibernetinių išpuolių. ES dokumentuose pabrėžiama, kad „ypatingos svarbos informacinės infrastruktūros objektai gyvybiškai būtini ES ekonomikos ir visuomenės plėtrai“, o informacinių technologijų ir interneto plėtra (skvarba) gerina ekonominius rodiklius ir užtikrina visuomenės socialinės gerovės kilimą bei piliečių gyvenimo kokybę.

Pastaraisiais metais ES kibernetinio saugumo sričiai skiriamas ypatingas dėmesys. 2012 m. Europos Komisija paskelbė konsultaciją kibernetinio saugumo teisinio reguliavimo srityje. Joje labai aktyviai dalyvavo tiek viešojo, tiek ir privataus sektoriaus subjektai.

2013 m. vasario 7 d. Europos Komisija ir ES vyriausioji užsienio reikalų ir saugumo politikos įgaliotinė paskelbė kibernetinio saugumo strategiją (toliau – Kibernetinio saugumo strategija) kartu su Komisijos direktyvos dėl tinklų ir informacinių sistemų saugumo siūlymu.

Kibernetinio saugumo strategija „Atvira, saugi ir patikima kibernetinė erdvė“ yra išsami ES vizija, kaip geriausiai užkirsti kelią kibernetinės

veiklos sutrikdymui bei atakoms ir kokių atsakomųjų priemonių imtis. Taip siekiama remti europines laisvės ir demokratijos vertybes bei užtikrinti saugią skaitmeninės ekonomikos plėtrą. Konkrečiais veiksmais stengiamasi didinti informacinių sistemų atsparumą elektroniniams nusikaltimams ir stiprinti ES tarptautinę kibernetinio saugumo politiką bei kibernetinę gynybą.

Teigiama, kad elektroninės erdvės saugumui užtikrinti naudojamos priemonės nėra savitikslės. Svarbiausias tikslas – pasiekti, kad internetas ir toliau liktų atviras bei laisvas, ir užtikrinti, kad principai ir vertybės, kurie galioja „offline“, galiotų ir „online“ aplinkoje.

Kibernetinio saugumo strategijoje nustatomi penki strateginiai prioritetai:

1) įgyti kibernetinį atsparumą;
2) radikaliai sumažinti elektroninių nusikaltimų skaičių;
3) sukurti kibernetinės gynybos politiką ir pajėgas, kiek tai susiję su bendra saugumo ir gynybos politika;
4) plėtoti pramonės ir technologinius išteklius, skirtus kibernetiniam saugumui užtikrinti;
5) sukurti nuoseklią tarptautinę elektroninės erdvės politiką ir remti pagrindines ES vertybes.

Toliau kiekvienas iš šių prioritetų aptartinas atskirai.

1. **Įgyti kibernetinį atsparumą**.

Tam, kad užtikrintų kibernetinį atsparumą, tiek viešasis, tiek privatus sektoriai turi plėtoti kibernetinio atsparumo galimybes ir glaudžiai tarpusavyje bendradarbiauti. Šiame kontekste minėtina *ENISA*, kuri buvo įkurta 2004 m., ir daugelis kitų teisinio reguliavimo priemonių, skirtų elektroninių ryšių rizikai valdyti ar asmens duomenims apsaugoti. Tačiau, neatsižvelgiant į visas priemones, visoje ES egzistuoja daugybė spragų, ypač susijusių su nacionaliniais pajėgumais tarptautinių incidentų atveju ir su privataus sektoriaus įsitraukimu sprendžiant kibernetinio saugumo klausimus. Dėl to Kibernetinio saugumo strategija siejama su teisinio reguliavimo siūlymais, įskaitant:

– Minimalių bendrųjų reikalavimų nacionalinėms informacijos infrastruktūroms nustatymą. Valstybės narės būtų įpareigotos skirti kompetentingas institucijas, įkurti gerai veikiančius CERT, priimti nacionalines informacijos infrastruktūros strategijas ar atlikti kitus veiksmus.
– Įkurti koordinuotus prevencijos, aptikimo ir reagavimo mechanizmus, įgalinančius dalytis informacija ir bendradarbiauti su kompetentingomis nacionalinėmis institucijomis.

– Gerinti privataus sektoriaus įsitraukimą ir pasirengimą. Kadangi daugumą tinklų ir informacinių sistemų valdo privatūs subjektai ar bendrovės, privataus sektoriaus įsitraukimas užtikrinant kibernetinį saugumą yra kritiškai svarbus.

2. **Radikaliai sumažinti elektroninių nusikaltimų skaičių**.

Kuo ilgiau gyvename skaitmeniniame pasaulyje, tuo daugiau veiklos galimybių suteikiame elektroniniams nusikaltėliams. Elektroniniai nusikaltimai yra viena iš labiausiai plintančių nusikaltimų rūšių. Elektroniniai nusikaltėliai tampa vis labiau kvalifikuoti. Elektroniniams nusikaltimams dažniausiai būdinga sąlygiškai maža rizika ir didelis pelnas. Nusikaltėliai naudojasi tuo, kad elektroninėje erdvėje gana sunku aptikti jų pėdsakus. Be to, elektroniniams nusikaltimams neegzistuoja valstybių sienos. Dėl to teisėsaugos institucijos turi tarpusavyje bendradarbiauti, keisti informacija ir veiksmais, kad galėtų duoti tinkamą atkirtį šiai nuolat didėjančiai grėsmei.

Dėl to teigiama, kad ES turi būti laikomasi griežtų ir efektyvių įstatymų, nukreiptų prieš elektroninius nusikaltimus. Pabrėžtina, kad Konvencija dėl elektroninių nusikaltimų yra vienintelis teisiškai įpareigojantis tarptautinis dokumentas, sukuriantis reikiamą kovos su elektroniniais nusikaltimais sistemą, kurią turi įgyvendinti prie konvencijos prisidėjusios valstybės. Tačiau ir Europos Komisija turėtų imtis atitinkamų veiksmų, įskaitant direktyvų ar kitų dokumentų elektroninių nusikaltimų srityje išleidimą ir tobulinimą ar raginimą valstybes ratifikuoti Konvenciją dėl elektroninių nusikaltimų.

Šiame kontekste daug tikimasi iš Europos elektroninių nusikaltimų centro[72], kuris laikomas pagrindine kovos su elektroniniais nusikaltimais priemone. Numatoma, kad Europos elektroninių nusikaltimų centras susitelks į tris pagrindines elektroninių nusikaltimų rūšis: sukčiavimą, įsilaužimą ir elektroninius nusikaltimus vaikams.

3. **Sukurti kibernetinės gynybos politiką ir pajėgumus, kiek tai susiję su bendra saugumo ir gynybos politika**.

Kibernetinio saugumo pastangos ES apima ir kibernetinės gynybos dimensiją. Tam, kad būtų užtikrintas informacijos ir komunikacijos sistemų atsparumas, kibernetinės gynybos pajėgumų plėtra turi būti koncentruota į aptikimą, atsaką ir išteklių atkūrimą po kibernetinių atakų. Šiame kontekste labia svarbi kibernetinės gynybos politika ir galimybių duoti atkirtį kibernetinėms atakoms didinimas. Ypač turėtų būti skatinama privataus ir valstybinio sektorių sąveika, siekiant apsaugoti interneto išteklius nuo kibernetinių atakų.

[72] Įkurtas Europole.

4. **Plėtoti pramonės ir technologinius išteklius, skirtus kibernetiniam saugumui užtikrinti**.

ES turi puikias tyrimo ir plėtros galimybes, tačiau dauguma pasaulio technologijų lyderių, kuriančių inovatyvius ICT produktus ir paslaugas, yra įsikūrę už ES ribų. Dėl to kyla rizika, kad Europa taps priklausoma nuo ICT produktų, kildinamų ne iš Europos, ir nuo saugumo sprendimų, priimamų užsienyje. Todėl daugelis kibernetinio saugumo sprendimų turėtų būti priimami būtent Europoje.

5. **Sukurti nuoseklią tarptautinę elektroninės erdvės politiką ir palaikyti svarbiausias ES vertybes**.

Komisija turi vykdyti tinkamą elektroninės erdvės politiką, kuri užtikrintų geresnį tarptautinių partnerių ir organizacijų įsitraukimą ir glaudesnį bendradarbiavimą bei glaudesnius ryšius su bendruomenėmis ir privačiu sektoriumi.

Vienas iš pagrindinių ES tarptautinės elektroninės erdvės politikos aspektų – skatinti, kad elektroninė erdvė būtų laikoma tokia vieta, kur užtikrinamos žmogaus teisės ir laisvės.

Funkcijos ir atsakomybė pagal ES kibernetinio saugumo strategiją

Šiuolaikinėje visuomenėje kibernetiniai incidentai neturi sienų. Visi dalyviai, siekdami užtikrinti kibernetinį saugumą tiek nacionaliniu, tiek ir ES lygiu, turėtų dirbti kartu. Kadangi gali būti taikomi skirtingi teisės aktai ir skirtingos jurisdikcijos, vienas iš svarbiausių ES uždavinių – išgryninti visų pagrindinių „žaidėjų“ vaidmenis ir atsakomybę.

Šiuo metu nepalaikoma centralizuotos europinės priežiūros koncepcija. Manoma, kad nacionalinės vyriausybės gali geriausiai organizuoti kibernetinių atakų prevenciją ir atsaką į jas bei plėtoti ryšius su privačiu sektoriumi. Be abejo, dėl galimos tarptautinės rizikos kilmės efektyvus nacionalinis atsakas dažniausiai reikalautų ES lygio įsitraukimo.

ES kibernetinio saugumo strategijoje yra išskiriami trys lygiai: nacionalinis, ES ir tarptautinis, kuriais būtų veikiama, siekiant užtikrinti kibernetinį saugumą.

Nacionaliniu lygiu teigiama, kad valstybės narės turi turėti atitinkamas elektroninių nusikaltimų prevencijos ir gynybos struktūras. Šios struktūros turėtų užtikrinti reikiamus pajėgumus kovojant su kibernetiniais incidentais. Koordinavimo veiklą šioje srityje turėtų vykdyti ministerijos. Kibernetinio saugumo strategijose valstybės narės turėtų nustatyti įvairių nacionalinių institucijų funkcijas. Be to, turėtų būti užtikrinamas reikiamas apsikeitimas informacija ne tik tarp valstybės institucijų, bet ir su privačiu sektoriumi. Kibernetinių incidentų atveju turėtų būti užtikrinamas atitinkamų saugumo planų įgyvendinimas, įskaitant ir atitinkamų funkcijų bei atsakomybės nustatymą.

ES lygiu irgi yra daugybė institucijų: *ENISA*, *Europol* ir *EDA*, aktyviai veikiančių kibernetinio saugumo srityje. Tarp minėtųjų institucijų ypač svarbus bendradarbiavimas tokiose srityse kaip rizikos valdymas, mokymai, apsikeitimas geriausia praktika ir kt.

Tarptautiniu lygiu labai svarbu koordinuoti tarpusavio veiksmus kibernetinio saugumo srityje. Europos Komisija tarptautiniu lygiu remia pagrindines vertybes ir palaiko viešą bei skaidrų kibernetinių technologijų naudojimą. Be to, Europos Komisija pasisako už bendradarbiavimą su pagrindiniais tarptautiniais partneriais ir organizacijomis: Europos Taryba, *EBPO* ir kt.

Pasiūlyta tinklų ir informacinių sistemų saugumo direktyva yra pagrindinė bendrosios strategijos sudėtinė dalis, todėl reikės, kad visos valstybės narės, pagrindiniai interneto teikėjai ir ypatingos svarbos infrastruktūros objektų, pvz., e. prekybos platformų ir socialinių tinklų, operatoriai bei energijos, transporto, bankininkystės ir sveikatos priežiūros paslaugų operatoriai visoje ES užtikrintų saugią ir patikimą skaitmeninę aplinką. Pasiūlytoje direktyvoje nustatytos šios priemonės:

a) valstybės narės turi priimti tinklų ir informacinių sistemų saugumo strategiją bei skirti kompetentingą nacionalinę tinklų ir informacinių sistemų saugumo instituciją, turinčią užtektinai tinkamų finansinių ir žmogiškųjų išteklių, kuri galėtų užkirsti kelią tinklų ir informacinių sistemų saugumo rizikai ir incidentams, juos spręsti ir imtis atsakomųjų priemonių;

b) sukurti valstybių narių ir Komisijos bendradarbiavimo mechanizmą: saugia infrastruktūra būtų iš anksto pranešama apie riziką ir incidentus, bendradarbiaujama ir reguliariai rengiami tarpusavio vertinimai;

c) kai kurių sektorių (finansinių paslaugų, transporto, energetikos, sveikatos priežiūros) ypatingos svarbos infrastruktūros objektų operatoriai, informacinės visuomenės paslaugų teikėjai (visų pirma programinės įrangos parduotuvių e. prekybos platformų, mokėjimo internetu, nuotolinių kompiuterinių išteklių paslaugų, paieškos sistemų, socialinių tinklų) ir viešojo administravimo institucijos turi patvirtinti rizikos valdymo praktiką ir pranešti apie svarbiausius saugumo incidentus savo pagrindinėse tarnybose.

Reikėtų pabrėžti, kad direktyvos tekstas vis dar svarstomas, įskaitant ir sektorius, kuriems ketinama taikyti įpareigojimus. Galutinio direktyvos teksto 2015 m. lapkričio mėnesį dar nebuvo. Tačiau artimiausiu metu direktyvą vis tiek planuojama priimti.

4 skirsnis. Instituciniai kibernetinio saugumo aspektai (ENISA)

Kaip institucija paminėtina Europos informacijos ir tinklų saugumo agentūra (*ENISA*).

Teikdama pasiūlymą dėl Europos Parlamento ir Tarybos reglamento dėl *ENISA* įsteigimo, Europos Komisija pripažino, kad tinklų ir informacijos apsauga yra vienas svarbiausių saugumo politikos klausimų. Tokiomis aplinkybėmis siekiant sustiprinti Bendrijos, valstybių narių ir verslo bendruomenės gebėjimą užkirsti kelią didžiausiems tinklų ir informacijos saugumo pavojams, juos nagrinėti ir į juos reaguoti, 2004 m. kovo 10 d. pagal Europos Parlamento ir Tarybos reglamentą (EB) Nr. 460/2004 penkerių metų laikotarpiui buvo įkurta *ENISA*. Ši institucija įsteigta „siekiant užtikrinti aukštą ir veiksmingą Bendrijos tinklų ir informacijos saugumo lygį, [...] siekiant Europos Sąjungos piliečių, vartotojų, įmonių ir valstybinio sektoriaus organizacijų labui formuoti tinklų kultūrą ir informacijos apsaugą, tuo prisidedant prie sklandaus vidaus rinkos funkcionavimo“, kitaip tariant, siekia – koordinuoti elektroninių ryšių tinklų ir informacijos saugumo veiksmus Europos lygmeniu“. Po penkerių metų minėtosios institucijos veikla vis dar buvo tęsiama. Savo būstinę agentūra turi Graikijoje.

ENISA tikslai:

- Svarbiausias *ENISA* tikslas – Europos lygmeniu koordinuoti elektroninių ryšių tinklų ir informacijos saugumo veiksmus;
- Agentūra siekia stiprinti Bendrijos, šalių narių ir verslo bendruomenės pajėgumus siekiant užkirsti kelią tinklų ir informacijos saugumo problemoms, jas aptikti ir tinkamai reaguoti;
- Teikti pagalbą ir patarti Europos Komisijai bei šalims narėms klausimais, susijusiais su tinklų ir informacijos saugumu;
- Remiantis nacionalinėmis ir visos Bendrijos pastangomis, skatinti aktyvų valstybinio ir privataus sektorių dalyvių bendradarbiavimą;
- Paprašyta Komisijos *ENISA* padeda atlikti techninius parengiamuosius darbus atnaujinant ir tobulinant Bendrijos teisės aktus, reglamentuojančius tinklų ir informacijos saugumo sritį.

Agentūrai skirtos tokios užduotys: rinkti atitinkamą informaciją, siekiant analizuoti esamus ir kylančius pavojus, ypač tuos, kurie gali paveikti elektroninių ryšių tinklų atsparumą ir perduodamos informacijos autentiškumą, vientisumą bei slaptumą. Be to, agentūra kuria „bendruosius metodus“, skirtus užkirsti kelią saugumo problemoms, prisidėti prie informuotumo gerinimo, skatinti „turimos geriausios patirties“ ir „įspėjimo būdų“ mainus bei pavojų vertinimo ir valdymo veiklą.

Agentūrai dar patikėta stiprinti tinklų ir informacijos apsaugos srities subjektų bendradarbiavimą, teikti paramą Komisijos ir valstybių narių dialogo su pramone metu, sprendžiant su techninės ir programinės įrangos apsauga susijusias problemas ir prisidedant prie Bendrijos pastangų bendradarbiauti su trečiosiomis valstybėmis, o prireikus ir su tarptautinėmis organizacijomis, skatinant bendrą pasaulinį požiūrį į tinklų ir informacijos apsaugos problemas, tokiu būdu prisidedant prie bendros tinklų ir informacijos apsaugos kultūros kūrimo.

ENISA viešai skelbia savo ataskaitas, kurios prieinamos šios institucijos tinklalapyje *http://www.enisa.europa.eu*.

5 skirsnis. Kibernetinio saugumo reglamentavimas įstatymo lygmeniu Lietuvoje

Teisinio kibernetinio saugumo reguliavimo užuomazgų Lietuvoje atsirado jau 2006 m., kai Lietuvos Respublikos Vyriausybė nutarimu Nr. 1211 patvirtino Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymo koncepciją. Minėtoji Koncepcija parengta įgyvendinant Lietuvos Respublikos Vyriausybės 2006–2008 m. programos įgyvendinimo priemonių, patvirtintų Lietuvos Respublikos Vyriausybės 2006 m. spalio 17 d. nutarimu Nr. 1020 (Žin., 2006, Nr. 112-4273), 157 punktą.

Šioje Koncepcijoje buvo numatyta, jog Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymas reglamentuos santykius, susijusius su elektroninių ryšių tinklų ir informacijos saugumu (toliau vadinama – tinklų ir informacijos saugumas), sudarys saugios informacinės visuomenės plėtros ir didesnio vartotojų pasitikėjimo ja sąlygas. Remiantis šia koncepcija, svarbiausias įstatymo tikslas turėjo būti toks – apibrėžti visuomeninių santykių, susijusių su tinklų ir informacijos saugumu, teisinio reguliavimo pagrindus ir juos įtvirtinti. Įstatymas užpildys ir su elektroninių ryšių paslaugų teikimu susijusių santykių teisinio reguliavimo spragas, kiek tai susiję su tinklų ir informacijos saugumu teikiant elektroninių ryšių paslaugas.

Pagal Koncepciją įstatymu turėjo būti nustatyta:

- aiški valstybės institucijų struktūra tinklų ir informacijos saugumo srityje, kad nebūtų dubliuojamos atsakingų institucijų funkcijos ir jos galėtų veiksmingai tarpusavyje bendradarbiauti;
- nustatyti bendrieji tinklų ir informacijos saugumo reikalavimai, daugiausia skirti vartotojams apsaugoti nuo tinklų ir informacijos saugumo incidentų;

- valstybės ir savivaldybių institucijų tinklų ir informacinių sistemų, saugaus informacijos perdavimo tarp valstybės ir savivaldybių institucijų, kritinių informacinių infrastruktūrų tinklų ir informacijos saugumo reikalavimai;
- aiški tinklų ir informacijos saugumo lygio įvertinimo sistema, reglamentuojanti tinklų bei informacijos saugumo audito atlikimą, techninės ir programinės įrangos saugumo įvertinimą. Ši sistema daugiausia bus taikoma valstybės ir savivaldybių institucijų tinklams ir informacinėms sistemoms, kritinėms informacinėms infrastruktūroms, didesnių įmonių ir informacinės visuomenės paslaugų teikėjų tinklams bei informacinėms sistemoms, t. y. tiems atvejams, kai tinklų ir informacijos saugumas dažniausiai užtikrinamas laikantis atitinkamos saugumo politikos.

Patvirtinus šią koncepciją, buvo sudaryta darbo grupė ir pradėtas rengti Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymo projektas. Darbo grupė parengė įstatymo projektą, tačiau pats įstatymas taip ir nebuvo priimtas. Pagal projektą, įstatymas turėjo reglamentuoti visuomeninius santykius, susijusius su elektroninių ryšių tinklų ir informacijos saugumu, nustatant bendruosius elektroninių ryšių tinklų ir informacijos saugumo užtikrinimo reikalavimus bei visuomeninius santykius, susijusius su valstybės ir vietos savivaldos institucijų bei kritinių informacinių infrastruktūrų elektroninių ryšių tinklų ir informacijos saugumu bei elektroninių ryšių tinklų ir informacijos saugumo audito bei techninės ir programinės įrangos saugumo vertinimu.

Tam tikros teisinės nuostatos numatytos Lietuvos Respublikos valstybės informacinių išteklių įstatyme, tačiau yra reglamentuota tik valstybės informacinių išteklių sauga bei saugos įgaliotinio institutas. Deja, šios juridinės teisės normos nereglamentuoja informacijos saugos privačiame sektoriuje, be to, ir informacijos sauga valstybės institucijų sektoriuje reglamentuojama fragmentiškai, pvz., įstatyme nenumatyta informacijos saugos institucinės kontrolės ir politikos formavimo sistema. Tai, kad teisės aktuose nėra įvardyta nė vienos už informacijos saugumo koordinavimą atsakingos institucijos, kuri turėtų įgaliojimus ir išteklių ne tik rengti ar vertinti teisės aktus, bet ir atlikti realius informacijos saugumo auditus, kaip problemą kelia ir dr. Saulius Jastiuginas *(www.technologijos.lt*, 2013).

Iš sektorinių teisės aktų – įstatymų, paminėtinas Lietuvos Respublikos elektroninių ryšių įstatymas. Šio įstatymo nuostatos dėl elektroninių ryšių informacijos saugos iš esmės buvo išplėstos įgyvendinant vieną iš ES elektroninių ryšių paketo direktyvų – direktyvą 2009/136/EB. Dėl to Elektroninių ryšių įstatyme (pastarieji įstatymo pakeitimai padaryti 2011 m.

birželio 28 d.) atsirado gana nemažai teisės normų dėl elektroninės informacijos saugos. Šis įstatymas taikomas ir privačiam sektoriui, t. y. elektroninių ryšių tinklų ir (ar) paslaugų teikėjams.

Elektroninių ryšių paslaugų saugumo ir vientisumo klausimu įstatyme nustatyta, kad viešųjų ryšių tinklų ar paslaugų teikėjai privalo įgyvendinti tinkamas technines ir organizacines priemones savo teikiamų tinklų ar paslaugų saugumo lygiui, atitinkančiam iškilusią grėsmę, užtikrinti ir užkirsti kelią saugumo incidentams arba sumažinti jų poveikį viešųjų ryšių tinklams ir viešųjų el. ryšių paslaugų gavėjams. Be to, turi būti užtikrintas nepertraukiamas viešųjų el. ryšių paslaugų teikimas. Įstatyme dar nustatyta pareiga viešųjų ryšių tinklų ar paslaugų teikėjui apie asmens duomenų saugumo pažeidimus nedelsiant pranešti Valstybinei duomenų apsaugos inspekcijai ir (ar) abonentui, registruotam naudotojui ar kitam asmeniui, jeigu pažeidimas gali turėti neigiamą poveikį jo privatumo saugumui, išskyrus atvejus, kai jis Valstybinei duomenų apsaugos inspekcijai įrodo, kad ėmėsi tinkamų techninių priemonių, užtikrinančių, kad tam neįgalioti asmenys negalėtų susipažinti su asmens duomenimis. Toks teisinis reguliavimas, įpareigojantis pranešti apie asmens duomenų saugumo pažeidimus, ES direktyvoje siejamas su tapatybės vagystės prevencija. Direktyvos Nr. 2009/136/EB preambulėje nurodoma, kad dėl asmens duomenų saugumo pažeidimo, jeigu jis tinkamai ir laiku neišaiškinamas, susijęs abonentas arba asmuo gali patirti didelių ekonominių nuostolių arba socialinės žalos, įskaitant ir su tapatybe susijusį sukčiavimą.

Be to, svarbu paminėti Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymą. Šio įstatymo nuostatos reglamentuoja valdomų ir tvarkomų asmens duomenų saugumą. Įstatymas taikomas tiek valstybiniam, tiek privačiam sektoriui, ir nesvarbu, kuriam iš jų priklauso asmens duomenų valdytojas.

2014 m. gruodžio 11 d. Lietuvos Respublikos Seimas priėmė Kibernetinio saugumo įstatymą. Pabrėžtina, kad įstatymas priimtas beveik neturint koncepcijos, nes senoji koncepcija buvo patvirtinta dar 2006 m. gruodžio 6 d. Lietuvos Respublikos Vyriausybės nutarimu Nr. 1211 ir įstatymo priėmimo metu jau buvo pasenusi ir neaktuali daugeliu atžvilgių. Pavyzdžiui, senojoje koncepcijoje nebuvo analizuotas Nacionalinio kibernetinio saugumo centro reikalingumas, galimos jo funkcijos, teisės ir pareigos.

Šis įstatymas nustato kibernetinio saugumo politiką formuojančias ir įgyvendinančias institucijas, jų kompetenciją, funkcijas, teises ir pareigas, valstybės informacinių išteklių valdytojų ir (arba) tvarkytojų, ypatingos svarbos informacinės infrastruktūros valdytojų, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų ir elektroninės informacijos

prieglobos paslaugų teikėjų pareigas bei atsakomybę ir kibernetinio saugumo užtikrinimo priemones. Įstatymu gana nuosekliai ir aiškiai apibrėžiamos valstybinio sektoriaus institucijų atsakomybės už kibernetinį saugumą ribos. Labai aktualu, kad Kibernetinio saugumo įstatymas taikomas ne tik valstybiniam, bet ir privačiam sektoriui, atskirai numatomos pareigos ne tik elektroninių ryšių, bet ir prieglobos paslaugų teikėjams, o svarbiausia – įstatymas numato ypatingos svarbos informacinę infrastruktūrą, kurios nemažą dalį valdo privatus sektorius.

Vienas iš svarbiausių aspektų, kad įstatymu reglamentuojama ypatingos svarbos informacinė infrastruktūra, kuri yra apibrėžiama kaip „elektroninių ryšių tinklas ar jo dalis, informacinė sistema ar jos dalis, informacinių sistemų grupė ar pramoninių procesų valdymo sistema ar jos dalis, nepaisant to, ar jos valdytojas yra privatus ar viešojo administravimo subjektas, kuriuose įvykęs kibernetinis incidentas gali padaryti didelę žalą nacionaliniam saugumui, šalies ūkiui, valstybės ir visuomenės interesams."

Pagal įstatymą, „ypatingos svarbos informacinės infrastruktūros valdytojai atsako už jų valdomos ypatingos svarbos informacinės infrastruktūros kibernetinį saugumą ir privalo savo lėšomis užtikrinti jų valdomos ypatingos svarbos informacinės infrastruktūros atitiktį Vyriausybės nustatytiems organizaciniams ir techniniams kibernetinio saugumo reikalavimams." Įstatymas tokiems valdytojams nustato nemažai pareigų, susijusių su informacijos teikimu, planų rengimu ir kt.

Be ypatingos svarbos informacinės infrastruktūros valdytojų pareigų, įstatymas detaliai reglamentuoja ir Viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų bei elektroninės informacijos prieglobos paslaugų teikėjų pareigas kibernetinio saugumo srityje.

Atskirai paminėtina, kad įstatyme reglamentuojami policijos įgaliojimai kibernetinio saugumo srityje. Pagal šį įstatymą, „policija teisės aktų nustatyta tvarka vykdydama kibernetinių incidentų, galimai turinčių nusikalstamos veikos požymių, užkardymą ir tyrimą:

1) renka, analizuoja ir apibendrina informaciją apie kibernetinius incidentus, galimai turinčius nusikalstamos veikos požymių;
2) nustato viešojo administravimo subjektams, valdantiems ir (arba) tvarkantiems valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojams, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjams, elektroninės informacijos prieglobos paslaugų teikėjams informacijos, reikalingos kibernetiniams incidentams, galimai turintiems nusikalstamos veikos požymių, užkardyti ir tirti, pateikimo tvarką;

3) turi teisę duoti motyvuotus nurodymus ne ilgiau kaip 48 valandoms be teismo sankcijos, ilgesniam laikui – su apylinkės teismo sankcija, apriboti viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų ir elektroninės informacijos prieglobos paslaugų teikimą paslaugų gavėjui, kai paslaugų gavėjas ar jo naudojama informacinė ir ryšių technologijų įranga galimai dalyvauja nusikalstamoje veikoje, ir (arba) nurodyti viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjui ar elektroninės informacijos prieglobos paslaugų teikėjui taikyti priemones, šalinančias nusikalstamų veikų kibernetinėje erdvėje priežastis. Tokiais atvejais apylinkės teismo pirmininkui ar jo įgaliotam teisėjui pateikiamas teikimas dėl veiksmų teisėtumo ar pagrįstumo patvirtinimo motyvuota nutartimi. Jeigu terminas baigiasi poilsio ar švenčių dieną, teikimas pateikiamas ne vėliau kaip kitą darbo dieną po poilsio ar švenčių dienos. Jeigu teisėjas nepatvirtina nurodytų veiksmų teisėtumo ar pagrįstumo motyvuota nutartimi, nurodymas nedelsiant stabdomas;
4) turi teisę duoti motyvuotus nurodymus viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų ir elektroninės informacijos prieglobos paslaugų teikėjui išsaugoti informaciją, susijusią su jų teikiamomis paslaugomis, iš kurios galima nustatyti naudotos ryšio paslaugos tipą, taikytas technines priemones ir naudojimo laiką, abonento tapatybę, pašto, geografinės padėties adresą, telefono ir bet kokį kitą prieigos numerį, informaciją apie sąskaitas ir atliktus mokėjimus paslaugos sutarties arba susitarimo pagrindu ir kitą informaciją ryšių aparatūros įrengimo vietoje, turimą pagal paslaugos sutartį arba susitarimą, šią informaciją gauti, taip pat teisės aktų nustatyta tvarka, kai yra motyvuota teismo nutartis, gauti paslaugų naudotojo srauto duomenis ir kontroliuoti perduodamos informacijos turinį.“ Šioms nuostatoms detalizuoti priimami įstatymo įgyvendinamieji teisės aktai.

Lietuvos Respublikos kibernetinio saugumo įstatymas reglamentuoja ir vadinamąjį informacinį kibernetinio saugumo tinklą. „Kibernetinio saugumo informacinis tinklas, kurio valdytojas – Nacionalinis kibernetinio saugumo centras, yra saugi informacijos mainų platforma, kurios paskirtis yra dalytis informacija apie galimus ir įvykusius kibernetinius incidentus, taip pat rekomendacijomis, nurodymais, techniniais sprendimais ir kitomis priemonėmis, užtikrinančiomis kibernetinį saugumą ir bendradarbiavimą tarp kibernetinio saugumo informacinio tinklo narių kibernetinio saugumo srityje. Kibernetinio saugumo informaciniu tinklu gali naudotis tik tie subjektai, kurie atitinka Kibernetinio saugumo informacinio tinklo

nuostatuose nurodytus reikalavimus. Kibernetinio saugumo informaciniame tinkle skelbiama aktuali viešojo administravimo subjektų, valdančių ir (arba) tvarkančių valstybės informacinius išteklius, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų, elektroninės informacijos prieglobos paslaugų teikėjų ir ypatingos svarbos informacinės infrastruktūros valdytojų paskirtų asmenų ar padalinių, atsakingų už kibernetinio saugumo organizavimą ir kibernetinių incidentų valdymą, kontaktinė informacija.“ Minėtasis informacinis tinklas 2015 m. pabaigoje dar neveikė.

Galima konstatuoti, kad kibernetinio saugumo įstatymas formaliai užpildo tam tikras buvusias teisinio reguliavimo spragas. Iš trūkumų paminėtina, kad įstatymu nereglamentuojami savireguliacijos ir visuomenės švietimo klausimai. Be to, trūksta detalaus kibernetinės gynybos pagrindų reglamentavimo.

Tam, kad įstatymo nuostatos veiktų visa apimtimi, būtina priimti įstatymo įgyvendinamuosius teisės aktus. Dalis šių teisės aktų 2015 m. pabaigoje jau buvo priimti[73], kitą dalį (Nacionalinį kibernetinių incidentų valdymo planą, Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašą ir kt.) planuojama priimti artimiausiu metu.

6 skirsnis. Strateginiai kibernetinio saugumo dokumentai

Prieš nagrinėjant Lietuvos strateginius dokumentus, paminėtina kai kurių užsienio valstybių praktika.

Neatsižvelgiant į 2013 m. ES komunikato dėl kibernetinio saugumo strategiją, apie 2011 m. ES valstybėse pradėta aktyviau priiminėti nacionalines kibernetinio saugumo strategijas. 2015 m. pabaigoje iš dvidešimt aštuonių ES valstybių nacionalines kibernetinio saugumo strategijas turėjo dvidešimt dvi valstybės, tačiau šešios iš jų – vis dar ne.

Kibernetinio saugumo reguliavimo srityje kaip pažangiausias Europos valstybes galima įvardyti šias: Suomiją, Norvegiją, Čekiją, Jungtinę Karalystę, Vokietiją, Prancūziją. Visos minėtosios valstybės turi patvirtintas valstybines kibernetinio saugumo strategijas, užtikrinančias kibernetinio saugumo reguliavimo tęstinumą. Kuriant šias strategijas buvo perimta ES, EBPO ir kita kibernetinio saugumo reguliavimo patirtis. Minėtųjų

[73] Pvz., Informacijos, reikalingos kibernetiniams incidentams, galimai turintiems nusikalstamos veikos požymių, užkardyti ir tirti, pateikimo, policijos nurodymų vykdymo bei kibernetinių incidentų tyrimo tvarkos aprašas; Techninių kibernetinio saugumo priemonių diegimo ir valdymo valstybės informaciniuose ištekliuose ir ypatingos svarbos informacinėje infra-struktūroje tvarkos aprašas ir kt.

valstybių strategijos nacionaliniu lygiu įtvirtina svarbiausius tolesnės informacinių sistemų plėtros principus; numato, kad būtina kompleksiškai nacionaliniu lygiu reguliuoti kibernetinio saugumo procesus; reguliavimo apimtis – visa nacionalinė kibernetinio saugumo infrastruktūra, apimanti tiek privataus, tiek ir viešojo (taip pat ir valstybinio) sektorių elektroninę informaciją; išskirti du kibernetinio saugumo institucinės sistemos lygiai: politikos formavimo ir kontrolės; aiškiai įvardijamos institucijų kompetencijos kibernetinio saugumo srityje ribos; daug dėmesio skiriama kibernetinio saugumo politikai ir kontrolei koordinuoti; privatus ir valstybinis sektoriai skatinami visapusiškai bendradarbiauti užtikrinant kibernetinį saugumą.

Detaliau galima palyginti šių trijų valstybių kibernetinio saugumo strategijas[74]: Jungtinės Karalystės, Vokietijos ir Prancūzijos.

Jungtinės Karalystės kibernetinio saugumo strategija „Jungtinės Karalystės apsauga ir palaikymas skaitmeniniame pasaulyje“ patvirtinta 2011 m. lapkritį. Joje nustatyta kibernetinio saugumo rizika 2015 metams: iš dinamiškos, tvirtos ir saugios elektroninės erdvės gauti didžiulę ekonominę ir socialinę vertę, kur šalies veiksmai, valdomi esminių laisvės vertybių, teisingumo, skaidrumo ir įstatymų galios, didins gerovę, nacionalinį saugumą ir formuos tvirtą visuomenę. Siekdama iki numatyto termino įgyvendinti šią viziją, Jungtinė Karalystė kelia šiuos keturis tikslus:

1. Kovoti su elektroniniais nusikaltimais Jungtinėje Karalystėje ir tapti viena iš saugiausių pasaulyje verslo elektroninėje erdvėje plėtros šalių.
2. Būti atsparesnei kibernetiniams išpuoliams ir gebėti geriau ginti savo interesus elektroninėje erdvėje.
3. Jungtinė Karalystė padeda formuoti atvirą, stabilią ir energingą elektroninę erdvę, kuria šalies visuomenė galės saugiai naudotis, tai padėtų palaikyti atviras visuomenes.

Jungtinė Karalystė turi puikių žinių, įgūdžių ir gebėjimų, leidžiančių įgyvendinti visus išsikeltus elektroninės erdvės saugumo užtikrinimo tikslus.

Vokietijos kibernetinio saugumo strategija patvirtinta 2011 m. vasarį. Joje nenustatytos datos, todėl galima daryti išvadą, kad minėtoji strategija bus aktuali iki kitos strategijos patvirtinimo arba iki esamos atnaujinimo. Vokietijos strategijoje išskiriami šie svarbiausi e. erdvės saugumo strateginiai tikslai ir priemonės saugumui užtikrinti:

1) ypatingos svarbos informacinių struktūrų apsauga;
2) saugios informacinės technologijos (toliau – IT) Vokietijoje;

[74] Ekspertų vertinimu, šios valstybės pasirinktos kaip labiausiai pažengusios kibernetinio saugumo ir jo teisinio reguliavimo užtikrinimo srityje.

3) IT apsaugos stiprinimas viešojo valdymo sektoriuje;
4) Nacionalinis reagavimo į kibernetines nelaimes centras;
5) Nacionalinė kibernetinės erdvės apsaugos taryba;
6) efektyvi nusikaltimų kontrolė ir kibernetinėje erdvėje;
7) efektyvūs koordinuoti veiksmai siekiant užtikrinti kibernetinį saugumą Europoje ir pasaulyje;
8) patikimų ir vertų pasitikėjimo informacinių technologijų naudojimas;
9) personalo plėtra federalinėje valdžioje;
10) tinkami reagavimo į kibernetinius išpuolius įrankiai.

Prancūzijos informacinių sistemų gynybos ir saugumo strategija priimta 2011 m. vasarį, nors pačioje Strategijoje jokios konkrečios datos neminimos. Prancūzijos strategijoje nurodyti šie svarbiausi tikslai:

1) įgyti pasaulinę galią kibernetinės gynybos srityje;
2) apsaugoti Prancūzijos gebėjimą priimti sprendimus saugant informaciją, susijusią su jos suverenitetu;
3) stiprinti kibernetinį svarbiausių nacionalinių infrastruktūrų saugumą;
4) užtikrinti elektroninės erdvės saugumą.

Apibendrinus minėtųjų valstybių kibernetinio saugumo strategijų nuostatas, galima matyti, kad visos valstybės kelia šiuos svarbiausius klausimus:

– glaudaus bendradarbiavimo tiek nacionaliniu, tiek tarptautiniu lygiu bei informacijos keitimosi;
– kritinės informacinės infrastruktūros apsaugos;
– visuomenės informavimo;
– IT apsaugos stiprinimo viešajame sektoriuje;
– saugių IT naudojimo ir kt.

Šios strategijos ir jų nuostatos galėtų būti puikus pavyzdys kitoms valstybėms kuriant kibernetinio saugumo strategijas.

Pabrėžtina, jog, be šių strategijų, kurios buvo priimtos beveik vienu metu, Vokietijoje 2013 m. jau yra parengtos ir siūlomos priimti teisinės nuostatos dėl kibernetinio saugumo.

Reikėtų atkreipti dėmesį, kad Jungtinės Karalystės kibernetinio saugumo strategijos apžvalgoje buvo išnagrinėtos ir palygintos devynių valstybių[75] kibernetinio saugumo strategijos. Šios dar buvo lyginamos su JK kibernetinio saugumo strategija. Palyginimo išvadose pateikti rezultatai

[75] Australija, Kinija, Estija, Prancūzija, Vokietija, Indija, Japonija, Rusija ir JAV.

rodo, kad JK kibernetinio saugumo strategija išsiskiria savo „svoriu“, kurio jai suteikė JK vyriausybė, turėdama tikslą sudaryti saugias sąlygas elektroninei komercijai ir kitiems svarbiems santykiams plėtoti. Keletas kitų rezultatų:

- keturios valstybės, kaip ir JK, kibernetinio saugumo programose yra išsikėlusios tikslą kovoti su elektroniniais nusikaltimais;
- visos tirtosios valstybės turi tikslą gerinti atsparumą kibernetinėms atakoms ir užtikrinti savo nacionalinį saugumą;
- tik viena valstybė, kaip ir JK, palaiko atviros visuomenės idėją;
- visos valstybės kelia tikslą plėtoti kibernetinio saugumo žinias ir pajėgumus užtikrinant kibernetinį saugumą.

Be to, paminėtina, kad 2014–2015 m. atlikus naujų tyrimų buvo palygintos daugumos ES valstybių nacionalinės kibernetinio saugumo strategijos. Tyrimus atliko ENISA 2014 m.[76], o BSA – 2015 m.[77]. Šie tyrimai atskleidė bendrus strategijų panašumus ir skirtumus. Tyrimų rezultatai prieinami viešai.

1. IT saugos strategija ir Elektroninės informacijos saugos valstybės institucijų informacinėse sistemose strategija

Atitinkamos srities strateginio teisinio reguliavimo poreikis Lietuvoje atsirado dar 2001 m., kai Lietuvos Respublikos Vyriausybė 2001 m. gruodžio 22 d. priėmė nutarimą Nr. 1625 „Dėl Informacijos technologijų saugos valstybinės strategijos ir jos įgyvendinimo plano patvirtinimo“ (toliau – 2001 m. strategija), šiuo nutarimu buvo patvirtinta pirmoji nacionalinė informacinių technologijų saugos strategija, tačiau tuo metu „kibernetinio saugumo“ terminas dar nebuvo vartojamas. Svarbiausias šios strategijos tikslas – reglamentuoti tik valstybinių institucijų ir įstaigų saugumą, o informacinių privataus sektoriaus technologijų sauga nebuvo reglamentuojama. Turint omenyje, kad dažniausiai 85–90 proc. kibernetinės infrastruktūros valdoma privataus sektoriaus, ir žiūrint iš dabartinio teisinio reguliavimo pozicijų galima teigti, kad tuo metu buvo padaryta didelė klaida, nesiekiant reguliuoti privataus sektoriaus IT saugos. Ši teisinio reguliavimo spraga Lietuvoje buvo ištaisyta, tačiau gerokai vėliau.

2006 m. Lietuvos elektroninės informacijos saugos valstybės institucijų informacinėse sistemose valstybinė strategija iki 2008 m. (toliau – Valstybinė strategija) ir jos įgyvendinimo priemonių planas Lietuvos

[76] https:</www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/an-evaluation-framework-for-cyber-security-strategies-1>.

[77] http:<cybersecurity.bsa.org/index.html>.

Respublikos Vyriausybės nutarimu Nr. 601 buvo patvirtinti 2006 m. birželio 19 dieną. Jau iš strategijos pavadinimo tapo aišku, kad Valstybinė strategija buvo skirta išimtinai valstybės institucijų sektoriui. Jau pats pavadinimas rodo, kad vartojamas kitas terminas – „elektroninės informacijos sauga".

Svarbiausi Valstybinės strategijos iškelti tikslai buvo tokie:

- Tobulinti elektroninės informacijos saugos koordinavimą ir priežiūrą. Šiam tikslui pasiekti numatyti tokie uždaviniai: užtikrinti elektroninės informacijos saugos koordinavimą; sukurti efektyvią kovos su nusikalstamomis veikomis, vykdomomis elektroninės informacijos perdavimo aplinkoje, sistemą.
- Teisės aktais reguliuoti elektroninės informacijos saugą. Šiam tikslui pasiekti numatyti tokie uždaviniai: priimti teisės aktus, reguliuojančius elektroninės informacijos saugą; elektroninės informacijos saugą reglamentuoti saugos dokumentais.
- Kelti elektroninės informacijos saugos kultūrą. Šiam tikslui pasiekti numatyti tokie uždaviniai: valstybės tarnautojus ir darbuotojus, dirbančius pagal darbo sutartis, mokyti elektroninės informacijos saugos; skatinti elektroninės informacijos saugos svarbos suvokimą.
- Tobulinti elektroninės informacijos perdavimo infrastruktūros saugą. Šiam tikslui pasiekti numatytas uždavinys – tobulinti Saugiame valstybiniame duomenų perdavimo tinkle saugomos ir perduodamos elektroninės informacijos saugą.
- Skatinti elektroninės informacijos saugos užtikrinimo projektų įgyvendinimą. Šiam tikslui pasiekti numatytas uždavinys – įgyvendinant elektroninės informacijos saugos projektus, naudotis privataus sektoriaus patirtimi.

Šioje strategijoje, kaip ir 2001 m., buvo paskirtos institucijos, atsakingos už šios strategijos įgyvendinimą. Palyginti su ankstesniąja strategija, institucinis modelis taikomas gerokai plačiau, paskirtos septynios institucijos, atsakingos už 2006 m. strategijoje numatytų priemonių įgyvendinimą, tačiau ir vėl – tik valstybiniame sektoriuje. Be to, nebuvo aiškiai atskirtos institucijų funkcijos, ypač politikos formavimo ir įgyvendinimo kontekste – atsakingosios institucijos buvo nurodytos tik kaip atsakingi priemonių plano vykdytojai. Nebuvo įvardyta ir pagrindinė Lietuvos elektroninės informacijos saugos institucija.

Reikėtų pabrėžti, kad neatsižvelgiant į šioje strategijoje užsibrėžtus tikslus, uždavinių, skirtų šiems tikslams pasiekti, formuluotės buvo tik deklaratyvios, abstrakčios ir nekonkrečios.

Minėtoji Valstybinė strategija nustojo galioti 2008 m. ir nuo to laiko Lietuvoje nebuvo jokios galiojančios elektroninės informacijos saugos strategijos ar programos.

2. Lietuvos kibernetinio saugumo programa

Lietuvos Respublikos Vyriausybės 2011 m. birželio 29 d. nutarimu Nr. 796 „Dėl elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 m. programos patvirtinimo“ buvo patvirtinta Kibernetinio saugumo plėtros programa 2011–2019 m. (toliau – Kibernetinio saugumo programa). Atkreiptinas dėmesys, kad Kibernetinio saugumo programa buvo patvirtinta dar 2011 m., kai Europos Komisija net nebuvo paskelbusi konsultacijos dėl ES kibernetinio saugumo strategijos, todėl ši programa formaliai nebuvo derinama su ES kibernetinio saugumo strategija.

Kibernetinio saugumo programa parengta atsižvelgiant į tai, kad valstybės ir visuomenės gyvenime vis didesnę reikšmę įgyja informacinėmis ir ryšių technologijomis tvarkoma bei perduodama elektroninė informacija, o atsiradusios didesnės elektroninės informacijos tvarkymo galimybės paskatino nacionalinių ir globalių informacinių visuomenių kūrimąsi ir sudarė sąlygas toliau modernizuoti šalių ūkius bei efektyviau valdyti valstybę, tačiau tuo pat metu į elektroninę erdvę perkeliama vis daugiau informacijos, sparčiai automatizuojami įvairūs šalies valdymo ir ūkio veiklos procesai, o globali kibernetinė erdvė ir joje teikiamos viešosios paslaugos tapo patraukliu atskirų asmenų, nusikalstamų grupuočių, politinių jėgų ir kitų subjektų taikiniu.

Programos paskirtis – nustatyti elektroninės informacijos saugos (kibernetinio saugumo) plėtros tikslus ir uždavinius, kad būtų užtikrintas elektroninės informacijos ir kibernetinėje erdvėje teikiamų paslaugų konfidencialumas, vientisumas ir prieinamumas, elektroninių ryšių tinklų, informacinių sistemų ir ypatingos svarbos informacinės infrastruktūros apsauga nuo incidentų ir kibernetinių atakų, asmens duomenų ir privatumo apsauga, be to, nustatyti uždavinius, kurių įgyvendinimas leistų užtikrinti bendrą kibernetinės erdvės ir joje veiklą vykdančių subjektų saugumą.

Strateginis programos tikslas – plėtoti elektroninės informacijos saugą Lietuvoje, užtikrinti kibernetinį saugumą ir pasiekti, kad 2019 m. teisės aktų nustatytus elektroninės informacijos saugos (kibernetinio saugumo) reikalavimus atitinkančių valstybės informacinių išteklių dalis pasiektų 98 proc. visų valstybės informacinių išteklių, vidutinis ypatingos svarbos informacinės infrastruktūros incidentų likvidavimo laikas sumažėtų iki 0,5 val., o saugiai kibernetinėje erdvėje besijaučiančių Lietuvos gyventojų dalis pasiektų 60 procentų.

Nustatyti šie Kibernetinio saugumo programos įgyvendinimo tikslai:

1. Pasiekti, kad būtų užtikrintas valstybės informacinių išteklių saugumas.

Kaip nurodoma programoje, šio tikslo siekiama, nes, išskyrus valstybinį sektorių (Lietuvos Respublikos Vyriausybei atskaitingose įstaigose ir institucijose), nėra sukurta elektroninės informacijos saugos valdymo koordinavimo sistema. Vidaus reikalų ministerijai trūksta įgaliojimų tinkamai vykdyti elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo kontrolę ir koordinavimą, be to, valdymo ir priežiūros struktūra valstybės ir valstybės institucijų mastu nėra hierarchinė, trūksta Lietuvos viešojo ir privataus sektorių subjektų bendradarbiavimo, tai neleidžia veiksmingai planuoti elektroninės informacijos saugos (kibernetinio saugumo) srities plėtros; informacinių technologijų esami ir nuolat aptinkami nauji pažeidžiamumai, jų laiku nepašalinus, sudaro sąlygas trikdyti informacinių išteklių ir ypatingos svarbos informacinės infrastruktūros objektų funkcionavimą, o šių pažeidžiamumų aptikimo ir šalinimo veiksmingumas didėja centralizuojant šią veiklą. Atitiktis keliamiems elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams užtikrina informacinių išteklių saugos valdymą pagal tarptautinių standartų reikalavimus ir gerosios praktikos pavyzdžius, tačiau Lietuvoje nesuformuota veiksminga atitikties valdymo struktūra; organizacijos informacinės brandos modelis leidžia informacinių išteklių valdytojams geriau suvokti informacinių išteklių saugos poreikį ir veiksmingiau valdyti informacinių išteklių saugą. Įvairios valstybės ir visuomenės veiklos sritys nevienodai priklausomos nuo informacinių išteklių ir paslaugų naudojimo, todėl, siekiant veiksmingai paskirstyti lėšas, būtina telkti pastangas ir informacinius išteklius tose srityse, kur ši priklausomybė didesnė; nusikalstamų veikų kibernetinėje erdvėje sparčiai daugėja, o dideli incidentai net gali sukelti nacionalinio masto krizę.

Interneto ir kitų informacinės infrastruktūros paslaugų teikėjų teikiamos paslaugos dažnai neužtikrina paslaugų naudotojų saugos. Ekonominiu sunkmečiu elektroninės informacijos saugai (kibernetiniam saugumui) skiriama nepakankamai dėmesio ir informacinių išteklių, o taikant kolektyvinės saugos principą būtų veiksmingiau naudojami informaciniai ištekliai; nėra sukurtas informacinių išteklių ir infrastruktūros rezervas, skirtas ypatingos svarbos infrastruktūros ir informacinių išteklių veikimui palaikyti kritiniais atvejais. Patikimas tapatybės nustatymas sumažina didelės dalies grėsmių, susijusių su kibernetine erdve, keliamą riziką ir skatina vartotojų pasitikėjimą internetu.

Saugia kibernetine erdve (elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimu) yra suinteresuoti visi subjektai, kurių veikla

susijusi su kibernetinėje erdvėje teikiamomis paslaugomis (valstybės institucijos, privatūs ūkio subjektai, akademinė bendruomenė ir kiti). Bendradarbiaujant vykdomi elektroninės informacijos saugos (kibernetinio saugumo) projektai leidžia užtikrinti visų dalyvaujančių šalių interesų apsaugą.

Kibernetinė erdvė yra globali, neturinti nacionalinių ribų, taigi įvairios grėsmės joje plinta labai sparčiai. ES ir *NATO* skiria daug dėmesio e. informacijos ir ypatingos svarbos informacinės infrastruktūros saugai. Kolektyvinės apsaugos principu tikslinga vadovautis ne tik nacionaliniu, bet ir tarptautiniu lygiu. Kompetentingų specialistų bendradarbiavimas, keitimasis turima informacija ir patirtimi yra būtina veiksmingo išankstinio perspėjimo ir prevencinės veiklos sąlyga.

2. *Užtikrinti veiksmingą ypatingos svarbos informacinės infrastruktūros funkcionavimą*.

Šio tikslo siekiama, nes ypatingos svarbos informacinės infrastruktūros saugumas užtikrinamas tik žinybiniu lygmeniu, nesuformuota koordinavimo struktūra, neišanalizuoti šios infrastruktūros objektų tarpusavio ryšiai ir sutrikdymo poveikis nacionaliniu mastu, nevykdomas veiklos tęstinumo planavimas. Bandymų įsilaužti būdas (angl. *penetration test*) yra objektyviausias siekiant įsitikinti, ar tinkamai veikia saugos sistema, tačiau jo taikymas nereglamentuotas, tiesiog nėra tokių bandymų praktikos. Veiksminga stebėsenos sistema sudaro sąlygas užtikrinti incidentų prevenciją.

3. *Siekti užtikrinti Lietuvos gyventojų ir šalyje esančių asmenų saugumą kibernetinėje erdvėje*.

Šio tikslo siekiama, nes ne visi elektroninės informacijos vartotojai rūpinasi elektroninės informacijos sauga (kibernetiniu saugumu), šiuo metu stinga ir ateityje, tikėtina, vis labiau stigs kvalifikuotų elektroninės informacijos saugos specialistų. Bazinės elektroninės informacijos saugos (kibernetinio saugumo) žinios ir įrankiai leidžia jos vartotojams išvengti daugelio grėsmių kibernetinėje erdvėje.

Kibernetinės erdvės saugumui užtikrinti būtina nenutrūkstamai veikianti ir tinkamai valdoma sistema, apimanti visą incidentų gyvavimo ciklą: išankstinio perspėjimo, prevencijos, aptikimo, likvidavimo ir tyrimo fazes. Siekiant kovoti su kenksminga programine įranga nuotoliniu būdu valdomų kompiuterių tinklais ar kitais kenkiamosios veiklos kibernetinėje erdvėje būdais, veiksminga blokuoti interneto prieigą kenkiamąją veiklą vykdantiems asmenims ir (ar) įrenginiams. Šiuo metu visuomenėje yra susiformavęs stereotipas dėl nebaudžiamumo už neteisėtus veiksmus kibernetinėje erdvėje, todėl svarbu šį stereotipą kuo greičiau paneigti.

Kibernetinės atakos, kurių šaltinis yra užsienyje, gali ir turi būti stabdomos ties virtualiu Lietuvos kibernetinės erdvės perimetru, siekiant

išvengti jų poveikio šalies vidaus elektroninių ryšių tinklams. Lietuvos interneto srauto mainų (*ISM*) mazgas yra natūraliai susiformavęs subjektas, į kurį patogu ir veiksminga telkti Lietuvos kibernetinės erdvės (ir virtualaus perimetro) apsaugos pajėgumus.

Šiuo metu vyrauja kibernetinėje erdvėje teikiamų paslaugų unifikavimo ir centralizavimo tendencija, siekiant įgyvendinti vieno langelio principą; šia tendencija tikslinga naudotis ir užtikrinant šių paslaugų saugą. Vartotojų pasitikėjimas kibernetinėje erdvėje teikiamomis paslaugomis yra vienas svarbiausių šių paslaugų populiarumo ir tolesnės plėtros veiksnių.

Kiekvienam tikslui keliami ir atitinkami uždaviniai. Visa tai įmanoma pasiekti tik turint gana gerai parengtų specialistų, kurių įgytas išsilavinimas būtų glaudžiai susijęs su informacinių technologijų ir informacijos saugumo vadyba. Lietuvos Respublikos Vyriausybės nutarime yra pabrėžiama, kad jau šiuo metu yra jaučiamas kvalifikuotų informacijos saugos specialistų trūkumas, ir numatoma, kad ateityje tas trūkumas tik dar labiau didės. Tokių specialistų stygius yra akcentuojamas ir ES dokumentuose, ir nurodant bei aprašant programos tikslus.

Paminėtina, kad kibernetinio saugumo programos vertinimo kriterijai ir jų reikšmės pateikiami šios programos priede. Kibernetinio saugumo programos įgyvendinimą koordinuoja Lietuvos Respublikos vidaus reikalų ministerija, o už šios programos tikslų ir uždavinių įgyvendinimą atsako priede nurodytos įstaigos bei institucijos.

Analizuojant Lietuvos kibernetinio saugumo programą ES kibernetinio saugumo strategijos ir direktyvos bei kitų nagrinėtųjų užsienio valstybių kibernetinio saugumo strategijų kontekste, pabrėžtina, kad programa neužtikrina visapusiškos Lietuvos kibernetinio saugumo strategijos ir kol kas neatitinka visų 2013 m. ES kibernetinio saugumo strategijoje nustatytų kibernetinio saugumo prioritetų bei neužtikrina kitų valstybių kibernetinio saugumo strategijose numatytų kai kurių svarbiausių tikslų ir uždavinių:

1) nenumatytos valstybės ir privataus sektoriaus bendradarbiavimo kibernetinio saugumo srityje priemonės. Turint omenyje, kad šiuo metu dauguma infrastruktūros priklauso privačiam sektoriui, toks bendradarbiavimas yra būtinas;
2) per mažai dėmesio skiriama e. nusikaltimams ir jų kiekiui mažinti. Kaip rodo tyrimai, šių nusikaltimų latentiškumas yra didžiulis. E. nusikaltimai yra kibernetinių atakų pavadinimas baudžiamosios teisės kontekste, todėl šiai nusikaltimų rūšiai programoje turėtų būti skiriamas deramas dėmesys;

3) nenumatyta išsami ir sisteminė kibernetinės gynybos politika. Šiuo metu Lietuvoje nėra nustatyta, kokių veiksmų turėtų būti imamasi kilus kibernetinei grėsmei, kokios yra atskirų „žaidėjų“ funkcijos ir atsakomybė, kam teikiami prioritetai saugant kritinę infrastruktūrą nuo kibernetinių atakų, kokie institucijų ir privataus sektoriaus veiksmai kibernetinių atakų atveju. Šį trūkumą būtina kuo skubiau šalinti;
4) neaptariami instituciniai klausimai, nedetalizuojamos atitinkamų institucijų funkcijos ir atsakomybė kibernetinio saugumo srityje;
5) nenumatyti tikslai ir uždaviniai, susiję su visuomenės informavimu ir švietimu, nors tai ir būtina šiuolaikinei informacinei visuomenei, nes kibernetinio saugumo grėsmė dažniausiai susijusi su galutiniais interneto vartotojais;
6) kai kurios užsibrėžtos priemonės yra sunkiai įgyvendinamos arba nepamatuojamos, o tam tikrus indikatorius gali būti sunku įvertinti.

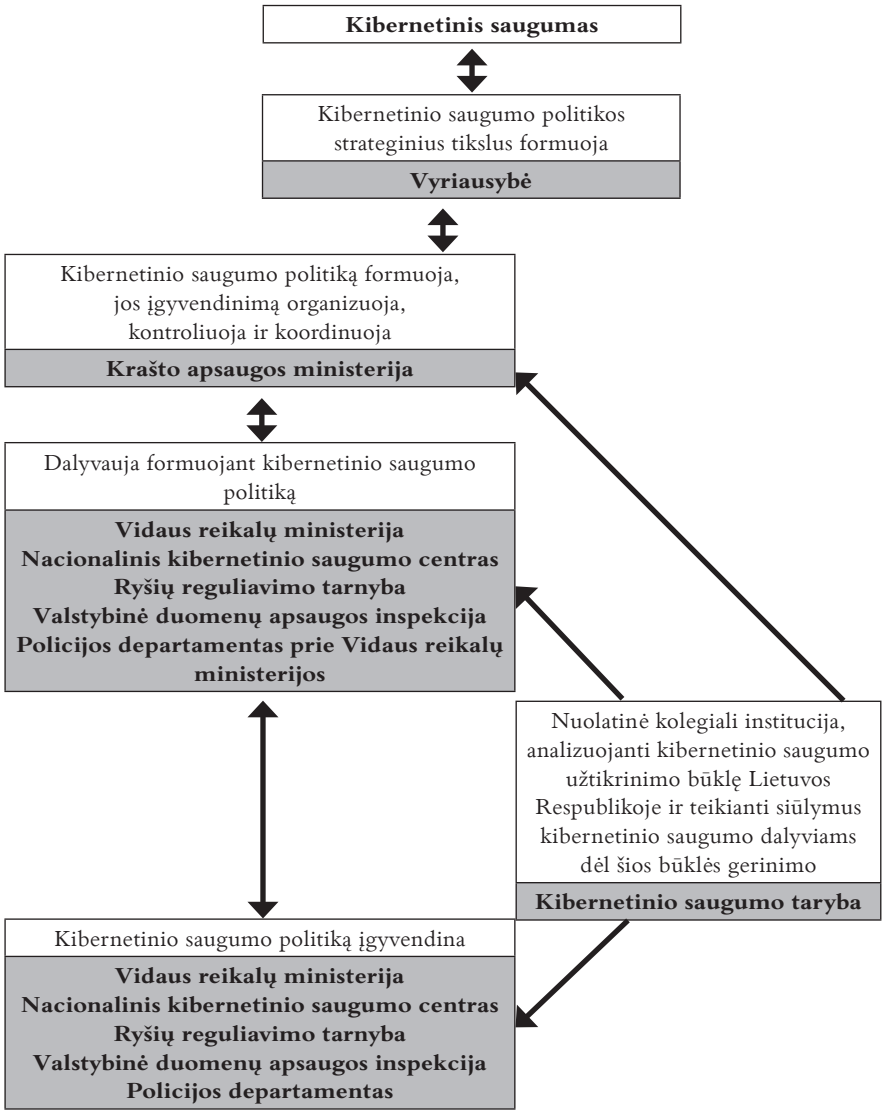
Bendrai pabrėžtina, kad strategijoje iškelti tikslai ir uždaviniai nelabai konkretūs (abstraktūs), ne visais atvejais atspindi elektroninės erdvės keliamus pavojus ir riziką. Tikslams ir uždaviniams pasiekti nėra sukurta kibernetinio saugumo valdymo koordinavimo sistema ir nenumatytas konkrečių lėšų skyrimas.

Nors ir *ENISA*, ir kitos organizacijos savo tinklalapiuose nurodo, kad Lietuva turi patvirtintą kibernetinio saugumo strategiją, vis dėlto kyla klausimas, ar ši programa laikytina visaverte kibernetinio saugumo strategija. Ji neatitinka kompleksinės Lietuvos kibernetinio saugumo vizijos su tipiniais tokios vizijos elementais. Programoje nėra numatytų principų, prioritetų ir kitų elementų. Manytina, kad Lietuvai reikia visaapimančios ir visavertės kibernetinio saugumo strategijos, orientuotos į šiuolaikines grėsmes ir kibernetinio saugumo aktualijas.

7 skirsnis. Instituciniai kibernetinio saugumo Lietuvoje aspektai

Kibernetinio saugumo įstatymo 4 str. 1 d. yra numatyta, kad kibernetinio saugumo politikos strateginius tikslus ir jiems pasiekti būtinas priemones nustato Lietuvos Respublikos Vyriausybė. Taigi galima teigti, kad Vyriausybė yra pagrindinė institucija, formuojanti strateginę kibernetinio saugumo politiką.

Kibernetinio saugumo įstatymo 4 str. 2 d. numatytos institucijos, atsakingos už kibernetinį saugumą (žr. 10 pav.):



10 pav. Institucijos, atsakingos už kibernetinį saugumą

Kaip matyti iš pateiktos schemos, šioje įstatymo dalyje yra aiškiai išskirtos valstybės institucijos, atsakingos už kibernetinį saugumą Lietuvoje bei šio įstatymo nuostatų įgyvendinimą, ir jų vaidmuo kibernetinio saugumo srityje, tačiau tokių institucijų yra gana daug.

Kibernetinio saugumo politiką formuoja, jos įgyvendinimą organizuoja, kontroliuoja ir koordinuoja Lietuvos Respublikos krašto apsaugos

ministerija. Lietuvos Respublikos vidaus reikalų ministerija, Nacionalinis kibernetinio saugumo centras, Lietuvos Respublikos ryšių reguliavimo tarnyba, Valstybinė duomenų apsaugos inspekcija ir Policijos departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos formuojant kibernetinio saugumo politiką dalyvauja tiek, kiek šiuo įstatymu priskirtoms funkcijoms atlikti reikia nustatyti viešojo administravimo subjektų, valdančių valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojų, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų ir elektroninės informacijos prieglobos paslaugų teikėjų veiklos teisinį reguliavimą.

Įgyvendinant Kibernetinio saugumo įstatymo nuostatas, 2015 m. sausio 1 d. buvo įsteigtas Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos, kuriam pavesta analizuoti nacionalinę kibernetinio saugumo padėtį, rengti kibernetinio saugumo būklės ataskaitas, teikti konsultacijas ir rekomendacijas kibernetinio saugumo klausimais bei kibernetinių incidentų metu užtikrinti valstybės informacinių išteklių kibernetinį saugumą. Tai yra svarbiausia Lietuvos kibernetinio saugumo institucija.

Pagal Kibernetinio saugumo įstatymą, Nacionalinis kibernetinio saugumo centras, pagal kompetenciją įgyvendindamas kibernetinio saugumo politiką ir vykdydamas valstybės informacinių išteklių ir ypatingos svarbos informacinių infrastruktūrų kibernetinių incidentų valdymo padalinio veiklą:

1) pagal savo kompetenciją rengia ir teikia pasiūlymus krašto apsaugos ministrui dėl organizacinių ir techninių kibernetinio saugumo reikalavimų valstybės informaciniams ištekliams ir ypatingos svarbos informacinei infrastruktūrai;
2) atlieka valstybės informacinių išteklių ir ypatingos svarbos informacinės infrastruktūros atitikties organizaciniams ir techniniams kibernetinio saugumo reikalavimams stebėseną;
3) rengia tipinius kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planus;
4) teikia konsultacijas ir rekomendacijas valstybės informacinių išteklių valdytojams ir ypatingos svarbos infrastruktūros valdytojams kibernetinio saugumo klausimais;
5) analizuoja nacionalinę kibernetinio saugumo situaciją ir rengia nacionalinio kibernetinio saugumo būklės ataskaitas;
6) ne rečiau kaip kartą per metus rengia nacionalinio kibernetinio saugumo būklės ataskaitas ir jas teikia krašto apsaugos ministrui;

7) rengia ypatingos svarbos informacinių infrastruktūrų kibernetinės gynybos planus;
8) valdo kibernetinio saugumo informacinį tinklą;
9) vykdo informacijos sklaidą kibernetinio saugumo klausimais;
10) laikydamasis krašto apsaugos ministro nustatytos tvarkos, reaguoja į kibernetinius incidentus valstybės informaciniuose ištekliuose ir ypatingos svarbos informacinėse infrastruktūrose;
11) atlieka kitas Lietuvos Respublikos teisės aktuose nustatytas funkcijas kibernetinio saugumo užtikrinimo srityje."

2015 m. įsteigta Kibernetinio saugumo taryba, kuri yra nuolatinė patariamoji kolegiali institucija. Tarybos funkcijos yra šios: analizuoti kibernetinio saugumo užtikrinimo būklę, teikti siūlymus dėl šios būklės gerinimo valstybės institucijoms, formuojančioms ir įgyvendinančioms kibernetinio saugumo politiką, patarinėti valstybės informacinius išteklius tvarkantiems subjektams, viešųjų ryšių tinklų, elektroninių paslaugų teikėjams, šios srities verslo įmonėms, mokslo ir studijų institucijoms. Pagal Kibernetinio saugumo įstatymą, Kibernetinio saugumo taryba yra sudaroma iš kibernetinio saugumo politiką formuojančių ir įgyvendinančių valstybės institucijų, informacinių technologijų srityje veiklą vykdančių verslo subjektų atstovų, mokslo ir studijų institucijų atstovų, ypatingos svarbos informacinės infrastruktūros valdytojų, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų, elektroninės informacijos prieglobos paslaugų teikėjų atstovų, o prireikus ir iš kitų asmenų. Kibernetinio saugumo tarybai vadovauja Krašto apsaugos ministerijos atstovas.

Atskirai paminėtina viena iš labiausiai savo veikla su kibernetiniu saugumu susijusių institucijų – Lietuvos Respublikos ryšių reguliavimo tarnyba (toliau – Tarnyba).

2005 m. kovo 24 d. Lietuvos Respublikos Vyriausybės nutarimas Nr. 315 „Dėl Lietuvos Respublikos Vyriausybės 2004–2008 m. programos įgyvendinimo priemonių patvirtinimo" numatė Lietuvos Respublikos ryšių reguliavimo tarnyboje iki 2006 m. pabaigos įsteigti kompiuterinių incidentų tyrimo padalinį *CERT*[78]. 2008 m. liepos 9 d. Lietuvos Respublikos Vyriausybės nutarimu Nr. 678 Lietuvos Respublikos ryšių reguliavimo tarnybos nuostatai, patvirtinti Lietuvos Respublikos Vyriausybės 2004 m. rugpjūčio 19 d. nutarimu Nr. 1029 „Dėl Lietuvos Respublikos ryšių

[78] CERT (angl. *Computer Emergency Response Team)*, arba CSIRT (angl. *Computer Security Incident Response Team)* – tai tinklų ir informacijos saugumo incidentų tyrimų grupė, kurios svarbiausias tikslas – operatyviai reaguoti į saugumo incidentus elektroninių ryšių tinkluose ir koordinuoti veiksmus juos šalinant, ypač kai kyla potenciali tinklo funkcionalumo ar duomenų saugumo rizika.

reguliavimo tarnybos nuostatų patvirtinimo“ (Žin., 2004, Nr. 131-4734), papildyti nauju 8.43 punktu dėl *CERT* veiklos: „8.43. Vykdo nacionalinio elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinio CERT veiklą.“ Be šių nuostatų dėl *CERT*, Tarnybos nuostatose dar nurodyta, jog ji dalyvauja Europos tinklų ir informacijos saugumo agentūros, įkurtos 2004 m. kovo 10 d. Europos Parlamento ir Tarybos reglamentu Nr. 460/2004 dėl Europos tinklų ir informacijos saugumo agentūros įkūrimo, veikloje.

Taigi Lietuvos nacionalinis *CERT* šiuo metu įeina į Lietuvos Respublikos ryšių reguliavimo tarnybos sudėtį. Vykdant nacionalinio *CERT* padalinio veiklą, svarbiausi Tarnybos uždaviniai yra šie:

- koordinuoti *CERT* padalinių ir teikėjų veiksmus Lietuvos Respublikoje stabdant incidentų plitimą ir šalinant jų padarinius iš viešųjų ryšių tinklų ir informacinių sistemų;
- pagal kompetenciją atlikti incidentų tyrimus viešuosiuose ryšių tinkluose ir informacinėse sistemose;
- vykdyti incidentų prevenciją viešuosiuose ryšių tinkluose ir informacinėse sistemose;
- pagal kompetenciją atstovauti Lietuvos Respublikai palaikant santykius su užsienio valstybių incidentų tyrimo institucijomis ir *CERT* padaliniais.

CERT-RRT savo veiklą pradėjo 2006 m. spalio 2 dieną. Lietuvos Respublikos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys *CERT-LT*) atlieka elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimus, veiksmų koordinavimą sprendžiant incidentus, rengia rekomendacijas apie grėsmes, organizuoja seminarus.

Vieni iš pagrindinių *CERT-RRT* dokumentų – statistinės ataskaitos, kurios prieinamos tinklalapyje *www.cert.lt*. Remiantis 2015 m. III ketvirčio ataskaita, *CERT-LT* per 2015 m. III ketvirtį ištyrė 9 708 incidentus pagal iš Lietuvos elektroninių ryšių paslaugų teikėjų, užsienio *CERT* tarnybų, atliekančių tarptautinius incidentų tyrimus, ir iš Lietuvos interneto naudotojų gautus pranešimus. „Kone pusė visų incidentų yra susijusi su kompiuterių naudotojų tinklo įrenginiais, turinčiais pavojingų saugumo spragų – 4 490. Antrojoje vietoje pagal incidentų skaičių yra kenkimo programinė įranga (virusai, Trojos arkliai ir pan.) – 2 612 atvejų. Taip pat per nurodytą laikotarpį buvo užfiksuoti 1 686 informacinių sistemų užvaldymai. *CERT-LT* tyrimų duomenys rodo, kad dauguma aptiktų kompiuterių už-

valdymo atvejų buvo atlikti automatizuotomis priemonėmis ir susiję su pažeidžiama įranga internete.“

CERT-LT registruoja ir skelbia informaciją apie botnetuose aptiktų kompiuterių aktyvumą interneto svetainėje *https://www.cert.lt/botnet*. Vartotojas, kilus įtarimui, kad jo kompiuteris gali būti įtrauktas į tokio tinklo veiklą, gali pasitikrinti *CERT-LT* tinklalapyje *https://www.cert.lt/tikrinti*, ar kompiuterio interneto protokolo (IP) adresas nėra užfiksuotas *CERT-LT* duomenų bazėje kaip dalyvaujantis vykdant kenkiamąją veiklą. Tinklalapyje *https://www.cert.lt/tikrinti* įdiegta papildoma funkcija, leidžianti tiksliai informuoti interneto vartotojus apie pastebėtą žalingą veiklą, vykdomą jų kompiuteriais, kurie naudoja ne tik statinius, bet ir dinaminius kompiuterio interneto protokolo (*IP*) adresus.

8 skirsnis. Elektroninės informacijos saugos reguliavimas valstybiniame sektoriuje

Galima sakyti, kad pirmą kartą šiuo elektroninės informacijos saugos klausimu valstybiniame sektoriuje rimtai buvo susidomėta tik 2000 m., kai buvo atliktas pirmas valstybės informacinės infrastruktūros padėties įvertinimas. Viena iš pagrindinių šio vertinimo sričių buvo informacijos saugos suvokimo lygis, šios srities politika ir tuometis vyriausybinių įstaigų apsaugos lygis. Įvertinimas parodė esamos informacinės infrastruktūros trūkumus, būtent tai, kad daugelyje vyriausybinių įstaigų informacija apskritai yra nepakankamai saugoma. Informacijos saugos kontrolė tuo metu buvo labai silpna. Norint apsaugoti informacijos infrastruktūrą nuo išpuolių, kurie galėjo pakenkti Vyriausybės įstaigų veiklai, beveik visose saugos srityse reikėjo gerinti padėtį. Viena svarbiausių silpnos apsaugos priežasčių – bendras nesuvokimas, kad rūpintis sauga yra būtina. Iš kitų priežasčių galima paminėti nepatyrusius saugos srityje dirbančius specialistus ir finansavimo (saugai užtikrinti reikalingų lėšų) trūkumą.

Būtina pabrėžti, kad išskirtinė valstybinio sektoriaus informacinių sistemų ypatybė – būtinumas griežtai ir centralizuotai nustatyti tiesioginio valdymo bei kontrolės principus. Šiuo atveju būtinas saugos lygis turi būti nustatomas visų pirma atsižvelgiant į valstybės ir nacionalinio saugumo interesus ir tik paskui – į galimas išlaidas. Todėl informacijos technologijų saugos svarbą bene pirmą kartą valstybiniu mastu Lietuvos valstybės institucijose nurodė Informacijos technologijų saugos valstybinė strategija, patvirtinta 2001 m. gruodžio 22 d. Lietuvos Respublikos Vyriausybės nutarimu Nr. 1625.

Kaip jau minėta, pastaruoju metu elektroninės informacijos saugos valstybės institucijų sektoriuje strategijos aspektai buvo įtvirtinti Elektroninės informacijos saugos valstybės institucijų informacinėse sistemose valstybinėje strategijoje iki 2008 metų. Elektroninės informacijos saugos valstybės institucijų informacinėse sistemose valstybinė strategija iki 2008 m. nustatė svarbiausius elektroninės informacijos saugos užtikrinimo principus, tikslus ir uždavinius bei jų įgyvendinimą. Tačiau jau pats strategijos pavadinimas rodo, iki kurių metų galios minėtoji strategija. Deja, po 2008 m. šios strategijos nepakeitė joks kitas strateginis elektroninės informacijos saugos dokumentas, tad šiuo metu Lietuvoje iš esmės nėra galiojančios elektroninės informacijos saugos valstybės informacinėse sistemose strategijos.

Neatsižvelgiant į tai, elektroninės informacijos saugos valstybiniame sektoriuje reguliavimas išlieka kaip atskira sritis. Visų pirma paminėtinas Lietuvos Respublikos valstybės informacinių išteklių įstatymas, kurio tikslas – užtikrinti tinkamą valstybės informacinių išteklių kūrimą, tvarkymą, valdymą, naudojimą, priežiūrą, sąveiką, planavimą, finansavimą ir saugą. Penktasis įstatymo skyrius reglamentuoja valstybės informacinių išteklių saugą. Pagal įstatymo 43 str.:

- tvarkant valstybės informacinius išteklius, privaloma naudoti saugos priemones, skirtas duomenų ir informacijos tikslumui užtikrinti bei apsaugoti juos ir registrui pateiktus dokumentus ir (arba) jų kopijas nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, sugadinimo, atskleidimo, neteisėto pasisavinimo, paskelbimo, pateikimo ar kitokio panaudojimo ir nuo bet kokio kito neteisėto tvarkymo;
- siekiant užtikrinti valstybės informacinių išteklių saugą, vadovaujantis Vyriausybės patvirtintais elektroninės informacijos saugos reikalavimais, rengiami, derinami ir tvirtinami valstybės informacinės sistemos ar registro saugos dokumentai. Registro ar valstybės informacinės sistemos valdytojas gali tvirtinti visų jo valdymo sričiai priskirtų registrų ar valstybės informacinių sistemų bendrus saugos dokumentus. Organizuojant valstybės informacinių išteklių saugą, rekomenduojama vadovautis pripažintų standartizacijos organizacijų ir standartizacijos institucijų priimtais ir paskelbtais standartais;
- už informacijos saugą pagal savo kompetenciją atsako valstybės informacinės sistemos valdytojas ir tvarkytojas. Už registro duomenų ir registro informacijos saugą pagal savo kompetenciją atsako registro valdytojas ir tvarkytojas. Registro ar valstybės informacinių sistemų tvarkytojai privalo saugos nuostatuose ir kituose saugos dokumentuose nustatyta tvarka užtikrinti reikiamas technines ir organizacines saugos priemones bei tokių priemonių naudojimą.

Įstatymo 43[1] str. reglamentuoja informacinių išteklių atitikties nustatytiems elektroninės informacijos saugos reikalavimams stebėseną, o 44 str. įveda saugos įgaliotinio institutą. Stebėseną atlieka Lietuvos Respublikos vidaus reikalų ministerija, kuri yra apskritai atsakinga už valstybinio sektoriaus elektroninės informacijos saugą.

Antra, detalūs elektroninės informacijos saugos reikalavimai nurodyti atitinkamuose įstatymo įgyvendinamuosiuose teisės aktuose. 2013 m. liepos 24 d. Lietuvos Respublikos Vyriausybės nutarimu Nr. 716 buvo patvirtinti trys pagrindiniai dokumentai:

1) bendrųjų elektroninės informacijos saugos reikalavimų aprašas;
2) saugos dokumentų turinio gairių aprašas;
3) valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašas.

Bendrųjų elektroninės informacijos saugos reikalavimų aprašo tikslas – sudaryti sąlygas saugiai automatiniu būdu tvarkyti valstybės registrų (kadastrų) (toliau – valstybės registras) ir žinybinių registrų duomenis, dokumentus ir informaciją, valstybės informacinių sistemų ir kitų informacinių sistemų informaciją. Šio aprašo 6 p. nurodyta, jog užtikrinant elektroninės informacijos saugą rekomenduojama vadovautis Lietuvos standartais LST ISO/IEC 27001:2006, LST ISO/IEC 27002:2009 ir kitais Lietuvos bei tarptautiniais „Informacijos technologija. Saugumo metodai“ grupės standartais, nurodančiais, kaip saugiai tvarkyti elektroninę informaciją.

Pagal Bendrųjų elektroninės informacijos saugos reikalavimų aprašo 7 p., informacinės sistemos valdytojas privalo turėti pagal Lietuvos Respublikos Vyriausybės patvirtintas Saugos dokumentų turinio gaires parengtus ir su Vidaus reikalų ministerija suderintus bei patvirtintus šiuos saugos dokumentus:

- Saugos nuostatus.
- Saugaus elektroninės informacijos tvarkymo taisykles.
- Informacinės sistemos veiklos tęstinumo valdymo planą.
- Informacinės sistemos vartotojų administravimo taisykles.

Bendrieji elektroninės informacijos saugos reikalavimai irgi reglamentuoja saugos organizavimą, incidentų valdymą, rizikos vertinimą, informacinės sistemos pokyčių valdymą, informacinių technologijų saugos atitikties vertinimą ir informacinės sistemos vartotojų atsakomybę.

Antruoju svarbiu Vyriausybės patvirtintu dokumentu – Saugos dokumentų turinio gairių aprašu – nustatomas valstybės registro (kadastro), žinybinio registro, valstybės informacinės sistemos ir kitų informacinių

sistemų duomenų saugos nuostatų, Saugaus elektroninės informacijos tvarkymo taisyklių, Informacinės sistemos veiklos tęstinumo valdymo plano ir Informacinės sistemos naudotojų administravimo taisyklių turinys.

Trečiasis minėtuoju Vyriausybės nutarimu patvirtintas dokumentas – Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašas – reglamentuoja valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų klasifikavimą pagal juose tvarkomos elektroninės informacijos svarbą ir elektroninės informacijos svarbos nustatymą. Remiantis šiomis taisyklėmis, elektroninė informacija pagal svarbą skirstoma į keturias kategorijas: ypatingos svarbos elektroninė informacija, svarbi elektroninė informacija, žinybinės svarbos elektroninė informacija ir kita elektroninė informacija.

Konkretūs informacijos saugos reikalavimai, keliami minėtosioms kategorijoms nustatyti, pateikiami Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos techniniuose saugos reikalavimuose. Šiuo dokumentu nustatomi minimalūs elektroninės informacijos techniniai saugos reikalavimai, keliami Lietuvos Respublikos Vyriausybei atskaitingų valstybės institucijų ir įstaigų informacinėms sistemoms. Pavyzdžiui, papildomas pirmosios kategorijos informacinių sistemų elektroninės informacijos saugos reikalavimas – institucija turi naudoti Lietuvos standarte LST ISO-IEC 17799:2006 nurodytas technines saugos priemones.

Siekiant gerinti ir koordinuoti elektroninės informacijos saugą, 2006 m. Lietuvoje buvo įsteigta Elektroninės informacijos saugos koordinavimo komisija, kurios personalinė sudėtis tvirtinama atskiru Lietuvos Respublikos Vyriausybės nutarimu. Komisijos uždaviniai yra šie:

- koordinuoti neįslaptintos elektroninės informacijos (toliau – elektroninė informacija) saugos užtikrinimą;
- skatinti elektroninės informacijos saugos kultūros kėlimą;
- inicijuoti elektroninės informacijos saugos projektų rengimą.
- Komisija, vykdydama jai pavestus uždavinius, atlieka šias funkcijas:
- dalyvauja įgyvendinant valstybės politiką elektroninės informacijos saugos informacinių sistemų srityje;
- Lietuvos Respublikos Vyriausybės įstatymo ir Lietuvos Respublikos Vyriausybės darbo reglamento, patvirtinto Lietuvos Respublikos Vyriausybės 1994 m. rugpjūčio 11 d. nutarimu Nr. 728 (Žin., 1994, Nr. 63-1238; 2003, Nr. 27-1089), nustatyta tvarka rengia teisės aktų projektus, susijusius su elektroninės informacijos sauga;
- nagrinėja elektroninės informacijos saugos tobulinimo tendencijas, stebi didžiausių pavojų esamoms ir būsimoms informacinėms

vertybėms pokyčius informacinėse sistemose;
- valstybės institucijoms teikia rekomendacijas, kaip stiprinti elektroninės informacijos saugą;
- koordinuoja elektroninės informacijos saugos projektų įgyvendinimą;
- skatina valstybės institucijas bendradarbiauti elektroninės informacijos saugos srityje;
- bendradarbiauja su privačiu sektoriumi elektroninės informacijos saugos srityje;
- atlieka kitas jai pavestas funkcijas.

Lietuvos Respublikos vidaus reikalų ministras savo įsakymu dar yra patvirtinęs Saugaus elektroninės informacijos teikimo sutartį. Sutarties dalykas: sutartimi teikėjas įsipareigoja saugiai automatiniu būdu teikti sutarties priede nurodytą elektroninę informaciją gavėjui, o gavėjas įsipareigoja ją naudoti sutartyje nurodytu tikslu, sąlygomis ir tvarka.

Lietuvos Respublikos Vyriausybė yra patvirtinusi Valstybės informacinių sistemų steigimo ir įteisinimo taisykles, kurios nustato valstybės informacinių sistemų (išskyrus valstybės ir žinybinius registrus) steigimo, kūrimo ir įteisinimo, modernizavimo bei likvidavimo procedūras.

Informacinių technologijų saugos atitiktis vertinama pagal Lietuvos Respublikos vidaus reikalų ministro patvirtintą Informacinių technologijų saugos atitikties vertinimo metodiką. Remiantis šia metodika, informacinių technologijų saugos atitiktis informacinėse sistemose vertinama dviem etapais: vertintojas parengia informacinių sistemų saugos atitikties vertinimo ataskaitą ir ją pateikia įstaigos vadovui, kuris organizuoja trūkumų šalinimo priemonių plano rengimą. Kaip įgyvendinamas trūkumų šalinimo priemonių planas, prižiūri įstaigos saugos įgaliotinis.

Reikėtų paminėti, kad Lietuvos Respublikos vidaus reikalų ministro įsakymu dar buvo patvirtintos ir Interneto tarnybinių stočių apsaugos rekomendacijos. Jos apibrėžia visumą bendrojo pobūdžio priemonių, kurios būtinos valstybės institucijose ir įstaigose esančioms tarnybinėms stotims apsaugoti nuo išorinių bei vidinių grėsmių ir yra skirtos kompiuterių tinklui, turinčiam ryšį su internetu, sukurti, siekiant užtikrinti interneto tarnybinių stočių saugą.

Be to, kiekvienos organizacijos, užtikrinančios informacinių technologijų saugą, pagalbine knyga tapo 2002 m. liepos 1 d. įsigaliojęs Lietuvos standartas „Informacijos technologija. Praktiniai informacijos saugumo valdymo aspektai“, tapatus tarptautiniam standartui ISO/IEC 17799:2000, kuris 2004 m. buvo išverstas ir patvirtintas valstybine kalba. Šis standartas

nurodo gerąją praktiką, kuria turi vadovautis organizacijos, kurdamos savo informacijos saugos politiką.

Žinių įtvirtinimo klausimai

1. Kaip suprantamas kibernetinis saugumas?
2. Kokie yra kibernetinio saugumo principai?
3. Kokie strateginiai kibernetinio saugumo prioritetai deklaruojami Kibernetinio saugumo strategijoje?
4. Kokios pagrindinės priemonės yra numatytos Kibernetinio saugumo direktyvoje?
5. Kokios valstybės yra priėmusios kibernetinio saugumo strategijas?
6. Kokie yra pagrindiniai Lietuvos kibernetinio saugumo koncepcijos elementai?
7. Kokie yra svarbiausi Lietuvos kibernetinio saugumo programos 2011–2019 m. tikslai?
8. Kokius pagrindinius aspektus reglamentuoja Lietuvos Respublikos kibernetinio saugumo įstatymas?

/XI/ *skyrius*

Teisiniai nano-, biotechnologijų ir robotikos aspektai

/ 499–534 / *puslapiai*

1 skirsnis. Teisinis biotechnologijų reglamentavimas

Per pastaruosius tris dešimtmečius biotechnologijų mokslas ir pramonė ypač greitai plečiasi ir sudaro sąlygas tiek naujoms galimybėms, tiek naujoms potencialioms grėsmėms visuomenei ir tarptautinei bendruomenei. Biotechnologijų teisė yra tipinis pavyzdys, kaip visuomenė reaguoja į problemas bei iššūkius, kykančius dėl mokslinių inovacijų ir technologinių pokyčių.

Pastaraisiais dešimtmečiais biotechnologijų šaka ypač sparčiai plėtojosi būtent dėl technologinių proveržių. Moksliniai atradimai suteikė naujų biotechnologijų taikymo galimybių sveikatos apsaugos, žemės ūkio, maisto gamybos ir gamtos apsaugos srityse, o technologijos sugebėjo pateisinti viltis, kad bus galima patenkinti pasaulyje esantį maisto ir sveikatos apsaugos poreikį. Tuo pat metu biotechnologijos kelia svarbių politinių, etinių ir aplinkosaugos iššūkių bei skatina viešas plačias diskusijas. Tarp skirtingų šalių atsiranda didžiulių skirtumų, atsižvelgiant į tai, kaip jos geba plėtoti, taikyti ir reguliuoti naujus biotechnologijų produktus bei paslaugas. Dėl šių skirtumų kyla įtampa palaikant tarptautinius šalių santykius.

Esamas teisinis biotechnologijos reglamentavimas iš esmės pateikia biotechnologijoms pritaikytą teisinių principų, bendrųjų taisyklių ir gairių dėl šių technologijų keliamų iššūkių ir pokyčių rinkinį. Jais paremta sistema, sudaryta iš teisinių, administracinių, teisminių ir pritaikomų funkcijų, skirtų šiems susitarimams įgyvendinti, yra biotechnologijų teisinio reguliavimo pagrindas ir sudaro jų teisinį režimą. Esama biotechnologijų teisine aplinka siekiama rasti pusiausvyrą tarp ekonominių interesų, saugumo bei tvaraus socialinio ir ekonominio plėtros siekio.

Teisinis bet kokių naujų technologijų reguliavimas apskritai turėtų būti pagristas pusiausvyros principu tarp pavojų, kuriuos kelia visos naujos technologijos, ir naudos, kurią jos gali teikti visai žmonijai. Šią pusiausvyrą svarbu rasti tiek tarptautinės teisės ir praktikos, tiek nacionaliniu lygmeniu.

Galima išskirti keturis pagrindinius aspektus, kurie yra svarbiausi reguliuojant biotechnologijas tarptautinėje teisėje:

1) kam priklauso biotechnologijų ištekliai (iš to kyla klausimas, kokie valdymo modeliai yra arba turėtų būti taikomi reguliuojant tokius išteklius);
2) koks yra biotechnologijų, jų reguliavimo ir aplinkos apsaugos ryšys;
3) kaip sąžiningumas, teisingumas ir sąžiningas naudos padalijimas turėtų būti apibrėžiami biotechnologijų kontekste;
4) ar žmogaus teisių principai ir normos prieštarauja esamoms biotechnologijų plėtros tendencijoms ir reguliavimui, ir jeigu iš tiesų

taip yra, kaip ir kokiu būdu reikėtų mėginti rasti pusiausvyrą tarp šių principų ir normų.

2 skirsnis. Biotechnologijos samprata ir teisinis apibrėžimas

Žodis „biotechnologija“ yra sudurtinis, jis sudarytas iš priešdėlio bio-, reiškiančio biologinis, ir žodžio „technologija“. Šį terminą 1919 m. pirmasis sugalvojo vengrų mokslininkas K. Ereky. Nuo pat pradžių biotechnologijos samprata buvo pateikiama labai įvairiai.

Pastaruosius tris dešimtmečius dominuoja biotechnologijos kaip manipuliacijos mikroorganizmais siekiant atlikti tam tikras užduotis ar valdyti biologinį procesą apibrėžimas. Biotechnologija dažniausiai yra tapatinama su genų inžinerija. Biotechnologinės manipuliacijos paprastai apima genų perdavimą iš vieno gyvo organizmo kitam arba į sintetinį junginį, naudojant pažangiausias *DNR* pertvarkymo technologijas. Ji apima bet kokias technologijas, kurios naudoja biologines sistemas, gyvus organizmus ar jų darinius, siekiant kurti, gaminti, keisti ar juos pritaikyti augalams, produktams, prekėms, gyvūnams ar procesams, skirtiems tam tikrai užduočiai atlikti ar konkrečiai naudoti.

Biotechnologijas yra naudinga taikyti medicinos (raudonoji biotechnologija), vandens (mėlynoji biotechnologija), žemės ūkio (žalioji biotechnologija) ir pramonės (baltoji biotechnologija) srityse. Šiuolaikinė biotechnologija glaudžiai susijusi su naujų vaistų ir terapijų kūrimu, naujais tyrimų instrumentais, didėjančiu grūdų derliumi, atsparesnių grūdų ir augalų kūrimu, maisto skonio, tekstūros ir maistinės vertės gerinimu, užterštumo mažinimu, žmogaus sukurtų teršalų šalinimu ir kitais naudojimo būdais.

Bet kokios biotechnologijos kūrimo laikas nuo teorijos iki materialaus produkto yra gerokai ilgesnis nei informacinių technologijų ir paprastai trunka nuo setynerių iki dešimties metų. Moksliniai biotechnologijų tyrimai yra labai brangūs, pvz., biofarmacijos srityje atliekami tyrimai naujam produktui ar procesui sukurti, plėtoti, testuoti ar jį paruošti rinkai vidutiniškai kainuoja nuo 250 iki 300 mln. JAV dolerių.

1982 m. grupė ekspertų *EBPO* valstybėms narėms pasiūlė bendrą biotechnologijos apibrėžimą, kuris biotechnologiją apibūdino kaip „mokslinių ir inžinerinių principų taikymą apdirbant biologinių agentų medžiagas, siekiant sukurti naujus produktus ir paslaugas“. Šis apibrėžimas vis dar plačiai naudojamas ir išlieka aktualus, nes yra ypač platus.

2005 m. *EBPO ad hoc* Biotechnologijų darbo grupė parengė bendru sutarimu pagrįstą biotechnologijos apibrėžimą. Pagal šį apibrėžimą – biotechnologija yra mokslo ir technologijų taikymas gyviems organizmams ir jų dalims, produktams ir modeliams tam, kad kuriant žinias, produktus ir paslaugas būtų galima keisti gyvas ir negyvas medžiagas. Prie šio apibrėžimo dar pateikiamas sąrašas objektų, kurie vienareikšmiškai laikytini biotechnologijų objektu. Minėtiesiems objektams priskiriama: *DNR* ir (ar) *RNR*, baltymai ir kitos molekulės, ląstelės ir audinių kultūros bei inžinerija, biotechnologijos procesų metodai, genų ir *RNR* vektoriai, bioinformatika, nanobiotechnologija ir t. t. *EBPO* biotechnologijos apibrėžimas yra labai platus, nes jis apima visą moderniąją biotechnologiją ir daug tradicinių bei periferinių veiklos rūšių.

Sparti biotechnologijų plėtra per pastaruosius tris dešimtmečius sukėlė daugybę viešų pasaulinių diskusijų apie jos teikiamas galimybes ir keliamą grėsmę. Biotechnologijų plėtra tarptautinei bendruomenei šiuo metu kelia tam tikrų svarbių esminių klausimų, tokių kaip klonavimas, chimeriniai organizmai, organų auginimas, genetinės manipuliacijos, sintetinė gyvybė ir pan., ir lemia poreikį tarptautiniu lygmeniu sukurti bendrą apibrėžimą, kuris leistų nustatyti teisinę visos biotechnologijų srities sistemą ir taisykles.

Pagal 1992 m. Jungtinių Tautų konvencijos dėl Biologinės įvairovės 2 str., biotechnologija yra apibūdinama taip: „bet koks technologijos pritaikymas, kuris naudoja biologines sistemas, gyvus organizmus arba jų darinius tam, kad sukurtų ar keistų produktus ar procesus dėl konkretaus jų panaudojimo“.

Kartachenos protokolo dėl bioapsaugos 3 str. biotechnologiją apibūdina kaip „(a) *in vitro* nukleiną ir metodus, jų tarpe rekombinantinę dezoksiribonukleino rūgštį (*DNR*), ir tiesioginę nukleino rūgšties injekciją į ląsteles ar organoidus arba (b) ląstelių, esančių už taksonominės šeimos, sintezę, kuri įveikia natūralią fiziologinę dauginimosi ar rekombinacijos kliūtis ir kuri nėra technologija, naudojama tradiciniame veisime ir atrankoje“. Kadangi nėra konkretesnio tarptautiniu mastu pripažinto legalaus apibrėžimo, Biologinės įvairovės konvencija yra svarbus šaltinis.

Kaip jau minėta, pastarieji trys dešimtmečiai išsiskiria ypač aktyvia biotechnologijų plėtra. Geriausias visą biotechnologijos sritį reprezentuojantis pavyzdys – genetiškai modifikuotų organizmų (*GMO*) pritaikymas žemės ūkiui.

Aktyvūs *GMO* tyrimai buvo pradėti XX a. aštuntajame dešimtmetyje. Technologija turėjo galimybę būti labai naudinga, pvz., didinant žemės ūkio produkcijos kiekį ir maisto produktų maistinę vertę bei tam tikrą

naudą aplinkai, pvz., pesticidų naudojimo mažėjimas. Pirmasis *GMO* buvo sukurtas 1973 m., tačiau pirmasis *GMO* augalas buvo išaugintas tik 1983 metais. Pagal *GMO* skaičių ir genetinių manipuliacijų apimtį, pirmosios kartos *GMO* išlieka labiausiai paplitę. Šiuo metu (2012 m.) herbicidams atsparios *GM* kultūros sudaro apie 73 proc. komerciškai apsodinto *GMO* augalų ploto visame pasaulyje, toliau minimas atsparumas vabzdžiams (18 proc.) ir sujungti genai (pvz., atsparūs ir herbicidams, ir vabzdžiams) (8 proc.). Naujesnių kartų *GMO*, kurie yra atsparūs virusams ir turi geresnės kokybės požymių, sudaro mažiau nei vieną procentą visų pasaulyje auginamų *GM* kultūrų.

Pirma reikšminga *GM* kultūrų sėja (2,6 mln. ha) įvyko tik 1996 m., beveik vien tik JAV. Nuo 1996 iki 2003 m. pasaulinė teritorija, kur auginamos biotechnologijomis paveiktos kultūros, padidėjo keturiasdešimt kartų. 2003 m. JAV buvo didžiausia teritorija, kur augo *GM* kultūros, iš viso sudarė apie 63 proc., toliau ėjo Argentina (21 proc.), Kanada (6 proc.), Brazilija (4 proc.), Kinija (4 proc.) ir Pietų Afrika (1 proc.).

3 skirsnis. Svarbiausi biotechnologijų teisės principai

Biotechnologijų teisė yra sparčiai besiplėtojanti ir labai specializuota teisės sritis, tačiau ji dubliuojasi su keliomis kitomis teisinio reguliavimo sritimis: intelektinės nuosavybės, aplinkos, maisto, civilinės atsakomybės, verslo ir tarptautine teise.

Remiantis prigimtiniu naujųjų technologijų globalumo požymiu, svarbiausi biotechnologijų teisės principai turėtų būti nustatyti tarptautinėje teisėje.

Tarptautinės teisės požiūriu biotechnologijos aptariamos atsirandančioje bendrojo režimo biotechnologijų teisėje, kurią sudaro keturi principai:

1) bendrojo žmonijos intereso principas;
2) teisingo naudos pasidalijimo principas;
3) atsargumo principas;
4) savitarpio paramos aplinkos ir prekybos režimų principas.

Kaip jau minėta, optimalus teisinis biotechnologijų reguliavimas turėtų atspindėti šių principų balansą.

Tarptautinėje praktikoje yra taikomi trys galimi biotechnologijos reguliavimo modeliai:

1) „modernus nuolatinio suverenumo“ režimas;
2) „bendrojo paveldo“ režimas;
3) „bendrojo rūpesčio“ režimas.

„Bendrojo rūpesčio“ režimas gali būti laikomas „bendrojo paveldo“ režimo modifikacija, tačiau jis labai skiriasi nuo pastarojo, todėl negali būti atskirtas. Pagal „bendrojo rūpesčio“ koncepciją, „pasaulio ištekliai [...] nėra „priklausomi“ tarptautinei visuomenei nedalomumo pagrindu, kaip bendrasis paveldas, priešingai, jie išlieka kaip tradicinio suvereniteto arba laisvės režimo subjektas, tačiau jų valdymas reikalauja holistiško požiūrio, kad būtų atsižvelgta į bendrąjį žmonijos interesą nustatant ir užtikrinant jų apsaugą. Šia prasme bendrasis rūpestis pasitelkiamas kaip teisinis pagrindas įteisinant teisinės intervencijos formas atskirų valstybių vidaus jurisdikcijos srityje ir bendroms erdvėms taikomus galimus laisvės principo apribojimus.

„Bendrojo rūpesčio“ koncepcija yra pagrįsta susitarimu, pagal kurį pagarba tam tikroms esminėms vertybėms neturi būti palikta individualiam valstybių disponavimui arba *inter se*, tačiau yra pripažinta ir sankcionuota tarptautinės teisės kaip visoms valstybėms rūpimas klausimas. „Bendrojo rūpesčio“ režimas laikytinas vienu iš svarbiausių tarptautinio biotechnologijos režimo ramsčių, atsirandančių iš valstybinės praktikos, pabrėžiant, kad bendras rūpestis yra koncepcinė susitarimų, kuriais siekiama apsaugoti svarbiausius biosferos komponentus, matrica ir asocijuojasi su globalios aplinkosaugos atsakomybės idėja. Teisiškai „bendras rūpestis“, be to, kad yra kelių aplinkosaugos sutarčių pagrindas (pvz., Bendroji konvencija dėl klimato kaitos, Madrido aplinkosaugos protokolas prie Antarktikos sutarties, Ozono konvencija ir jos Monrealio protokolas, Ramsaro pelkių konvencija ir Dykumėjimo konvencija) dar yra kertinis teisinių instrumentų, reguliuojančių biotechnologijas ir bioįvairovę, elementas (tarp jų Biologinės įvairovės konvencija ir *FAO* sutarties dėl augalų genetikos išteklių maiste ir žemės ūkyje). „Bendrojo rūpesčio“ režimas vadovaujasi racionalaus, taupaus ir tvaraus bioįvairovės ir biotechnologijos naudojimo skatinimo bei įgyvendinimo požiūriu, pasiskolintu iš aplinkosaugos teisės, kuri siūlo nuo abipusio požiūrio pereiti prie valstybių įsipareigojimų šioje srityje.

„Modernus suverenus pastovus režimas“ grindžiamas postulatais, išdėstytais Bioįvairovės konvencijos preambulėje, ir reiškia, kad valstybės turi suverenias teises į savo biologinius išteklius.

Dar vienas aktualus biotechnologijų teisinio reglamentavimo principas – rūpestingumo *(due dilligence)*. Šis principas yra pateiktas Stokholmo deklaracijos dėl Aplinkos ir plėtros 21 principe (1972 m. birželio 16 d.) ir Rio de Žaneiro deklaracijos dėl Aplinkos ir plėtros 2 principe (1992 m. birželio 14 d.). Rūpestingumo principas nustato įsipareigojimą, kuris yra privalomas kiekvienai valstybei, kad būtų užkirstas kelias kitų valstybių teritorijai ar bendroms erdvėms padaryti žalos, galinčios atsirasti dėl biotechnologinės veiklos, siejamos su genetiškai modifikuotų medžiagų

išleidimu į aplinką. Biotechnologijų, kurių pažangumo pobūdis gali labai pasunkinti įvertinimą, ar „patikrinimas“ buvo tikrai atliktas, kontekste, rūpestingumas yra papildomas atsargumo principas.

Atsargumo principas inspiravo Kartachenos protokolą dėl bioapsaugos Biologinės įvairovės konvencijoje, nors jos tikslus apibrėžimas ir veikimo aspektas vis dar yra diskusijų objektas. Principas valstybių įsipareigojimų nuostatose gali būti apibrėžiamas taip: „priimti ir toleruoti teisės aktų ar administracinių priemonių, kurios yra reikalingos užkirsti kelią galimai numatomam pavojui aplinkai“. Kai kurie radikalūs komentatoriai, siekiantys įgyvendinti religines ar politines programas, aiškina, kad „atsargumo principas“ reiškia ekonominės ar technologinės veiklos, kuri gali kelti bet kokią numanomą grėsmę arba kuriai neegzistuoja įvertinimo ar valdymo metodai, plėtros atidėjimą arba net uždraudimą.

Atsargumo principas turėtų būti suprantamas kaip įprastas teisės principas, taikomas kartu su kitais, o ne kaip vienintelis biotechnologijų teisinio reguliavimo principas. Skirtumų tarp skirtingų biologinio saugumo praktikų didėjimas ir sutarimo tarptautiniu lygiu trūkumas patvirtina šią išvadą.

Visų naujųjų technologijų teisė pateikia prieštaringus principus ir skirtingose valstybėse formuluoja ne tuos pačius tikslus. Naujausios technologijos (biotechnologijos, nanotechnologijos, robotika) komplikuoja įstatymų leidėjų, siekiančių išlaikyti pusiausvyrą tarp tikslų siekimo ir apribojimų, padėtį. Pavyzdžiui, prieštaravimai tarp valstybės suvereniteto dėl išteklių, esančių jos teritorijoje, ir „bendrojo paveldo“ ir (ar) “bendrojo rūpesčio“ principų. Atsiranda dar daugiau esminių apribojimų, viena vertus, tokių kaip būtinybė išsaugoti mokslinių tyrimų laisvę ir teisė visiems gauti naudos iš mokslo ir technologijos pažangos, tačiau, kita vertus, biotechnologijų reguliavimo sritis taip pat apima žmogaus orumą ir sąžiningumą. Deja, besiplečiančios ekstremalios ir radikalios, etninės ir religinės pasaulėžiūros ir politinės koncepcijos trukdo ieškoti racionalios pusiausvyros.

Tarptautiniu lygmeniu nėra nė vienos išsamios teisinės priemonės, kuri apimtų visus biotechnologijos ar jos produktų aspektus. Tačiau kai kurie esami tarptautiniai susitarimai yra tiesiogiai susiję su biotechnologija.

Daugelis tarptautinių organizacijų irgi įsipareigojo nustatyti standartus, pirmiausia susijusius su biotechnologijos poveikiu sveikatai, aplinkai, žemės ūkiui, prekybai, etniniams ir socialiniams bei ekonominiams aspektams. Tarp šių organizacijų yra *Codex alimentarius*, Pasaulio sveikatos organizacija *(PSO)*, Jungtinių Tautų maisto ir žemės ūkio organizacija *(MŽŪO)*, Jungtinių tautų aplinkos apsaugos programa *(JTAP)*, Jungtinių tautų švietimo, mokslo ir kultūros organizacija (angl. *UNESCO)*, Jungtinių tautų pramonės plėtros organizacija (angl. *UNIDO)* ir t. t.

Tarptautinių susitarimų ir standartų bei taisyklių, susijusių su biotechnologija, kūrimo plėtra gali padėti daugeliui valstybių, ypač besivystančių, priimant atitinkamus su biotechnologija susijusius įstatymus ir tuo pat metu skatinant nacionalinių biotechnologijos reguliavimo nuostatų suderinimą tarptautiniu lygiu. Ilgainiui biotechnologijų teisės praktikos ir sutartys tiek nacionaliniu, tiek tarptautiniu lygiu prisidės prie tarptautinės biotechnologijos teisės formavimo.

4 skirsnis. Didžiausios teisinio biotechnologijų reglamentavimo problemos

Genų modifikavimo metodikos yra pripažintos ir nusistovėjusios biotechnologijos priemonės, teikiančiomis nemenką naudą įvairiose srityse. Tačiau pripažįstama, kad ši nauja technologija kelia ir potencialią grėsmę žmonių sveikatai bei aplinkai, nes sukuriami objektai skiriasi nuo tradicinių gamtoje egzistuojančių jų atitikmenų. Galimas žalingas poveikis žmonių sveikatai, toks kaip toksiškumas ir alergiškumas, buvo identifikuotas kaip atsirandantis dėl *GMO* produktų. Be to, mokslininkai diskutuoja dėl grėsmių, susijusių su horizontaliu modifikuotų genų perdavimu, atsparumu antibiotikams ir t. t. Vienas iš galimų *GMO* žalingų poveikių aplinkai yra invaziškumas ir atsparumas vystymuisi, netikslinis poveikis, biologinės įvairovės rizika ir t. t. Kadangi *GMO* naudojimas yra sąlygiškai trumpas, išlieka didelis mokslinis neaiškumas dėl ilgalaikio *GMO* poveikio žmogaus teisėms ir aplinkai.

Daugeliu biotechnologijos produktų tarptautiniu lygiu yra prekiaujama kaip prekėmis arba gamybos produktais. Pastaruoju metu biotechnologijos produktai yra vienas iš svarbiausių klausimų, darančių įtaką tarptautinei prekybai. Be to, didėja pripažinimas, kad *GM* produktai ir biotechnologija gali turėti didelį socialinį ir ekonominį poveikį. Be socialinių ir ekonominių sumetimų, vis daugiau valstybių atsižvelgia į kultūrinius, etinius ir religinius aspektus bei poveikį, kuris atsiranda dėl biotechnologijų. Modernioji biotechnologija kelia įvairių etinių klausimų, tokių kaip pakankamas maisto kiekis, ūkininkų pajamos, gamtinių išteklių išsaugojimas ir tvarus jų naudojimas, žmogaus teisių apsauga ir nešališkas dalijimasis biotechnologijų teikiama nauda. Dar reikėtų skirti dėmesio aiškinantis, kaip biotechnologijų naudojimas paveiks aplinkos vientisumą. Todėl biotechnologijos tapo vis dažniau viešas diskusijas keliantis ir susirūpinimą didinantis objektas. Nuo pat ankstyvųjų *GMO* plėtros dienų viso pasaulio politikai domėjosi, kaip naudoti ir plėtoti jų potencialą ir tuo pat metu tinkamai spręsti problemas, kurias kelia naujosios technologijos.

Iš tiesų *GMO* reguliavimas visą laiką buvo su *GMO* susijusių diskusijų centre. Tarptautinė teisė suteikia vieną iš būdų, kuriais toks susirūpinimas yra operacionalizuojamas virš nacionalinio lygmens.

Pirmieji *GM* pasėliai buvo sukurti tik 1980 metais. Šie pasėliai buvo išbandyti lauko tyrimų metu 1983 m. ir tik dešimtajame praėjusio amžiaus dešimtmetyje pirmieji *GM* pasėliai buvo parengti sukomercinti. Besikeičiantys reguliavimo metodai atspindi šią raidą. Ankstyvieji reguliavimo metodai buvo orientuoti į tai, kad laboratorijose ir lauko bandymų metu būtų laikomasi saugumo standartų ir tik dešimtajame praėjusio amžiaus dešimtmetyje reguliavimo metodai pradėjo apibrėžti tai, kaip elgtis su *GM* produktų prekyba, ir ypač sąlygas, kada gali būti duotas leidimas komerciškai auginti *GM* kultūras bei gaminti ir parduoti genetiškai modifikuotą maistą ir kitas prekes.

Egzistuoja dideli reguliavimo modelių, kuriuos taiko skirtingos valstybės, skirtumai. JAV, kuri buvo pirmoji valstybė, pradėjusi reguliuoti biotechnologiją, pritaikė *laissez-faire* artimiausią reguliavimo modelį. Maisto ir vaistų administracija (angl. *FDA*) 1992 m. išleido politinį pareiškimą, kuriame nustatė, kad biotechnologijų produktai yra laikomi tokiais pat saugiais kaip ir tradicinis maistas ir prieš pateikiant juos rinkai leidimą būtina gauti tik esant tam tikroms sąlygoms.

Šiuo metu dauguma valstybių yra nustačiusios teisinį biotechnologijų režimą ir specialias taisykles dėl biotechnologijų ir jų produktų. Pagrindiniai biotechnologijas kontroliuojančių įstatymų elementai yra laboratorijų kontrolė, produktų išleidimas į aplinką, rizikos analizė ir socialiniai bei ekonominiai aspektai prieš suteikiant leidimą prekiauti, be to, įstatymai reguliuoja žymėjimą, atsekamumo galimybę ir kitas stebėjimo priemones, reikalingas priežiūrai po leidimo suteikimo atlikti. Rizikos analizė apima rizikos valdymą ir informacijos apie riziką perdavimą.

Daugumos valstybių teisinis biotechnologijų režimas yra pagrįstas rizikos analize ir specialiomis atsargumo priemonėmis. Šios priemonės turėtų leisti užtikrinti aukštą žmonių sveikatos, aplinkos ir ekologinės sistemos apsaugos lygį.

5 skirsnis. Tarptautinis teisinio biotechnologijų reguliavimo kontekstas

Ankstesniame skyriuje aptartos problemos nacionaliniu lygiu atspindi globalias tendencijas. Biotechnologijų, kaip ir kitų naujųjų technologijų, globalumas pats savaime lemia nacionalinių priemonių ir teisinių režimų nepakankamumą ir negebėjimą spręsti technologijos keliamų problemų.

Šis kontekstas lėmė kelių tarptautinių dokumentų, skirtų dėmesiui į *GMO* poveikį atkreipti, priėmimą. Biotechnologijos potencialas prisidedant prie kai kurių problemų, susijusių su plėtra ir aplinka, buvo pripažintas 1992 m. JT konferencijoje dėl Aplinkos ir plėtros (Žemės viršūnių susitikimas, angl. *Earth Summit*), kurioje 21 darbotvarkės 16 skyrius buvo skirtas „Aplinkai palankiam biotechnologijos valdymui". Be to, kad buvo sudaromas būsimų derybų dėl konkretaus protokolo apie biosaugumą pagrindas, Biologinės įvairovės konvencijai būtina, jog susitariančiosios šalys nustatytų arba išlaikytų konkrečias priemones, skirtas su *GMO* susijusiai rizikai reguliuoti. Konvencijos 8(g) str. reikalauja, kad šalys nustatytų arba palaikytų priemones dėl rizikos, susijusios su gyvų modifikuotų organizmų, atsirandančių dėl biotechnologijų, naudojimu ir išleidimu į pasaulį, reguliavimu, valdymu ir kontrole tiek, kiek tai įmanoma ir tikslinga, nes tokie organizmai gali turėti neigiamą poveikį aplinkai, dėl kurio kiltų pavojus biologinės įvairovės išsaugojimui ir tvariam naudojimui, bei keltų grėsmę žmonių sveikatai.

Ši nuostata atspindi bendrą požiūrį, kad „gyvas modifikuotas organizmas" yra ne tas pats, kas jų genetiškai nemodifikuoti atitikmenys, ir jie turi tokias savybes, kurios iš esmės reikalauja rizikos žmonėms ir aplinkai įvertinimo.

Daugelis tarptautinių susitarimų, susijusių su biotechnologijomis, yra teisiškai privalomi arba stiprūs politiniai konsensusai, iš jų ir *JT* konvencija dėl jūros teisės (*UNCLOS*, 1982), Biologinės įvairovės konvencija (1992), *PPO* susitarimas dėl sanitarijos ir fitosanitarijos priemonių taikymo (*SPS Agreement*, 1994), *PPO* susitarimas dėl techninių kliūčių prekybai (*TBT Agreement*, 1994), Tarptautinė augalų apsaugos konvencija (1997), visuotinė UNIESCO deklaracija dėl žmogaus genomo ir žmogaus teisių (1997), Orhuso konvencija (1998), Biosaugos protokolas (2000 m.), Tarptautinė *UNESCO* deklaracija dėl žmogaus genetinių duomenų (2003 m.) ir Tarptautinė *UNESCO* deklaracija dėl bioetikos ir žmogaus teisių (2005 m.). Biosaugos protokolas yra pirmasis tarptautinis teisiškai privalomas susitarimas dėl *GMO* prekybos. Protokolas buvo pateiktas pasirašyti 2000 m. gegužę ir įsigaliojo 2003 m. rugsėjo 11 dieną. Nuo 2010 m. spalio 31 d. 159 valstybės ir ES ratifikavo šį protokolą arba prie jo prisidėjo. Tokiu būdu protokolo nuostatos galioja ir Lietuvoje.

Protokolo tikslas – laikantis atsargumo priemonių, išdėstytų Rio de Žaneiro deklaracijos 15 principe, papildomai prisidėti užtikrinant atitinkamą apsaugą saugių *GM*O, esančių modernios biotechnologijos, galinčios turėti neigiamą įtaką biologinės įvairovės išsaugojimui ir tvariam naudojimui, perdavimo, tvarkymo ir naudojimo lygį bei atsižvelgiant į riziką žmonių sveikatai.

Šį protokolą pasirašiusios šalys turi užtikrinti, kad bet kokių *GMO* plėtojimas, tvarkymas, transportavimas, naudojimas, perdavimas ir išleidimas turi būti vykdomi taip, kad būtų užkirstas kelias arba bent jau sumažinta rizika biologinei įvairovei ir pavojus žmonių sveikatai.

Be to, protokolas leidžia šalims imtis veiksmų, kurie padėtų geriau saugoti biologinę įvairovę nei tie, kurie išvardyti protokole, su sąlyga, kad tokie veiksmai yra suderinami su protokolo tikslu ir atitinka šalies įsipareigojimus pagal tarptautinę teisę. EB teisės aktai dėl *GMO* yra vieni iš griežtesnių priemonių pavyzdžių.

Protokole yra daug svarbių nuostatų dėl atsargumo principo; informuoto sutikimo ir sutarimo; dalijimosi informacija; atitikties mechanizmo; visuomenės dalyvavimo; atsakomybės ir žalos atlyginimo; pajėgumų didinimo bei finansinių išteklių besivystančioms valstybėms ir t. t.

Atsižvelgiant į atsargumo principą, protokolo 1 str. nurodyta, kad protokolo tikslo turi būti siekiama laikantis atsargumo požiūrio, išdėstyto Rio de Žaneiro deklaracijos dėl aplinkos ir plėtros 15 principe.

10 str. toliau detalizuoja *GPO* importo tvarką dėl apgalvoto jų išleidimo. 10(6) str. teigiama, kad „mokslinių įrodymų trūkumas dėl nepakankamo kiekio atitinkamos mokslinės informacijos ir žinių apie galimą neigiamą gyvų pakeistų organizmų poveikį bioįvairovės išsaugojimui ir tvariam naudojimui šalyje, į kurią tai yra importuojama, taip pat atsižvelgiant į riziką žmonių sveikatai, neturi sulaikyti šalies nuo sprendimo priėmimo, kaip priklauso, atsižvelgiant į aptariamo gyvo modifikuoto organizmo importą“.

Protokolas suteikia svarbų vaidmenį atsargumo principui priimant sprendimą dėl *GMO* importo dėl mokslinio netikrumo. Reikia pabrėžti, kad nuostatos dėl atsargumo nėra suformuluotos kaip įsipareigojimai, bet kaip teisės prevencinių veiksmų imtis.

7 ir 8 str. yra aprašoma informuoto sutikimo ir sutarimo procedūra. 7(1) str. nurodoma, kad informuoto sutikimo ir sutarimo procedūra bus taikoma prieš pirmą tikslinį *GMO*, kuriuos ketinama įvesti į importuojančios šalies aplinką, tarpvalstybinį judėjimą. 8 str. reikalauja eksportuojančias šalis kompetentingai nacionalinei institucijai pranešti arba įpareigoti eksportuotoją pranešti apie importuojančią šalį. Pranešime turi būti informacija, nurodyta protokolo 1 priede, ir rizikos įvertinimas. Pagal 11 ir 20 str., biosaugos agentūra yra įkurta tam, kad spręstų klausimus, susijusius su didele prekyba *GPO*. Agentūra dar atlieka daugiašališko keitimosi informacija mechanizmo funkciją.

Protokolo 23 str. yra numatytos priemonės dėl aiškaus visuomenės dalyvavimo. Susitariančiosios šalys: (a) remia ir supaprastina sąlygas visuomenės žinojimui didinti, švietimui ir dalyvavimui saugiai perkeliant,

tvarkant ir naudojant *GPO*, siekiant išsaugoti ir tvariai naudoti bioįvairovę; (b) užtikrinti visuomenės žinojimą, jos švietimą suteikiant prieigą prie informacijos apie *GPO*, kurie yra nurodyti protokole kaip tie, kuriuos galima importuoti; (c) konsultuotis su visuomene sprendimų, susijusių su *GMO*, priėmimo proceso metu ir visus priimtus sprendimus padaryti viešai prieinamus visuomenei; ir (d) kiekviena šalis turi stengtis informuoti visuomenę apie informacijos apie biosaugos agentūros prieinamumą.

26 str. leidžia šalims atsižvelgti į socialinius ir ekonominius aspektus priimant sprendimus dėl *GPO* importo, tačiau laikantis savo tarptautinių įsipareigojimų, jeigu šie aspektai yra lemiami *GPO* poveikio bioįvairovės išsaugojimui ir tvariam naudojimui. Tačiau sprendimų priėmimą gali lemti tik socialiniai ir ekonominiai aspektai, susiję su potencialia bioįvairovės netektimi, o ne platesne prasme. Norima pasakyti, kad į socialinius ir ekonominius veiksnius neturėtų būti atsižvelgiama įvardijant pavojus ir atliekant rizikos vertinimą. Šalys yra skatinamos bendradarbiauti mokslinių tyrimų ir apsikeitimo informacija apie socialinį ir ekonominį *GPO* poveikį, ypač susijusį su vietos bendruomene, srityje.

Biosaugos protokole yra dauguma esminių elementų, susijusių su biotechnologijų reguliavimo požiūriu. Kol nebuvo protokolo, negaliojo jokie globalūs teisiškai privalomi instrumentai, apibrėžiantys *GPO* perdavimą, saugų naudojimą ir gautų biotechnologinių rezultatų pritaikymą neigiamo poveikio aplinkai kontekste, kuris galėtų paveikti bioįvairovę. Protokolas gali būti vertinamas kaip pats išsamiausias ir svarbiausias tarptautinis susitarimas dėl biotechnologijų, tačiau jis nėra vienintelis. Kuriant ir formuojant tarptautinę biotechnologijų teisę, kiti tarptautiniai susitarimai turi veikti lygiagrečiai su Biosaugos protokolu.

6 skirsnis. Teisinis biotechnologijų reglamentavimas ES ir Lietuvoje

Teisinis ES biotechnologijų reglamentavimas yra įvairiapusis. Svarbiausi reglamentavimo klausimai yra šie: ribotas biomodifikuotų organizmų naudojimas, sąmoningas jų paskleidimas aplinkoje, naudojimas maistui ir pašarui, atsekamumas ir ženklinimas, augalininkystė ir sėklininkystė, medicinos produktai, intelektinės nuosavybės teisės biomodifikuotų organizmų atžvilgiu, darbuotojų sauga, pavojingų bioproduktų transportavimas, atsakomybė už žalą aplinkai, eksportas į trečiąsias šalis.

Suvokdama biotechnologijų svarbą technologinei ir ekonominei plėtrai, ES priėmė specialius teisės aktus, susijusius su gyvybės mokslų ir biotechnologijų mokslo bei verslo plėtros skatinimu. Tokie specialūs teisės aktai yra:

1) Komisijos pranešimas Tarybai, Europos Parlamentui, Ekonomikos ir socialinių reikalų komitetui bei Regionų komitetui – Gyvybės mokslai ir biotechnologija – Strategija Europai (COM(2002) 27 galutinis);
2) Komisijos pranešimas Europos Parlamentui, Tarybai ir Europos ekonomikos ir socialinių reikalų komitetui – Gyvybės mokslai ir biotechnologija – Strategija Europos pažangos ataskaitai ir gairės ateičiai (COM(2003) 96 galutinis);
3) Komisijos ataskaita Europos Parlamentui, Tarybai ir Europos ekonomikos ir socialinių reikalų komitetui – Gyvybės mokslai ir biotechnologija – Strategija Europai dėl antrosios pažangos ataskaitos ir gairių ateičiai (COM(2004) 250 galutinis).

Svarbiausi minėtini ES biotechnologijų teisės aktai yra šie:

1) 1990 m. balandžio 23 d. Tarybos direktyva 90/219/EEC dėl riboto genetiškai modifikuotų mikroorganizmų naudojimo, papildyta papildomais reglamentais ir vėlesniais pakeitimais;
2) 2001 m. kovo 12 d. Europos Parlamento ir Tarybos direktyva dėl apgalvoto genetiškai modifikuotų organizmų išleidimo į aplinką ir Tarybos direktyvos 90/220/EEC panaikinimo su papildomais reglamentais ir vėlesniais pakeitimais; pagal šią direktyvą priimami komisijos sprendimai, leidžiantys GM organizmų patekimą į ES rinką;
3) 2005 m. rugpjūčio 16 d. Komisijos rekomendacijos 2005/637/EC dėl priemonių, kurių reikia imtis leidimo turėtojui tam, kad išvengtų galimos žalos sveikatai ir aplinkai tuo atveju, jei įvyktų netyčinis aliejinių rapsų (*Brassica napus L.*, GT73 line – MON-00073-7), genetiškai modifikuotų, kad būtų atsparūs herbicidui glifosatui, išsiliejimas;
4) 2003 m. rugsėjo 22 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 1829/2003 dėl genetiškai modifikuoto maisto ir pašarų;
5) 2004 m. balandžio 6 d. Komisijos reglamentas (EC) Nr. 641/2004 dėl išsamių Europos Parlamento ir Tarybos reglamento (EC) Nr. 1829/2003 dėl paraiškų teikimo dėl naujų genetiškai modifikuotų maisto ir pašarų taisyklių, pranešimas apie esamus produktus ir atsitiktinio ar techniškai neišvengiamo genetiškai modifikuotų medžiagų atsiradimo, kurių atsiradimą lėmė palankus rizikos įvertinimas;
6) 1997 m. sausio 27 d. Europos Parlamento ir Tarybos reglamentas (EC) Nr. 258/97 dėl naujų maisto produktų ir naujų maisto produktų komponentų;

7) 1997 m. liepos 29 d. Komisijos rekomendacijos 97/618/EC dėl mokslinių aspektų ir informacijos, kuri yra būtina remti paraiškas dėl naujų maisto produktų ir maisto produktų komponentų įvedimo į rinką, pateikimo bei pirminio įvertinimo ataskaitų pagal Europos Parlamento ir Tarybos reglamentą (EC) Nr. 258/97;
8) 2002 m. sausio 28 d. Europos Parlamento ir Tarybos reglamentas (EC) Nr. 178/2002, nustatantis bendruosius maisto teisės principus, įsteigiantis Europos maisto saugos tarnybą ir nustatantis su maisto sauga susijusias procedūras;
9) 2003 m. rugsėjo 22 d. Europos Parlamento ir Tarybos reglamentas (EC) Nr. 1830/2003 dėl genetiškai modifikuotų organizmų atsekamumo ir ženklinimo bei maisto produktų ir pašarinių produktų, pagamintų iš genetiškai modifikuotų organizmų, atsekamumo ir iš dalies pakeičiant direktyvą 2001/18/EC;
10) 2004 m. sausio 14 d. Komisijos reglamentas (EC) Nr. 65/2004 įsteigiantis sistemą unikalių identifikatorių, skirtų genetiškai modifikuotiems organizmams, kūrimui ir priskyrimui;
11) 2004 m. spalio 4 d. Komisijos rekomendacija 2004/787/EC dėl techninių gairių, skirtų mėginių ėmimui ir genetiškai modifikuotų organizmų bei iš genetiškai modifikuotų organizmų pagamintų medžiagų arba produktų aptikimui reglamento (EC) Nr. 1830/2003 kontekste;
12) 2003 m. liepos 23 d. Komisijos rekomendacija 2003/556/EC dėl nacionalinių strategijų ir geriausių praktikų kūrimo gairių, siekiant užtikrinti genetiškai modifikuotų pasėlių ir tradicinio bei ekologiško ūkininkavimo koegzistenciją;
13) 2004 m. vasario 24 d. Tarybos sprendimas 2004/869/EC Europos Bendrijos vardu dėl tarptautinės sutarties dėl augalų genetinių išteklių maistui ir žemės ūkiui išvadų;
14) 1993 m. liepos 22 d. Tarybos reglamentas (EEC) Nr. 2309/93, nustatantis Bendrijos procedūras dėl medicininių produktų, skirtų žmonėms ir veterinariniam naudojimui, priežiūros ir leidimų išdavimo, bei įsteigiantis Europos medicininių produktų vertinimo agentūrą;
15) 2001 m. lapkričio 6 d. Europos Parlamento ir Tarybos direktyva 2001/83/EC dėl Bendrijos kodekso, reglamentuojančio žmonėms skirtus medicininius produktus;
16) 1998 m. lapkričio 6 d. Europos Parlamento ir Tarybos direktyva 2001/82/EC dėl Bendrijos kodekso, reglamentuojančio veterinariniam naudojimui skirtus produktus;

17) 1998 m. liepos 6 d. Europos Parlamento ir Tarybos direktyva 98/44/EC dėl teisinės biotechnologinių išradimų apsaugos;
18) 1994 m. liepos 27 d. Tarybos reglamentas (EC) Nr. 2100/94 dėl Bendrijos augalų veislių teisinės apsaugos;
19) 2000 m. rugsėjo 18 d. Europos Parlamento ir Tarybos direktyva 200/54/EC dėl darbuotojų apsaugos nuo rizikos, susijusios su biologinių agentų poveikiu darbe;
20) 2004 m. balandžio 21 d. Europos Parlamento ir Tarybos direktyva 2004/35/EC dėl atsakomybės už aplinkos apsaugą siekiant išvengti ir ištaisyti žalą aplinkai;
21) 2002 m. birželio 25 d. Tarybos nutarimas 2002/628/EC Europos Bendrijos vardu dėl Kartachenos protokolo dėl biosaugos išvadų;
22) 2003 m. liepos 15 d. Europos Parlamento ir Tarybos reglamentas (EC) Nr. 1946/2003 dėl tarpvalstybinio genetiškai modifikuotų organizmų judėjimo.

7 skirsnis. Teisinė biotechnologinių išradimų apsauga

Biotechnologinių išradimų patentavimas yra atskira biotechnologijų teisinio reguliavimo problema. Bendriausia prasme biotechnologiniai išradimai išplėtė patentų teisės objektus, iškėlė naujų klausimų dėl išradimo lygių kriterijų.

JAV biotechnologinių išradimų patentavimas iš esmės plėtojosi pats savaime, buvo vadovaujamasi principu, kad išradimų apsauga turi būti neutrali visoms technologinėms sritims. Europoje nuspręsta šių išradimų ypatumus aiškiai reglamentuoti teisės aktais.

Biotechnologinių išradimų patentavimo taisyklės Europoje nustatytos gana senokai. Nuo 1998 m., kai buvo priimta Direktyva 98/44/EC dėl biotechnologinių išradimų teisinės apsaugos, ES laikoma viena liberaliausių genetinės medžiagos patentavimo jurisdikcijų pasaulyje, nes šioje direktyvoje tiesiogiai numatyta galimybė patentuoti izoliuotą genetinę medžiagą. Atkreiptinas dėmesys, kad tai pirmasis ES teisės aktas, kuriuo sureguliuoti materialiniai patentų teisės klausimai. Iki šios direktyvos ir po jos priėmimo materialiniai patentų teisės klausimai yra arba tarptautinės (ne ES), arba nacionalinės teisės objektas. Net ir naujasis ES patentų režimas, nustatytas 2012 m., iš esmės nėra ES teisės dalis ir reguliuoja procedūrinius patentų ekspertizės, išdavimo ir gynimo klausimus.

Direktyvoje 98/44/EC nustatytos materialinės biotechnologijų patentabilumo taisyklės. Kaip galimi patentuoti laikomi nauji, išradimo lygio ir turintys pramoninį pritaikomumą išradimai, net jeigu jie susiję su

objektu, kurį sudaro ar į kurio sudėtį įeina biologinė medžiaga arba procesai, kuriais biologinė medžiaga gaunama, apdorojama ar naudojama. Biologinė medžiaga, kuri išskiriama iš natūralios aplinkos arba gaminama techninių procesų būdu, irgi gali būti išradimo objektas, net jeigu iki tol ji egzistavo gamtoje.

Pagal direktyvą, vadovaujantis etinėmis ir humanitarinėmis nuostatomis, nustatyta, kad galimu patentuoti išradimu negali būti žmogaus kūnas jokiais jo formavimosi ir raidos etapais, nei paprasčiausias vieno iš jo elementų atradimas, nei geno seka ar jos dalis. Tradiciškai negalimais patentuoti išradimais laikomos augalų ir gyvūnų veislės bei biologiniai augalų ir gyvūnų išvedimo būdai (selekcija).

Iš žmogaus kūno išskirtas ar kitaip techninio proceso būdu izoliuotas elementas, geno seka ar jos dalis gali būti patentuojami net tada, jeigu to elemento sudėtis yra tapati natūralaus elemento sudėčiai. Genams patentuoti labai svarbus konkretus techninis pritaikomumas, pvz., nepakanka nustatyti, jog tam tikra seka atsakinga už konkrečią funkciją, tačiau ji turi būti realiai naudojama techninei problemai spręsti.

Kaip negalimi patentuoti laikomi ir tokie išradimai, kurių komercinis naudojimas prieštarautų viešajai tvarkai ar moralei; tačiau jų eksploatavimo nederėtų tokiu laikyti vien dėl to, kad jį draudžia įstatymai ar kiti teisės aktai. Į šią kategoriją patenka:

a) žmonių klonavimo būdai;
b) žmogaus lytinių ląstelių genetinės linijos tapatumo modifikavimo būdai;
c) žmonių embrionų naudojimas pramoniniams ar komerciniams tikslams;
d) genetinio gyvūnų tapatumo modifikavimo būdai, kurie gali jiems sukelti kančių be apčiuopiamos naudos žmonėms ar gyvūnams, bei kaip tokio proceso rezultatas gauti gyvūnai.

Atkreiptinas dėmesys, kad tiek klonavimas, tiek chimerinės manipuliacijos nėra draudžiami šia direktyva. Tokių veiksmų draudimai gali būti nustatyti nacionaliniuose įstatymuose, tačiau pati direktyva riboja tik galimybę patentuoti.

Pabrėžtina, kad genų patentai direktyvoje iš esmės yra leidžiami. Direktyvoje 98/44/EC nustatyta, jog medžiagos, išskirtos (izoliuotos) iš gyvo organizmo (tai pat ir žmogaus kūno), įskaitant visą ar dalinę geno seką, gali būti išradimo objektas ir gali būti patentuojamos, jeigu tenkinami bendrieji galimybės patentuoti kriterijai. Genetinės sekos kaip informacija *per se* yra negalimos patentuoti, tačiau izoliuota molekulė (pvz., DNR ar RNR

fragmentas), kurioje atkurta minėtoji genetinė informacija, yra galima patentuoti. Iš esmės tai reiškia, jog izoliuota ar susintetinta DNR ar RNR molekulė, jeigu ji sprendžia konkrečią techninę problemą ir yra nauja, ją galima patentuoti.

Direktyva 98/44/EC buvo iškart kritikuojama dėl plataus leidimo patentuoti izuoliuotą genetinę medžiagą. Nyderlandų vyriausybė, siekdama anuliuoti šią Direktyvą, kreipėsi į *ESTT*. Šis atmetė skundą ir palaikė izoliuotos genetinės medžiagos ir genetinės informacijos galimybę patentuoti, taip įgalindamas genetinės medžiagos patentavimą Europoje (byla C-377/98). Vėliau pats teismas šiek tiek apribojo genų patentų praktinę vertę – byloje C-428/08 atsisakė apriboti pašarų, kurie buvo pagaminti iš genetiškai modifikuotų sojos augalų (kurių modifikuoti genai buvo patentuoti), pardavimą pagal patento savininko reikalavimus, tačiau atsisakė labiau riboti pačią genetinės medžiagos galimybę patentuoti.

Analizuodamas ir aiškindamas Direktyvos 98/44/EC normas dėl žmogaus embrionų patentavimo draudimo, *ESTT* naujoje praktikoje pasisakė ir dėl galimybės patentuoti embrionines kamienines ląsteles. Byloje C-34/10 *ESTT* iš esmės nurodė, kad „direktyvoje siekiama eliminuoti bet kokią patentabilumo galimybę, kai gali kilti pavojus žmogaus orumui“. Tokiu būdu embrioninių kamieninių ląstelių linijos ir jų manipuliavimo metodai pripažinti kaip negalimi patentuoti. Paminėtina, kad šis sprendimas pats savaime nepanaikino visų išduotų patentų, susijusių su embrioninių kamieninių ląstelių linijomis ir jų manipuliavimo metodais, tačiau tokių patentų gynimas teisme dėl minėtojo *ESTT* sprendimo ginčo atveju būtų labai komplikuotas.

2013 m. birželio pradžioje JAV Aukščiausiasis Teismas išsprendė *Myriad* bylą, kurioje pirmą kartą pasisakė dėl genetinės medžiagos patentavimo. Iki *Myriad* bylos JAV (569 U.S. 12-398 (2013) nebuvo teisinio aiškumo dėl genetinės medžiagos patentų. Galimybės patentuoti klausimus kiekvienu atveju individualiai sprendė JAV patentų ir prekių ženklų biuras. *Myriad Genetics* dar 1995 m. pateikė paraiškas žmogaus BRCA2 genų mutantinėms sekoms, kurias 2013 m. pavasarį plačiausiai išgarsino Angelinos Jolie mastektomijos atvejis. Būtent BRCA2 patentas yra vienas iš kelių patentų, kurie buvo ginčijami *Myriad* byloje.

JAV Aukščiausiasis Teismas *Myriad* sprendimu iš esmės nustatė analogiškas taisykles, kurios jau penkiolika metų galiojo ES.

Abstrakti genetinė medžiaga ar naujai identifikuota genetinės informacijos seka negali būti patentuojama. Tačiau jeigu abstrakti genetinė medžiaga ar naujai identifikuota genetinės informacijos seka yra: 1) pakankamai funkciškai izoliuota (pvz., konkrečiai pagrįsta, kad būtent ši seka koduoja

tam tikrą baltymą ar esminę jo dalį); 2) išskirta kaip atskira molekulė, kuri natūraliai gamtoje neegzistuoja (ji egzistuoja tik *DNR/RNR* sudėtyje); 3) padeda atlikti konkrečią techninę užduotį (pvz., jos įterpimas į kitą organizmą įgalina tokį organizmą sintetinti atitinkamą baltymą), tokiu atveju leidžiama patentuoti.

Iki *Myriad* precedento JAV patentų teisėje nebuvo aiškiai nustatytos minėtosios genetinės medžiagos galimybės patentuoti sąlygos, todėl pasitaikė atvejų, kai buvo patentuojami abstraktūs naujų genetinės informacijos sekų atradimai ir šiais patentais buvo mėginama apriboti diagnostinį genetinės informacijos naudojimą.

Myriad precedento tikrai negalima laikyti genų patentų draudimu. Šis precedentas vienareikšmiškai įteisina racionalų genetinės medžiagos patentavimą. Jo didžiausia svarba – apriboti abstraktūs genų patentai. Vis dėlto tiek *ESTT* sprendimai, tiek *Myriad* byla parodo, jog etiniu ar religiniu požiūriu genų patentai išlieka itin sudėtinga problema.

Atskira biotechnologinių išradimų teisinės apsaugos problema – generinės konkurencijos skatinimas. Tiek JAV, tiek ES, siekdamos skatinti konkurenciją biofarmacijos srityje, yra nustačiusios specialią biofarmacinių išradimų patentinės apsaugos išimtį – vadinamąją *Bolar* išimtį, kuri supaprastina konkurencinių generinių produktų pateikimą į rinką ir leidžia pradėti konkuruojančio generinio produkto gamybą, bandymus ir pasiruošimą jį pateikti į rinką tuo laikotarpiu, kol galioja patentinė originalaus produkto apsauga. Daugelyje valstybių, tarp jų ir Lietuvoje, ši išimtis apima ne tik konkuruojančius generinius produktus, bet ir tam tikrus biofarmacinius preaparatus. Ši išimtis pirmą kartą 1984 m. nustatyta JAV, o nuo 2005 m. spalio 30 d. ir ES.

Nors mokslininkams ir būdinga nuomonė, kad ši išimtis visada egzistavo kaip bendrosios patentuotų technologijų tyrimų išimties dalis, įtvirtinus ją pozityviojoje teisėje atsirado didesnis teisinis aiškumas, paskatinęs biofarmacijos verslo plėtrą. Šis atvejis yra pozityvaus teisinio reguliavimo sėkmės pavyzdys ir įrodymas.

8 skirsnis. Teisinis biotechnologijų reguliavimas Lietuvoje

Lietuva, būdama ES narė, nuo 2004 m. gegužės 1 d. įgyvendina visus minėtuosius ES teisės aktus. Atkreiptinas dėmesys, kad dalis ES teisės aktų yra tiesioginio taikymo aktai, t. y. jie tiesiogiai galioja ir Lietuvoje.

Apskritai Lietuva pasižymi itin konservatyviu požiūriu į biomodifikuotus organizmus, ypač žemės ūkio biotechnologiją. Šalyje iki šiol nėra leidžiami biomodifikuotų organizmų lauko bandymai. Lietuva buvo viena iš kelių naujųjų ES narių, dėl kurios Komisijos sprendimu 2004/297/EB

buvo padaryta išimtis atidedant Direktyvų 2002/53/EB ir 2002/55/EB nuostatų įsigaliojimą dėl naujausių technologijų sėklų platinimo.

Kita vertus, Lietuva kaip vieną iš inovatyviausių naujojo verslo šakų siekia pritraukti modernų biotechnologijų verslą ir jį skatinti. Lietuvos inovacijų 2010–2020 m. strategijoje nurodoma, kad inovacijas versle skatins ES struktūrinė parama, kuri kartu su tinkamai veikiančiu inovacijų paramos infrastruktūros įstaigų tinklu sudaro palankias sąlygas mokslinių tyrimų plėtrai tam tikruose sektoriuose: gamtos išteklių ir žemės ūkio, biomedicinos, biotechnologijų ir kt. Dar pabrėžiama, kad pažangiausios ir vidutiniškai pažangios technologijos turėtų padėti tradicinei pramonei virsti inovatyvia vartojimo produktų pramone. Kaip viena iš didelį potencialą Lietuvoje turinčių pramonės šakų yra įvardijamas ir biotechnologijų sektorius, kuris gali padėti Lietuvos įmonėms kurti didelę pridėtinę vertę ir konkurencingai veikti tarptautinėje rinkoje[3].

2009 m. duomenimis, Lietuvos biotechnologijų pramonėje dirbo apie 2 500 žmonių, biotechnologijų verslo apyvarta siekė apie 300 mln. litų, o šio verslo sektoriaus sukuriamas produktas sudarė apie 0,9 proc. šalies BVP. Tai didesnė dalis nei Didžiojoje Britanijoje, Ispanijoje ar Nyderlanduose.

Aukštųjų technologijų plėtros 2011–2013 m. ir Pramoninės biotechnologijos plėtros Lietuvoje 2011–2013 m. programose biotechnologijos įvardijamos kaip prioritetinė Lietuvos verslo šaka, be to, siekiama ir planuojama, kad bus sukurta naujų, konkurencingų produktų, įgyta daugiau žinių, parengta daug aukštos kvalifikacijos specialistų, stabdomas protų nutekėjimas, sudaryta palanki aplinka biotechnologijos plėtrai ir investicijoms. Numatoma, kad iki 2013 m. biotechnologijos pramonėje bus sukurta „200 naujų darbo vietų; metinė realizacija pasieks 0,4–0,5 mlrd. litų; tikimasi 100–200 mln. litų užsienio investicijų“. Paminėtina, kad visos šios priemonės iš esmės skirtos ne žemės ūkio biotechnologijų plėtrai.

Apskritai Lietuvos padėtį dėl biotechnologijų teisinio reglamentavimo apibūdina tam tikras neapsisprendimas. Viena vertus, žemės ūkio biotechnologija, kuri yra viena plačiausių ir itin perspektyvių biotechnologijos sričių, yra labai griežtai apribota, kita vertus, siekiama maksimalios pramoninės biotechnologijos plėtros. Toks nenuoseklumas nėra naudingas biotechnologijų verslo ir mokslo plėtrai Lietuvoje, nes daugelis tarptautinių biotechnologijų įmonių ir mokslo įstaigų veikia abiejose srityse. Tarp šių dviejų biotechnologijų šakų yra daug sąveikos ir kryžminių galimybių. Lietuva priklauso ES, kurios bendrojoje rinkoje jau cirkuliuoja daugybė žemės ūkio biotechnologijos produktų, tad ilgalaikis atsiribojimas nuo jų yra ir neįmanomas, ir nenaudingas.

9 skirsnis. Teisinio nanotechnologijų reguliavimo ypatumai ir principai

Nanotechnologijos yra naujausia mokslo technologinė sritis, su kuria siejami svarbiausi ateities technologijų proveržiai ir socialinė ekonominė raida. Nanotechnologijas sudaro įvairūs technologijų ir produktų deriniai, kurių skiriamasis požymis – itin smulkios juos sudarančios dalelytės.

Prognozės, kad nanotechnologijos taps perspektyviausia nauja technologija, o jų išlaidos nuo 13 mlrd. JAV dolerių 2005 m. padidės iki daugiau negu vieno trilijono JAV dolerių 2015 m., šiuo metu atrodo konservatyvios. 2005–2010 m. laikotarpiu nanotechnologijos tapo ne tik mokslinių tyrimų objektu, bet ir realiais produktais. 2008 m. pabaigoje apie 800 produktų, kuriuos patys gamintojai įvardijo kaip pagrįstus nanotechnologijomis, buvo laisvai platinami rinkoje. Šiuo metu kiekvieną savaitę į rinką vidutiniškai pateikiama nuo trijų iki keturių naujų nanotechnologijomis pagrįstų produktų, t. y. minėtieji produktai vartotojams yra gana plačiai prieinami. Su nanotechnologijomis siejamas globalių problemų, tokių kaip alternatyvioji energetika, maisto ir vandens tiekimas, sprendimas. Deja, nors ir turi milžinišką potencialą, nanotechnologijos irgi gali kelti dar iki šiol nežinomą ir net nenumanomą riziką, dėl to neišvengiamai kyla etinių ir teisinių klausimų.

Daugelio pasaulio šalių vyriausybės ir verslo grupės nanotechnologijų tyrimus laiko prioritetine mokslo valstybinio finansavimo sritimi, taip tikėdamosi nanotechnologijų sparčios raidos ir pažangos. Šia prasme ne išimtis yra ir Lietuva. Nanotechnologijų tyrimai ir plėtra kaip prioritetinė sritis yra įvardijama Aukštųjų technologijų plėtros programoje, patvirtintoje Lietuvos Respublikos Vyriausybės 2006 m. spalio 24 d. nutarimu Nr. 1048, ir Lietuvos Respublikos Vyriausybės 2007 m. vasario 7 d. nutarime Nr. 166 „Dėl prioritetinių Lietuvos mokslinių tyrimų ir eksperimentinės plėtros krypčių patvirtinimo“ bei vėlesniuose teisės aktuose.

Pastaruoju metu ES, JAV ir kitose išsivysčiusiose valstybėse vyksta itin aktyvi mokslinė diskusija dėl nanotechnologijų teisinio reguliavimo ir jo vaidmens. Nors kai kurios interesų grupės reikalauja griežto nanotechnologijų reguliavimo ir priežiūros, įstatymų leidėjams kol kas labai trūksta informacijos ir žinių, kurios sudarytų būtinas tinkamo nanotechnologijų reguliavimo prielaidas. Tokia padėtis kelia dilemą – teisinio reguliavimo trūkumas gali pakirsti verslo ir visuomenės pasitikėjimą nanotechnologijomis, o skubotas ir netinkamas reguliavimas gali tapti kliūtimi plėtoti ir taikyti nanotechnologijų pagrindu kuriamus socialiai naudingus produktus. Be to, kai kurie nanotechnologijų aspektai iš esmės patenka į esamo

teisinio reguliavimo objektą. Greta valstybinio reguliavimo gausu įvairių interesų grupių siūlymų ir iniciatyvų dėl nanotechnologijų reguliavimo. Tokį netiesioginį ar neformalų reguliavimą neišvengiamai teks pakeisti formaliu ir kryptingu teisiniu reguliavimu, kuriuo bus siekiama spręsti nanotechnologijų rizikos klausimus, skatinti jų naudingumą ir socialinį bei ekonominį proveržį. Nanotechnologijų ateitis labai priklausys nuo teisinių ir politinių ateinančio dešimtmečio sprendimų.

10 skirsnis. Nanotechnologijų samprata

Prieš pradedant nagrinėti reguliavimą, būtina aptarti svarbiausius techninius nanotechnologijų aspektus. Nanotechnologijoms reguliuoti yra būtinos aiškios „nanotechnologijų“, „nanodalelių“ ir „nanomedžiagų“ sąvokos. Vienas iš galimų nanotechnologijų apibrėžimo būdų yra pagrįstas dydžiu, kuriam esant laikoma, jog vyksta nanodalelių sąveikos ir kiti procesai. Deja, nanotechnologijų savybių apibrėžimas pagal dalelių dydį yra diskusijų objektas, tad vienodų sąvokų iki šiol nėra. Išsiskiria nuomonės, kokio dydžio daleles ir medžiagas – iki 100, iki 200 ar iki 300 nanometrų (nm) – reikėtų priskirti nanotechnologijoms. Norint suvokti šios technologijos dydžių ribas, vertėtų paminėti, kad žmogaus plaukas yra apie 80 000 nm storio.

Medžiagos dalelės, kurių dydis siekia iki keleto šimtų nanometrų, pasižymi neįprastomis, specifinėmis, tik nanodalelėms būdingomis fizikinėmis ir biologinėmis savybėmis, pvz., inertiškos medžiagos nanodalelės gali turėti toksinį poveikį. Nanomedžiagos, mažesnės nei 300 nm, gali lengvai prasiskverbti pro ląstelių membraną ir pažeisti joje vystančius biologinius procesus. Pabrėžtina, kad medžiagų, turinčių savyje nanometro dydžio dalelių, pasitaiko ir natūralioje aplinkoje, jos jau dešimtmečius yra naudojamos dėl savo išskirtinių savybių, pvz., kizelgūras, bentonitas, diatominė žemė, kaolinas, talkas ir kt.

Didžiuma esamų reguliavimo iniciatyvų nanotechnologijas apibrėžia kaip apimančias pagamintas (nenatūralios kilmės) nanodaleles, kurių vidutinis dydis yra iki 200 nm. ES ir JAV nacionalinės nanotechnologijų iniciatyvos (*US National Nanotechnology Initiative*) dokumentuose nanotechnologijos apibrėžtos kaip „materijos, kurios dydis apytiksliai yra nuo 1 iki 100 nm, supratimas ir kontroliavimas“.

Istoriškai natūralios ir dirbtinės cheminės medžiagos teisiškai buvo reguliuojamos nustatant ne dydžio, o masės kriterijus. Toks reguliavimas – nustatant maksimalius leistinus medžiagų kiekius – visame pasaulyje taikomas nuodingosioms ir kenksmingosioms cheminėms medžiagoms reguliuoti. Nanotechnologijų atveju nanodalelių kiekiai vargu ar viršys šiuos

nustatytus ribinius dydžius (kilogramais ar gramais) dėl itin mažo nanodalelių dydžio ir svorio. Atlikti moksliniai tyrimai rodo, kad nanodalelių toksiškumas labiau sietinas su paviršiaus plotu, o ne svoriu, todėl kuriant teisinį reguliavimą į šiuos veiksnius reikėtų atsižvelgti. Dėl labai didelio nanodalelių paviršiaus ir tūrio santykio, palyginti su didesnėmis dalelėmis, bei poveikio, kuris pasireškia mikro lygiu, bet plačiau nepastebimas, daugelio nanotechnologijų gaminių savybės labai skiriasi, palyginti su tų pačių medžiagų, kurių dalelių dydis yra didesnis, savybėmis. Todėl medžiagos, kurios neturi jokio poveikio biologiniams procesams arba būdamos didesnės yra net naudingos, įgijusios nanomedžiagos pavidalą, gali tapti kenksmingomis arba net mirtinomis. Visa tai yra viena svarbiausių nanotechnologijų reguliavimo prielaidų.

11 skirsnis. Nanotechnologijų reguliavimo prielaidos ir principai

Kitoms naujųjų technologijų sritims taikomas reguliavimas ir jo principai parodo nanotechnologijų reguliavimo keliamą riziką ir teikiamą naudą, tačiau būtina pabrėžti, kad rekomenduoti konkrečių reguliavimo būdų technologijai, kuri kol kas yra labiau hipotetinė ir naudojama tik iš dalies, irgi yra rizikinga.

Apskritai reguliavimas gali atlikti dvejopą vaidmenį: jis gali būti arba leidžiantis (pozityvus), arba ribojantis (negatyvus). Be to, itin reikšmingas bet kokios technologinės srities plėtros trukdis – jos reguliavimo neapibrėžtumas. Jis dažniausiai atlieka ribojančio reguliavimo vaidmenį.

Ryškiausi ribojančio reguliavimo pavyzdžiai galėtų būti reguliavimas, nustatantis teisės subjektams kvalifikacinius reikalavimus, sukuriantis administracinę priežiūrą arba net apskritai draudžiantis tam tikras mokslo tyrimų sritis. Tačiau reguliavimas gali vaidinti ir pozityvų vaidmenį: suteikti ūkiui ir mokslininkams aiškias gaires, kokios mokslo tyrimų sritys yra pageidaujamos, ir, o tai ne mažiau svarbu, – kaip galės būti panaudojami jų darbo vaisiai. Pozityvus reguliavimas taip pat vaidina svarbų vaidmenį pritraukiant privačių investicijų. Tai patvirtina ypač greitas rizikos kapitalo investicijų į nanotechnologijas didėjimas JAV po to, kai 2001 m. JAV vyriausybė paskelbė Nacionalinę nanotechnologijų iniciatyvą (angl. *US National Nanotechnology Initiative)*. Pozityvus valstybinis reguliavimas irgi gali stiprinti visuomenės ir vartotojų pasitikėjimą technologija ir taip padėti kurti jos plėtrai palankią aplinką. Apskritai pozityvus teisinis reguliavimas gali suvaidinti teigiamą vaidmenį skatinant technologijos plėtrą ir kontroliuojant jos keliamą riziką, o negatyvus reguliavimas ir draudimai dažniausiai siejami su didesne ir sunkiai kontroliuojama rizika.

Kai kuriose nanotechnologijoms artimose technologinėse srityse (pvz., chemijos ar kosmetikos) tradicinis reguliavimo vaidmuo vis dėlto yra neigiamas – prevencinis. Tokio reguliavimo tikslas – riboti technologinių produktų keliamus pavojus ir riziką. Prevencinis reguliavimas gali būti kelių lygių: gali apsiriboti tik atskaitomybe ir naujų technologijų kontrole prieš pateikiant jas į rinką, o maksimalus prevencinis reguliavimas gali nustatyti išankstinio administracinio tvirtinimo procedūras, kurios taikomos prieš pateikiant naujas technologijas į rinką. Administracinė farmacijos preparatų ir medicinos procedūrų kontrolė yra geriausias tokio reguliavimo pavyzdys. Praktikoje galimas ir visiškas tam tikrų technologijų draudimas (pvz., įstatymais draudžiamas žmonių klonavimas).

Daugelyje valstybių technologijos reguliuojamos kompleksiškai – ir pozityviai, ir negatyviai. Nanotechnologijos irgi gali būti reguliuojamos šiuo būdu.

Nanotechnologijų reguliavimo būtinumą iš esmės lemia specifinės šių technologijų rizikos rūšys, iš jų paminėtinos:

- sauga gaminant ar naudojant nanodaleles;
- vartotojų saugumas naudojant nanotechnologijomis pagrįstus gaminius;
- žala aplinkai, kurią padaro gamybos atliekos ir gatavi gaminiai, galintys patekti į orą, vandenį ar dirvožemį;
- neprognozuojami nekontroliuojamų nanotechnologijų padariniai;
- valdžios naudojimasis nanotechnologijomis ribojant pilietines teises;
- dvejopos paskirties naudojimas, taip pat ir kariniams tikslams;
- nanotechnologijų metodų ir inovacijų teisinė apsauga.

Svarbus technologijų reguliavimo aspektas – nacionalinio lygio ir regioninio ar globalaus reguliavimo derinimas. Nacionalinis teisinis reguliavimas turi tam tikrų pranašumų. Jis gali būti geriau pritaikytas prie socialinio bei kultūrinio konteksto ir suteikti galimybę eksperimentuoti, rastis požiūrių įvairovei ir išoriniam vertinimui, kas yra veiksminga, o kas ne. Be to, nacionalinio lygio reguliavimas gali skatinti tarptautinę konkurenciję (galimybę technologijoms ir investicijoms judėti į palankesnes jurisdikcijas). Pozityvus nacionalinis reguliavimas vieną ūkio šaką ar technologinę sritį gali remti labiau negu kitas, nustatyti griežtesnius ar laisvesnius aplinkos apsaugos ar darbo standartus negu kitos šalys, skirti dėmesio mokslo tyrimų ir jų rezultatų taikymo finansavimo šaltiniams. Dėl tokios priežasčių įvairovės ir eksperimentavimo vertingumo, nacionalinių ūkio interesų požiūriu nanotechnologijoms geriausiai tinka nacionalinio lygio reguliavimas.

Minėtieji nacionalinio reguliavimo pranašumai gali turėti ir neigiamų padarinių. Nacionalinis reguliavimas gali visiškai neatsižvelgti į tarptautinę nanotechnologijų įtaką, pvz., tarptautinio masto taršą ar pavojingų arba dvejopo naudojimo medžiagų kontrolę.

Kai kuriais atvejais tarptautinė jurisdikcijų konkurencija irgi kelia neigiamų socialinių padarinių. Tai puikiai parodo šiuo metu Lietuvoje vykstantys teisminiai procesai dėl užsienio lažybų portalų blokavimo.

Istoriškai daugumai naujųjų technologijų buvo taikomi tik nacionaliniai teisės aktai. Daugeliu atveju skirtingi režimai ir požiūriai netrikdė technologijų pažangos. Informacinių technologijų ir biofarmacijos pramonės įmonės sėkmingai veikia, nors iki šiol nėra suderinto tarptautinio lygio reguliavimo. Kitų sričių veikla (pvz., finansinės paslaugos ES bendrojoje rinkoje) dėl nacionalinių reguliavimo skirtumų yra gerokai sunkiau vykdoma. Šiais atvejais aiškus tarptautinis reguliavimas yra pageidautinas. Svarbiausias argumentas už tarptautinį (ar bent jau regioninį) nanotechnologijų reguliavimą yra globali nanotechnologijų rinka ir jų keliama rizika, kuri neabejotinai turi tarptautinį poveikį.

Jau šiuo metu nanotechnologijos galėtų būti bent iš dalies reguliuojamos tarptautiniu mastu, taikant tarptautinę teisę. Pavyzdžiui, tais atvejais, kai nanotechnologijų veikla vienoje šalyje skleidžia taršą į kitą, šios šalies subjektai gali pateikti ieškinį dėl žalos atlyginimo Tarptautiniam Teisingumo Teismui, nors jokių specialių tarptautinių susitarimų dėl nanotechnologijų žalos ir nėra. Vienas iš tarptautinės teisės siūlomų nanotechnologijų reguliavimo principų – vadinamasis atsargumo principas. Šis principas reikalauja perkelti įrodinėjimo pareigą – įrodyti absoliutų technologijos saugumą – šios technologijos arba veiklos vykdytojui. Kai kurie mokslininkai tvirtina, kad atsargumo principas įgijo paprotinės tarptautinės teisės statusą, nes jis yra įtrauktas į kai kurių tarptautinių aplinkos apsaugos susitarimų turinį ir vertinamas nagrinėjant tarptautines bylas, tačiau ši išvada kelia abejonių dėl nesuderinamumo su kai kurių valstybių (ypač JAV) nacionaline teise. Be to, maksimaliai taikomas atsargumo principas, atsiradus bent mažiausiai teorinei žalos galimybei, iš esmės užkerta kelią technologijų plėtrai. Tai aiškiai rodo diskursas dėl genetiškai modifikuotų organizmų reguliavimo Europoje. Atsižvelgiant į tai, kad nanotechnologijų draudimas tarptautiniu lygiu yra neįmanomas, labiausiai tikėtinas kompleksinis nanotechnologijų reguliavimas derinant atsargumo ir pozityvaus reguliavimo principus. Tokio kompleksinio reguliavimo tikslas turėtų būti efektyvus ir atsakingas nanotechnologijų keliamos tarptautinės rizikos valdymas.

Ligšiolinė mokslinė diskusija dėl nanotechnologijų reguliavimo, be svarbiausių apibrėžimo ir principų klausimų, nagrinėja ir nanotechnologijų reguliavimo subjektų bei specialaus reguliavimo problemas.

Nors akivaizdu, kad tarptautiniu lygiu būtina suderinti nanotechnologijų standartus, šiuo metu nėra ne tik bendro tarptautinio nanogaminių ar nanotechnologijų reguliavimo, bet ir kartu priimtų apibrėžimų. Tarptautiniuose teisės aktuose iki šiol nėra apibrėžtas iš nanodalelių sudarytų ir tradicinės formos medžiagų skirtumas. Nanomedžiagos tarptautiniu mastu yra beveik nereguliuojamos – nėra nustatytų tarptautinių reikalavimų, kad prieš naudojant šias medžiagas komerciniams gaminiams su jomis būtų atliekami sveikatos ir saugos bandymai ar poveikio aplinkai vertinimas, jeigu tos medžiagos jau buvo patvirtintos tradicinės formos. Kaip jau minėta, nėra bendrai priimtų nanotechnologijų apibrėžimų ar terminologijos, juo labiau nėra bendrų tarptautinių nanodalelių toksiškumo bandymo ir standartizuotų nanodalelių poveikio aplinkai vertinimo protokolų.

Sprendžiant, ar nanotechnologijoms gali būti taikomas ir pakankamas esamas reguliavimas, svarbu įvertinti, ar nanotechnologijos kelia tik joms būdingų specifinių rizikų, ar ir bendrųjų, kurios jau yra sureguliuotos. Nors bendrasis cheminių medžiagų reguliavimas gali apimti ir nanotechnologijas, esama akivaizdžių jo spragų – neatitiktis nanotechnologijų ypatumams. Tai sudaro sąlygas kai kuriems nanotechnologiniams produktams visiškai išvengti reguliavimo. Tokią padėtį rodo kosmetikos priemonių reguliavimas, kuriamas atsižvelgiant tik į žmonių sveikatai keliamą riziką, bet nevertinant kosmetikos priemonių poveikio visai ekosistemai. Tokių reguliavimo spragų gali daugėti plėtojant ir sukomercinant sudėtingesnes ateities nanotechnologijas. Kaip jau minėta, tokių reguliavimo spragų galima būtų išvengti reikalaujant įvertinti visas specifines nanotechnologijų rizikas, tačiau esama pernelyg negatyvaus reguliavimo rizikos.

Daugelyje jurisdikcijų jau yra nustatytas reikalavimas kiekvienu atskiru atveju vertinti naujų medžiagų ar produktų saugą prieš pateikiant juos į rinką. Esamose reguliavimo sistemose istoriškai yra vertinama ir natūralios gamtinės kilmės nanomedžiagų sauga (pvz., kizelgūro, bentonito, diatominės žemės, kaolino, talko ir kt.). Sauga beveik visada yra vertinama remiantis moksliniu rizikos matavimu. Neleidžiamos į rinką arba ribojamos medžiagos ar gaminiai, kurių naudingumas yra susijęs su rizika. Bet kurios medžiagos reguliavimo pagrindas – teisingas jos fizinių ir cheminių savybių vertinimas bei techninės specifikacijos. Remiantis šiomis savybėmis ir specifikacijomis, nustatomos reguliavimo ribos, o neretai – ir pats konkrečios medžiagos apibrėžimas. Tikslus apibūdinimas, išreikštas išsamiomis techninėmis specifikacijomis, irgi yra esminė prielaida susieti mokslines studijas, kuriose vertinama medžiagos sauga, su pozityviuoju reguliavimu. Deja, reguliuojant chemijos, kosmetikos ar farmacijos gaminius vertinamos bendrosios medžiagos savybės, o techninėse specifikacijose nepateikiama

pakankamai išsamios informacijos apie dalelių savybes, kurios galėtų užtikrinti, kad reguliavimo subjektai atliktų saugos pagal teisingus fizinius ir cheminius parametrus vertinimą. Šiuo požiūriu „nanotechnologijų“ ar „nanodalelių“ apibrėžimai yra esminės tiek pozityviojo, tiek negatyviojo nanotechnologijų reguliavimo prielaidos. Esamas reguliavimas, į jį neįtraukus „nanotechnologijų“ ar „nanodalelių“ apibrėžimų, yra akivaizdžiai nepakankamas nei pozityviąja, nei negatyviąja prasme ir daugeliu atveju sukuria tik reguliavimo neapibrėžtumo situaciją.

Visiškai naujo *(sui generis)* nanotechnologijų teisinio reguliavimo kūrimas, grindžiamas vien tik fiziniu medžiagą sudarančių dalelių dydžiu, irgi nėra tinkamas atsakas į nanotechnologijų keliamas rizikas. *Sui generis* nanotechnologijų reguliavimas neužpildytų daugumos reguliavimo spragų ir pats savaime nepakeistų medžiagos saugos vertinimo taisyklių. Apskritai kiekvienam naujam reguliavimui neišvengiamai kenkia neaiškumas ir spragų gausa. Tą aiškiai rodo daugiau kaip dešimtmečio *sui generis* duomenų bazių teisinės apsaugos patirtis Europoje. Dar vienas svarbus nanotechnologijų specialiajam reguliavimui prieštaraujantis argumentas – numatomas jų taikymas ir poveikis, galintis sukelti daugiausia rizikos, iš esmės tik ateities klausimas, todėl apskritai neaišku, kaip reguliuoti technologijas, kurių galimybės šiuo metu yra tik spėjamos. Nanomedžiagų praktinis naudojimas šiuo metu kelia daug iššūkių, kurie nelabai skiriasi nuo tų, kurių pasitaiko pradedant naudoti kiekvieną naują medžiagą ir su kuriais galima geriau susidoroti tik darant nedidelius esamų reguliavimo sistemų pakeitimus, negu kuriant išvis naują reguliavimą. Visa tai suteikia prioritetą išplėsti esamą, o ne kurti naują, teisinį nanotechnologijų reguliavimą, pvz., nustačius nanodalelių apibrėžimą, į šių dalelių savybes galėtų būti atsižvelgiama vertinant saugą ir jos galėtų būti įtrauktos į technines specifikacijas.

Paminėtina ir nanotechnologijų pramonės savireguliavimo galimybė. 2008 m. Technologijų vertinimo informacijos centro (angl. *International Center for Technology Assessment)* ataskaitoje dėl Nanotechnologijų ir nanomedžiagų priežiūros principų konstatuojama, kad šiuo metu rinkoje yra šimtai plataus vartojimo prekių, į kurių sudėtį įeina nanomedžiagos, iš jų: kosmetikos, apsaugos nuo saulės priemonių, sporto, aprangos, elektronikos, maisto, kūdikiams ir vaikams skirtų prekių bei jų pakuočių. Dar pabrėžiama, kad nanotechnologijų grėsmės iš esmės yra emocinės ir numanomos, nes šiuo metu nėra vienareikšmių įrodymų, kad dabar naudojamos nanomedžiagos gali kelti didelį pavojų sveikatai, saugai ir aplinkai. Be to, nanotechnologijų keliami socialiniai, ekonominiai ir etiniai klausimai dar laukia savo sprendimo. Kita vertus, šiuo metu niekur pasaulyje nėra nustatyta nei valstybinės nanogaminių priežiūros, nei aiškių jų ženklinimo

reikalavimų, niekas nežino, kada gresia nanotechnologijų keliamas pavojus, ir niekas nekontroliuoja galimos žalos sveikatai ar aplinkai. Siūloma neatidėliojant imtis nanotechnologijų teisinio reguliavimo iniciatyvos vadovaujantis tokiais principais:

1) atsargumo;
2) specialaus nanotechnologijoms skirto reguliavimo;
3) visuomenės ir dirbančių žmonių sveikatos bei saugos;
4) aplinkos apsaugos;
5) skaidrumo;
6) visuomenės dalyvavimo;
7) platesnio poveikio vertinimo;
8) gamintojo civilinės atsakomybės.

Vis dėlto ankstesniųjų mėginimų reguliuoti naujas technologines sritis sėkmė buvo labai įvairi – nuo visiškai nepasitvirtinusios ES duomenų bazių *sui generis* teisinės apsaugos iki kai kuriose jurisdikcijose nustatytų ideologiškai motyvuotų ortodoksiškų genetiškai modifikuotų medžiagų draudimų.

Nanotechnologijų teisinė apsauga esamoje intelektinės nuosavybės teisinio reguliavimo sistemoje irgi susiduria su specifiniais iššūkiais. Neaišku, ar gali būti taikoma teisinė apsauga nanoformos medžiagoms, kurių tradicinėms formoms ji anksčiau arba apskritai nebuvo nustatyta, arba jau yra pasibaigusi (pvz., patentas). Iki šiol iš esmės sutariama tik dėl to, kad nanotechnologiniai išradimai, atitinkantys bendruosius galimybės patentuoti kriterijus, gali būti patentuojami. Akivaizdu, kad intelektinės nuosavybės apsaugos įstatymai turės būti pritaikyti prie nanotechnologijų reikalavimų taip, kaip jie buvo pritaikyti kompiuterinės programinės įrangos, elektroninių duomenų bazių ir genetiškai modifikuotų biologinių medžiagų teisinei apsaugai.

12 skirsnis. Esamos nanotechnologijų reguliavimo iniciatyvos

Šiuo metu ES nanotechnologijų reguliavimas iš esmės yra svarstymo stadijos, nors keletas iniciatyvų jau artėja prie įstatymų leidybos. ES yra sudaryta speciali nanotechnologijų darbo grupė – Besivystančių ir naujai identifikuotų rizikų sveikatai mokslo komitetas (angl. *The Scientific Committee on Emerging and Newly Identified Health Risks, SCENIHR*). Jis 2006 m. paskelbė oficialią poziciją dėl nanotechnologijų ir jų teisinio reguliavimo. Ši pozicija, kaip ir kiti su nanotechnologijų reguliavimu susiję ES dokumentai, skelbiami specialiajame ES nanotechnologijų tinklalapyje.

SCENIHR nanotechnologijas savo dokumentuose apibrėžia kaip darinius ir priemones, kurių bent viena dimensija yra maždaug šimtamilijoninės milimetro dalies (100 nanometrų) ar mažesnė. 2004 m. Europos Komisijos komunikate COM(2004)338 „Kelias į Europos nanotechnologijos strategiją“ pasiūlytas „integruotas, saugus ir atsakingas požiūris“ dabar sudaro ES nanotechnologijų politikos esmę. 2005 m. Europos Komisijos priimtas Europos veiksmų planas 2005–2009 m. COM(2005)243 nustatė nanotechnologijų reguliavimo pagrindus, o 2008 m. birželį Komisijos priimtame komunikate COM(2008)366 „Nanomedžiagų reguliavimo aspektai“ daroma išvada, kad esama Bendrijos reguliavimo sistema *iš esmės* apima su nanomedžiagomis susijusius elementus, kurie gali kelti riziką sveikatai, saugai ir aplinkos apsaugai. Neatmesdama galimybės keisti esamą reguliavimą, Komisija pabrėžė, kad sveikatos, saugos ir aplinkos apsauga turi būti stiprinama veikiau gerinant esamų teisės aktų įgyvendinimą, negu priimant naujus teisės aktus.

Pastaruoju metu nanotechnologijų reguliavimo iniciatyvą perėmė Europos Parlamentas. Jis suabejojo, ar dėl aiškių nanotechnologijų reguliavimo nuostatų nebuvimo Bendrijos teisėje šis institutas gali būti laikomas tinkamai reguliuojamu, atsižvelgiant į su nanotechnologijomis susijusią riziką. Europos Parlamento teikimu, specifinės nuostatos, susijusios su nanomedžiagomis, buvo įtrauktos arba numatomos įtraukti į teisės aktus, reglamentuojančius kosmetikos priemones, naujus maisto produktus ir papildus. Visų pirma, pakeitus esamus teisės aktus, buvo aiškiai nustatyta (paminint tekste), kad nanomedžiagos yra teisiškai reglamentuojamos pagal REACH režimą (ES reglamentą dėl cheminių medžiagų registracijos, įvertinimo, autorizacijos ir apribojimų). REACH reglamentas įsigaliojo 2007 m. birželio 1 dieną. Juo buvo modernizuota ir patobulinta ankstesnė ES chemines medžiagas reglamentuojanti teisės aktų sistema, nes šis reglamentas priimtas kaip valstybėse narėse tiesiogiai taikytinas ES teisės aktas. Svarbiausi REACH tikslai – užtikrinti aukšto lygio žmonių sveikatos ir aplinkos apsaugą nuo rizikos, kurią gali kelti cheminės medžiagos, skatinti alternatyvius techninių bandymų metodus, laisvą medžiagų apyvartą vidaus rinkoje ir konkurenciją bei inovacijas. REACH nustato pramonės atsakomybę už cheminių medžiagų keliamos rizikos vertinimą ir valdymą bei atitinkamos informacijos apie saugą pateikimą vartotojams. Jeigu būtina, pagal REACH teisinį režimą ES gali imtis papildomų priemonių dėl labai pavojingų medžiagų. Pagal REACH reglamento pakeitimus dėl nanotechnologijų, šių technologijų gaminių gamintojai ir importuotojai, laikydamiesi REACH reikalavimų, privalo pateikti visus žinomus šių gaminių poveikio sveikatai ir saugos duomenis. Pabrėžtina, kad privaloma vienus metus teikti duomenis nuo to laiko, kai produktas pateko į rinką.

2010 m. birželį Europos Parlamentas per savo Aplinkos apsaugos komitetą balsavo už siūlomus 2002 m. ES direktyvos dėl tam tikrų pavojingų medžiagų naudojimo elektros ir elektroninėje įrangoje apribojimo pakeitimus, ribojančius nanosidabro ir ilgų daugiasienių anglies nanovamzdelių naudojimą elektros ir elektronikos gaminiams. Pakeitimuose reikalaujama, kad elektros ir elektronikos medžiagos, į kurių sudėtį įeina nanomedžiagų, būtų atitinkamai ženklinamos, o nanomedžiagas naudojantys gamintojai privalėtų Europos Komisijai teikti visų minėtųjų nanomedžiagų saugos duomenis. Pabrėžtina, kad nanotechnologinių gaminių ženklinimo forma ir būdas dar nėra nustatyti, be to, neaišku, kas konkrečiai turėtų būti ženklinama (pvz., ar konkretus elektroninei įrangai priklausantis tranzistorius, pagamintas naudojant nanotechnologijas, ar pati įranga, kuriai panaudotas toks tranzistorius). Europos Parlamento aplinkos apsaugos, visuomenės sveikatos ir maisto saugos komitetas irgi siūlė kontroliuoti nanotechnologijų naudojimą gaminant maisto produktus žmonėms. Ši priemonė visiškai draudžia į ES rinkas tiekti iš klonuotų gyvūnų ar vykdant nanotechnologijų procesus pagamintą maistą, jeigu nebuvo atliktas specialus tokio maisto rizikos dėl galimo poveikio sveikatai vertinimas. Rizikos vertinimo būdai irgi turėtų būti patvirtinti kaip leistini, t. y. saugumo bandymams neturėtų būti naudojami stuburiniai gyvūnai. Reikalaujama, kad visi ingredientai, į kurių sudėtį įeina nanomedžiagų, būtų aiškiai paženklinti išvardijant jų sudėtines dalis ir skliausteliuose parašant nuorodą „nano“. Nanomedžiagų apibrėžimas irgi yra įtraukiamas į siūlomą tekstą, formuluojant jį taip: „nanomedžiaga reiškia tarptautiniu mastu gaminamą medžiagą su viena ar daugiau išorinių dimensijų ar ne didesne negu 100 nm vidaus struktūra“. Naujasis reglamentas bendru Europos Parlamento ir valstybių narių susitarimu galėjo būti priimtas 2010 m. pabaigoje arba 2011 metais.

Iš pradžių JAV vyravo į ES poziciją panašus požiūris. Dar 2005 m. Jungtinių Valstijų maisto ir vaistų administracija (angl. *The United States Food and Drug Administration, FDA)* nepriėmė jokių naujų specialių nanotechnologijas reglamentuojančių teisės aktų, vietoj to ji subūrė Nanotechnologijų interesų grupę, vienijančią FDA centrų, atsakingų už įvairių medžiagų ar produktų vertinimą ir reglamentavimą, atstovus. Tokia interesų grupė užtikrina informacijos derinimą ir perdavimą. 2006 m. rugsėjį FDA nusprendė, kad turi būti identifikuoti nanomedžiagų šaltiniai, jų judėjimas aplinkoje, problemos, kurių jie gali kelti žmonėms, gyvūnams ar augalams, ir šių problemų išvengimo ar sušvelninimo būdai. Pradėjus JAV reguliuoti nanotechnologijas, iš esmės buvo vykdoma stebėjimo ir nesikišimo politika, ir tokios pozicijos laikomasi iki šiol.

Vis dėlto JAV požiūris ilgainiui visiškai pasikeitė ir gana radikaliai nutolo nuo ES, kai 2007 m. FDA nusprendė, kad nereikalingas joks specialus nanodalelių reguliavimas ar ženklinimas. 2008 m. gruodžio 10 d. JAV nacionalinė mokslo tyrimų (angl. *National Research Council)* taryba paskelbė pranešimą, siūlantį griežčiau reguliuoti nanotechnologijas, nustatant specialias taisykles. Tokios taisyklės galėtų būti nanotechnologijomis pagrįstų produktų ženklinimas, kuris, kaip jau aptarta anksčiau, priimtas naujausiose ES iniciatyvose. Vis dėlto dauguma JAV teisės mokslininkų laikosi nuomonės, kad specialus nanotechnologijų ženklinimo reikalavimas yra nereikalingas ir netinkamas. Svarbiausias argumentas – nėra vienareikšmiškai žinomi nanotechnologijų pavojai, apie kuriuos žmonės turėtų būti įspėti, o ženklinant produktus tiesiog pateikti nuorodą „nano“ atrodo beprasmiška dėl didelės esamų ir numatomų nanotechnologijų produktų įvairovės. Netinkami atrodo ir Nanotechnologijų bei jų bendro ar specifinio naudojimo moratoriumai, nes potenciali nanotechnologijų nauda atrodo būsianti milžiniška, o kokia nors jų vartojimo rizika kol kas nepasireiškė. Atsižvelgdamos į šiuos argumentus, JAV specialių taisyklių dėl nanotechnologinių produktų iki šiol nepriėmė, o nanotechnologijų reguliavimas iš esmės išlieka pozityvus.

13 skirsnis. Nanotechnologijų reguliavimo perspektyvos

Įdomu pabrėžti, kad nanotechnologijų reguliavimo iššūkiai yra gana panašūs į tuos, kuriuos kėlė ir iki šiol kelia kitos inovacinės technologijos, t. y. biotechnologijos (ypač genų inžinerija) ir informacinės technologijos (geras pavyzdys galėtų būti elektroninės duomenų bazės). Dėl šių technologijų reguliavimo, kaip ir kitų naujovių atveju, kilo labai panašių mokslinių ginčų ir daugiau ar mažiau sėkmingai buvo vadovaujamasi tuo pačiu atsargumo principu. Dėl biotechnologijų (genų inžinerijos būdu gautos medžiagos) ES priėmė griežtus prevencinius teisės aktus, gerokai ribojančius šias technologijas ir atskiriančius jas nuo visuomenės, o JAV buvo siekiama minimalios reguliavimo intervencijos. Dėl to JAV pritraukė neabejotinai daugiau investicijų į biotechnologijas ir pasiekė didesnės jų pažangos. Duomenų bazių *sui generis* teisinės apsaugos atveju 1996 m. ES drąsiai rizikavo priimdama naujus teisės aktus, o JAV laikėsi konservatyvaus požiūrio (nepriėmė jokių specialių teisės aktų). Deja, ES specialiu reguliavimu nepavyko paskatinti duomenų bazių pramonės ir ji ligi šiol kenčia dėl reguliavimo spragų bei neaiškumo.

Atsižvelgiant į šią patirtį, be kitų valstybės iniciatyvų, dar vertėtų papildomai analizuoti neformalaus nanotechnologijų reguliavimo alternatyvas, pvz., tarpnacionalinį dialogą ir dalijimosi informacija forumus, tokius kaip Tarptautinis dialogas apie atsakingus nanotechnologijų mokslo tyrimus

(angl. *The International Dialogue on Responsible Research and Development of Nanotechnology)*. Kaip matyti iš ES 2008 m. liepos Komisijos rekomendacijos C(2008)424 dėl Atsakingų nanomokslinių ir nanotechnologinių tyrimų kodekso, iniciatyvos, priimtos po nuoseklių vyriausybių ir suinteresuotų asmenų tarpusavio diskusijų, irgi gali būti naudingos numatant ateities perspektyvas. Visiškas savireguliavimas taip pat įmanomas. Tokio savireguliavimo pavyzdys gali būti nevyriausybinių subjektų iniciatyvos, pvz., Įžvalgų instituto (angl. *Foresight Institute)* sukurtos Molekulinės nanotechnologijos atsakingos plėtros gairės (angl. *Foresight Guidelines for Responsible Nanotechnology Development)*. Suinteresuotieji asmenys iš esmės savanoriškai deklaruoja atitiktį tokioms savireguliacinėms iniciatyvoms, o jų įgyvendinimas užtikrinamas etikos ir prestižo svertais.

Teisinis nanotechnologijų reguliavimas ateityje turėtų remtis šiais trimis principais:

1) reguliavimas turėtų būti *lankstus ir pritaikomas*. Per ateinančius vieną ar du dešimtmečius nanotechnologijos plėtosis dramatiškai ir sparčiai; šiuo metu neįmanoma numatyti daugelio jų taikymo galimybių ir rizikos veiksnių. Protinga ir efektyvi reguliavimo sistema turės sudaryti sąlygas operatyviai pritaikyti reguliavimą atsirandančioms naujoms technologijoms;
2) reguliavimas turėtų būti *novatoriškas*. Bent kol kas nėra pakankamo pagrindo, kad įstatymais būtų galima nustatyti tradicinę kontrolę, kaip antai, rizikos ar emisijos standartus ar tam tikros veiklos ar gaminių ribojimą. Tokioms mažoms valstybėms kaip Lietuva drąsus ir inovacinis reguliavimas irgi galėtų padėti pritraukti investicijų į nanotechnologijų mokslo tyrimus ir suteikti pranašumą prieš kitas jurisdikcijas;
3) reguliavimas turėtų būti *tarptautinis*. Nanotechnologijas aktyviai tyrinėja visos išsivysčiusios valstybės. Tarptautiniu mastu suderintas požiūris į nanotechnologijų reguliavimą būtų priimtinesnis už kiekvienos valstybės taikomą skirtingą nacionalinį reguliavimą, kuris ateityje galėtų būti nesutarimų ir prekybos ginčų, tokių, kurie dabar yra susiję su genetiškai modifikuotais maisto produktais, priežastis.

Pradinis daugelio nacionalinių vyriausybių atsakas į nanotechnologijas turi bendrų požymių (išskyrus ženklinimą ir vartotojų informavimo klausimus), todėl oficialiai suderintas tarptautinis reguliavimo sprendimas yra įmanomas. Daugelis nanotechnologijų gamintojų ir tyrėjų yra tarptautinės įmonės, vykdančios veiklą daugelyje valstybių, todėl suderintas teisinis reguliavimas būtų naudingas tokioms įmonėms ir nanotechnologijų plėtrai apskritai.

Kadangi būsima nanotechnologijų plėtra ir jas naudojant gaunami gaminiai bei rizika yra labai neaiškūs ir gali sparčiai evoliucionuoti per ateinančius dešimtmečius, reguliuojant šią sritį būtinas lankstumas. Nanotechnologijų reguliavimas turėtų nustatyti institucinę ir procedūrinę struktūrą, gebančią operatyviai kurti tarptautiniu lygiu suderintą oficialų reguliavimą, galintį spręsti naujų nanotechnologijų potencialios rizikos, krizių ar incidentų klausimus. Be to, laipsniškai papildomas ir tobulinamas reguliavimas irgi yra būtinas technologijai, kuri ateityje gali plėtotis nenumatytomis ir svarbiomis kryptimis. Neprivalomi teisės aktai (pvz., Komisijos rekomendacijos) arba savireguliacija taip pat turi būti integruoti į kompleksinį nanotechnologijų valstybinį reguliavimą.

ES ir JAV požiūrių į nanotechnologijų reguliavimą palyginimas leidžia nustatyti bent vieną esminį bendrą institutą – privalomą informacijos atskleidimą. Be to, reguliavimo subjektai ir ES, ir JAV iš esmės pripažįsta, kad nanotechnologijos gali kelti ir specifinę riziką. Nors JAV laikosi pozicijos, kad numanomos rizikos rūšys negali būti teisinio reguliavimo pagrindas, tačiau ES pozicija linkusi vertinti ir potencialias rizikas bei dėl atsargumo taikyti specialias taisykles (pvz., ženklinimą). Jeigu reguliavimo subjektai nori efektyviai tvarkytis su nauja rizika ir naujomis problemomis, jie privalo turėti galimybę laiku susipažinti su aktualiais technologijos plėtros ir rizikos nustatymo duomenimis bei surinkti išsamius duomenis apie šias technologijas ir jų keliamą riziką. Ne mažiau svarbi yra ir savininko konfidencialios informacijos bei intelektinės nuosavybės teisių į nanotechnologijų inovacijas apsauga.

Apibendrinant tai, kas pasakyta, akcentuotini trys ryškūs skirtingi požiūriai į nanotechnologijų reguliavimą. Pirmasis – elgtis su nanotechnologijų gaminiais taip pat, kaip ir su kitais produktais, ir reguliuoti juos pagal galiojančius teisės aktus, taikomus ne nanoproduktams. Antrasis požiūris yra pagrįstas atsargumo principu, kuris suponuoja reikšmingus nanotechnologijų produktų apribojimus ar net draudimus, ir pirmenybę teikia naujiems specialiai nanotechnologijoms skirtiems teisės aktams. Trečiasis požiūris, susiejantis abiejų ankstesnių požiūrių elementus, reikalauja naujų taisyklių (pvz., ženklinimo), bet daugiausia remiasi esamais, o ne nanoproduktams taikomais, teisės aktais. Esamų iniciatyvų analizė rodo, kad ES vadovaujasi trečiuoju požiūriu, o JAV – daugiau pirmuoju.

Atsargumo principo taikymas teisiškai reguliuojant nanotechnologijas gali būti pražūtingas, nes jis neužkirs kelio nepageidaujamai šių technologijų plėtrai (kai kurios valstybės jo vis tiek nesilaikys), tačiau stabdys pozityvią technologijų plėtrą, pernelyg sureikšmins galimą riziką ir supriešins visuomenę.

Tikimasi, kad per ateinančius du dešimtmečius nanotechnologijų raida bus itin sparti, tad įstatymų leidėjai turi būti pasirengę į tai atsižvelgti laipsniškai pildydami ir tobulindami esamus teisės aktus. Šiuo atveju gali būti naudingos nevyriausybinių ir savireguliavimo institucijų iniciatyvos, nes jos, kaip rodo informacinių ir ryšių technologijų bei biotechnologijų reguliavimo patirtis, greičiau prisitaiko prie pokyčių.

Akivaizdu, kad nanotechnologija ir didesnioji su ja susijusios rizikos dalis yra tarptautinės, todėl reikalingas supranacionalinis teisinis reguliavimas. Mažose valstybėse, tokiose kaip Lietuva, tarptautinis reguliavimas suteiktų būtino pasitikėjimo verslui, moksliniams tyrimams bei vartotojams ir padėtų išvengti ideologinių spekuliacijų. Kita vertus, pozityvus nacionalinis reguliavimas įstatymų leidėjams sudaro sąlygas kurti palankesnę aplinką nacionalinės nanotechnologijų pramonės proveržiui. Be to, tokioms mažoms valstybėms kaip Lietuva gali būti naudinga trumpą laikotarpį (kol bus nustatytos tarptautinės taisyklės) naudotis nanotechnologijų nacionalinio reguliavimo galimybėmis, nustatant minimalų pozityvų reguliavimą be specialių taisyklių. Tai ne tik gali padėti į šią pramonės sritį pritraukti investicijų, bet ir gauti netiesioginės naudos (šalies kaip technologijoms palankios jurisdikcijos garsinimas, patirtis reguliuojant technologijas).

14 skirsnis. Teisiniai robotikos aspektai

Nors robotika yra palyginti sena technologijų sritis, ji dažniausiai siejama su kitų technologijų laimėjimais. Robotikai ypač aktualūs nanotechnologijų ir informacinių technologijų laimėjimai, kurie per pastarąjį dešimtmetį leido sukurti visiškai autonominius robotus.

Dauguma esamų robotų nėra autonominiai – jie tik įrankiai, tokie kaip kastuvas ar transporto priemonė, palengvinantys žmonių darbą. Kaip ir kiekvienas įrankis, jie gali būti naudojami neteisėtiems veiksmams, tačiau tokį jų naudojimo būdą lemia juos valdančio žmogaus valia, veiksmai ar neveikimas, o ne pats įrankis.

Per pastarąjį dešimtmetį dėl spartaus technologinio progreso robotikos srityje įvyko du reikšmingi pokyčiai: sukurtas ir įdiegtas dirbtinis intelektas, vadinasi, tam tikrą dalį arba net ir visus sprendimus dėl savo veikimo robotas priima pats; dėl kitų technologijų robotai tapo nepriklausomi nuo žmogaus, pvz., dėl naujosios kartos maitinimo šaltinių robotams nereikalingas nuolatinis maitinimo (elektros) šaltinis, jie nėra fiziškai (laidais ar pan.) susiję su konkrečia fizine alokacija, gali būti valdomi per atstumą ir veikti kitame žemyne ar net kitoje planetoje. Dirbtinis intelektas ir nuotolinės bevielės technologijos įgalino sukurti daugiau ar mažiau

autonominius robotus. Tokie robotai gali veikti nepriklausomai nuo žmogaus ir savarankiškai priimti konkrečius sprendimus dėl tam tikro veiksmo ar neveikimo.

Kita pastarojo dešimtmečio tendencija – robotų integravimas į visas kasdienio gyvenimo sritis – nuo lifto, kuris atsižvelgdamas į keleivių srautus tam tikru dienos metu pats sprendžia, kelintame aukšte laukti keleivių, iki išmanaus autopiloto automobiliuose ar autonominių pakilimo ir nusileidimo sistemų, kurios įmontuotos į šiuolaikinius lėktuvus.

Šiandien autonominis automobilis, kuris realaus pasaulio sąlygomis gali kirsti visą JAV teritoriją nuo Atlanto iki Ramiojo vandenyno, yra realybė.

Savaime suprantama, kad tokiose specializuotose srityse kaip metalo, automobilių, pavojingose aplinkose veikianti pramonė ir pan. autonominiai robotai yra daugiau ar mažiau įprasta kasdienybė.

Pastarojo dešimtmečio kariniai konfliktai irgi atskleidė iki šiol nežinotą robotikos naudojimą kariniams tikslams. Paaiškėjo, kad kariniai robotai laboratorijose yra kuriami bei tobulinami jau ne vieną dešimtmetį ir yra pajėgūs atlikti realias karines užduotis – tiek puolamuosius veiksmus, tiek humanitarines misijas (krovinių, sužeistųjų gabenimas ir pan.). Negana to, pavojingiausiuose pasaulio regionuose – Afganistane ar Jemene – robotai, ginkluoti naujausiais ginklais, sudaro priešakinę karo veiksmų liniją. Nors deklaruojama, kad kovos sprendimus, ar naudoti ginkluotę, priima šiuos robotus per atstumą valdantys žmonės, tam tikrus dalykus (pvz., gynybinio manevravimo reaguojant į priešo atsakomąją ugnį) robotai jau geba spręsti savarankiškai. Paminėtina, kad robotų naudojimo puolamiesiems veiksmams atvejų pastaruoju metu labai padaugėjo. Manoma, kad vien 2012 m. nuo robotų paleistos ugnies tokiose karinio konflikto zonose kaip Afganistanas ar Jemenas žuvo daugiau kaip du tūkstančiai žmonių.

Net ir neautonominiai robotai kelia tam tikrų teisinių problemų, tačiau jos yra arba specializuotos, pvz., kaip jau minėta, robotikoje plačiai naudojamos nano- ir informacinės technologijos, kurios reguliuojamos specifiškai, arba bendrojo pobūdžio ir sprendžiamos vadovaujantis bendrosiomis teisės normomis (pvz., didesnio pavojaus šaltinio sukeltos žalos atlyginimas).

Autonominiai robotai kelia akivaizdžių ir visiškai naujų teisinių problemų, su kuriomis visuomenė dar nesusidūrė, – autonominis robotas gali padaryti didelės žalos žmogui arba turtui, taip pat ir atimti gyvybę. Galiausiai jis gali priimti sprendimą veikti visuomenei visiškai nepriimtinu būdu (pvz., atlikti karinius veiksmus belaisvių ar sužeistųjų atžvilgiu), nes bent jau šiuo metu robotams nesuvokiamos bendražmogiškosios vertybės.

Šios priežastys lėmė, kad svarbiausiuose teisės mokslo centruose jau keletą metų vyksta aktyvios diskusijos dėl specialaus teisinio režimo nustatymo robotams ir ypač autonominių robotų reguliavimo.

Kai kurie mokslininkai mano, kad robotams nereikia specialaus teisinio režimo, nes autonominius įrankius žmonės naudoja jau tūkstančius metų ir jie patenka į esamų teisinių režimų ribas. Turimi omenyje naminiai gyvūnai, gyvuliai ir pan., kurie esant tam tikroms situacijoms sprendimus gali priimti ir veiksmų imtis visiškai autonomiškai, be to, gali nužudyti ar sunkiai sužaloti žmogų, įskaitant ir savo šeimininką.

Vis dėlto sunku nesutikti su kita nuomone, kuri pabrėžia, kad robotų keliami pavojai yra nepalyginamai didesni nei naminių gyvūnų. Šiuo atveju primintina analogija su EŽTT išvada dėl žalos potencialo lyginant internetą ir tradicinę spausdintinę žiniasklaidą (2011 m. gegužės 5 d. sprendimas byloje *Pravoye Delo and Shtekel v. Ukraine*, Nr. 33014/05). Ginkluotas robotas ar net autonominis automobilis gali būti prilyginamas masinio naikinimo ginklui, o jo sukeltus padarinius gali būti itin sudėtinga suvaldyti.

Teisinis robotikos reguliavimas susiduria su panašiais iššūkiais kaip bio- ar nanotechnologijų teisinis reguliavimas. Viena vertus, esama akivaizdaus pozityvaus robotikos ir dirbtinio intelekto technologijų potencialo, galimybių spręsti didžiausias socialines ir ekonomines problemas, kita vertus, nevisiškai aiški robotikos technologijų keliama rizika, be to, gana neaiškūs jų valdymo būdai. Griežtas robotikos reguliavimas neabejotinai turėtų neigiamų padarinių technologiniam progresui, be to, apskritai nelabai aišku, kaip reikėtų riboti dirbtinio intelekto sprendimų autonomiją, nes visiška autonomija yra viena iš svarbiausių intelekto, kaip jis yra suvokiamas, savybių.

Trumpalaikėje perspektyvoje teisinis robotikos reguliavimas iš esmės suvedamas į filosofinę bei etinę diskusiją ir reikalavimą, kad visus robotų priimtus sprendimus patikrintų ir patvirtintų žmogus. Tokia taisyklė – automatinių ir autonominių technologinių sprendimų žmogiškoji kontrolė – pirmą kartą nustatyta dar 1980 m. Europos Tarybos konvencijoje dėl asmens duomenų apsaugos ir perkelta į Direktyvą 95/46/EC dėl asmens duomenų teisinės apsaugos (15 straipsnis). Ilgalaikėje perspektyvoje akivaizdu, kad autonominių robotų naudojimas civiliniams ir kariniams tikslams tarptautiniu ir nacionaliniu lygmeniu reikalaus kokybiškai naujo teisinio reguliavimo tiek tarptautinėje viešojoje, tiek privatinėje teisėje.

Žinių įtvirtinimo klausimai

1. Kokie yra pagrindiniai tarptautinio biotechnologijų reglamentavimo klausimai?
2. Kaip teisėje apibrėžiamos biotechnologijos?
3. Kokie yra biotechnologijų teisės principai?
4. Kaip suprantamas atsargumo principas ir kokia yra jo kilmė?
5. Kaip reglamentuojami genetiškai modifikuoti organizmai?
6. Kokios teisinio biotechnologijų reglamentavimo iniciatyvos Lietuvoje?
7. Kokiems biotechnologijų išradimams netaikoma patentinė apsauga?
8. Kokios yra nustatytos genetinės medžiagos patentavimo sąlygos?
9. Kodėl biotechnologijų patentams reikalingas pratęstas galiojimo laikotarpis?
10. Kokia speciali patentų teisių išimtis nustatoma skatinant generinę konkurenciją?
11. Koks yra teisinis nanotechnologijų apibrėžimas?
12. Kokie yra svarbiausi teisinio nanotechnologijų reguliavimo principai?
13. Kaip teisiniam nanotechnologijų reguliavimui yra taikomas atsargumo principas?
14. Kodėl būtina reguliuoti nanotechnologijas ir kodėl jų nacionalinis reguliavimas yra neperspektyvus?
15. Kokie yra teisinio nano-, bio- ir kitų naujųjų technologijų reguliavimo pagrindiniai panašumai ir skirtumai?
16. Kokių teisinių grėsmių kelia dirbtinis intelektas ir autonominiai robotai?
17. Ar teisines taisykles galime paversti techninėmis komandomis, kurioms paklustų dirbtinis intelektas ir autonominiai robotai?

/XII/ *skyrius*

Elektroniniai demokratijos instrumentai

/ 535–557 / *puslapiai*

1 skirsnis. E. demokratija: paprasta ar sudėtinga?

> *Jūs – šio pasaulio studentai, niekada nepamirškite, kad už kiekvienos naudojamos technologijos yra kažkas, kas ją naudoja, ir tas kažkas yra visuomenė. ... Technologija yra ginklas, o visi, kas mano, kad pasaulis nėra toks tobulas, koks jis turėtų būti, privalo kovoti, kad technologijų ginklas būtų panaudotas visuomenės gerovei sukurti. ... Kiekviena technologija turėtų būti naudojama taip, kad būtų sukurta gerovė kuo didesniam žmonių skaičiui, kad mes galėtume kurti ateities visuomenę, nesvarbu, kokiu vardu ji būtų vadinama.*
>
> ERNESTO (Che) GUEVARA DE LA SERNA
>
> 1963 m. rugsėjo 29 d. kalbos, skirtos architektūros studentų tarptautiniam suvažiavimui, ištrauka.

Terminas „demokratija“ (graikiškai „demos“ (liaudis) + „kratos“ (valdau) reiškia tokią valdymo formą, kai visi piliečiai turi lygią teisę dalyvauti valdant šalį. Šią teisę piliečiai tiesiogiai įgyvendina per referendumus arba per savo išrinktus atstovus. Nors ir nėra tikslaus, visuotinai priimtino demokratijos apibrėžimo, lygybė ir laisvė nuo seniausių laikų yra svarbiausi demokratijos principai. Šie principai įgyvendinami, kai saugoma visų piliečių lygybė prieš įstatymą ir ginamos vienodos politinės teisės (pvz., balsavimas ir kandidatavimas).

Demokratijos funkcionalumas ir esmė kinta nuo pat jos atsiradimo istorijos, visus 2 500 metų. Klaidinga būtų manyti, kad demokratija buvo įvesta vienintelį kartą ir visiems laikams liko nepakitusi. Demokratijos procesas ne kartą buvo keičiamas ir naudojamas skirtingose visuomenėse, o demokratijai įgyvendinti buvo pasitelkiamos skirtingos formos ir instituciniai demokratijos įgyvendinimo mechanizmai. Pasaulio istorinė raida, sparčiai besiplėtojančios ir pasaulyje naudojamos technologijos lemia, kad demokratijos įgyvendinimo procesas ir formos kinta nuo pat senovės iki šių laikų, o galutinis demokratijos vystymosi etapas dar tikrai nėra pasiektas ir net neįsivaizduojama, kaip gali atrodyti „šiuolaikinė ateities“ demokratija po dviejų ar trijų dešimtmečių.

Demokratiniai procesai iš esmės apima informacijos srautų judėjimą ir komunikacijos tarp visuomenės sluoksnių praktiką, todėl galima teigti, kad pastarieji du dešimtmečiai turėjo ypač daug įtakos demokratijos kaitos procesams, nes būtent šis laikotarpis yra siejamas su didžiausiu techniniu progresu, kurį lėmė informacinių ir komunikacinių technologijų proveržis

pasaulyje bei globalizacija. XX a. pabaigoje ir XXI a. pradžioje atsirado ir sparčiai plėtojosi internetas bei kitos modernios informacinės ir telekomunikacinės technologijos. Tai laikotarpis, kuris pakeitė visuomenės tarpusavio bendravimo ypatumus, informacijos sklaidos ir prieinamumo bei pasiekiamumo, visuomenės nuomonės reiškimo galimybes. Jį drąsiai galima vadinti visuomenės skaitmenizacijos laikotarpiu, kuriam galioja tam tikri nuo įprasto, skaitmeninėmis technologijomis nepagrįsto bendravimo besiskiriantys, skaitmeninės informacijos sklaidos, prieinamumo ir jos vertinimo visuomenėje dėsniai, pvz., keitimasis informacija tarp visuomenės atstovų, vienas nuo kito esančių už kelių tūkstančių kilometrų, arba bendravimas keliais komunikavimo kanalais vienu metu.

Informacinių ir telekomunikacinių technologijų plėtra šiuolaikinėje visuomenėje yra labai sparti, ir visos šiuolaikinio gyvenimo sritys yra neįsivaizduojamos be šių technologijų naudojimo. Tačiau pasauliniu mastu šių technologijų naudojimas demokratijos procesams užtikrinti dar nėra toks dažnas reiškinys. Galima teigti, kad visuomenėje demokratijos procesas dažniausiai yra siejamas su rinkimais ir savo valios pareiškimu balsavimo metu. Pats balsavimo procesas ir jo rezultatų skaičiavimas egzistuoja ne vieną dešimtmetį, tačiau visuomenė nuolat ieško galimybių, kaip, naudojantis technologiniais išradimais, supaprastinti šiuos abu procesus.

Elektroninio balsavimo istorija prasideda maždaug nuo XIX a. vidurio, kai buvo pradėtas naudoti telegrafas. Šis balsavimo sistemų tobulinimo etapas vyko iki XX a. pradžios ir yra siejamas su išradimais, kuriuos padarė šie pasaulio mokslininkai: De Brette'as, W. Siemensas, T. Edisonas, J. Meyris. Minėtieji mokslininkai savo darbais siekė patobulinti balsavimo procesą, naudojant elektromechaninius ir mechaninius prietaisus. Šį elektroninio balsavimo plėtros etapą galime vadinti balsavimo idėjų atsiradimo ir plėtojimo etapu.

Kitas elektroninio balsavimo plėtros etapas yra siejamas su mums dabar jau įprastų technologijų plėtros etapu, kuris prasidėjo po antrojo pasaulinio karo. Šį laikotarpį galima pavadinti e. balsavimo priešistore. Šiuo metu buvo iš esmės suformuluotos idėjos ir žengti pirmieji žingsniai kuriant šiuolaikines elektroninio balsavimo sistemas, kurių veikla yra paremta naujausių informacinių ir telekomunikacijų technologijų plėtros aspektais: buvo pradėtas masiškai gaminti pirmasis kompiuteris IBM 650 (1953 m.), atsirado *ARPANET* tinklas, plačiajai visuomenei buvo pristatytas pasaulinis interneto tinklas (1990 m.). Svarbiausi šio laikotarpio įvykiai, turėję įtakos balsavimo sistemų evoliucijai, gali būti siejami su E. Frommu, kuris 1955 m. apibūdino situaciją, kai susitikimuose dalyvaujantys asmenys, naudodamiesi techniniais įrenginiais, galėjo pareikšti savo nuomonę apie tam tikrus per

visuomenės susitikimus svarstytus klausimus, ir su pirmosios sistemos, kuri buvo panaši į kompiuterinę elektroninio balsavimo sistemą (M. Turoffo 1970 m. sukurta *EMISARI* (angl. *Emergency Management Information System and Reference Index)* ir buvo skirta kompiuterinėms konferencijoms, atsiradimu. Ši sistema leido vartotojams svarstyti jiems aktualius klausimus ir reikšti savo nuomonę. Galima teigti, kad *EMISARI* sistema tapo elektroninių informacijos apsikeitimo sistemų prototipu ir sudarė palankias sąlygas ateityje svarstyti elektroninių rinkimų organizavimo galimybes.

Trečiąjį elektroninių balsavimų plėtros etapą, prasidėjusį paskutiniuoju XX a. dešimtmečiu ir vykstantį iki dabar, galima pavadinti šiuolaikinių e. balsavimo technologijų ir i. balsavimo (internetinio balsavimo) atsiradimo bei plėtros etapu. Šiuo laikotarpiu daug pasaulio šalių išbandė technologijas, kurios palengvino balsavimo ir balsų skaičiavimo procesus, vykdydamos balsavimo procesą pasinaudojo naujausiomis informacinėmis ir telekomunikacijų technologijomis. Laikotarpis nuo 2000 m. ir iki šių dienų iš esmės yra elektroninio balsavimo sistemų plėtros ir nesėkmių metas. Vienos šalys, pvz., Estija, yra sukūrusios ir naudoja savo rinkimų sistemą bei nesiruošia jos atsisakyti, o kitos, pvz., Nyderlandai, atsisako tam tikrų elektroninių rinkimų technologijų. Šis laikotarpis elektroninių rinkimų raidai yra įdomus tuo, kad ateityje galima sulaukti tam tikrų netikėtų sprendimų: interneto technologijomis pagrįstos balsavimo sistemos gali tapti vienintelės rinkimams naudojamos sistemos, jos gali būti transformuojamos į mobiliųjų technologijų balsavimo sistemas ir pan., o gali tiesiog išnykti, nors tai ir nelabai tikėtina.

Kaip jau buvo pabrėžta anksčiau, pats demokratijos procesas ir jo funkcionalumas nėra statinis, bet kinta ilgiau nei 2 500 metų, o rinkimai yra svarbiausias demokratijos elementas, kuris atspindi visuomenės valią vykstant demokratijos funkciniam procesui. Siekiant parodyti demokratijos mechanizmo kaitą visuomenėje, galima pateikti demokratijos proceso kaitą visuomenės vystymosi kontekste. Pavyzdžiui, svarbiausias pirmykštės demokratijos proceso požymis – daugumos susirinkusių visuomenės individų pritarimu priimami demokratijos sprendimai, o susirinkimuose galėjo dalyvauti visi visuomenės nariai. Kitas demokratijos plėtros etapas gali būti tapatinamas su visuomenės atstovų, kurie buvo renkami kaip visuomenės sluoksnių nuomonės reiškėjai, dalyvavimu priimant sprendimus. Šis modelis pradėtas įgyvendinti XVIII a. pabaigoje ir ilgainiui tapo pagrindiniu modeliu, kuris užtikrina demokratijos procesą šiuolaikinių demokratinių valstybių valdymo kontekste. Šių modelių pritaikymas demokratijos procesams yra vadinamas pirmąja ir antrąja demokratijos transformacija (*Dahl*, 1989). Šiuo metu, kai yra matomas visuomenės politinio susidomėjimo ir

aktyvumo rinkimų metu sumažėjimas bei padidėjęs naujausių informacinių ir telekomunikacinių technologijų skverbimasis į visas gyvenimo sritis, galime kalbėti apie vykstančią trečiąją demokratijos transformaciją – elektroninės demokratijos šiuolaikinėje visuomenėje atsiradimą ir plitimą (*Krimmer, Triessnig, Volkamer*, 2007).

K. Annanas yra pasakęs, kad „...nors demokratija ir turi būti daugiau negu laisvieji rinkimai, taip pat yra tiesa, ... kad ji negali būti ir mažesnė". Svarbiausias demokratijos požymis yra rinkimai, jų metu visa visuomenė gali pareikšti savo nuomonę, o šiuolaikinių informacinių ir telekomunikacinių technologijų proveržis atveria plačias galimybes naujos demokratijos rūšies – e. demokratijos ir jos „ramsčio" e. rinkimų – plėtrai pasaulyje.

Kaip jau buvo minėta anksčiau, šiuo metu e. balsavimo ir i. balsavimo technologijos sparčiai skverbiasi į mūsų gyvenimą. Turbūt nėra nė vienos pasaulio šalies, kuri negalvotų apie e. demokratijos įgyvendinimą ir informacinių bei telekomunikacinių technologijų pritaikymą balsavimams, tačiau reikia pabrėžti, kad ne visos šalys, įgyvendinusios idėją rinkimams naudoti elektronines balsavimo sistemas, vienodai taiko šiuolaikines technologijas. Kai kurios šalys (JAV, Brazilija, Vokietija), mėginančios modernizuoti savo rinkimų sistemas, yra priėmusios sprendimą naudoti technologines priemones balsavimo apylinkėse, o kitos valstybės (Estija, Austrija) naująsias technologijas naudoja nuotoliniams balsavimams.

Svarbiausias dalykas, kuris lemia valstybės galimybes modernizuoti savo balsavimo sistemas, yra teisinis elektroninio balsavimo proceso reglamentavimas, susijęs su šalies rinkimų įstatymo pakeitimu. Pvz., Brazilija savo rinkimų sistemą reformavo XX a. paskutiniuoju dešimtmečiu – nuo 1996 m. pradėjo naudoti elektroninio balsavimo sistemas. Kanadoje municipalitetų rinkimams e. balsavimo sistemos naudojamos nuo 1990 m., tačiau tai nėra visuotiniams šalies rinkimams pritaikyta sistema – vis dar yra naudojami ir popieriniai rinkimų biuleteniai. Australijoje elektroninės rinkimų sistemos pradėtos naudoti nuo 2001 m., kai 2000 m. gruodį buvo papildytas rinkimų įstatymas. Indija pirmą kartą elektroninio balsavimo technologijas pritaikė 1982 m. rinkimams Keralos provincijoje. Vėliau Indijos Aukščiausiasis Teismas pripažino, kad elektroninių balsavimo technologijų naudojimas prieštarauja įstatymams. Tik po aštuoniolikos metų buvo priimti Indijos rinkimų įstatymo pakeitimai ir nuo 2003 m. visi rinkimai Indijoje yra vykdomi naudojant elektroninius įrenginius. JAV nuo 1990 m. elektroniniai įrenginiai per rinkimus yra naudojami skirtingose valstijose. Kiekviena valstija gali pati pasirinkti, ar ji pasitelks elektroninius prietaisus rinkimams. Senojo žemyno šalys elektroniniais rinkimais pradėjo rimtai domėtis apie 2000 metus. Šiose valstybėse buvo keičiami

teisės aktai, leidžiantys elektroninius įrenginius aprobuoti rinkimų apylinkėse ir rinkimams naudoti interneto technologijas. XX a. pabaigoje XXI a. pradžioje Norvegija, Nyderlandai, Portugalija, Jungtinė Karalystė, Airija, Vokietija, Prancūzija padarė savo teisės aktų, reglamentuojančių rinkimus, pakeitimus tam, kad būtų galima atlikti elektroninių rinkimų sistemų bandymus. 2004 m. ES buvo patvirtinta rekomendacija „Dėl teisinių, organizacinių ir techninių normų, taikomų rinkimuose balsuoti elektroniniu būdu“. Šis dokumentas teikia rekomendacijas ir nusako pagrindines gaires, kurios yra labai svarbios organizuojant elektroninius rinkimus.

Patį svariausią žingsnį pasaulinės e. demokratijos link žengė Estija, ji 2005 m. pirmoji organizavo teisiškai pripažintus rinkimus, kuriems buvo naudojamos interneto technologijos, tačiau i. balsavimo Estijoje kelias nebuvo paprastas. Keletą mėnesių prieš 2005 m. rinkimus Estijos prezidentas Aukščiausiajam Teismui pateikė i. balsavimo sistemos nuostatus, kad gautų išaiškinimą, ar asmenys, balsuojantys elektroniniu būdu ir galintys vėliau pakeisti savo sprendimą, neįgyja pranašumo prieš asmenis, nesinaudojančius e. rinkimais. Konstitucinis Teismas priėmė sprendimą, kuris leido Estijai naudoti i. balsavimo mechanizmus vykdant šalies demokratinius procesus.

Lietuvoje nuo 2006 m. elektroninių balsavimo sistemų naudojimo idėja vis iškyla į viešumą – nors tais metais buvo patvirtinta balsavimo internetu per rinkimus ir referendumus koncepcija, iki šiol nėra priimti atitinkamų teisės aktų pakeitimai, kurie leistų naudoti elektronines priemones balsavimams Lietuvoje, tačiau 2015 m. vasarį Lietuvos Respublikos Vyriausybė pritarė siūlymui įteisinti balsavimą internetu.

Nors jau buvo pabrėžta, kad elektroniniai ir internetiniai rinkimai yra viena iš e. demokratijos formų, būtina akcentuoti, kad e. rinkimai iš esmės yra trečias ir pats svariausias žingsnis e. demokratijos link. Piliečių įtraukimas į demokratinius ir sprendimų priėmimo valstybėje procesus, be abejo, yra vienas iš svarbiausių naujojo valdymo uždavinių, bet jis nėra išsprendžiamas tol, kol pasaulio šalių vyriausybės yra nutolusios nuo savo rinkėjų.

A. Wiliamsonas yra pabrėžęs, kad paskutiniaisiais XX a. dešimtmečiais įvyko radikalus visuomenės pokytis, kurio svarbiausias aspektas buvo visuomenės kultūros kaita ir judėjimas nuo bendruomenės prie individualizmo. Pasak jo, mes jau esame ne tik piliečiai, bet ir vartotojai. Viešųjų paslaugų supratimo kaita, naujosios viešosios vadybos atsiradimas, visuomenės pasikeitimas sutapo su technologijų revoliucija, ir viso to padarinys – valdininkų nutolimas nuo visuomenės. Valdžios struktūros, net ir mėgindamos konsultuotis su piliečiais, dažniausiai nepaiso jų nuomonės ir labiau pasitiki ekspertais bei konsultantais, nors šie ekspertai paprastai būna prieš tai

valdžiusių vyriausybių atstovai. Moksliniai tyrimai ir rinkimų rezultatai rodo, kad visuomenės domėjimasis politiniu gyvenimu yra gerokai sumažėjęs ir būtent dėl šios priežasties politinės kampanijos tampa vis labiau panašios į prekių ženklų valdymo ir rinkodaros triukus (*Williamson*, 2011).

Mokslininkai yra pabrėžę, kad dauguma piliečių savo politinę apatiją stengiasi pateisinti padidėjusiu gyvenimo tempu ir laiko stoka, tačiau tai nėra didžiausia problema. Svarbiausia piliečių nedalyvavimo politiniuose procesuose priežastis – valdžios nenoras įtraukti juos į sprendimo priėmimo procesą. Nors valdžia ir pripažįsta, kad naujosios technologijos atveria naujus e. demokratijos horizontus, tačiau šių technologijų naudojimas nėra toks paprastas ir jis neužtikrina staigaus visuomenės įtraukimo į šalies politinius procesus.

S. Cliftas (*Clift*, 2004) yra pabrėžęs, kad šalių vyriausybės turi būti aktyvios ir tarti lemiamą žodį dėl e. demokratijos įgyvendinimo, nes jos yra viešąjį interesą formuojančios institucijos ir demokratijos garantas. Užtikrindamos e. demokratijos plėtros procesus vyriausybės turi:

1. Valdyti šiuolaikinius jau egzistuojančius demokratinius procesus ir stengtis palaikyti jų įgyvendinimą e. erdvėje, nepaisydamos jokio pasipriešinimo, kuris atsiranda dėl greitos informacinių ir telekomunikacinių technologijų raidos ir visuomenės nepasitikėjimo šiomis technologijomis demokratijos įgyvendinimo kontekste.
2. Inkorporuoti ir adaptuoti numatomas e. demokratijos strategijas ir tikslus taip, kad jos galėtų patenkinti ir išplėsti dalyvaujamosios demokratijos principus, tokiais būdais ir metodais būtų suteikta galimybė į demokratinius procesus įtraukti kiek galima daugiau piliečių.

Piliečių įtraukimas į dalyvaujamosios demokratijos procesą gali užtikrinti, kad pasaulio šalių vyriausybės tinkamai atsižvelgs į piliečių nuomonę, be to, galės tinkamai konsultuotis su piliečiais bei tiksliai ir greitai reaguos į jų teikiamus siūlymus bei pateisins jų lūkesčius.

Šiuolaikinės visuomenės kelias e. demokratijos link yra sunkus, tačiau neišvengiamas. Būtina prisiminti, kad vien tik informacinių technologijų naudojimas nėra panacėja, ir jis neužtikrins greito ir paprasto ėjimo visuotinio dalyvavimo proceso link. Elektroninės demokratijos įgyvendinimas yra sunkus kelias, tačiau jeigu einama apgalvotais maršrutais ir konkrečiai nustatytais etapais, tikslas tikrai bus pasiektas.

Analizuojant e. demokratijos įgyvendinimo perspektyvą iš valdžios pozicijos reikėtų atkreipti dėmesį į keturis svarbiausius aspektus, kuriais valdžios institucijoms būtina vadovautis tikintis sėkmingo proceso:

1. Suprasti dabartinius politinius procesus, vykstančius e. erdvėje, ir nustatyti aiškius šių procesų kitimo matavimo kriterijus. Šie kriterijai privalo būti nukreipti ne tik į valdžios institucijų veiklos vertinimą, bet ir į piliečių patirties apibendrinimą bei jų nuomonės analizę.
2. Dokumentuoti valdžios institucijų įgyvendintas gerąsias praktikas ir jomis dalytis viešojoje erdvėje.
3. Pasistengti sukurti visuomenę, kurios svarbiausias tikslas – politinio ir visuomeninio aktyvumo patenkinimas, kitaip tariant, stengtis sukurti politiškai brandžią ir visuomeniškai aktyvią visuomenę.
4. Naudojantis sukaupta patirtimi ir gerosiomis praktikomis kurti įrankius bei galimybes visuomenei aktyviau dalyvauti demokratijos procesuose (*Clift*, 2004).

Kaip jau buvo minėta, šiuolaikinės informacinės ir telekomunikacinės technologijos atveria plačiausius kelius pertvarkyti visuomenei suprantamus demokratijos procesus į naujuosius e. demokratijos, kitaip dar vadinamos dalyvaujamosios demokratijos, principus. Tačiau naivu tikėtis, kad vien tik technologijų naudojimas gali pakeisti visuomenės požiūrį. Elektroninės demokratijos formavimas grįstas tik žmogiškuoju faktoriumi, kitaip tariant žmogaus poreikiai ir savęs supratimas yra svarbiausias aspektas, formuojantis e. demokratijos procesus visuomenėje, o informacinės ir telekomunikacinės technologijos yra tik „šios cheminės reakcijos katalizatorius“. Be individų motyvacijos ir noro ką nors keisti visuomenėje ar politinėje šalies struktūroje ir tam naudoti šiuolaikines telekomunikacines technologijas, negalimas joks naujos demokratijos formos atsiradimas ar plėtra.

e. demokratijos samprata

e-demokratija yra labai platus procesas, kurio tikslai ir funkcijos yra skirtingai vertinami įvairių pasaulio mokslininkų. Nėra bendro e. demokratijos apibrėžimo, keletas jos sąvokų yra pateikiama žemiau:

- e. demokratija yra procesas, kurio metu vykdomas visuomenės informavimas, komunikavimas su visuomene ir jos įtraukimas į šalies politinių sprendimų priėmimo procesą, ilgainiui pakeičiant politinių debatų ir šalies politinės sistemos esmę. Elektroninės demokratijos proceso dalyviai šiame kontekste yra ne tik politinės partijos ir jų atstovai, bet ir vyriausybinės organizacijos, visuomenės atstovai (organizacijos ir individai).
- e. demokratija turėtų būti plačiai plėtojama ir įtraukiama į šalies politinius procesus, nes dabartinių *ITT* plėtra glaudžiai siejama su šalių politinių ir valdymo procesų kompiuterizavimu. Vienas iš svarbiausių e. demokratijos tikslų – pakeisti visuomenės nuomonę dėl

dalyvavimo šalies politiniame gyvenime ir paskatinti ją aktyviau bendradarbiauti su valdžia. Šis bendradarbiavimas neturi apsiriboti tik e. rinkimų organizavimu, jis turi aprėpti ir gyventojų informavimą bei konsultavimąsi su jais formuojant šalies vidaus politiką. Siekiant įgyvendinti aukščiau minėtus tikslus, didžiausią vaidmenį atlieka techninė revoliucija, kuri vyksta pastaruosius du dešimtmečius.

- e. demokratija yra instrumentas. Pasitelkus *ITT*, jis leidžia įtraukti piliečius į dialogą su valdžia ir įgalina juos bendradarbiauti su tais asmenimis, kuriems jie suteikė politinę galią, naudojamą siekiant pagerinti piliečių gyvenimą, keičiant visuomenės informavimą ir skatinant naują politinį dialogą tarp valdžios atstovų ir visuomenės. Elektroninė demokratija nėra paskirtos baudos mokėjimo už greičio viršijimą kelyje surinkimo instrumentas (t. y. e. valdžios paslaugų teikimas), ji yra konsultavimosi su visuomene priemonė, kuri gali padėti nustatyti, koks greitis ar kelio ženklas turi būti įrengtas tam tikrame kelio ruože. Elektroninė demokratija yra įrankis, kuris ateityje turi būti naudojamas kaip priemonė, suteikianti visuomenei galimybę dalyvauti priimant svarbiausius šaliai ir nacionalinei politikai sprendimus.
- e. demokratija yra įrankis, kuris įgalina vyriausybes palengvinti piliečių dalyvavimą šalies valdyme naudojant skaitmenines ir telekomunikacines technologijas. Šis procesas gali būti paskatintas naudojantis tokiomis priemonėmis kaip e. forumai, e. konsultacijos, e. referendumai, e. balsavimas ir kt.
- e. demokratija yra informacinių ir telekomunikacinių technologijų naudojimas vykstant vietos valdžios, regiono, šalies ar globaliems politiniams procesams, kai į juos įtraukiamos vyriausybės, tautos išrinkti politikai, žiniasklaida, politinės partijos, interesų grupės, visuomeninės organizacijos, tarptautinės politinės institucijos ir piliečiai.
- e. demokratija dar yra apibrėžiama kaip „vyriausybė, kurioje aukščiausioji valdžia priklauso tautai ir vykdo tautos valią, pareikštą tiesiogiai arba netiesiogiai per atstovavimo sistemas“. Elektroninė demokratija yra paprasčiausias technologinių priemonių naudojimo būdas, siekiant palengvinti demokratinių procesų vyksmą.
- e. demokratija ir internetas suteikia galimybę ir parodo būdą, kaip „perkrauti“ (angl. *upload)* demokratinius procesus šalyse ir atgaivinti teigiamus santykius tarp piliečių ir jų išrinktų valdžios atstovų.

Galima pabrėžti, kad anksčiau pateikiamos e. demokratijos sąvokos dažniausiai apima skirtingus dalykus, tačiau svarbiausias jas susiejantis tikslas gali būti vienareikšmiškai įvardijamas: e. demokratija – tai procesas, kurio metu naudojant elektronines technologijas ir komunikacijos kanalus siekiama išplėsti demokratijos galias ir į sprendimo priėmimo procesą įtraukti kiek galima daugiau piliečių. Galima sakyti, kad svarbiausias e. demokratijos siekis – pakeisti nusistovėjusias politines sistemas ir ateityje pereiti prie hibridinės valdymo formos, kurios pagrindiniais veikėjais taptų politikai, tiesiogiai besikonsultuojantys su savo rinkėjais.

Pasaulyje buvo ir yra vykdoma daug projektų, susijusių su e. demokratija. Mokslininkai nagrinėjo ir nagrinėja e. demokratijos procesus, tačiau dauguma iš jų pritaria idėjai, kad didžiausia e. demokratijos įgyvendinimo kliūtis yra technologijos. Kad ir kaip paradoksaliai tai skambėtų, tačiau technologijos, kurios skatina e. demokratiją, tuo pat metu ir sukelia kliūčių jos plėtrai. Technologijos, kurios yra naudojamos įgyvendinant e. demokratijos procesus, nėra neutralios: jos gali būti naudojamos kaip gerinantis ar bloginantis veiksnys ir tas veiksnys priklauso tik nuo to asmens ar grupės, kuri tą technologiją valdo ir kontroliuoja. Mokslininkai sutaria, kad pasitikėjimas technologijomis, naudojamomis e. demokratijos procesams, yra labai svarbus aspektas, tačiau žmonių pasitikėjimas technologijomis ar nepasitikėjimas jomis dažniausiai kyla dėl jų nesuprantamumo. Naujosios technologijos priemonės, organizuojant e. demokratijos procesus, taip pat ir e. valdžios paslaugas, turi būti viešinamos ir pristatomos visuomenei naudojantis šiuolaikinėmis e. rinkodaros technologijomis.

e. demokratijos plėtros kliūtys.

Moksliniuose šaltiniuose yra pabrėžiama, kad per mokslininkų diskusijas buvo nustatytos keturios grupės kliūčių, galinčių turėti įtakos e. demokratijos plėtrai. Kliūtys yra šios: politinės, dalyvavimo, organizavimo ir technologinės.

Politinės e. demokratijos kliūtys.

Per pasaulio mokslininkų diskusijas buvo išskirtos keturios politinių kliūčių grupės:

- Apibrėžtumo. Pasaulio mokslininkai laikosi keleto pozicijų, susijusių su e. dalyvavimu *(Williamson*, 2011). Kai kurie iš jų mano, kad e. dalyvavimas turi būti e. valdžios informacinėmis ir ryšio technologijomis (internetu) teikiamų viešųjų e. paslaugų dalimi, kiti mokslininkai oponuoja, kad e. dalyvavimas yra atskira funkcinė valdžios sritis, kurios pagrindinis komunikavimo įrankis yra šiuolaikiškos ryšio technologijos. Taigi galima teigti, kad net tarp pasaulio mokslininkų nėra bendro sutarimo ir yra „painiava (...)

tarp dviejų sričių e. demokratijos ir e. administracijos (...). Šių terminų esminis skirtumas yra tas, kad e. administravimas iš esmės yra valdžios jau dabar vykdoma funkcija, o e. demokratija yra siektinas dalykas, kurio tikslas – pagerinti demokratinius procesus pasitelkiant komunikacijas" *(Williamson*, 2011). Mokslininkai teigia, kad realus piliečių dalyvavimas, vykstant e. demokratijos procesams, priklauso nuo valdžios noro įtraukti juos į patį valdymo procesą. Mokslininkai išreiškė nuomonę, kad svarbiausias e. dalyvavimo populiarumo kaitos rodiklis labiausiai priklausys nuo valdžios instituto, o konkrečiau, nuo valdžios iniciatyvos ir sprendimų, apie ką ir su kuriais visuomenės atstovais ir kokiais pagrindais diskutuoti.

- Institucinė. Politikai ir valdininkai mano, kad e. demokratija yra pavojinga (bent jau jos įgyvendinimo pradžia). Valdžios institucijos ir politikai bijo bendradarbiavimo su piliečiais neišmėgintais būdais: nežino, kokia bus piliečių ir visuomenės reakcija, negali prognozuoti politinių ir institucinių procesų kaitos įdiegus šalyje tokius procesus. Tai yra vienas iš aspektų, kuriuos pabrėžia mokslininkai: įdiegta e. demokratija tikrai gali pradėti veikti ir tada teks atsižvelgti į visuomenės sprendimus, kad ir kokie nepatogūs politiniams procesams jie būtų. Iš esmės reikalinga nuodugni struktūrizuota galimų pasikeitimų analizė, tačiau šią analizę turi atlikti ne valdžia ar valdžios pasamdyta verslo organizacija ar ekspertai. Mokslininkai pabrėžia, kad šios analizės iniciatoriai turi būti valdžios, mokslo ir visuomenės atstovų „konglameratas", o tyrimo rezultatai gali tapti gairėmis, kurios leistų patobulinti šiuolaikinį valdymą, nes svarbiausias e. demokratijos tikslas, pasak mokslininkų, yra ne valdžios kaita, o jos pritaikymas ir patobulinimas, atsižvelgiant į šiuolaikiško gyvenimo realijas.
- Kompleksiškumo. Elektroninės demokratijos plėtros praktikos kompleksiškumo stoka šalyje lemia skirtingus jos įgyvendinimo aspektus, į kuriuos atsižvelgiama įgyvendinant e. demokratiją vietos ir šalies valdžios institucijų lygiu. Mokslininkai *(Williamson*, 2011) teigia, kad diegiant e. demokratijos procesus yra būtinas aukščiausių šalies politinių jėgų palaikymas. Dažnai yra girdimos diskusijos ir politikų nuomonės dėl e. demokratijos procesų įdiegimo į šalies valdymo sistemą. Lietuvoje net buvo žengtas žingsnis e. rinkimų sistemos sukūrimo ir jos naudojimo įteisinimo link, deje, šie žingsniai dažnai būna paskutiniai, kurios žengia aukščiausioji šalies valdžia, o jų pažadai ir norai netampa realybe. Ši problema yra didžiulė e. demokratijos plėtros kliūtis ir galima drąsiai teigti, kad be tvirto

politinio nusiteikimo, politinės valios ir e. demokratijos palaikymo aukščiausiuose valdžios sluoksniuose šio proceso neįmanoma įgyvendinti.

- Viešumo. Pasaulio mokslininkai pabrėžia, kad e. demokratijos viešumas yra sveikintinas, tačiau naujosios technologijos iš dalies ne tik skatina, bet ir stabdo e. demokratijos plėtrą. Norėdama paskatinti e. demokratijos procesą, pati visuomenė turi aiškiai suvokti, kaip viskas veikia. A. Lupia teigia, kad yra trys didelės e. demokratijos ir e. dalyvavimo procesų kliūtys: dėmesio stoka (didelis mus supančios informacijos kiekis sumenkina informacijos apie e. demokratiją pateikimą visuomenei), patikimumo stoka (žmonės nepasitiki politikais) ir susivienijimo stoka (visuomenės neorganizuotumas). T. Westenas pabrėžia, kad visuomenėje dar egzistuoja ir žinojimo stoka, kai žmonėms nelabai suprantama pačių politinių procesų eiga ir jie nežino, kas, kodėl ir kaip gali jai atstovauti. Kol piliečiai nesupras, kaip veikia politinė sistema ir kas jai atstovauja, jiems nebus aišku, ir kaip veikia e. demokratija.

Dalyvavimo kliūtys.

Pasaulio mokslinėje literatūroje labai daug rašoma apie kliūtis, kurios lemia pasyvų žmonių dalyvavimą šalių politiniuose procesuose. Tokios kliūtys būdingos ir e. demokratijai. Didžiausia mokslininkų pabrėžiama problema yra elektroninė atskirtis ir naujųjų technologijų naudojimo kultūros stoka, kurią lemia tam tikri demografiniais aspektai (amžius, tautybė ir kt.). Antra problema yra tai, kad žmonės siekia individualumo e. demokratijos kontekste ir dauguma norėtų spręsti tik sau aktualias problemas. Trečioji mokslininkų įvardijama problema yra piliečių nesupratimas, kaip jie, pasitelkę e. demokratiją ir e. dalyvavimą, gali veikti šalies politinius procesus. E. demokratija turi būti remiama, ir tik tada, kai piliečiai pamatys, kad jų nuomonė yra reikalinga politiniams procesams vykti ir į tą nuomonę yra atsižvelgiama, jie taps kur kas aktyvesni ir labiau suinteresuoti e. demokratijos plėtra.

Organizavimo kliūtys.

Mokslininkai pabrėžia, kad e. demokratijos procesai ir projektai yra retokai pristatomi visuomenei. Reikalinga stipri socialinė rinkodara, kurios svarbiausias tikslas – išpopuliarinti e. demokratijos įgyvendinimo idėjas visuomenėje. Ši turi jaustis esanti ne žaislas politiko rankoje, o veiklos kryptį ir veiksmus politikui nurodantis instrumentas. Be to, mokslininkai pabrėžia, kad reikėtų vengti vykdyti e. demokratijos projektus tada, kai žinoma, kad jie yra pasmerkti žlugti. Dėl tokių nevykusių projektų visuomenė susidaro prastą nuomonę apie visą e. dalyvavimo ir e. demokratijos idėją.

Techninės kliūtys.

Esame įpratę, kad technologijos keičia mūsų gyvenimą ir e. demokratijos kontekste jos tampa savotišku jungtuku, kuris gali įjungti e. demokratijos procesus. Tačiau reikėtų nepamiršti vieno dalyko: technologijos yra tik įrankis, kuris, deja, nėra neutralus. Visos technologijos sukurtos tam, kad galėtų atlikti tam tikrą funkciją, o tos funkcijos tikslą žino tik jos kūrėjas. Judant e. demokratijos link reikėtų nepamiršti, kad to judėjimo negalima apriboti tik viena platforma – internetu. Būtina atsižvelgti ir į galimybes naudoti kitas technologines platformas: mobilųjį tinklą, televiziją ir kt.

Demokratijos procesas nuolat kinta nuo pat jos atsiradimo. Demokratijos kitimas nuo tiesioginės link atstovaujamosios buvo stebimas ilgą laikotarpį, tačiau šiuolaikinės technologijos ir jų skverbimasis į gyvenimą suteikia galimybę atstovaujamąją demokratiją keisti į hibridinį modelį, kai egzistuoja valdymas, kuris yra grindžiamas konsultavimusi su piliečiais. Šis modelis gali iš esmės pakeisti ne tik piliečių nuomonę, bet ir politines šalių sistemas.

2 skirsnis. Elektroninių rinkimų sistemos

Politinių partijų ir įvairių valstybių vyriausybių atstovai įžvelgė, kad pasaulyje atsiradęs visuotinis interneto tinklas ir informacinių technologijų plėtra gali reikšmingai veikti šalyse vykstančius politinius procesus. Kaip jau buvo minėta anksčiau, technologijos suteikė galimybę jas naudoti organizuojant rinkimus. Pirmieji mėginimai naudoti technologijas per rinkimų procesą buvo Brazilijos elektroninių rinkimų projektas, kuris buvo įgyvendintas per 1996 m. Brazilijoje vykusius parlamento rinkimus *(Krimmer, Triessnig, Volkamer*, 2007). Nors tai buvo rinkimų sistema, kuriai nenaudotos interneto technologijos, ji tapo vėliau sukurtos internetinės balsavimo sistemos prototipu *(Volkamer, Hutter*, 2004).

Galima teigti, kad e. balsavimas ir e. referendumai yra svarbiausi e. demokratijos įrankiai, kurie leidžia rinkėjams gana aktyviai dalyvauti politiniuose valstybių procesuose. Didėjant visuotinei kompiuterizacijai ir informacinių bei telekomunikacinių technologijų naudojimui, visuomenėje atsiranda ir didesnis domėjimasis šių technologijų naudojimu šalies politiniam gyvenimui. Internetinis balsavimas yra vienas iš būdų, kiek galima mažesnėmis pastangomis „priversti“ didesnę visuomenės dalį aktyviai dalyvauti šalies politiniuose procesuose. Be abejonės, tam, kad toks procesas būtų sklandus ir kuo didesnė visuomenės dalis, naudodamasi naujosiomis sistemomis, dalyvautų rinkimuose, visuomenei būtina išaiškinti visų e. rinkimų sistemų veikimo mechanizmus.

Europos Tarybos ministrų komitetas 2004 m. rugsėjo 30 d. per 898-ąjį deleguotųjų ministrų susitikimą patvirtino Valstybių narių Ministrų komiteto „Rekomendaciją (2004)11 dėl teisinių, organizacinių ir techninių normų, taikomų balsavimui rinkimuose elektroniniu būdu“.

Pabrėžiant, kad balso teisė yra vienas svarbiausių demokratijos principų, į visus kitus demokratinių rinkimų ir referendumų principus turėtų būti atsižvelgiama ir įdiegus e. rinkimų sistemas. Elektroniniai rinkimai turi būti saugūs ir patikimi *(Remmert*, 2004). Tam, kad e. balsavimo sistemos taptų patrauklios visuomenei ir ateityje papildytų ar pakeistų įprastines (popierines) balsavimo sistemas, joms turi būti taikomi šie esminiai ir neabejotinai svarbūs principai:

Visuomeniškumas ir visuotinis pripažinimas. Galimybė visiems balsavimo teisę turintiems rinkėjams užtikrinti dalyvavimą rinkimuose, o rinkėjų identifikavimą ir registraciją privalu atlikti teisėtomis priemonėmis. Ši nuostata iš esmės turi remtis penkiomis svarbiausiomis taisyklėmis:

- kiekvienas asmuo, turintis teisę pareikšti savo apsisprendimą, gali tai padaryti;
- galimybė dalyvauti rinkimuose turi būti užtikrinama juridiškai;
- balsavimo technologijos ir priemonės turi būti suprantamai paaiškintos rinkėjams ir neturi būti jokių ribojimų norint susipažinti su rinkimams naudojamomis technologijomis;
- e. balsavimas yra tik papildoma pagrindinio balsavimo priemonė;
- balsavimui naudojama infrastruktūra turi būti prieinama visiems rinkėjams (*Gritzalis*, 2002).

Pasirinkimo laisvės principas, užtikrinantis, kad rinkėjas, naudodamasis e. balsavimo sistema, nebuvo verčiamas to daryti, be to, reikšdamas savo nuomonę nebuvo ir technologiškai paveiktas. Iš esmės užtikrinant ši principą, turi būti atsižvelgiama į dar kelis aspektus: balsavimo sistema turi užtikrinti rinkėjui galimybę balsuoti „tuščiu biuleteniu“.

Lygybės principas. Turi būti užtikrinta rinkimuose dalyvaujančių partijų, kandidatų ir balsavimo teisę turinčių rinkėjų teisių lygybė. Svarbiausias e. balsavimo reikalavimas – ir popierinio, ir elektroninio variantų balsavimo biuleteniai turi būti identiški. Įgyvendinant šį principą, privaloma užtikrinti ir politinių partijų vienodą prieinamumo galimybę stebėti e. balsavimo sistemas ir pačią šių e. balsavimų trukmę. Kai kurie ekspertai e. balsavimo sistemas rekomenduoja įrengti taip, kad e. balsavimas įvyktų anksčiau nei „popieriniai“ rinkimai.

Slaptumo principas turi užtikrinti, kad visą laiką, kol vyks balsavimas, e. balsai būtų slapti, iki pat galutinio jų skaičiavimo, ir nė vienas asmuo

negalėtų susieti balsavusio žmogaus su jo balsu; būtų aiškiai atskirtos registravimosi balsuoti ir balsavimo fazės; vartotojas jokiomis priemonėmis, kurios yra susietos su balsavimo sistema, negalėtų teikti informacijos apie savo pasirinkimą. Būtina pabrėžti, kad slaptumo principas turi apimti ir tai, kad balsavimo sistemoje privalo būti sukonstruota tiksli balsų skaičiavimo ir, jeigu būtina, jų perskaičiavimo galimybė, neidentifikuojant balsavusiojo asmenybės (angl. *International Working Group for Data Protection*, 2001).

Tiesiogiškumo principas nusako būtinybę vykdyti rinkimus taip, kad kiekvienas balsas būtų tiesiogiai įrašytas ir suskaičiuotas. Siekiant neapkrauti e. balsavimo sistemų ir supaprastinti jų veikimą, dažniausiai visi per rinkimų procesą gauti balsai yra saugomi užkoduoti ir yra atkoduojami tik rinkimams pasibaigus.

Demokratijos principas. Šiuo principu privaloma užtikrinti e. balsavimo sistemų atitiktį įprastinių tradicinių balsavimo sistemų principams. Savaime suprantama, kad atsiranda tam tikrų specialiųjų reikalavimų, kurie turėtų būti taikomi e. balsavimo sistemoms. Šie reikalavimai apima kuriamų ar jau sukurtų e. balsavimo sistemų teisėtumą, skaidrumą, saugumą ir tikslumą. E. balsavimo sistemos naudotojai turi suprasti jos veikimo būdą, tačiau kartais to tiesiog neįmanoma padaryti, nes tam tikri individai neturi informacinėms technologijoms perprasti reikalingų elementarių žinių. Kitaip tariant, pasitikėjimas e. balsavimo sistemomis yra grįstas pasitikėjimu technologijomis ir balsuojančio asmens pasirengimu jas įsisavinti ir naudoti.

Lyginamoji elektroninių rinkimų sistemų modelių analizė

Elektroninių rinkimų sistemos gali būti skirstomos pagal tai, kiek ciklų privalu užbaigti rinkėjui, norinčiam pareikšti savo valią rinkimuose. Dauguma pasaulyje egzistuojančių šiuolaikinių e. rinkimų modelių yra skirstomi į vienos ir dviejų fazių, kartais vadinamų vieno ir dviejų ciklų modeliais. Be to, egzistuoja vadinamieji n-fazių (n-ciklų) modeliai, nes juos naudojant reikalaujama, kad rinkėjas, pareikšdamas savo valią rinkimuose, atliktų daugiau nei du balsavimo ciklus. Kiekviena balsavimų sistemos fazė numato tam tikrų rinkėjo veiksmų atlikimą konkrečiai nustatytu laiku. Visos fazės eina viena paskui kitą ir negali būti tarpusavyje keičiamos vietomis. Elektroninio balsavimo sistemos fazės nebūtinai turi atitikti fazes, kurios yra aprašytos techninėse specifikacijose (angl. *Election Markup Language, EML)*. Kai kurios iš šių fazių gali būti vienodos, tačiau kai kurios balsavimo modelio fazės gali būti visoje sistemoje sujungtos į keletą EML fazių. Pavyzdžiui, elektroninėje balsavimo sistemoje gali būti reikalaujama rinkėjo registracijos ir galimybės „atiduoti balsą“ už jam patinkantį kandidatą dviem skirtingais žingsniais (*Prosser, Kofler, Krimmer, Unger*, 2009). *EML* požiūriu, vartotojo registracija balsavimo sistemoje

atitinka pirmąją fazę, o pati balsavimo procedūra, vertinant iš elektroninių balsavimų sistemos modelio pozicijos, yra antroji fazė. Po rinkimų iškelti uždaviniai, esantys sistemoje ir aprašomi *EML*, nėra nagrinėjami, nes jie nėra reikšmingi rinkėjui *(Rössler*, 2004).

Vienos fazės modelis.

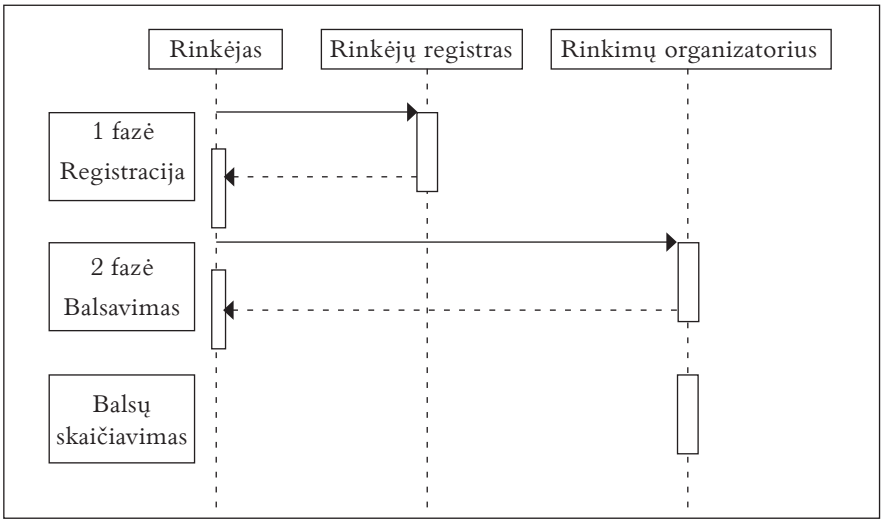
Vienos fazės modeliu grįstos e. balsavimo sistemos yra labai retos. Šio modelio esmė – rinkėjas, norintis pareikšti savo valią rinkimuose, tai gali padaryti vienu paprastu veiksmu. Taikiant tokius modelius, pradedančiam balsuoti rinkėjui nereikia savęs identifikuoti sistemoje e. priemonėmis. Žiūrint iš rinkėjo pozicijos, toks balsavimas vyksta vienu ciklu. Sunkiai įsivaizduojama, kaip galima pritaikyti tokiu modeliu grįstą balsavimo sistemą e. rinkimams, vykdomiems nuotoliniu būdu, nes visiškai neįmanoma užtikrinti, kad vartotojas nebalsuos daugiau kaip vieną kartą ir nebus pažeista nuostata, leidžianti pasitelkus elektroninių rinkimų sistemą balsuojančiam piliečiui „atiduoti balsą“ tik vieną kartą (angl. *Recommendation Rec(2004)11 of the Committee of Ministers)*. Iš esmės vienos fazės balsavimo sistemos modelis gali būti taikomas tik tiems e. rinkimams, kurie yra vykdomi kontroliuojamoje aplinkoje: rinkimų apylinkėse, balsavimo kioskuose ir kitose vietose, kur yra patikrinama prie balsadėžės patenkančio rinkėjo tapatybė. Nors tokia balsavimo sistema ir nėra tobula, ji vis tiek turi pranašumą prieš tradicinius „popierinius balsavimus“: rinkėjas, atėjęs į balsavimo apylinkę ir nuėjęs į balsavimo vietą, negalėtų sugadinti balsavimo biuletenio ir bet kuriuo atveju turėtų pareikšti savo valią, o jeigu būtų vykdomas balsų pirkimas rinkimų metu, rinkėjai neturėtų jokio įrodymo „balso pirkėjui“, kad balsavo būtent taip, kaip ir buvo sutarta. Šis e. rinkimų modelis nėra tobulas, bet jis gali būti derinamas ir taikomas kartu su dviejų fazių modeliu *(Rössler*, 2004).

Dviejų ir n-fazių modelis.

Dauguma pasaulyje naudojamų e. balsavimo sistemų yra grįstos dviejų fazių modeliu. Šis modelis yra pavaizduotas žemiau (žr. 11 paveikslą). Paprastai per pirmąją balsavimų modelio fazę rinkėjas privalo save identifikuoti balsavimų sistemoje, kuri jam išduoda tam tikrą „leidimą balsuoti“ ir tokiu būdu rinkėjas gauna priėjimą prie antrosios pagrindinės modelio fazės – balsavimo *(Rössler*, 2004).

Kartais tarp pirmosios (registravimosi) ir antrosios (pagrindinės) balso atidavimo fazių e. rinkimų sistema gali iš rinkėjo pareikalauti papildomų veiksmų. Vadinamuoju n-fazių modeliu balsuojantis asmuo gauna e. rinkimų sistemos pranešimus, kurie iš besiregistruojančiojo balsuoti reikalauja save identifikuoti keliose atsakingų institucijų identifikavimo sistemose, tai darant tam tikrais atskirais veiksmais. Esant tokiai situacijai, registravimosi

fazė yra padalijama į keletą žingsnių – tokia e. balsavimo sistema yra pagrįsta n-fazių modeliu.



11 pav. Dviejų fazių balsavimo sistemos modelis (*Rössler*, 2004)

Apibendrinant vienos, dviejų ir n-fazių e. rinkimų sistemų diegimo ypatumus ir įvertinant jų aukščiau įvardytus pranašumus ir trūkumus, galima teigti, kad gana kritiškai žiūrint į pasaulines rinkimų organizavimo tendencijas realiai gali būti svarstomos tik elektroninių rinkimų n-fazių modelio diegimo ir plėtojimo galimybės.

3 skirsnis. Elektroninių rinkimų sistemų saugumo problematika

Visos šalys supranta, kad e. rinkimai panaikina visas geografines tradicinių rinkimų sistemų ribas. Rinkimų sistemos nėra koncentruotos vienoje geografinėje vietovėje, rinkimų apylinkėje ir yra pasiekiamos iš bet kurio pasaulio taško. Tai gali gerokai padidinti elektroninių atakų, nukreiptų prieš elektroninio balsavimo sistemas, kiekį. E. rinkimų sistemos ir jose organizuojami procesai gali tapti labai patraukliu taikiniu asmenims, užsiimantiems neteisėta veika. Tiesioginio balsavimo sistemos privalo būti patikimos, turi pelnyti visuomenės pasitikėjimą, kurį suinteresuoti asmenys gali mėginti sugriauti, paversdami e. rinkimų sistemas „baisiąja rinkimų dienos istorija“ (*Crown Copyright*, 2002).

Norint sukurti patikimą ir gerai apsaugotą e. balsavimo sistemą, reikalingas ilgas ir kruopštus daugelio sričių specialistų: informacinių techno-

logijų, kompiuterių saugumo, informacinių sistemų projektuotojų, darbas, be to, būtina susilaikyti nuo bet kokių išankstinių prielaidų, prognozių ar spėlionių, kas galėtų nutikti, kai bus iki galo parengta ir įdiegta elektroninio balsavimo sistema. Nuomonė apie e. balsavimo saugumą yra suformuota remiantis e. balsavimo sistemos konfigūracija, tačiau šie duomenys yra viešai prieinami ir gali būti panaudoti sistemai sukompromituoti.

Be to, ypač svarbu išnalizuoti e. balsavimo sistemoms kylančias grėsmes ir atskleisti galimus jų „užpuolimo" būdus, kurie gali sukelti visuomenės nepasitikėjimą e. balsavimo sistemomis ir sužlugdyti jų diegimą ir naudojimą, vykdant rinkimų procesus.

Aukščiau išvardytos grėsmės gali būti skirstomos pagal jų sukėlėjų tipus. Trumpai tariant, grėsmės yra išorinės ir vidinės. Daugiau dėmesio visada yra skiriama išorinėms grėsmėms, tačiau tai nėra pati teisingiausia pozicija, kurios turėtų būti laikomasi, nes kur kas lengviau pažeisti sistemą iš vidaus. Tokie (vidiniai) įsilaužimai į kompiuterines sistemas, pasak mokslininkų, sudaro apie 80 proc. visų įvykdytų įsilaužimų *(Uselis*, 2000) ir tai tik tie, kurie buvo aptikti arba paviešinti.

Vidinės grėsmės

Išskiriamos trys pagrindinės grupės, kurios gali būti potencialūs vidinių grėsmių sukėlėjai:

- Pirmoji grupė yra teisėti e. balsavimo sistemų vartotojai. Jie gali ieškoti silpnų sistemos vietų arba saugumo spragų ir, turėdami užtektinai techninių žinių bei pakankamą jiems suteiktą suinteresuotų asmenų paskatą, pažeisti e. balsavimo sistemą. Dažniausiai šie veiksmai atliekami siekiant finansinės naudos.
- Antrajai grupei priklauso asmenys, kurie gali siekti pasinaudoti elektroninių balsavimo sistemų operatorių (administratorių) privilegijuotomis pozicijomis tam, kad gautų naudos dėl e. balsavimo sistemos pažeidžiamumo. Šios grupės atstovai dažniausiai siekia pasinaudoti valstybės tarnautojais arba kitų organizacijų darbuotojais, kurie kuria e. balsavimo sistemas. Tokie darbuotojai gali turėti pakankamai žinių ir priėjimą prie e. balsavimo sistemų. Pagrindiniai šių grėsmių sukėlėjų motyvai – gaunama finansinė nauda arba tiesiog asmeninis pasitenkinimas, savo talento atskleidimas vykdant neteisėtą veiką. Elektroninių balsavimo sistemų operatoriai ir valstybės tarnautojai turi būti morališkai pasirengę tokiems suinteresuotų piktavalių veiksmams, jeigu visa informacija apie saugumo skyles jiems yra pateikiama.
- Trečioji didelė grupė yra valstybės tarnautojai, kurie turi priėjimą prie e. balsavimo sistemų, tačiau nėra susiję su e. balsavimo

sistemos naudojimu. Šie asmenys gali patys dalyvauti organizuojant vidines e. balsavimo sistemos atakas arba joms vadovauti. Motyvai, dėl kurių šie asmenys gali vykdyti neteisėtą veiką, dažniausiai būna finansinio pobūdžio arba tiesiog siektini asmeniniai konkrečiai neįvardijami tikslai (*Crown Copyright*, 2002).

Išorinės grėsmės.

- Pavieniai programišiai, ieškantys, kaip neigiamai paveikti e. balsavimo sistemas vien tam, kad patirtų asmeninį pasitenkinimą atakuodami valstybės sistemą arba tokiu būdu pareikštų protestą prieš vyriausybės vykdomą politiką. Šie asmenys dažniausiai ieško galimybės prieiti prie duomenų, juos sugadinti arba pavogti dėl asmeninės naudos arba tiesiog norėdami neteisėtai juos paviešinti.
- Labai nedaug nuo pavienių programišių skiriasi kita tikslinė pažeidėjų grupė, t. y. nusikalstamos organizacijos arba pavieniai nusikaltėliai. Šios grupės arba asmenys, pvz., informacijos tarpininkai, irgi gali norėti gauti neteisėtą prieigą prie e. balsavimo sistemų tam, kad šių sistemų išteklius panaudotų asmeniniams tikslams.
- Protestuojančių asmenų grupės arba vadinamieji haktivistai gali mėginti nukreipti savo veiksmus prieš e. balsavimo sistemas turėdami tikslą parodyti savo priešiškumą dėl šių sistemų naudojimo balsavimo procesams arba jas sugadinti, arba tam, kad gautus duomenis panaudotų asmeniniams tikslams, arba iškreiptų balsavimo sistemoje esančią informaciją.
- Užsienio žvalgybų tarnybos gali būti suinteresuotos gauti tam tikros informacijos apie asmenis. Ateityje šią informaciją jos galėtų panaudoti kontržvalgybai arba šnipinėjimui. Šios tarnybos, naudodamos gautą informaciją, galėtų veikti šalies politikos formavimą arba manipuliuoti turima balsavimo informacija, siekdamos daryti įtaką balsavimo rezultatams.
- Teroristinės organizacijos gali būti suinteresuotos gauti e. balsavimo sistemose saugomos informacijos apie privačius asmenis. Šios organizacijos, naudodamos turimas žinias, gali būti suinteresuotos, pvz., rengti teroro aktus. Be to, jos gali tyrinėti e. balsavimo sistemas ir jose balsavimo metu kaupiamą informaciją, kad suprastų, kokios yra balsavimo tendencijos ir, esant reikalui, darytų įtaką balsavimo rezultatams arba trukdytų vydyti sklandų balsavimo procesą.

4 skirsnis. Elektroninio balsavimo sistemų pažeidžiamumas

Atskleidus svarbiausius e. rinkimų problematikos aspektus, tikslinga išanalizuoti dažniausiai pasitaikančius techninių užpuolimų (atakų) metodus, kuriais naudojasi neteisėtą veiką vykdantys asmenys, siekdami sutrikdyti informacinių sistemų funkcionavimą:

- Elektroninio balsavimo sistemų saugumo spragų paieškos testai (angl. *penetration tests)* gali daryti teigiamą įtaką visuomenės nuomonei apie e. balsavimą. Tam, kad jie būtų efektyvūs, reikia tiesiog modifikuoti sistemoje saugomus duomenis ir viešai skelbti apie pasiektus teigiamus rezultatus. Saugumo spragų paieškos testai galėtų būti atliekami ne tik per balsavimą, bet ir jam pasibaigus. Atakas rengiantiems asmenims pakaktų tiesiog atskleisti balsuojančių asmenų autentifikavimo informaciją, kuria jie naudojasi prisijungdami prie e. balsavimo sistemos. Ši informacija galėtų būti panaudota tam, kad susietų balsuojantį asmenį su jo balsu. Spragų paieškos testai galėtų būti naudojami ir turint tikslą pakeisti oficialių balsavimo svetainių turinį. Pakeistos e. balsavimo svetainių nuorodos gali daryti įtaką duomenų konfidencialumui ir vientisumui skaičiuojant balsus, o tai gali lemti rinkimų, vykdomų elektroniniu būdu, pripažinimą negaliojančiais. Mažai tikėtina, kad individualios vartotojų sistemos (asmeniniai kompiuteriai) bus patrauklus taikinys atakas vykdantiems programišiams. Labiau tikėtina, kad programišiai gali bandyti sugadinti tarnybines e. balsavimo sistemų stotis. Tokiu atveju būtų atvertas priėjimas prie didesnio duomenų kiekio *(Crown Copyright*, 2002).
- Vienas iš atvejų yra galimybė, kad į e. balsavimo sistemų tarnybines stotis prieš rinkimus arba jų metu bus įdiegta kenkiamoji programinė įranga (angl. *Malicious Software)*. Tai galima padaryti naudojantis elektroniniu paštu arba išoriniu ryšiu su tarnybine stotimi. Didelis prisijungimų prie e. balsavimo sistemos tarnybinės stoties kiekis gali gerokai padidinti kenkiamosios programinės įrangos plitimo tarnybinėje stotyje galimybę. Tokiu būdu e. balsavimo sistema gali būti sugandinta. Pvz., jeigu būtų įdiegta Trojos arklio tipo programa, gali būti pažeistas duomenų konfidencialumas ir (arba) vientisumas. Toks duomenų pažeidimas atitinkamiems šalies pareigūnams gali sudaryti sąlygas pasinaudoti savo turima teise paskelbti rinkimų rezultatų pripažinimą negaliojančiais. Interneto naršyklių ir operacinių sistemų, kuriomis naudojasi e. balsavimo sistemų vartotojai, saugumo spragos gali suteikti galimybę į tarnybines stotis įdiegti kenkiamąją programinę įrangą. Ataką vykdantis asmuo, naudojamą kenkiamąją programinę įrangą gali

sukonfigūruoti taip, kad jokios antivirusinės programos jos neaptiktų tol, kol ji bus aktyvuota vartotojo kompiuteryje. Tai gali įvykti tiesiog per pačius rinkimus. Pvz., Trojos arklio tipo programa gali kompromituoti balsuojančio asmens per rinkimus pareikštą nuomonę, apie jo pasirinkimą informuodama ne tik e. balsavimo sistemos tarnybinę stotį, bet ir trečiąją šalį, arba be balsuojančio asmens žinios tiesiog pakeisti jo pasirinkimą, prieš siunčiant duomenis į e. balsavimo sistemos tarnybinę stotį.

- Dar vienas pažeidimas, kuris gali tapti didžiausia naudojimosi e. balsavimo sistemomis problema, – paslaugų ribojimas (angl. *Denial of Service)*. Vienu metu daugelio vartotojų naudojama e. balsavimo sistema gali tapti laikinai nepasiekiama. Nusikaltėlių ataka ir netinkamas vartotojų naudojimasis e. balsavimo sistema gali lemti jos laikiną nepasiekiamumą, blogiausiu atveju – nepasiekiamumą per visą balsuoti skirtą laiką. Tokiu atveju balsuojantys asmenys neturėtų galimybės naudotis e. balsavimo sistemos teikiamomis paslaugomis ir dėl atakų, kurios būtų nukreiptos prieš komunikacijų kanalus. Reikėtų pabrėžti, kad esama tikimybės, jog bus atakuojamas vartotojo įrenginys (asmeninis kompiuteris). Tokiu atveju balsuojantis asmuo negalės pasinaudoti jam suteikta balsavimo teise.
- *DNS* (angl. *Domain Name Service)* atakos irgi gali būti naudojamos e. balsavimo sistemoms kompromituoti. Nusikaltėliai klastoja *DNS* įrašus ir gali sukurti netikras e. balsavimo sistemų kopijas. Į tokias netikras sistemas besikreipiantys suklaidinti rinkėjai netinkamoje vietoje išreiškia savo valią. Šiuo atveju bus ne tik surinkta informacijos apie balsuojančius asmenis, bet ir jų balsai nepasieks tikrosios balsavimo sistemos. Vykdant tokio pobūdžio atakas, rinkėjai gali būti kompromituojami dėl tariamo balsavimo arba neteisėtai naudojamasi gautais duomenimis, gali būti klastojami rinkėjų balsai, todėl ir šiuo atveju rinkimai gali būti pripažinti negaliojančiais.
- Viena iš socialinės inžinerijos atakų – tam tikro balsavimo būdo propagavimas, naudojantis tikslinėmis rinkimų kampanijos akcijomis (pvz., „nebalsavau elektroniniu būdu“). Visuomenei atitinkamai pateikus informaciją apie e. balsavimo sistemas ir tiesiog surengus keletą akcijų, per kurias būtų tvirtinama, kad toks balsavimo būdas yra nesaugus ir gali būti naudojamas tik tam, kad būtų klastojami rinkimų rezultatai, galima gerokai sumažinti vartotojų pasitikėjimą šiuo balsavimo būdu. Tada nebus pasiekta jokio rezultato, kurio yra tikimasi diegiant e. balsavimo sistemas *(Crown Copyright*, 2002).

Taigi, kuriant e. balsavimo sistemas, reikėtų daugiau dėmesio skirti šių sistemų pažeidžiamumo analizei, be to, nepamiršti apie atsarginių ir besidubliuojančių sistemų bei ryšio linijų reikalingumą, nes galimi ir atsitiktiniai e. balsavimo sistemos sutrikimai: techninės įrangos ar ryšio linijų gedimai ir kt. Sugedus e. balsavimo sistemai, visos pastangos sklandžiai organizuoti rinkimus gali būti bevaisės, o visuomenės nuomonė apie balsavimo sistemos naudojimą ateityje bus jau susiformavusi ir ją pakeisti gali būti labai sunku.

Pasaulyje jau yra pasinaudota keletu tokių iš aukščiau įvardytų ir išanalizuotų metodų. Galima paminėti Nyderlandų Karalystės ir JAV įvykius. Nyderlandų Karalystėje 2006 m. spalį organizacija „Mes nepasitikime balsavimo kompiuteriais“ (oland. *'Wij vertrouwen stemcomputers niet')* per nacionalinę televiziją pareiškė, kad jiems pavyko sėkmingai įsibrauti į *Nedap* balsavimo kompiuterius *(SiliconRepublic.com*, 2006). Organizacija parodė, kad, atlikus keletą nesudėtingų veiksmų, kurie užtrunka apie minutę, galima pakeisti balsavimo kompiuterio sudėtines dalis (mikroschemas), toks pakeitimas gali „išmokyti“ kompiuterį nelabai tiksliai įrašinėti balsavimo rezultatus ir net „žaisti šachmatais“. Ši organizacija dar parodė, kaip galima iš 20–30 metrų atstumo *(The Register*, 2006), naudojantis radijo bangų skeneriu, įvykdyti aktyviojo elektromagnetinio spinduliavimo *(TEMPEST)* ataką, kurios metu įmanoma nustatyti, kaip balsavo žmogus, ir dar sukelti grėsmę balsavimo slaptumui. Balsavimo mašinas iš Nyderlandų Karalystės ketino pirkti ir Airijos vyriausybė, tačiau šio sandorio buvo atsisakyta dėl to, kad balsavimo mašinos buvo pripažintos esančios labai nesaugios. 2005 m. JAV Kalifornijos valstija parėmė įsibrovimo į bendrovės „Diebold Election System“ balsavimo įrenginį testą *(Computerworld*, 2005). Šį testą atlikęs H. Hursti įrodė, kad įrenginys yra nesaugus dėl jam sukurti pritaikytų techninių sprendimų. Vėliau jis pateikė ataskaitą, kurioje aiškiai matyti brovimosi į šią sistemą veiksmų eiga. Be to, ataskaitoje nurodyta, kad balsavimo rezultatai priklauso tik nuo to, kaip yra užprogramuotas įrenginys. 2005 m. JAV ir Kanadoje rinkimams buvo naudojami 1 297 tokie įrenginiai *(Hursti*, 2005).

Atlikus detalią e. rinkimų sistemų pažeidimų metodų analizę, galima tvirtinti, kad e. balsavimo sistemos gali būti atakuojamos siekiant įvairiausių tikslų. Nors modeliuojamos ir kuriamos sistemos gali būti pripažintos saugiomis, negalima pamiršti, kad ateityje jų saugumas vis dėlto gali būti pažeistas. Tam tikslui reikėtų periodiškai atlikti sistemos saugumo pažeidžiamumo testus, nes nepažeidžiama sistema gali būti laikoma tik iki to momento, kol nėra įrodyta priešingai, o silpnų vietų aptikimo testai galėtų apsaugoti nuo įvykių, kurie neigiamai paveiktų žmonių pasitikėjimą e. rinkimų sistemomis.

Nors e. rinkimų sistemos ir yra plačiai skirtingų valstybių naudojamos šiuolaikiniams politiniams procesams vykdyti, jos vis dar nėra tobulos. Tikėtina, kad gana sparčiai plėtojantis naujosioms technologijoms, gali pasikeisti ir pačios e. rinkimų sistemos bei pasaulinės jų naudojimo tendencijos. Kuriant ir naudojant e. balsavimo (rinkimų) sistemas privalu laikytis tam tikrų reikalavimų ir užtikrinti, kad balsavimo sistemos bei jų veikimo principai būtų prieinami ir suprantami daugeliui vartotojų. Kartais dėl tam tikrų kompiuterinių ir techninių žinių stokos e. balsavimo sistemose vykstantys procesai gali būti nesuprantami visuomenei, vadinasi, bent jau šiuo metu arba vertinant iš ilgesnio laikotarpio perspektyvos, e. balsavimo sistemos galėtų būti tik kaip pagalbinis mechanizmas rengiant rinkimus, grindžiamus tradicinėmis rinkimų organizavimo formomis.

Būtina daugiau dėmesio skirti kuriamų e. rinkimų sistemų saugumui užtikrinti, pažeidžiamumui ir grėsmei identifikuoti bei mažinti. Laiku pritaikyti įsibrovimų į šias sistemas aptikimo testai ir nuolatinė ekspertų priežiūra daro įtaką tam, kad sistema būtų laiku atnaujinama ir saugi, o tai, savaime suprantama, gali lemti pasitikėjimą tokio pobūdžio sistemomis. Gyventojų pasitikėjimas e. rinkimų sistemomis reiškia ne ką kitą, kaip nematomą sistemos pridėtinę vertę, kurią sunku sukurti ir palaikyti, bet labai lengva prarasti, be to, toks praradimas reikštų visišką sistemos žlugimą.

Žinių įtvirtinimo klausimai

1. Ar terminai „e. balsavimas“ ir „i. balsavimas“ yra tapatūs? Kokie yra šių dviejų terminų skirtumai ar panašumai?
2. Ar e. rinkimų sistemų naudojimas yra svarbiausias tikslas vykdant e. demokratijos procesus? Kodėl?
3. Kaip galima būtų apibrėžti e. demokratiją?
4. Kokios e. demokratijos plėtros kliūtys yra įvardijamos mokslinėje literatūroje?
5. Kokių principų būtina laikytis norint sukurti ir pradėti naudoti e. balsavimo sistemas?
6. Kokie e. rinkimų sistemų modeliai egzistuoja pasaulyje ir kokie jų veikimo principai?
7. Ar e. rinkimų sistemos yra pažeidžiamos ir kas gali kelti joms grėsmę?
8. Kokie metodai gali būti naudojami siekiant sukompromituoti e. balsavimo sistemas?

Literatūra

1. Tarptautinės sutartys

1. Konvencija dėl elektroninių nusikaltimų. Valstybės žinios, 2004-03-07, Nr. 36-1188.
2. Konvencijos dėl elektroninių nusikaltimų Papildomasis protokolas dėl rasistinio ir ksenofobinio pobūdžio veikų, padarytų naudojantis kompiuterinėmis sistemomis, kriminalizavimo. Valstybės žinios. 2006-07-05, Nr. 75-2850. Prieiga per internetą: *<http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=279838>*.
3. Explanatory Report to the Convention on Cybercrime (adopted 8 November 2001, the Convention has been opened for signature in Budapest, on 23 November 2001). Prieiga per internetą: *<http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>*.

2. Europos Sąjungos teisės aktai ir kiti dokumentai

1. 2002 m. kovo 7 d. Europos Parlamento ir Tarybos direktyva 2002/19/EB dėl elektroninių tinklų ir su jais susijusių priemonių sujungimo ir prieigos prie jų (Prieigos direktyva). Prieiga per internetą: *<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0019:20091219:LT:PDF>*.
2. 2002 m. kovo 7 d. Europos Parlamento ir Tarybos direktyva 2002/20/EB dėl elektroninių ryšių tinklų ir paslaugų leidimo (Leidimo direktyva). Prieiga per internetą: *<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0020:20091219:LT:PDF>*.
3. 2002 m. kovo 7 d. Europos Parlamento ir Tarybos direktyva 2002/21/EB dėl bendros elektroninių ryšių tinklų ir paslaugų reguliavimo sistemos (Bendrąja direktyva). Prieiga per internetą: *<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0021:20091219:LT:PDF>*.
4. 2002 m. kovo 7 d. Europos Parlamento ir Tarybos direktyva 2002/22/EB dėl universaliųjų paslaugų ir paslaugų gavėjų teisių, susijusių su elektroninių ryšių tinklais ir paslaugomis (Universaliųjų paslaugų direktyva). Prieiga per internetą: *<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0022:20091219:LT:PDF>*.
5. 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privataus gyvenimo apsaugos elektroninių ryšių sektoriuje (Privatumo ir elektroninių ryšių direktyva). Prieiga per internetą: *<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0058:20091219:LT:PDF>*.
6. 2009 m. lapkričio 25 d. Europos Parlamento ir Tarybos direktyva 2009/136/EB iš dalies keičianti Direktyvą 2002/22/EB dėl universaliųjų paslaugų ir paslaugų gavėjų teisių, susijusių su elektroninių ryšių tinklais ir paslaugomis, Direktyvą 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje ir Reglamentą (EB) Nr. 2006/2004 dėl nacionalinių institucijų, atsakingų už vartotojų apsaugos teisės aktų vykdymą, bendradarbiavimo (OL 2009 L 337, p. 11).

7. 2009 m. lapkričio 25 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 1211/2009 dėl Europos elektroninių ryšių reguliuotojų institucijos (EERRI) ir Biuro įsteigimo. Prieiga per internetą: <*http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0001:0010:LT:PDF*>.
8. Commission recommendation on consistent non-discrimination obligations and costing methodologies to promote competition and enhance the broadband investment environment (project). Prieiga per internetą: <*http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1254*>.
9. Commission recommendation on relevant product and service markets within the electronic communications sector susceptible to *ex ante* regulation in accordance with Directive 2002/21/EC of the European Parliament and of the Council on a common regulatory framework for electronic communications networks and services, C(2007) 5406. Prieiga per internetą: <*http://ec.europa.eu/information_society/policy/ecomm/doc/library/proposals/rec_markets_en.pdf*>.
10. Communication from the Commision to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions. Creating a Safer Information Society by Improving the Security of Information Infrastructuresand Combating Computer-related Crime. Brusssels, 2001.01.26. COM (2000)890 final. Prieiga per internetą: <*http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2000:0890:FIN:EN:PDF*>.
11. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions. Network and Information Security: Proposal for A European Policy Approach. COM/2001/298. Prieiga per internetą: <*http://eur-lex.europa.eu/LexUriServ/site/en/com/2001/com2001_0298en01.pdf*>.
12. Communication from the Commission to the European Parliament, the Council and the Committee of the Regions Towards a general policy on the fight against cyber crime. Brussels, 2007.05.22, COM (2007) 267 final. Prieiga per internetą: <*http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF*>.
13. Computer-related crime. Council of Europe. Recomendation No. R(89)9, adopted by Committee of Ministers of the Council of Europe on 13 September 1989. Prieiga per internetą: <*http://www.oas.org/juridico/english/89-9&final%20Report.pdf*>.
14. Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems. [interaktyvus, žiūrėta 2011-06-27]. Prieiga per internetą: <*http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32005F0222:EN:NOT*>.
15. Council of Europe. Committee of Ministers. Recommendation No. R (95)13 of the Committee of Ministers to member States concerning Problems of Criminal Procedural law Connected with Information Technology. Prieiga per internetą: <*https://wcd.coe.int/wcd/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=536686&SecMode=1&DocId=528034&Usage=2*>.

16. 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.
17. 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.
18. 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. OJ L 178, 17/07/2000; p. 0001–0016.
19. Duomenų apsaugos direktyvos 29 straipsnio duomenų apsaugos darbo grupės 2009 m. birželio 12 d. nuomonė Nr. 5/2009 dėl socialinių tinklų internete. [2009] WP163.
20. Duomenų apsaugos direktyvos 29 straipsnio grupės 2002 m. gegužės 30 d. nuomonė 2/2002 „Dėl unikalių identifikatorių naudojimo telekomunikacijų galiniuose įrenginiuose:IPv6 pavyzdys“ (10750/02/EN/Galutinis WP 58).
21. Electronically Supplied Services. European Commission, Value Added Tax Committee (Article 29 of Directive 77/388/EEC) Guidelines TAXUD/2436/02 (Working paper n°372). Prieiga per internetą: <*http://www.belastingdienst.nl/common/dl/guidelines-e-services.pdf*>.
22. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 460/2004 2004 m. kovo 10 d. įsteigiantis Europos tinklų ir informacijos apsaugos agentūrą. Prieiga per internetą: <*http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2004R0460:20081101:LT:PDF*>.
23. Europos Parlamento ir Tarybos direktyva dėl atakų prieš informacines sistemas ir dėl Tarybos pamatinio sprendimo 2005/222/TVR panaikinimo pasiūlymas. Briuselis, 2010.9.30 KOM (2010) 517 galutinis. Prieiga per internetą: <*http://www.europarl.europa.eu/meetdocs/2009_2014/documents/com/com_com(2010)0517_/com_com(2010)0517_lt.pdf*>.
24. Europos Parlamento ir Tarybos 2014 m. liepos 23 d. reglamentas Nr. 910/2014 „Dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje“.
25. Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions. Cybersecurity strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN/2013/1 final. Prieiga per internetą: <*http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667*>.
26. Komisijos 2012 m. kovo 28 d. komunikatas COM/2012/140 Tarybai ir Europos Parlamentui. Kova su nusikalstamumu skaitmeniniame amžiuje. Europos kovos su elektroniniu nusikalstamumu centro kūrimas. Prieiga per internetą: <*http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0140:FIN:LT:PDF*>.
27. Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui bei regionų komitetui dėl ypatingos svarbos informacinės infrastruktūros apsaugos „Europos apsauga nuo didelio masto kibernetinių antpuolių ir veiklos sutrukdymo – geresnė parengtis, didesnis

saugumas ir atsparumas“. Briuselis, 2009.03.30, KOM (2009) 149 galutinis. Prieiga per internetą: <*http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:LT:PDF*>.

28. Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui bei Regionų komitetui dėl kovos su nepageidaujamu e. paštu, šnipinėjimo programomis ir žalinga programine įranga COM (2006) 688 galutinis. Prieiga per internetą: <*http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0688:FIN:LT:PDF*>.
29. Komisijos komunikatas Tarybai, Europos Parlamentui, Europos Ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui. Saugios informacinės visuomenės strategija – „Dialogas, partnerystė ir teisių suteikimas“. COM/2006/251. Prieiga per internetą: <*http://eurlex.europa.eu/Notice.do?mode=dbl&lang=en&ihmlang=en&lng1=en,lt&lng2=cs,da,de,el,en,es,et,fi,fr,hu,it,lt,lv,nl,pl,pt,sk,sl,sv,&val=427504:cs*>.
30. Opinion 05/2012 on Cloud Computing, adopted July 1st, 2012. Prieiga per internetą: <*http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf*>.
31. Pasiūlymas Europos Parlamento ir Tarybos reglamentui dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, Briuselis, 2012-06-04, COM(2012)238final. Prieiga per internetą: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0238:FIN:LT:PDF>.
32. Proposal for a Directive of European Parliament and the Council concerning measures to ensure a high common level of network and information security across the Union, COM/2013/48 final. Prieiga per internetą: <*http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1666*>.
33. Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final. Prieiga per internetą: <*http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf*>.
34. Recommendation of the Committee of ministers to member states on legal, operational and technical standards for e-voting, Zurich, 2004. P. 45-138.
35. Report from the Comission to the Council Based on Article 12 of the Council Framework Decision of 24 February 2005 on attacks against information systems. Brussels, 2008.07.14 COM (2008) 448 final. Prieiga per internetą: <*http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0448:FIN:EN:PDF*>.
36. 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.
37. Tarybos direktyva 2009/140/EB, iš dalies keičianti Direktyvą 2002/21/EB dėl elektroninių ryšių tinklų ir paslaugų bendrosios reguliavimo sistemos, keičianti Direktyvą 2002/19/EB dėl elektroninių ryšių tinklų ir susijusių priemonių sujungimo ir prieigos prie jų ir Direktyvą 2002/20/EB dėl elektroninių

ryšių tinklų ir paslaugų leidimo. Prieiga per internetą: <*http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0037:0069:lt:PDF*>.

38. Žalioji knyga. Apie Europos programą dėl ypatingos svarbos infrastruktūros objektų apsaugos. Briuselis, 2005.11.17 KOM (2005) 576 (galutinis). Prieiga per internetą: <*http://eur-lex.europa.eu/LexUriServ/site/lt/com/2005/com2005_0576lt01.pdf*>.

3. Lietuvos Respublikos teisės aktai

1. Aiškinamasis raštas dėl Konvencijos dėl elektroninių nusikaltimų ratifikavimo. Prieiga per internetą: <*http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=223058*>.
2. Informacinės visuomenės plėtros komiteto prie Lietuvos Respublikos Vyriausybės direktoriaus 2008 m. gruodžio 1 d. įsakymas „Dėl viešojo administravimo institucijų informacinių sistemų interoperabilumo sistemos funkcionavimo taisyklių patvirtinimo“ Nr. T-228. Valstybės žinios, 2008, Nr. 145-5850.
3. Lietuvos Respublikos administracinių bylų teisenos įstatymas. Valstybės žinios, 1999, Nr. 13-308.
4. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas. Valstybės žinios, 2008, Nr. 22-804.
5. Lietuvos Respublikos asmens tapatybės kortelės įstatymas. Valstybės žinios, 2001, Nr. 97-3417, 2 str. 1 d.
6. Lietuvos Respublikos baudžiamojo proceso kodekso 154 straipsnio pakeitimo ir papildymo įstatymas Nr. IX-1993. Valstybės žinios, 2002, Nr. 37-1341.
7. Lietuvos Respublikos civilinio proceso kodeksas. Valstybės žinios, 2002, Nr. 1340-42.
8. Lietuvos Respublikos civilinis kodeksas. Valstybės žinios, 2000, Nr. 74-2262.
9. Lietuvos Respublikos dokumentų ir archyvų įstatymas. Valstybės žinios, 1995, Nr. 107-2389.
10. Lietuvos Respublikos elektroninio parašo įstatymas. Valstybės žinios, 2000, Nr. 61-1827.
11. Lietuvos Respublikos elektroninių ryšių įstatymas. Valstybės žinios, 2004. Nr. 69-2382.
12. Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymo projektas Nr. 373-02. Prieiga per internetą: <*http://www.lrs.lt/pls/proj/dokpaieska.showdoc_l?p_id=5050&p_query=&p_tr2=&p_org=&p_fix=n&p_gov=n*>.
13. Lietuvos Respublikos gyventojų registro įstatymas. Valstybės žinios, 1999, Nr. 28-793.
14. Lietuvos Respublikos informacinės visuomenės paslaugų įstatymas. Valstybės žinios, 2006, Nr. 65-2380.
15. Lietuvos Respublikos įstatymas dėl Konvencijos dėl elektroninių nusikaltimų papildomo protokolo dėl rasistinio ir ksenofobinio pobūdžio veikų, padarytų naudojantis kompiuterinėmis sistemomis, ratifikavimo. Valstybės žinios, 2006, Nr. 75-2848.

16. Lietuvos Respublikos paso įstatymas. Valstybės žinios, 2001, Nr. 99-3524.
17. Lietuvos Respublikos pelno mokesčio įstatymas. Valstybės žinios, 2001, Nr. 110-3992 (aktuali redakcija).
18. Lietuvos Respublikos pridėtinės vertės mokesčio įstatymas. Valstybės žinios, 2002, Nr. 35-1271.
19. Lietuvos Respublikos saugaus eismo automobilių keliais įstatymas. Valstybės žinios, 2000, Nr. 92-2883.
20. Lietuvos Respublikos Seimo nutarimas „Dėl balsavimo internetu rinkimuose ir referendumuose koncepcijos patvirtinimo“, 2006, Nr. X-912.
21. Lietuvos Respublikos teisingumo ministro 2008 m. liepos 22 d. įsakymas „Dėl teisingumo ministro 2006 m. gegužės 19 d. įsakymo Nr. 1R-160 „Dėl civilinės metrikacijos taisyklių patvirtinimo“ pakeitimo“ Nr. 1R-294. Valstybės žinios, 2008, Nr. 88-3541.
22. Lietuvos Respublikos teisingumo ministro 2012 m. gruodžio 13 d. įsakymas Nr. 1R-332 „Dėl procesinių dokumentų pateikimo teismui ir jų įteikimo asmenims elektroninių ryšių priemonėmis tvarkos aprašo patvirtinimo“. Valstybės žinios, 2012, Nr. 147-7579.
23. Lietuvos Respublikos teismų įstatymas. Valstybės žinios, 2002, Nr. 17-649
24. Lietuvos Respublikos valstybės informacinių išteklių įstatymas Nr. XI1807. Valstybės žinios, 2011, Nr. 163-7739.
25. Lietuvos Respublikos vidaus reikalų ministro 2008 m. rugsėjo 10 d. įsakymas „Dėl motorinių transporto priemonių vairuotojo pažymėjimų išdavimo taisyklių patvirtinimo“ Nr. 1V-328. Valstybės žinios, 2008, Nr. 106-4060.
26. Lietuvos Respublikos vidaus reikalų ministro 2014 m. gruodžio 1 d. įsakymas Nr. 1V-820 „Dėl nacionalinės elektroninės atpažinties informacinės sistemos nuostatų patvirtinimo“.
27. Lietuvos Respublikos Vyriausybės 2011 m. birželio 29 dienos nutarimas Nr. 796 „Dėl elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programos patvirtinimo“. Valstybės žinios, 2011, Nr. 83-4033, 2011, Nr. 106 (atitaisymas).
28. Lietuvos Respublikos Vyriausybės nutarimas dėl Lietuvos Respublikos elektroninių ryšių įstatymo koncepcijos patvirtinimo, 2003 m. kovo 10 d. Nr. 302, 2003, Nr. 26-1039.
29. Lietuvos Respublikos Vyriausybės nutarimas Nr. 1211 „Dėl Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymo koncepcijos patvirtinimo.“ Valstybės žinios, 2006, Nr. 134-5081.
30. Lietuvos Respublikos Vyriausybės nutarimas Nr. 601 „Dėl elektroninės informacijos saugos valstybės institucijų informacinėse sistemose strategijos iki 2008 metų ir jos įgyvendinimo priemonių plano patvirtinimo.“ Valstybės žinios, 2006, Nr. 70-2575.
31. 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.

4. Tarptautinių institucijų dokumentai

1. Model Tax Convention on Income and on Capital. Condensed Version / OECD 22 July 2010.
2. Taxation and electronic commerce. Implementing The Ottawa Taxation Framework Conditions. Organisation for Economic Co–operation and Development, 2001.
3. UNCITRAL Model Law on Electronic Commerce. 2001. Prieiga per internetą: <*http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf*>.
4. UNCITRAL United Nations convention on the use of electronic communications in international contracts, New York 2005. Prieiga per internetą: <*http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2005 Convention*>.
5. UNIDROIT Tarptautinių komercinių sutarčių principai. 1994. Prieiga per internetą: <*http://www.unidroit.org/english/principles/contracts/main.htm*>.

5. Specialioji literatūra

1. ABRAMAVIČIUS, A. Baudžiamoji teisė: specialioji dalis. 2 knyga. Vilnius: Eugrimas, 2000.
2. ALCOFF, L.; HAMES-CARCIA, M.; MOYA, P. M. L. Identity Politics Reconsidered. Palgrave Macmillan. Basingstoke, 2006
3. AMBRASIENĖ, D.; BARANAUSKAS, E. Civilinė teisė. Prievolių teisė. Vilnius: Mykolo Romerio universitetas, 2006.
4. BAINBRIDGE, D. Data protection. – Emis Professional pub., 2005.
5. BAINBRIDGE, D. Introduction to Computer Law. Fourth edition. Pearson Education Limited, 2000.
6. BAINBRIDGE, D. I. Intellectual Property (9th ed.). Pearson. London, 2012.
7. BASU, S. Taxation of Electronic Commerce. The Journal of Information, Law and Technology. 2001 (1). Prieiga per internetą: <*http://elj.warwick.ac.uk/jilt/01-2/basu1.html*>.
8. BEYNON-DAVIES, P. E-business. Houndmills. Palgrave Macmillan, 2004.
9. BLYTHEL, S. E. A critique of german e-commerce law and recommendations for improvement, 2012.
10. BLUVŠTEINAS, J.; BIELIŪNAS, E.; JUSTICKIS,V. IR KITI. Kriminologija. Pradai, 1994.
11. BRENNER, S. W. Cybercrime. Criminal Threats from Cyberspace. Library of Congress Cataloging, 2010.
12. BRENNER, S. W. Cyberthreats: The Emerging Fault Lines of the Nation State. Oxford University Press, 2009.
13. BRITZ, T. M. Computer Forensics and Cyber Crime: An Introduction. Pearson Education, 2009.
14. BROADHURST, R. Content crimes: criminality and sencorship in Asia. The Challenge of Cybercrime Conference on 15-17 September, 2004. Palais de l`Europe, Strasbourg, France. Prieiga per internetą: <*http://ceps.anu.edu.au/publications/pdfs/broadhurst_pubs/broadhurst-content_cybercrimes.pdf*>.

15. BULLER, D. J.; WITTOW, M. H. Cloud computing:emerging legal issues for access to data anywhere, anytime. Journal of Internet law – Aspen publishers, 2010.
16. CANE, P.; CONAGHAN, J. The New Oxford Companion to Law. Oxford University Press Inc, 2006.
17. CAREY, P. Data protection: a practical guide to UK and EU law. – Oxford university press, 2004.
18. CATCHPOLE, J. The Regulation Of Electronic Commerce: A Comparative Analysis Of The Issues Surrounding The Principles Of Establishment. International Journal of Law and IT, 2001.
19. CIVILKA, M. Elektroninės komercijos reguliavimas tarptautinėje ir ES teisėje, 2001. Prieiga per internetą: <*www.teisininkas.lt/downloads/EK_konsp.pdf*>.
20. CIVILKA, M. Elektroninės komercijos teisiniai aspektai: bendrieji klausimai. Vilniaus universiteto Informatikos teisės centras. Prieiga per internetą: <*www.itc.tf.vu.lt/mokslas/ek_vadovelis_final2.pdf*>.
21. CIVILKA, M. Elektroninio parašo naudojimo vidaus rinkoje problemos. Teisė, 2013.
22. CIVILKA, M.; LAMANAUSKAS T. Elektroninio parašo įteisinimas: probleminiai aspektai pagal ES ir LR teisę. Prieiga per internetą: <*www.rln.lt/download.php/fileid/9*>.
23. CIVILKA, M.; LAMANAUSKAS, T.; NOSINAITĖ, G.; SAULIŪNAS, D.; ŠTITILIS, D.; TOLIUŠIS, S.; ULEVIČIUS, L. Informacinių technologijų teisė. Vilnius: NVO teisės institutas, 2004.
24. CLIFT, S. e-Government and democracy. Representation and citizen engagement in the information age, 2004.
25. CORNISH, W. Intellectual Property: Omnipresent, Distracting, Irrelevant? Oxford University Press, 2004.
26. CORNISH, W. R. Intellectual Property – Patents, Copyright, Trade Marks and Allied Rights (7th ed.). Sweet & Maxwell. London, 2010.
27. ČĖSNA, R. Kai kurie elektroninių įrodymų panaudojimo civiliniame procese aspektai. *Jurisprudencija*, 2007.
28. ČĖSNA, R.; ŠTITILIS D. Kompiuterinės informacijos ir elektroninio dokumento apsauga viešajame administravime. Vilnius: Lietuvos teisės akademija, 2000.
29. DANAGHER, L. An Assessment of the Draft Data Protection Regulation: Does it Effectively Protect Data? European Journal of Law and Technology, 2012.
30. DAVIDAVIČIENĖ, V.; GATAUTIS, R.; PALIULIS, N.; PETRAUSKAS, R. Elektroninis verslas. Vilnius: Technika, 2009.
31. DE HERT, P.; KLOZA, D. Internet (access) as a new fundamental right. Inflating the current rights framework?, European Journal of Law and Technology, 2012.
32. DONTOGLOU, T. D. Competition@e-commercel.eu: an appropriate European approach to the anticompetitive implications in the online world. Liverpool law review. Prieiga per internetą: <http://www.springerlink.com/content/q1885x142u275670/fulltext.pdf?page=1>.

33. DURANTI, L.; CORINNE, R. M.; SHEPPARD, F. A. Electronic Records and the Law of Evidence in Canada: The Uniform Electronic Evidence Act Twelve Years Later. Archivaria, 2010.
34. FENNER, G. M. The Admissibility of Web-Based Evidence. Catholic University Law Review, 2013.
35. GARUCKAS, R.; KAZILIŪNAS, A. Elektroninio parašo teisinis reglamentavimas ir jo įgyvendinimo ypatumai Lietuvoje. Viešoji politika ir administravimas, 2008.
36. GERCKE, M. Internet-related identity thef. Project on Cybercrime, 2007. Prieiga per internetą: *<http://www.coe.int/T/DG1/LegalCooperation/Economiccrime/cybercrime/cy%20activity_events_on_identity_theft/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf>*.
37. GHOSH, S.; TURRINI, E. Cybercrimes: A Multidisciplinary Analysis. Springer-Verlag, 2010.
38. GOODE, S. The Admissibility of Electronic Evidence. The Review of Litigation, 2009.
39. GRADY, M. F.; PARISI, F. The Law and Economics of Cybersecurity. Cambridge University press, 2006.
40. GRAHAM J. Cyber Fraud: Tactics, Techniques and Procedures. Taylor&Francis Group, 2009.
41. GRIMM, R.; KRIMMER, R.; MEISSNER, N.; REINHARD, K.; VOLKAMER, M.; WEINAND, M. Security Requirements for Non-political Internet Voting. Austria, 2006.
42. GRITZALIS, A. D. Principles and requirments for a secure e-voting. Copenhagen, 2002.
43. HARDESTY, D. A. Electronic Commerce: Taxation & Planning, 2003.
44. HEIDERHOFF, B.; ŹMIJ, G. Law of e-commerce in Poland and Germany. Sellier European Law Publishers. München, 2005.
45. HIGGINS, G. E. Cybercrime: An Introduction to an Emerging Phenomen. Library of Congress Cataloging, 2010.
46. HOFFMAN, S. K. Identity Theft: A Reference Handbook. Santa Barbara, California, 2010.
47. HORNLE, J. Countering the dangers of online pornography - shrewd regulation of lewd content? European Journal of Law and Technology, 2011.
48. HURSTI, H. The Black Box Report. Security Alert: July 4, 2005 Critical Security Issues with Diebold Optical Scan Design, 2005.
49. ICOVE, D.; SEGER, K.; VONSTORCH, W. Computer Crime: A Crimefighters Handbook. Oreilly&Associates Inc., 1995.
50. International Working Group for Data Protection in Telecommunications. Common Position on the Use of the Internet in the Conduct of Elections, Vienna, 2001.
51. JARUKAITIS, I.; LAMANAUSKAS, T.; CIVILKA, M.; RAKAUSKAITĖ, A. Elektroninių ryšių teisė. Vilnius: Eugrimas, 2005.

52. JASTIUGINAS, S. Informacijos saugumo valdymas Lietuvos viešajame sektoriuje. Informacijos mokslai. Vilnius, 2011. Prieiga per internetą: < *http://www.leidykla.eu/fileadmin/Informacijos_mokslai/2011-57/7-25.pdf*>.
53. LAST, J. M. A Dictionary of Public Health. Oxford University Press Inc., 2007.
54. KÄBISCH, W. Tax Aspects of International Electronic Commerce. ESPRIT Project 27028 – Electronic Commerce Legal Issues Platform. Prieiga per internetą: <*http://www.eclip.org/documentsII/lawtechn/tax.zip*>.
55. KALINAUSKAITĖ, A. Elektroninė forma ir elektroninis parašas: Lietuvos teisinė bazė globaliame kontekste. Teisės problemos, 2012.
56. KATUOKA, S.; KIŠKIS, M.; PRANEVIČIUS, G. IR KT. Vartotojų teisių apsauga Lietuvoje ir Europoje. Vilnius: Mykolo Romerio universitetas, 2006.
57. KIŠKIS, M.; ŠTITILIS, D.; ROTOMSKIS, I.; PETRAUSKAS, R. Teisės informatika ir informatikos teisė. Vilnius: Mykolo Romerio universitetas, 2006.
58. KRIMMER, R.; TRIESSNIG, S.; VOLKAMER, M. The Development of Remote E-Voting Around the World: A Review of Roads and Directions, 2007.
59. KSHETRI, N. The Global Cybercrime Industry: Economic, Institutional and Strategic Perspective. Springer-Verlag, 2010.
60. KUNER, C. European Data Protection Law. Oxford University Press, Oxford, 2007.
61. KUNIGĖLIS, Š. Elektroninis parašas Lietuvoje. Vadovas, 2011.
62. LAMANAUSKAS, T. Elektroniniai duomenys kaip įrodinėjimo priemonė civiliniame procese. *Justitia*, 2001.
63. 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 Union, United States and Canada. Stan. Tech. L, 2004. Prieiga per internetą: < *http://stlr.stanford/STLR/Articles/04_STRL_4*>.
64. LAUŽIKAS, E.; MIKELĖNAS, V.; NEKROŠIUS, V. Civilinio proceso teisė: vadovėlis. *Justitia*. Vilnius, 2003.
65. LEMLEY, M. A.; MENELL, P. S.; MERGES, R. P.; SAMUELSON, P. Software and Internet Law (4th ed.). Aspen Law & Business. New York, 2011.
66. Lietuvių kalbos žodynas. Vilnius: Lietuvių kalbos institutas, 2005.
67. MANN, R. J.; WINN, J. K. Electronic Commerce. Second Edition. 2005.
68. MASON, S. Editor. Electronic evidence. Third edition. Lexis Nexis, London, 2012.
69. MASON, S. Editor. International Electronic Evidence. British Institute of International and Comparative Law. London, 2008.
70. MASON, S. Electronic evidence and the meaning of 'original'.Amicus Curiae The Journal of the Society for Advanced Legal Studies, 2009.
71. MAXWELL, W. Electronic Communications: The New EU Framework.: Oceana Publications, Inc., Dobbs Ferry. New York, 2002.
72. MAXWELL, W. Electronic Communications: the New EU Framework. Part I, Booklet 1.5. –Oceana Publications Inc. New York, 2002.

73. MERGES, R. P.; MENELL, P. S.; LEMLEY, M. A. Intellectual Property in the New Technological Age (6th ed.). Aspen Law & Business. New York, 2012.
74. MINYAN, W. Electronic evidence in China. Digital Evidence and Electronic Signature Law Review, 2008.
75. MITRAKAS, A. Information Security Law in Europe: Risks Checked. Information & Communications Technology Law, 2006.
76. MUSTEIKIS, L.; PAULAVIČIUS, A.; RAKALOVIČ, M. Elektroninis parašas ir jo pritaikymas Lietuvoje. *Iš*: 11-osios Lietuvos jaunųjų mokslininku konferencijos „Mokslas – Lietuvos ateitis“: straipsnių rinkinys. Vilnius, 2008.
77. NENOVA, M. B. EC electronic communications and competition law. Cameron May Ltd., 2006.
78. PETRAUSKAS, R.; ŠTITILIS, D. Lietuvos Respublikos baudžiamasis kodeksas nusikaltimų elektroninėje erdvėje konvencijos kontekste. *Jurisprudencija*, 2002.
79. PETRAUSKAS, R.; ŠTITILIS, D. Kompiuteriniai nusikaltimai ir jų prevencija. Lietuvos teisės akademija. Vilnius, 2000.
80. PETRAVIČIŪTĖ, I. Elektroniniai dokumentai organizacijos veikloje, 2005. Prieiga per internetą: <*http://www.archyvai.lt/archyvai/download/680/2005%20elektroniniai%20dokumentai%20organizacijoje.pdf*>.
81. PETRAVIČIŪTĖ, I. Elektroninių dokumentų autentiškumas: ilgalaikio išsaugojimo problemos. Knygotyra, 2006.
82. PIESLIAKAS, V. Lietuvos baudžiamoji teisė. Antra pataisyta ir papildyta laida. *Justitia*. Vilnius, 2009.
83. PIVEC, M. E.; BRINKERHOFF, S. E-mail in the workplace: limitation on privacy. Human Rights Magazine, 1999.
84. POLANSKI, P. P. International electronic contracting in the newest UN convention. Journal of international commercial law and technology, 2007. Prieiga per internetą: <*http://www.jiclt.com/index.php/jiclt/article/viewDownloadInterstitial/26/25*>.
85. PROSSER, A.; KOFLER, R.; KRIMMER, R.; UNGER, M. K. Security Assets in E-Voting. Electronic Voting in Europe –Technology, Law, Politics and Society, Workshop of the ESF TED Programme together with GI and OCG, Austria, 2004.
86. REED, C. Computer law. Seventh Edition. Oxford University Press, Oxford, 2011.
87. REICH, P. C.; WEINSTEIN, S.; WILD, C.; CABANLONG, A. S. CYBER, WARFARE: A Review of Theories, Law, Policies, Actual Incidents - and the Dilemma of Anonymity. European Journal of Law and Technology, 2010.
88. REMMERT, M. Towards European Standards on Electronic Voting. Electronic Voting in Europe – Technology, Law, Politics and Society, Workshop of the ESF TED Programme together with GI and OCG. Austria, 2004.
89. ROSENZWEIG, P. Cyberwarfare: how conflicts in cyberspace are challenging America and changing the world. Library of Congress Cataloging, 2013.

90. RÖSSLER, T. e-Voting. A survey and Introduction. Secure Information Technology Center. Austria, 2004.
91. ROWLAND, D.; MACDONALD, E. Information Technology Law. Cavendish Publishing Limited, 1997.
92. SAARENPAA, A. Data Protection – some comments from the Finnish point of view. Judicial Academy of Northern Finland. Rovaniemi, 2001.
93. SAMSON, M. H. Click-Wrap Agreement Held Enforceable, 1998.
94. SCHJOLBERG, S. A Global Treaty on Cybersecurity and Cybercrime, Second edition, 2011. Prieiga per internetą: <*http://www.cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime_Second_edition_2011.pdf*>.
95. SHOEMAKER, D.; CONKLIN, A. Cybersecurity: the Essential body of knowledge. Course technology, 2012.
96. SIEBER, U. Computer Crime and Criminal Information Law – The New Trends in International Risks and Information Society, 1988. Prieiga per internetą: <*http://www.uplink.com.au/lawlibrary/Documents/Docs/Doc122.html*>.
97. SIMAITIS, R. Informacinių ir elektroninių ryšių technologijų plėtra Lietuvos civiliniame procese. *Iš*: Vilniaus universiteto Teisės fakulteto mokslinių straipsnių rinkinys, Vilnius, 2012.
98. SOETE, L.; KAMP, K. The "Bit Tax": The Case For Further Research, 1996. Prieiga per internetą: <*http://www-edocs.unimaas.nl/abs/mer96019.htm*>.
99. SOETE, L.; WEEL, B. Cybertax. Futures, 1998.
100. STAN, Z. L.; ANIL, K. J. Encyclopedia of Biometrics. Springer Science Business Media, LLC, 2009.
101. SUSSKIND, R. Tomorrow's lawyers. An introduction to Your future. Oxford University Press, Oxford, 2013.
102. ŠTITILIS, D. Elektroniniai nusikaltimai: metodinė priemonė. Vilnius: Mykolo Romerio universitetas, 2011.
103. ŠTITILIS, D., *et al*. Tapatybės vagystės elektroninėje erdvėje kriminalizavimas: lyginamieji aspektai. Socialinių mokslų studijos, 2011.
104. ŠTITILIS, D. Kai kurie neteisėtos prieigos prie kompiuterinės informacijos kriminalizavimo aspektai. *Jurisprudencija*, 2003.
105. ŠTITILIS, D. Neteisėtos prieigos prie kompiuterinės informacijos kriminalizavimas. Informacijos mokslai, 2003.
106. ŠTITILIS, D. Privataus gyvenimo elektroniniuose ryšiuose ribojimas nusikaltimų tyrimo tikslais. *Jurisprudencija*, 2006.
107. ŠTITILIS, D. Teisinės atsakomybės pagrindų už neteisėtas veikas elektroninėje erdvėje nustatymo prolemos. Disertacija. Vilnius, 2002.
108. ŠTITILIS, D.; GUTAUSKAS, V.; MALINAUSKAITE, I. Asmens duomenų apsaugos virtualiuose socialiniuose tinkluose teisinė apsauga. Societal Innovations for Global Growth, 2012.
109. ŠTITILIS, D.; KLISAUSKAS, V. Criminalization of dangerous acts in cyberspace in criminal codes of Lithuania and Russia: comparative aspects. Matters of Russian and International Law, 2013.

110. ŠTITILIS, D.; KRIKŠČIŪNAS, R.; PETRAUSKAS, R. Kai kurie Konvencijos dėl elektroninių nusikaltimų proceso teisės skirsnio įgyvendinimo Lietuvoje aspektai. *Jurisprudencija*, 2005.
111. ŠTITILIS, D.; LAURINAITIS, M. *IP* telefonija – iššūkis elektroninių ryšių kontrolės, siekiant ištirti nusikaltimus, teisiniam reguliavimui. Socialinių mokslų studijos, 2009.
112. ŠTITILIS, D.; LAURINAITIS, M. Tapatybės vagystė elektroninėje erdvėje. Informacijos mokslai, 2009.
113. ŠTITILIS, D.; MALINAUSKAITĖ, I. Compliance with basic data protection principles in cloud computing: the aspect of contractual relations with end-users. EJLT European Journal of Law and Technology, 2014. Prieiga per internetą: <*http://ejlt.org/article/view/231/422*>.
114. ŠTITILIS, D.; PAKUTINSKAS, P.; DAUPARAITĖ, I.; LAURINAITIS, M. Preconditions for legal Regulation of Personal Identity in Cyberspace. *Jurisprudencija*, 2011.
115. ŠTITILIS, D.; PAKUTINSKAS, P.; DAUPARAITĖ, I.; LAURINAITIS, M. Tapatybės vagystė elektroninėje erdvėje: socialiniai, elektroninio verslo ir teisinio reguliavimo aspektai: kolektyvinė mokslo monografija. Vilnius: Mykolo Romerio universitetas, 2011.
116. ŠTITILIS, D.; PAŠKAUSKAS, Ž. Valstybės elektroninės informacijos saugos strategija – vienas iš pagrindinių elektroninės informacijos saugos reguliavimo instrumentų: lyginamoji analizė. *Jurisprudencija*, 2007.
117. ŠTITILIS, D.; PETRAUSKAS, R. Criminal Acts in Computer Systems and Their Legal Regulation. Databases & information systems. Proceedings of the 4th IEEE international Baltic workshop. Vilnius: Technika, 2000.
118. ŠTITILIS, D.; KLIŠAUSKAS, V. Elektroninės informacijos saugos reglamentavimas Lietuvoje ir Rusijoje: lyginamieji aspektai. Socialinės technologijos, 2012. Prieiga per internetą: <*http://www.mruni.eu/lt/mokslo_darbai/st/archyvas/dwn.php?id=340084*>.
119. TALBOT, J.; WELSH, D. Complexity and Cryptography. An Introduction. Cambridge, 2006.
120. TAMBURRINI, P. European Computer Law. Information Technology Law Group/Europe. Transnational Publishers, Inc., New York, 1996.
121. TER, W. B. Cybertax. 1997. Prieiga per internetą: <*http://www-edocs.unimaas.nl/abs/mer97019.htm*>.
122. The New Data Retention Directive. European Media, *IP* & IT Law Review, 2006.
123. ŪSELIS, D. Kompiuterinių nusikaltimų formos ir rūšys, 2000. Prieiga per internetą: <*http://www.sociumas.lt/lit/nr18/PC.asp*>.
124. VAITKEVIČIENĖ, R. Elektroninių duomenų naudojimo civiliniame procese galimybės. *Justitia*, 2005.
125. VOLEVODZ, A. G. Protivodeistvije kompiuternim prestuplenijam. Jurlitinform. Moskva, 2002.
126. VOLKAMER, M.; HUTTER, D. From Legal Principles to an Internet Voting System. Electronic Voting in Europe –Technology, Law, Politics and

Society, Workshop of The ESF TED Programme together with GI and OCG. Austria, 2004.
127. WARD, B. T.; SIPIOR, J. C.; HOPKINS, J. P.; PURWIN, C.; VOLONINO, L. Electronic discovery: rules for a digital age. Boston University Journal of Science & Technology Law, 2012.
128. WILLIAMS, M. Virtually criminal: Crime, deviance and regulation online. Routledge. New York, 2006.
129. WILLIAMSON, A. Disruption and Empowerment. Embedding citizens at the Heart of Democracy, 2011.
130. ŽILINSKAS, V.; KASPERAVIČIUS, P.; KIŠKIS, M. Intelektinė nuosavybė ir jos teisinė apsauga. Klaipėda: KU, 2007.

6. Mokslo darbai

1. STANKEVIČ, A. Teismingumas, taikytina teisė ir įrodinėjimas civilinėse bylose dėl neleistino informacijos skelbimo internete: galimybės ir problemos. Daktaro disertacija, socialiniai mokslai, teisė. Vilnius: VU, 2012.

7. Internetiniai saltiniai

1. Akdeniz Y. The Regulation of Pornography and Child Pornography on the Internet. The Journal of Information, Law and Technology (JILT), 1997. Prieiga per internetą: *<http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/1997_1/akdeniz1>*.
2. AS Sertifitseerimiskeskus. Prieiga per internetą: *<http://www.epracticel.eu/files/media/media_603.pdf>*.
3. Asmens tapatybės kortelės. Prieiga per internetą: *<http://www.pasienis.lt/lit/Asmens_tapatybes_korteliu_galiojimas_ir_/132>*.
4. Asmens tapatybę patvirtinančiu dokumentu siūloma laikyti ir vairuotojo pažymėjimą. Prieiga per internetą: *<http://www.vrm.lt/index.php?id=131&backPID=1340&pS=1270069200&pL=2591999&arc=1&tt_news=2466&>*.
5. Authencity of electronic records: A report, prepared for UNESCO (ICA Study 13-1). International council on Archives Committee on Archival Legal Matters. 2004. Prieiga per internetą: *<http://www.wien2004.ica.org/sites/default/files/Study13_2Erev.pdf>*.
6. Cybersecurity Strategy for Germany. 2011. Prieiga per internetą: *<https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf?__blob=publicationFile>*.
7. Cybervote, An innovative cyber voting system for Internet terminals and mobile phones, 2001. Prieiga per internetą: *<http://www.eucybervote.org/reports.html>*.
8. Computerworld, 2005. Prieiga per internetą: *<http://computerworld.com/governmenttopics/government/itgovernment/story/0,10801,106665,00.html>*.
9. Convention of Cybercrime CETS No.: 185, Status as of : 10/05/2011. Prieiga per internetą: *<http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=10/05/2011&CL=ENG>*.

10. Data protection – European Commission. Prieiga per internetą: <*http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm*>.
11. Data Protection Review: Impact on EU Innovation and Competitiveness, Europos Parlamentas, Briuselis, 2012. Prieiga per internetą: <*http://www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=78970*>.
12. Definition of cybersecurity, ITU. Prieiga per internetą: <*http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx*>.
13. Digital Agenda – Commission consults on a future EU Network and Information Security legislative initiative. Briuselis, 2012. Prieiga per internetą: <*http://europa.eu/rapid/press-release_IP-12-818_en.htm*>.
14. E – Teismas. Elektroninių paslaugų teisingumo vykdymo procese informacinė sistema. Naudotojo vadovas. 2013. Prieiga per internetą: <*https://e.teismas.lt/media/66909/epp_naudotojo_vadovas.pdf*>.
15. E. government in Germany. Prieiga per internetą: <*http://www.zenc.nl/uploads/d5/c7/d5c77e3fd3d6c8597075d263ab0057f2/egovernment_in_germany.pdf*>.
16. E.business strandarts in Germany. Prieiga per internetą: <*http://www.berlecon.de/research/en/reports.php?we_objectID=125*>.
17. eCommerce in Europe: trends and Outlook.
18. E-Estonia. Prieiga per internetą: <*http://e-estonia.com/*>.
19. Electronic Authentication Guideline. Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-63 Version 1.0.2. Prieiga per internetą: <*http://www.usda.gov/egov/egov_redesign/intranet/eauth/SP800-63V6.pdf*>.
20. Electronic contracts in the U.S. Prieiga per internetą: <*http://www.ejcl.org/53/art53-1.html*>.
21. Electronic Signature. Prieiga per internetą: <*http://electronicsignature.com/esignact/*>.
22. Elektroninis parašas Lietuvoje. Prieiga per internetą: <*http://www.elektroninisparasas.lt/olat/dmz/*>.
23. E-Sign Legislation - The milestone in the e-signature history. Prieiga per internetą: <*http://www.elock.com/resources-e-sign.html*>.
24. EU electronic signature regulation. Prieiga per internetą: <*http://www.eldos.com/security/articles/5743.php*>.
25. European Government CERTs (EGC) group. Prieiga per internetą: <*http://www.egc-group.org/*>.
26. Europos komisija: pranešimas spaudai. ES kibernetinio saugumo planu siekiama apsaugoti atvirą internetą, elektroninę laisvę ir galimybes. Briuselis, 2013. Prieiga per internetą: <*http://europa.eu/rapid/press-release_IP-13-94_lt.htm*>.
27. Europos Taryba, LTU-FO-02002. Prieiga per internetą: <*http://www.consilium.europa.eu/prado/LT/2812/docHome.html*>.
28. E-Voting Security Study, Crown Copyright, 2002. Prieiga per internetą: <*http://www.ictparliament.org/CDTunisi/ict_compendium/paesi/uk/uk54.pdf*>.

29. First INTERPOL information security conference to provide global platform for preventing and detecting high-tech crimes. Prieiga per internetą: <*http://www.interpol.int/public/ICPO/PressReleases/PR2010/PR070.asp*>.
30. France information systems defence and security strategy. 2011. Prieiga per internetą: <*http://www.ssi.gouv.fr/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf*>.
31. Germany el. invoice. Prieiga per internetą: <*http://www.e-invoice-gateway.net/knowledgebase/countryrelated/details/230/*>.
32. Global Risks 2008. 2008 m. pasaulinių grėsmių ataskaita. Prieiga per internetą: <*http://www.scribd.com/doc/6310131/Global-Risk-Report-2008*>.
33. Google targeted in e-mail scam. Prieiga per internetą: <*http://news.bbc.co.uk/2/hi/technology/8292928.stm*>.
34. Guide to Authentication Standards for Online Services. State Services Commission, June 2006, Version 1.0. ISBN 0–478–24461–4. Crown Copyright. Prieiga per internetą: <*http://www.e.govt.nz/plone/archive/services/authentication/standards/guide-to-authentication.1.html*>.
35. International Organization For Standards. *ISO* 15489-1. Information and Documentation – Records Management. Part 1. Prieiga per internetą: <*http://www.javeriana.edu.co/archivo/07_eventos/preservaciondigital/memorias/index_archivos/norma/iso_15489-1.pdf*>.
36. International review of criminal policy - United Nations Manual on the prevention and control of compute-related crime. Jungtinių tautų tarptautinėje kriminalinės policijos kompiuterinių nusikaltimų apžvalga. Prieiga per internetą: <*http://www.uncjin.org/Documents/irpc4344.pdf*>.
37. Interpol chief has Facebook identity stolen. Prieiga per internetą: <*http://www.networkworld.com/news/2010/091910-interpol-chief-has-facebook-identity.html*>.
38. Lithuania - Digital Media and Broadband Market Insights Statistics and Forecasts. Prieiga per internetą: <*http://www.budde.com.au/Research/Lithuania-Digital-Media-and-Broadband-Market-Insights-Statistics-and-Forecasts.html*>.
39. NGA progress report, *study* for ECTA, 2012. Prieiga per internetą: <*http://ebookbrowse.com/nga-progress-report-final-pdf-d335292546*>.
40. OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. Prieiga per internetą: <*http://www.oecd.org/document/48/0,3746,en_2649_34255_15582250_1_1_1_1,00.html*>.
41. Overview of electronic ID documents. Prieiga per internetą: <*https://www.bsi.bund.de/EN/Topics/ElectrIDDocuments/EID_nodel.html*>.
42. PHARE dvynių projekto LT02/IB-JH-02/03 „Asmens duomenų apsaugos administracinių ir techninių gebėjimų stiprinimas“ medžiaga. Prieiga per internetą: <*http://www.ada.lt*>.
43. Privatumo politika. Prieiga per internetą: <*http://rrt.lt/lt/privatumo-politika.html*>.
44. Report highlights uncertainty on cost of EU data protection reform, 2013. Prieiga per internetą: <*http://www.ico.org.uk/news/latest_news/2013/report-highlights-uncertainty-on-cost-of-eu-data-protection-reform-14052013*>.

45. Ryšių reguliavimo tarnybos informacija apie el. parašą. Prieiga per internetą: <*http://www.rrt.lt/lt/verslui/elektroninis-parasas/apie-e-parasa.html*>.
46. Siliconrepublic.com. 2006. Prieiga per internetą: <*http://www.siliconrepublic.com/news/news.nv?storyid=single7158*>.
47. Survey on the Cybercrime Convention (CETS 185) and its additional protocol (CETS 189). European Committee on Crime Problems. Prieiga per internetą: <*http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/default_en.asp*>.
48. The Sedona Conference® commentary on ESI Evidence&Admissability. 2008. Prieiga per internetą: <*https://thesedonaconference.org/publication/The%20Sedona%20Conference%C2%AE%20Commentary%20on%20ESI%20Evidence%20%2526%20Admissibility*>.
49. The Sedona Principles: Best Practices Recommendations&Principles for Addressing Electronic Document Production, Second Edition. 2007. Prieiga per internetą: <*http://www.sos.mt.gov/Records/committees/erim_resources/A%20%20Sedona%20Principles%20Second%20Edition.pdf*>.
50. The UK cyber security strategy: Landscape review. 2013. Prieiga per internetą: <*http://www.nao.org.uk/report/the-uk-cyber-security-strategy-landscape-review/*>.
51. U.S Electronic Signature. Prieiga per internetą: <*http://www.mmmlaw.com/Articles/ElectronicSignatureLegislation.htm*>.
52. U.S. Commerce Department. Prieiga per internetą: <*http://www.internetretailer.com/2012/02/16/e-commerce-sales-jump-16-2011*>.
53. U.S. Federal Trade Commission, Department Of Commerce. „Electronic signatures in global and national commerce act". Prieiga per internetą: <*http://www.secretary.state.nc.us/ecomm/pdf/fedsignatures.pdf*>.
54. UK cybersecurity strategy. Protecting and promoting the UK in a digital world, 2011. Prieiga per internetą: <*http://www.carlisle.army.mil/dime/documents/UK%20Cyber%20Security%20Strategy.pdf*>.
55. Valstybinės duomenų apsaugos inspekcijos Rekomendacija dėl slapukų naudojimo. Prieiga per internetą*:* <*http://www.ada.lt/images/cms/File/naujienu/slapuk_DS.pdf*>.
56. Vokietijos paslaugų teikėjų teikiamos paslaugos. Prieiga per internetą: <*http://www.bundesnetzagentur.de/media/archive/3612.pdf*>.
57. VU mokslininkas: informacijos saugumo klausimą reikia kelti jau šiandien. Technologijos.lt. Prieiga per internetą: <*http://www.technologijos.lt/n/technologijos/it/S-31575/straipsnis/VU-mokslininkas-informacijos-saugumo-klausima-reikia-kelti-jau-siandien?l=2&p=1*>.
58. Wij Vertrouwen Stemcomputers Niet. 2009. Prieiga per internetą: <*http://www.wijvertrouwenstemcomputersniet.nl/English*>.
59. Žmogaus teisių įgyvendinimas Lietuvoje: apžvalgos. Žmogaus teisių stebėjimo institutas. Prieiga per internetą: <*http://www.hrmi.lt*>.
60. Žmogaus teisių stebėjimo institutas: Privataus gyvenimo ribojimas elektroninių ryšių srityje nusikaltimų tyrimo ir prevencijos tikslais. 2005. Prieiga per internetą: <*http://www.hrmi.lt*>.

In-156 **Interneto** ir technologijų teisė : vadovėlis / [Darius Štitilis, Mindaugas Kiškis, Tadas Limba ... [et al.] ; Mykolo Romerio universitetas. – Vilnius : Registrų centras, 2016. – 576 p.

Aut. nurodyti antr. lapo kt. pusėje. – Bibliogr.: p. 558–574

ISBN 978-9955-30-214-8 (spausdinta)

ISBN 978-9955-30-213-1 (el. knyga)

Šiame vadovėlyje nagrinėjamos bendrosios informacinių technologijų bei teisės sąveikos problemos ir pateikiami naujų technologijų teisės pagrindai.
Vadovėlis yra skirtas visų lygių teisės studijų programų studentams, bet jame nagrinėjamos interneto, elektroninių ryšių, e. komercijos, e. sutarčių, e. įrodymų, nano- ir biotechnologijų bei robotikos teisinio reglamentavimo principai, intelektinės nuosavybės ir privatumo, asmens duomenų apsaugos elektroninėje erdvėje, elektroninių nusikaltimų ir kibernetinio saugumo pamatinės nuostatos turėtų sudominti ne tik studentus ir praktikuojančius teisininkus, bet ir informacinių technologijų specialistus bei visus tuos, kuriems kiekvieną dieną tenka naudotis informacinėmis technologijomis darbo ar asmeniniams tikslams.

UDK 004.738.5(094)(075.8)

INTERNETO IR TECHNOLOGIJŲ TEISĖ

Redagavo Jūratė Juknevičiūtė, maketavo Janina Kaminskaitė
Viršelio dailininkė Jūratė Juozėnienė
Parengė leidybai Algis Švedas

SL 1613. 2016-07-05. 72 sąlyginiai spaudos lankai
Tiražas 700 egz. Užsakymo Nr.

Išleido VĮ Registrų centras

Parengė VĮ Registrų centro Teisinės informacijos departamentas
Žirmūnų g. 68A, 09124 Vilnius
tel./faksas (8 5) 261 2806
www.teisineliteratura.lt, *leidyba@teisineliteratura.lt*

Spausdino STANDARTŲ SPAUSTUVĖ
S. Dariaus ir S. Girėno g. 39, 02189 Vilnius

Kaina sutartinė