ISSN 1392-1592. TEISĖS PROBLEMOS. 2010. Nr. 4 (70)

Vaidas KALPOKAS
Teisės instituto Kriminologinių tyrimų
skyriaus jaunesnysis mokslo darbuotojas
Gedimino pr. 39 / Ankštoji g. 1,
LT-01109 Vilnius
Tel.: (8 5) 210 16 74
El. p.: *vaidas@teise.org*

SKAITMENINĖS ERDVĖS REGULIAVIMAS IR KONTROLĖ: SAUGUMO ASPEKTAI[1]

Informacinės technologijos atvėrė naują žmonijos egzistavimo matmenį, vadinamąją skaitmeninę erdvę, kurioje 2011 m. pradžioje bus daugiau nei 2 milijardai gyventojų. Deja, svaiginančios galimybės, viliojančios į šią erdvę vis daugiau naujakurių, neišvengiamai susijusios su tam tikromis grėsmėmis ir pavojais. Kokios tai grėsmės? Ar skaitmeninėje erdvėje reikalingi vidinės tvarkos palaikymo mechanizmai, būtini bet kurios kitos žmonių bendruomenės išlikimui? Kas ir kokiais būdais galėtų užtikrinti tokių mechanizmų veikimą ekstrateritoriniame, decentralizuotame darinyje – internete? Tai klausimai, į kuriuos bent iš dalies mėginama atsakyti šiame straipsnyje.

ĮVADAS

Galime konstatuoti, kad informacinės technologijos (toliau – IT) tapo neatsiejama visuomenės ekonominio, socialinio bei kasdienio gyvenimo dalimi. Daugeliui mūsų šalies ir viso pasaulio gyventojų dalyvavimas virtualioje elektroninėje erdvėje vykstančioje veikloje tampa nebe naujovių tyrinėjimu ir išbandymu, o veikiau įprasta rutina. Vis tebedidėjančios plačiajuostės fiksuotos ar bevielės interneto prieigos galimybės, taip pat vis platesnis IT taikymas įvairiose valstybės valdymo ir paslaugų, ekonominės veiklos bei socialinio

[1] Straipsnio autoriaus ir žurnalo redakcijos vardu už vertingas pastabas ir pasiūlymus šiam straipsniui nuoširdžiai dėkojame Mykolo Romerio universiteto Socialinės informatikos fakulteto Elektroninio verslo katedros docentui dr. *Irmantui Rotomskiui*.

gyvenimo srityse sukuria tai, kas konceptualiai vadinama „skaitmenine ekonomika“.

Nors IT infrastruktūros išsivystymo bei naudojimo lygis skirtingose valstybėse yra nevienodas, skaitmeninė ekonomika funkcionuoja kaip globalus reiškinys. Valstybės, pripažindamos skaitmeninės ekonomikos svarbą siekiant ekonominių ir socialinių tikslų bei norėdamos būti konkurencingos, privalo visokeriopai skatinti gyventojų galimybes, supratimą ir norą naudotis IT teikiamais privalumais. Viena vertus, reikia siekti, kad IT plėtra apimtų kuo didesnę teritoriją ir santykinai nebrangi, sparti ir laisva interneto prieiga taptų prieinama kuo didesniam gyventojų skaičiui tiek didesniuose miestuose, tiek atokiuose šalies kampeliuose. Šio uždavinio įgyvendinimas (kuriam reikia atitinkamo finansavimo bei tam tikro valstybės ir verslo struktūrų bendradarbiavimo) pats savaime nėra labai sudėtingas ir Lietuvoje jau kurį laiką pakankamai sėkmingai vykdomas.[2] Kita vertus, greta techninės interneto prieigos galimybės užtikrinimo ne mažiau svarbus ir kur kas komplikuotesnis uždavinys, skatinant gyventojų pasitikėjimą ir naudojimąsi informacinėmis technologijomis – skaitmeninėje erdvėje formuoti ir palaikyti kiek įmanoma saugią vartotojui aplinką.

Ne paslaptis, kad IT plėtra ir skverbimasis į vis įvairesnes gyvenimo sritis šių technologijų vartotojams suteikia ne tik didesnę naudojimosi galimybių įvairovę, bet ir sukelia tam tikrų grėsmių. Kai kurios iš šių grėsmių (pvz., sukčiavimas, priekabiavimas, šantažas ir kt.) pakankamai gerai žinomos ir persikėlusios į elektroninę erdvę iš dar „ikiskaitmeninių“ laikų, kitos (pvz. neteisėtas prisijungimas, kompiuteriniai virusai, atakos prieš kompiuterines sistemas) atsirado

[2] Nuo 2004 iki 2008 m. Lietuvos gyventojams, įsigijusiems asmeninį kompiuterį bei įsirengusiems interneto prieigą, buvo taikoma gyventojų pajamų mokesčio lengvata. Nuo 2005 m. Lietuvoje, iš dalies finansuojant Europos Sąjungai, vykdomas projektas „Kaimiškųjų vietovių informacinių technologijų plačiajuostis tinklas (RAIN)“. Iki 2012 m. numatyta įgyvendinti antrąjį šio projekto etapą „Kaimiškųjų vietovių informacinių technologijų plačiajuosčio tinklo RAIN plėtra (RAIN-2)“, sudarant galimybes 98 proc. šalies kaimiškųjų teritorijų gyventojų, valstybės ir viešojo sektoriaus institucijų bei verslo organizacijų naudotis plačiajuosčio ryšio paslaugomis. Plačiau apie projektą žr. http://www.rain.lt. Taip pat pažymėtina, kad 2010 m. pradžioje Lietuva tapo pirmaujančia Europoje ir užėmė 5 vietą pasaulyje pagal šviesolaidinio interneto paplitimą namų ūkiuose (18 proc.). 2010 m. spalio mėn. duomenimis Lietuva (21 proc.) išlaiko pirmaujančią poziciją. Plačiau žr.: Europos Sąjungos naujokės ir toliau pirmauja pagal FTTH plėtrą. FTTH Council Europe pranešimas spaudai. Prieiga per internetą: http://www.ftthcouncil.eu/documents/press_release/2010/PR2010_EU_Ranking_mid_2010_Final_LI.pdf.

pradėjus plisti kompiuteriams ir internetui. Visas šias grėsmes vienija tai, kad jos kyla ir yra įgyvendinamos specifinėje aplinkoje – skaitmeninėje elektroninėje erdvėje, kurios galimybės leidžia kurti vis naujus tokios veiklos būdus.[3]

Įvairių valstybės institucijų, verslo įmonių funkcionavimas darosi vis labiau priklausomas nuo sklandaus ir saugaus IT pritaikymo ir veikimo. IT naudojimas tampa būtina sąlyga visuomenės ir skaitmeninės ekonomikos raidai, todėl su tuo susijusių grėsmių bei rizikos valdymas turėtų būti suprantamas kaip svarbi valstybės pastangų skatinant gyventojų dalyvavimą skaitmeninėje ekonomikoje dalis ir orientuotas į visą gyventojų populiaciją. Toliau straipsnyje apžvelgiamos informacinių technologijų naudojimo Lietuvoje ir kitose šalyse tendencijos bei su tuo susijusios grėsmės, aptariamos galimybės ir būdai šias grėsmes mažinti bei galimos valstybės institucijų ir kitų suinteresuotų šalių veiklos kryptys.

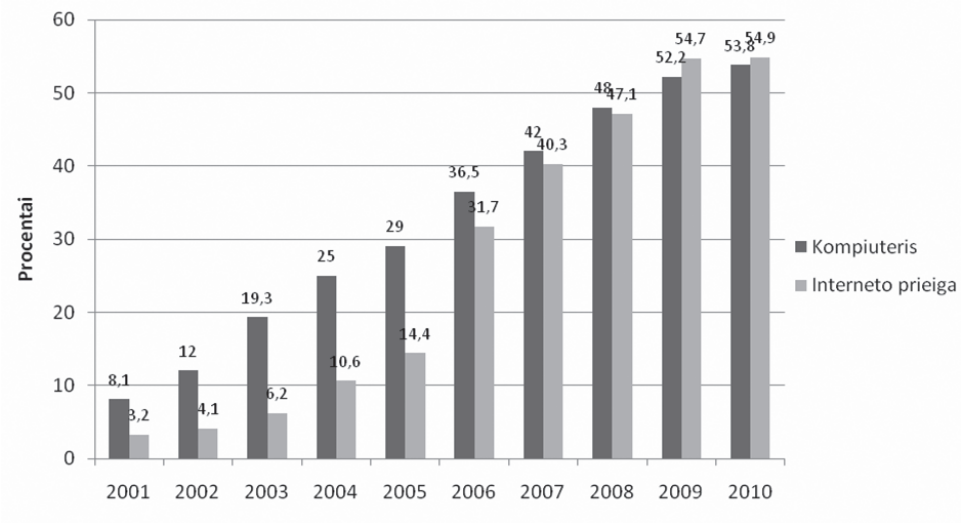
IT NAUDOJIMO TENDENCIJOS: GALIMYBĖS IR GRĖSMĖS

Jeigu IT saugumą laikysime veiksniu, skatinančiu vartotojų pasitikėjimą ir norą naudotis informacinėmis technologijomis bei tokiu būdu plečiančiu gyventojų dalyvavimą skaitmeninėje ekonomikoje, tuomet, siekiant tokio saugumo užtikrinimo, labai svarbu suprasti IT naudojimo tendencijų, suteikiamų galimybių bei potencialių grėsmių tarpusavio ryšį. Čia reikėtų atkreipti dėmesį į dvi aplinkybes. Visų pirma, IT raida pasižymi ypatinga dinamika, technologijų taikymo bei naudojimo būdai **nuolat kinta ir plečiasi**, todėl visi bandymai mažinti susijusias grėsmes neišvengiamai pasmerkti būti nuolatinėje prisitaikymo būklėje. Antra, kokios bebūtų priemonės, skirtos saugumo virtualioje erdvėje didinimui, jos turėtų būti planuojamos ir įgyvendinamos taip, kad kuo **mažiau ribotų pačias vartotojų galimybes** naudotis visais IT teikiamais privalumais. Kitaip tariant, turėtų būti išlaikomas toks saugumo priemonių ir suteikiamų galimybių balansas, kad pertekliniai ribojimai neatgrasintų vartotojų nuo naudojimosi IT, užuot tokį naudojimąsi skatinę.

[3] Plačiau žr. *Kalpokas V.* Nusikaltimai elektroninėje erdvėje: kriminologinės sampratos dilemos // Teisės problemos, 2009, Nr. 1; *Kalpokas V.* Nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui. Knygoje: Sakalauskas G., Dobrynina M., Justickaja S. [et al.]. Registruotas ir latentinis nusikalstamumas Lietuvoje: tendencijos, lyginamieji aspektai ir aplinkos veiksniai. Teisės instituto mokslo tyrimai. 7 tomas. Vilnius: Eugrimas, 2011, p. 168–183.

Pastarųjų metų IT plitimo tendencijas akivaizdžiai patvirtina ir statistiniai duomenys. Statistikos departamento prie Lietuvos Respublikos Vyriausybės duomenimis,[4] IT naudojimas Lietuvos namų ūkiuose plinta itin sparčiai (*1 pav.*).

1 pav. Namų ūkiai Lietuvoje, turintys asmeninį kompiuterį, interneto prieigą



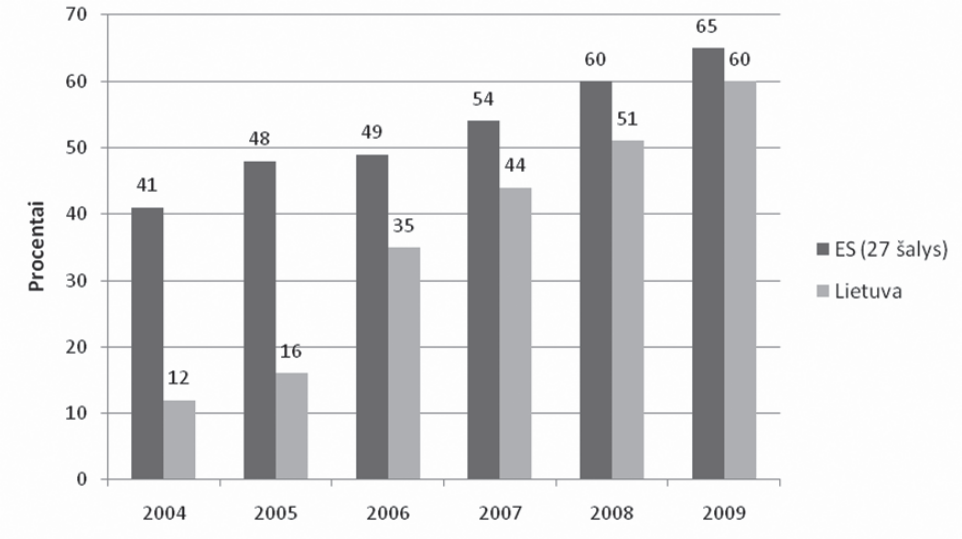
Nuo 2000 iki 2010 m. kompiuterius turinčių namų ūkių padaugėjo dešimteriopai ir šio laikotarpio pabaigoje jų dalis jau sudarė 53,8 proc. tarp visų namų ūkių. Interneto prieigos plėtra ypač paspartėjo po 2005 m., o 2010 m. pradžioje jau 54,9 proc. namų ūkių turėjo galimybę vienokiu ar kitokiu būdu prisijungti prie interneto. Taigi 2008–2009 m. gali būti laikomi tam tikro simbolinio lūžio metais, kai internetas ir asmeninis kompiuteris tapo prieinamas didžiajai (didesnei negu pusė ir, veikiausiai, vis didėsiančiai) Lietuvos namų ūkių daliai. Be to, 2010 m. interneto prieiga darbo vietoje naudojosi 62,6 proc. valstybės ir savivaldybių valdymo įstaigų darbuotojų, o tarp verslo įmonių interneto prieigą turėjo 96,9 proc. visų įmonių.[5]

[4] Statistikos departamentas prie Lietuvos Respublikos Vyriausybės. Informacinių technologijų naudojimo namų ūkiuose statistinio tyrimo duomenys. Prieiga per internetą: http://www.stat.gov.lt/lt/pages/view/?id=1584.

[5] Statistikos departamentas prie Lietuvos Respublikos Vyriausybės. Informacinių technologijų naudojimo įmonėse bei valstybės ir savivaldybių valdymo įstaigose tyrimų duomenys. Prieiga per internetą: http://www.stat.gov.lt/lt/pages/view/?id=1584.

Europos Sąjungos Statistikos biuro Eurostat duomenimis, Lietuva yra 17-toje vietoje tarp ES šalių ir vis dar šiek tiek atsilieka nuo ES vidurkio pagal interneto prieigos paplitimą namų ūkiuose,[6] tačiau nuo 2006 m. šis atsilikimas vis labiau mažėja (*2 pav.*). Europos Sąjungoje pagal šį rodiklį pirmauja Nyderlandai, kur net 90 proc. namų ūkių turi interneto prieigą, nedaug atsilieka Liuksemburgas (87 proc.), Švedija (86 proc.), Danija (83 proc.), taigi galima manyti, kad plėtros potencialas Lietuvoje vis dar išlieka pakankamai didelis.

2 pav. Namų ūkiai, turintys interneto prieigą. 27 ES šalių narių vidurkio ir Lietuvos duomenų palyginimas.



Pagal gyventojų naudojimąsi internetu Lietuva taip pat nedaug atsilieka nuo ES šalių vidurkio. 2009 m. reguliariai (ne rečiau kaip kartą per savaitę, bet ne kiekvieną dieną) internetu naudojosi 55 proc. 16–74 m. Lietuvos gyventojų (ES vidurkis – 60 proc.). Dažnai (kasdien arba beveik kasdien) internetu naudojosi 43 proc. Lietuvos gyventojų (ES vidurkis 48 proc.). Aktyviausiai internetu naudojasi jaunesnio amžiaus gyventojai. 2009 m. Lietuvoje tarp 16–24 m. respondentų net 82 proc. internetu naudojosi dažnai (ES vidurkis 73

[6] Eurostat. Households who have Internet access at home. Prieiga per internetą: http://epp.eurostat.ec.europa.eu/tgm/table.do?tab=table&init=1&plugin=1&language=en&pcode=tin00088.

proc.). Palaipsniui aktyvių interneto naudotojų skaičius didėja ir tarp vyresnio amžiaus gyventojų. 2004–2009 m. laikotarpiu dažnai internetu besinaudojančių 25–54 m. gyventojų Lietuvoje padaugėjo nuo 15 proc. iki 44 proc. (ES nuo 27 proc. iki 53 proc.), o 55–74 m. grupėje šis skaičius padidėjo nuo 3 proc. iki 10 proc. (ES nuo 8 proc. iki 23 proc.).[7]

Pateikti duomenys rodo nuoseklią ir pakankamai sparčią interneto prieigos ir jo naudojimo plėtrą. Nėra pagrindo manyti, kad artimiausioje ateityje ši tendencija keisis. Informacinės technologijos, internetas smelkiasi į kasdienį žmonių gyvenimą ir tampa viena iš neatsiejamų sudėtinių jo dalių. Kita vertus, vis daugiau kasdienio gyvenimo sričių persikelia į internetinę erdvę, atsiranda vis daugiau galimybių bendrauti, gauti paslaugas, prekes, informaciją, spręsti įvairiausius klausimus, nepakylant nuo kompiuterio. Pamažu nyksta anksčiau dažnai akcentuota skirtis tarp gyvenimo šiapus ir anapus kompiuterio ekrano arba, kitaip tariant, darosi vis sunkiau nubrėžti ribą tarp „realaus“ ir „virtualaus“ pasaulių, o ankstesnės dichotomijos tarp realybės ir virtualybės, visuomenės ir technologijų, lokalumo ir globalumo tampa vis mažiau aktualios.[8]

Eurostat pateikia duomenis ne tik apie interneto prieigos bei jo naudojimo paplitimą, bet ir apie kai kuriuos konkrečius naudojimosi internetu būdus. *3 pav.* pavaizduotas įvairių interneto naudojimo būdų paplitimas tarp Lietuvos gyventojų 2009 m. (kai kuriais atvejais pateikiami 2008 m. duomenys). Greta pavaizduotas atitinkamų interneto naudojimo būdų paplitimo tarp 27 ES šalių gyventojų vidurkis.

Iš karto pažymėsime, kad šis sąrašas tikrai neapima visos naudojimosi internetu galimybių įvairovės.[9] Tai suprantama, nes, viena vertus, tokių galimybių vis daugėja, o nuolat koreguoti kasmet pagal suderintą metodiką visoje ES atliekamo tyrimo klausimynus ko gero nėra taip paprasta. Kita vertus, galima

[7] Eurostat. Individuals frequently using the Internet. Prieiga per internetą: http://epp.eurostat.ec.europa.eu/tgm/table.do?tab=table&init=1&plugin=1&language=en&pcode=tin00092.

[8] *Aas K. F.* Beyond „the deserto f the real“: crime control in a virtual(ised) reality. Iš: Jewkes Y. (ed.). Crime Online. Portland: Willan Publishing, 2007, p. 166.

[9] Pvz., čia neatsispindi pastaruoju metu labai išpopuliarėjęs bendravimas vadinamuosiuose socialiniuose tinkluose. 2010 m. lapkričio 8 d. duomenimis vien populiariausiame *Facebook* socialiniame tinkle buvo užsiregistravę daugiau nei 756 000 vartotojų iš Lietuvos, t. y. beveik 36 proc. visų Lietuvos interneto vartotojų. Duomenys iš http://www.checkfacebook.com. Tiesa, 2010 m. Eurostat namų ūkių tyrimo klausimyne socialinių tinklų naudojimas jau yra paminėtas, nors ir neišskirtas į atskirą eilutę.

manyti, kad respondentų vertinimui pateikiami labiau socialiai priimtini interneto naudojimo būdų pasirinkimai, nuošalyje paliekant ne tokius pageidautinus ar net galimai neteisėtus. Kaip bebūtų, iš pateiktų duomenų matome, kad Lietuvos vartotojai internetą dažniausiai naudoja elektroninių dienraščių ar žurnalų skaitymui (49 proc.), susirašinėjimui elektroniniu paštu (47 proc.) bei informacijos apie prekes ir paslaugas paieškai (44 proc.). Toliau seka muzikos ar filmų parsisiuntimas, klausymas ar žiūrėjimas (32 proc. 2008 m. duomenimis) bei internetinė bankininkystė (32 proc.). Didelis atotrūkis nuo ES vidurkio matomas elektroninės prekybos srityje. Tik 8 proc. Lietuvos gyventojų užsakinėjo prekes ar paslaugas internetu, o visoje Europos Sąjungoje tokių respondentų buvo 37 proc. Pagal šį rodiklį Lietuva lenkia tik dvi ES valstybes: Rumuniją (2 proc.) ir Bulgariją (5 proc.) ir labai atsilieka nuo lyderių – Jungtinės Karalystės (66 proc.), Danijos (64 proc.), Nyderlandų bei Švedijos (po 63 proc.). Tiek Europos šalių patirtis, tiek mūsų šalyje matomos tendencijos, kai vis daugiau prekybos įmonių keliasi į internetinę erdvę,[10] leidžia manyti, kad yra pakankamai daug prielaidų elektroninės prekybos Lietuvoje apimčių didėjimui.

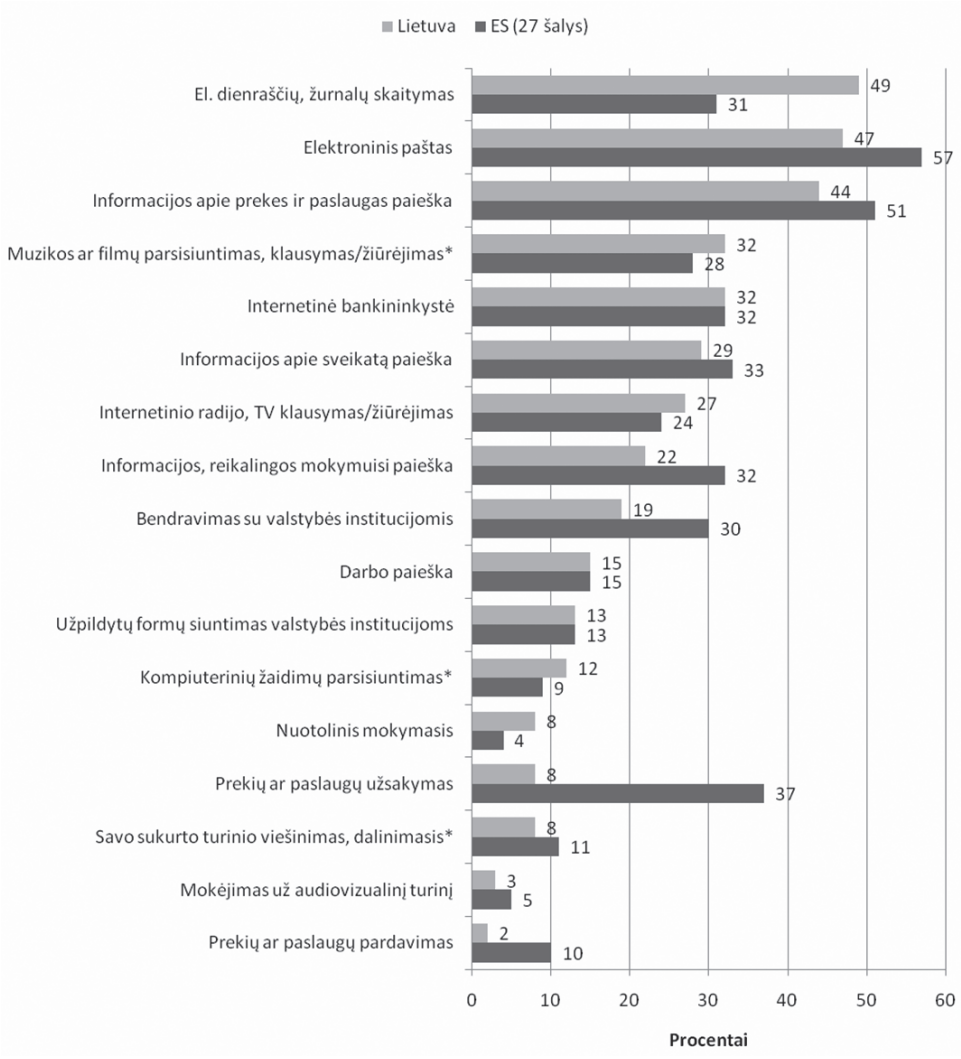
Be elektroninės prekybos įsigalėjimo tyrėjai išskiria dar keletą svarbių pastaraisiais metais IT srityje vykstančių procesų. Australijos vyriausybinės institucijos ACMA (angl. *Australian Communication and Media Authority*) atstovai savo metiniame pranešime, skirtame interneto saugumo problemoms,[11] pagrindinėmis aktualiomis tendencijomis laiko spartų trečiosios kartos mobiliųjų įrenginių (išmaniųjų telefonų, delninių kompiuterių ir pan.) plitimą bei vis didėjantį interneto interaktyvumą, t. y. socialinių sąveikų, pasinaudojant populiarių socialinių tinklų, tinklaraščių bei kitų interneto tarnybų galimybėmis, daugėjimą.

Naujosios kartos mobilieji įrenginiai tampa viena iš alternatyvių interneto prieigos platformų (naudojant juos ne tik interneto naršymui ar turinio peržiūrai, bet ir elektroniniam paštui, geolokacijai bei navigacijai, prisijungimui prie bankinių paslaugų teikėjų, socialinių tinklų, vaizdo bei garso įrašams ir dauge-

[10] *Simonavičius G.* Prekyba keliasi į internetą // LTV „Šiandien“, 2009 07 27. Prieiga per internetą: http://lrt.lt/news.php?strid=31489&id=5252379.

[11] ACMA (angl. *Australian Communications and Media Authority*). Online risk and safety in the digital economy: Third annual report to the Minister for Broadband, Communications and the Digital Economy on developments in internet filtering and other measures for promoting online safety. Prieiga per internetą: http://www.acma.gov.au/webwr/_assets/main/lib310554/online%20risk_safety_report_2010.pdf.

3 pav. Interneto naudojimo būdai 2009 m. (*2008 m.). 27 ES šalių narių vidurkio ir Lietuvos duomenų palyginimas



liui kitų tikslų), jie gali pakeisti atsiskaitymo priemones, vartotojai juose laiko informaciją, kuri gali būti **privati ar konfidenciali**. Pakankamai akivaizdu, kad toks jautrios informacijos koncentratas asmeniniame nešiojamame įrenginyje, kurio praradimo (vagystės, pametimo ar tiesiog laikino palikimo be priežiūros) tikimybė yra didesnė nei stacionaraus ar net nešiojamojo kompiuterio,

yra potenciali saugumo problema. Be to, pranešimo autoriai atkreipia dėmesį ir į tai, kad paplitus tokiems įrenginiams atsiranda daug didesnės galimybės vaikams naudotis internetu be suaugusiųjų žinios bei priežiūros.[12]

Internetui tampant vis labiau socialiam, jo turinio kūrimas darosi prieinamas ne tik specialių žinių bei techninių įgūdžių turintiems profesionalams, bet ir eiliniams vartotojams. Tinkle kuriasi ir sparčiai populiarėja įvairios tarnybos (pvz., *You Tube*, *Facebook*, *Wikipedia*, *Twitter* ir kt.), suteikiančios galimybes bendrauti, bendradarbiauti, keistis informacija, skelbti tekstus, nuotraukas, vaizdo įrašus visiškai nemokamai ir beveik be jokio specialaus pasirengimo. Šių tarnybų verslo modelis paremtas tuo, kad jų populiarumas ir priklauso nuo to, kaip aktyviai vartotojai užpildo jas savo įkeliama informacija t. y. turiniu. Saugumo problemos čia kyla tuomet, kai vartotojai, talpindami informaciją internete, taip padaro ją viešai prieinama ir ne visuomet susimąsto, kaip ši informacija gali būti panaudota trečiųjų šalių, neretai be pačių vartotojų sutikimo ar žinios. Informacijos talpinimas yra paprastas ir nereikalaujantis ypatingų pastangų, o jos apsaugojimas įvairiais privatumo nustatymais neretai yra kiek sudėtingesnis, tuo tarpu vartotojai ne visada apie tai tinkamai informuojami.[13]

Tai tik keletas pavyzdžių, rodančių, kaip informacinių technologijų raida sukuria vis gausėjančią paslaugų ir galimybių elektroninėje erdvėje įvairovę, pritraukia vis daugiau vartotojų, tačiau tuo pat metu pastariesiems atsiranda ir naujos potencialios saugaus naudojimosi internetu grėsmės.

INTERNETO (SU)VALDYMO PRIELAIDOS IR GALIMYBĖS

Nuo pat pradžių internetas buvo kuriamas kaip pavienius kompiuterius ar skirtingus nedidelius tinklus sujungiantis, lengvai plečiamas tinklas, o standartizuoti duomenų perdavimo protokolai buvo suprojektuoti taip, kad nereikėtų jokio centrinio operatoriaus ar kontroliuojančios institucijos. Tokia decentralizuota tinklo architektūra buvo siekiama užtikrinti sklandų duomenų perdavimą, kai sugedus ar kitaip išėjus iš rikiuotės vienai tinklo atšakai duomenys tuoj pat nukreipiami kitomis, veikiančiomis atšakomis ir nekliudomai pasiekia adresatą. Po to, kai internetas peržengė mokslinių tyrimų organizacijų ribas ir ėmė plisti per valstybių sienas, pakankamai ilgą laiką jam pavyko išvengti ży-

[12] Ten pat, p. 43.

[13] Ten pat, p. 36.

mesnės valstybinės valdžios institucijų įtakos ar specialaus teisinio reguliavimo. Formaliai valstybė aprobuodavo techninius duomenų perdavimo protokolų standartus, o interneto turiniui ir vartotojams turėjo galioti tas pats teisinis reguliavimas, kuris veikė ir anksčiau, ne skaitmeninėje erdvėje. Vis dėlto dėl tam tikrų skaitmeninės erdvės savybių (centralizuoto valdymo nebuvimo, transnacionalumo, santykinio anonimiškumo, šifravimo algoritmų panaudojimo galimybės, techniškai ir procedūriškai sudėtingo neteisėtos veiklos tyrimo ir kt.) toks reguliavimas ne visuomet būdavo adekvatus ar pakankamai efektyvus.

Pradiniu laikotarpiu, kai interneto vartotojų dar nebuvo daug, pakankamai sėkmingai veikė įvairūs savireguliaciniai mechanizmai, pvz., „tinklo etiketas“[14] – tam tikrų **elgesio standartų ir taisyklių rinkinys**, skirtas palengvinti bendravimą interneto bendruomenėse. Neretai pats internetas buvo suprantamas kaip tam tikra autonomiška, laisva nuo cenzūros ir įvairių valstybės suvaržymų erdvė, kurioje klesti informacijos ir žodžio laisvė bei demokratija. Tačiau tai truko neilgai. Laikui bėgant kompiuteriai paplito, interneto vartotojų sparčiai daugėjo, pats internetas buvo intensyviai komercializuojamas. Beprecedentė informacinių technologijų plėtra vyko įvairiausiose srityse: pramonėje, prekyboje, bankininkystėje, telekomunikacijoje, medicinoje, švietime, infrastruktūros ir valstybės valdyme ir, žinoma, kasdieniame žmonių gyvenime. Pasaulis skaitmenizavosi, kartu darėsi vis labiau priklausomas nuo IT, kūrėsi skaitmeninė ekonomika.

Lygiagrečiai ryškėjo ir kitos tendencijos: internete ėmė plisti kompiuteriniai virusai ir kitokios kenkėjiškos programos, kasmet didėjo įmonių patiriami nuostoliai dėl įsilaužimų į jų kompiuterių sistemas, daugėjo asmeninių duomenų bei tapatybės vagysčių, atsiskaitymų suklastotomis kredito kortelėmis, atsirado dideli užkrėstų ir iš vieno centro valdomų kompiuterių tinklai (angl. *botnet*), naudojami elektroninio pašto šiukšlių siuntimui, asmeninių duomenų vagystėms ar atakoms prieš kompiuterių sistemas. Muzikos įrašų bei kino filmų industrijos kompanijos skelbia kasmet patiriančios milijardus nuostolių dėl neteisėto jų kūrinių kopijavimo ir platinimo.[15] Be to, manoma, kad interneto teikiamomis galimybėmis naudojasi ir teroristinės organizaci-

[14] Netiquette Guidelines RFC 1885. Prieiga per internetą: http://tools.ietf.org/html/rfc1855.

[15] RIAA (angl. *Recording Industry Association of America*). Piracy: Online and on the Street. Prieiga per internetą: http://www.riaa.com/physicalpiracy.php.

jos, veikiančios ir koordinuojančios veiksmus įvairiose šalyse, o pastaruoju metu prabilta ir apie tai, kad kai kurios valstybės kuria karinius padalinius, skirtus karo veiksmams skaitmeninėje erdvėje ir galbūt jau naudoja juos tarpvalstybinių konfliktų metu.[16] Ilgainiui šios tendencijos ėmė kelti vis didesnį susirūpinimą. Valstybėms, suinteresuotoms skaitmeninės ekonomikos plėtojimu ir skatinimu bei kuriančioms vis labiau nuo informacinių technologijų priklausomą infrastruktūrą, saugumo elektroninėje erdvėje klausimas palaipsniui darėsi vis aktualesnis.

Didėjant supratimui, kad sparčiai besiplėtojanti, įvairiais pavidalais besireiškianti ir tradicinėmis priemonėmis sunkiai suvaldoma nelegali veikla internete gali būti kenksminga ne tik atskiriems interneto vartotojams, bet ir valstybių ekonominiams interesams, o potencialiai ir kritiniams infrastruktūros objektams ar net kelti grėsmę nacionaliniam saugumui, pradėta aktyviau ieškoti būdų, kaip nuo to apsisaugoti. Tarptautinės organizacijos, kai kurių valstybių valdžios bei teisėsaugos institucijos, interneto paslaugų teikėjų bei IT saugumo sprendimų verslo įmonės, nevyriausybinės organizacijos ėmėsi teikti teisinio reguliavimo pasiūlymus, viešo ir privataus sektorių bendradarbiavimo iniciatyvas, įgyvendinti konkrečias saugumo internete priemones.

Dar 1997 m. buvo parengtas *Europos Sąjungos veiksmų planas skatinant saugesnį interneto naudojimą*.[17] Pradinis šio Veiksmų plano tikslas buvo interneto vartotojų (ypač vaikų) apsauga nuo nepageidaujamo ar nelegalaus interneto turinio. 1999 m. buvo priimtas *1999–2004 m. Saugesnio interneto veiksmų planas*,[18] vėliau – *Saugesnio interneto programa 2005–2008 m.*,[19] o 2008 m. –

[16] Pvz., įvairiuose šaltiniuose pasirodę pranešimai apie tai, kad 2007 m. neramumų Estijoje, kilusių dėl paminklo tarybiniams kariams perkėlimo, metu Estijos IT infrastruktūra patyrė masyvias internetines atakas. Plačiau žr.: The cyber raiders hitting Estonia // BBC News 2007 05 17. Prieiga per internetą: http://news.bbc.co.uk/2/hi/europe/6665195.stm. Panašių atakų būta ir Gruzijoje 2008 m. Rusijos – Gruzijos karinio konflikto metu. Plačiau žr.: *Danchev D.* Coordinated Russia vs Georgia cyber attack in progress // ZDNet, 2008 08 11. Prieiga per internetą: http://www.zdnet.com/blog/security/coordinated-russia-vs-georgia-cyber-attack-in-progress/1670.

[17] Action Plan on promoting safe use of the Internet. Prieiga per internetą: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/97/1041.

[18] Action plan for a Safer Internet 1999–2004. Prieiga per internetą: http://europa.eu/legislation_summaries/information_society/l24190_en.htm.

[19] Safer Internet Programme 2005–2008 (Safer Internet Plus). Prieiga per internetą: http://europa.eu/legislation_summaries/information_society/l24190b_en.htm.

Saugesnio interneto programa 2009–2013 m.[20] Šie planai ir programos nenustatė konkretaus teisinio reguliavimo, o numatytiems tikslams pasiekti skyrė finansavimą kelioms veiklos sritims: geresniam visuomenės informavimui apie grėsmes internete, pranešimų centrų, į kuriuos būtų galima pranešti apie incidentus internete įkūrimui, savireguliacijos iniciatyvų šioje srityje skatinimui.

2001 m. parengta ir nuo 2004 m. liepos mėn. įsigaliojo Europos Tarybos konvencija *Dėl elektroninių nusikaltimų*[21] (toliau – Konvencija), kurioje numatomi prisijungusių šalių įsipareigojimai kriminalizuoti tam tikrus kompiuterinius nusikaltimus bei sukurti tarptautinį bendradarbiavimą palengvinančius mechanizmus. Kadangi Konvencijoje apibrėžiamos veikos nėra siejamos su konkrečiomis specifinėmis technologijomis, tai ji gali būti pakankamai lanksti ir prisitaikyti vykstant spartiems technologijų pokyčiams. Ši Konvencija iki šiol yra ko gero svarbiausias tarptautinis dokumentas, kuriuo siekiama padidinti saugumą elektroninėje erdvėje, prie jos prisijungti kviečiamos visos suinteresuotos šalys. Šiuo metu konvenciją pasirašė 46 valstybės, 30-yje iš jų konvencija ratifikuota, o 16-oje dar laukiama ratifikavimo.

2008 m. Estijoje buvo įsteigtas NATO korporacinis kibernetinės apsaugos centras,[22] kurio tikslas – parengti NATO kibernetinės apsaugos standartus ir svarbiausias plėtotės kryptis, taip pat atlikti ekspertizes tais atvejais, kai yra įtarimų dėl kibernetinių atakų.

2010 m. Europos Sąjungos užsienio reikalų ministrai paprašė Europos Komisijos atlikti galimybių studiją dėl *Kovos su kibernetiniu nusikalstamumu centro* įkūrimo.[23] Toks centras turėtų vertinti kibernetinių nusikaltimų tendencijas ES bei palengvinti dalinimąsi informacija tarp įvairių tokius atvejus nagrinėjančių nacionalinių tyrimų institucijų. Taip pat šis centras vertintų vals-

[20] An even safer internet for children. Prieiga per internetą: http://europa.eu/rapid/pressReleases Action.do?reference=IP/08/310&format=HTML&aged=0&language=EN&gui Language=en.

[21] Konvencija dėl elektroninių nusikaltimų. Prieiga per internetą: http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=228195&p_query=&p_tr2=.

[22] NATO (angl. *North Atlantic Treaty Organization*). NATO opens new centre of excellence on cyber defence. Prieiga per internetą: http://www.nato.int/docu/update/2008/05-may/e0514a.html.

[23] Council of the European Union. Council conclusions concerning an Action Plan to implement the concerted strategy to combat cybercrime. Prieiga per internetą: http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/114028.pdf.

tybių narių prevencines ir tyrimuose naudojamas priemones bei apmokytų šioje srityje besispecializuojančius policijos pareigūnus, teisėjus ir prokurorus.

Jungtinėse Amerikos Valstijose 2003 m. paskelbta *Nacionalinė skaitmeninės erdvės saugumo strategija*,[24] kurios pagrindiniai uždaviniai – kiberatakų prieš kritines Amerikos infrastruktūras prevencija, pažeidžiamumo kiberatakoms mažinimas bei žalos ir atsigavimo laiko mažinimas po įvyksiančių atakų. Šioje strategijoje, be kita ko, pripažįstama, kad Vyriausybė vien tik savo pastangomis nepajėgi užtikrinti saugumo internetinėje erdvėje. Privataus sektoriaus verslo kompanijos, smulkios įmonės, universitetai, kitos įstaigos, taip pat ir fiziniai asmenys besinaudojantys interneto teikiamomis galimybėmis privalo patys pasirūpinti savo valdomos pasaulinio kompiuterių tinklo dalies saugumu.

Apie tai, kokia reikšmė teikiama skaitmeninės erdvės saugumo problemoms, byloja ir faktas, kad jau kurį laiką JAV Federalinis tyrimų biuras kibernetinius nusikaltimus laiko viena iš prioritetinių savo darbo sričių.[25] Pagrindinės FTB tyrimų kryptys šioje srityje – kompiuteriniai įsilaužimai, vaikų seksualinis išnaudojimas, intelektinės nuosavybės teisių pažeidimai, sukčiavimas internete.

Australijoje 2005 m. jau minėta ACMA (angl. *Australian Communication and Media Authority*) sukūrė Australijos interneto saugumo iniciatyvą (AISI – angl. *Australian Internet Security Initiative*).[26] Tai – stebėjimo sistema, Australijos interneto teikėjų tinkluose aptinkanti užkrėstus kompiuterius, kurie gali būti sujungiami į iš išorės valdomus tinklus (angl. *botnets*) ar kitaip išnaudojami nelegaliai veiklai ir informuojanti apie tai interneto paslaugų teikėjus. Tuomet pastarieji gali kreiptis į savo vartotojus, prašydami ar padėdami imtis atitinkamų saugumo priemonių. Pradėjusi nuo 5-ių interneto paslaugų teikėjų, AISI šiuo metu bendradarbiauja su 80 IPT ir gali stebėti maždaug 90 proc. Australijos interneto vartotojų. Pažymėtina, kad šis interneto paslaugų teikėjų bendradarbiavimas yra savanoriškas ir nemokamas.

---

[24] DHS (angl. *Departament of Homeland Security*). The National Strategy of Secure Cyberspace. Prieiga per internetą: http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf.

[25] FBI (angl. *Federal Bureau of Investigation*). What We Investigate. Prieiga per internetą: http://www.fbi.gov/about-us/investigate/what_we_investigate.

[26] ACMA (angl. *Australian Comunications and Media Authority*). Australian Internet Security Initiative. Prieiga per internetą: http://www.acma.gov.au/WEB/STANDARD/pc=PC_310317.

Šiuo metu Australijos Vyriausybei pateiktos prieštaringai vertinamos rekomendacijos įpareigoti interneto paslaugų teikėjus ir vartotojus dar griežčiau rūpintis savo tinklų ir kompiuterių saugumu. Rekomendacijose nurodoma, kad interneto paslaugų teikėjai, prijungdami vartotojus prie interneto, privalėtų suteikti jiems bazines konsultacijas apie saugumą internete ir jų kompiuterių apsaugos priemones. Taip pat IPT turėtų privalomai informuoti vartotoją, jeigu jo IP adresas būtų identifikuotas kaip užkrėstas kenksminga programine įranga bei patarti, kur kreiptis dėl techninės pagalbos, jeigu tokios prireiktų. Be to, IPT turėtų nustatyti aiškias taisykles, pagal kurias interneto prieiga užkrėstiems kompiuteriams būtų laipsniškai apribojama, o esant būtinybei ir visai nutraukiama, kol užkrėsti kompiuteriai nebus sutvarkyti. Savo ruožtu interneto vartotojai paslaugų tiekimo sutartyje turėtų būti įpareigojami prieš prisijungdami prie interneto įdiegti savo kompiuteriuose antivirusines programas bei ugniasienes (angl. *firewall)*, nuolat jas atnaujinti bei imtis reikalingų priemonių, kai jiems pranešama apie įtariamą jų kompiuterių užkrėtimą.[27] Šie pasiūlymai sulaukia nemažai kritikos, nes baiminamasi, kad juos įgyvendinus gali būti pažeidžiamas interneto vartotojų privatumas. Nėra aišku, kaip būtų nustatoma, ar vartotojo kompiuteryje yra reikalaujama programinė įranga ir ar tai nevirstų privalomu vartotojų sekimu ir interneto cenzūra.

Japonijoje, reaguojant į *botnet* tipo virusų plitimą ir jų keliamą grėsmę, 2006 m. įkurtas specialus tuo užsiimantis centras.[28] Tai – Japonijos vyriausybės finansuojamas ir koordinuojamas projektas, jungiantis valstybės, interneto paslaugų teikėjų ir antivirusinę programinę įrangą kuriančių kompanijų pastangas apsaugoti interneto vartotojų kompiuterius nuo užkrėtimo bei padėti išvalyti virusus, jeigu kompiuteris buvo užkrėstas. Šis centras renka ir analizuoja kompiuterių tinkluose plintančių virusų pavyzdžius, kuria jų atpažinimui ir neutralizavimui reikalingas priemones, identifikuoja ir informuoja užkrėstus vartotojus bei pateikia jiems nuorodą į svetainę, iš kurios galima parsisiųsti nemokamas priemones infekcijai pašalinti. Kiekvienam informuotam vartotojui

[27] Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime. Standing Committee on Communications report on the inquiry into Cyber Crime, p. 144. Prieiga per internetą: http://www.aph.gov.au/house/committee/coms/cybercrime/report.htm.

[28] CCC (angl. *Cyber Crime Center*). Attention Rousing Activity. Prieiga per internetą: https://www.ccc.go.jp/en_activity/index.html.

suteikiamas atskiras skaitmeninis kodas, pagal kurį galima stebėti, ar į pranešimą buvo sureaguota.[29]

Apie panašią iniciatyvą 2009 m. pabaigoje paskelbta ir Vokietijoje.[30] Bendradarbiaujant Federaliniam IT saugumo biurui (vok. *Bundesamt für Sicherheit in der Informationstechnik*) bei interneto paslaugų teikėjams būtų nustatomi *bot* virusais užkrėsti interneto vartotojų kompiuteriai, vartotojai būtų nukreipiami į interneto svetainę, informuojančią, kokių saugumo priemonių reikėtų imtis. Vartotojai taip pat galėtų kreiptis į specialų telefoninės pagalbos centrą. Šis projektas turėjo pradėti veikti pirmoje 2010 m. pusėje.

Tai tik keletas pavyzdžių, kurie tikrai neatspindi nei visos internetinių grėsmių įvairovės, nei jau esamų ar siūlomų konkrečių kovos su šiomis grėsmėmis priemonių gausos. Kol kas sunku būtų nustatyti, kiek veiksmingai šios pastangos prisideda prie elektroninės erdvės saugumo užtikrinimo. Internetas, kaip globali informacinė erdvė, nėra saistomas valstybių sienų, jis nepavaldus kokiai nors konkrečios šalies teisinei jurisdikcijai. Pavienių valstybių teisėsaugos institucijos, tirdamos kompiuterinius nusikaltimus, susiduria su dideliais sunkumais, kai paaiškėja, kad nusikaltimo pėdsakai veda į kitas šalis, ypač tokias, kurios nėra saistomos esamų tarptautinių susitarimų, dvišalių įsipareigojimų, neturi atitinkamo nacionalinio lygmens teisinio reguliavimo arba apskritai dėl kokių nors kitų priežasčių nėra linkusios bendradarbiauti. Nepaisant jau egzistuojančių tarptautinių iniciatyvų, tokių kaip minėta Europos Tarybos konvencija *Dėl elektroninių nusikaltimų*, Tarptautinės ekonominio bendradarbiavimo ir plėtros organizacijos (OECD) *Informacinių sistemų ir tinklų saugumo gairės*,[31] Tarptautinės telekomunikacijų sąjungos (ITU) *Pasaulinio kibernetinio saugumo darbotvarkė*[32] ir kt., vis dar tebėra aktualus platesnio masto sprendimų šioje srityje poreikis. Šį klausimą buvo mėginta spręsti 2010 m. balandžio mėn.

---

[29] CCC (angl. *Cyber Clean Center*). What is Cyber Crime Center. Prieiga per internetą: https://www.ccc.go.jp/en_ccc/index.html.

[30] German ISPs team up with gov agency to clean up malware // The Register, 2009 12 09. Prieiga per internetą: http://www.theregister.co.uk/2009/12/09/german_botnet_blitz/.

[31] OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. Prieiga per internetą: http://www.oecd.org/document/42/0,3343,en_2649_34255_15582250_1_1_1_1,00.html.

[32] ITU (angl. *International Telecommunication Union*). Global Cybersecurity Agenda. Prieiga per internetą: http://www.itu.int/osg/csd/cybersecurity/gca/.

Brazilijoje vykusiame Jungtinių Tautų Nusikaltimų prevencijos ir baudžiamosios justicijos kongrese, tačiau bendro sutarimo nebuvo pasiekta.[33]

Be abejo, plataus masto tarptautinis susitarimas dėl bendradarbiavimo informacinių technologijų saugumo srityje būtų labai svarbus ir reikalingas atsakas į aktualius informacinės visuomenės poreikius. Vis dėlto, neverta tikėtis, kad vien pasiekus tokį susitarimą tuoj pat būtų išspręstos visos su IT saugumu ir nusikaltimais elektroninėje erdvėje susijusios problemos. Pastaraisiais metais vis labiau aiškėja, kad šioje srityje perspektyviausiu laikytinas sisteminis, daugiasluoksnis požiūris, apimantis visas suinteresuotas puses tiek tarptautiniame, tiek nacionaliniame lygmenyje ir atitinkamai paskirstantis jų veiklos kryptis bei atsakomybę. Jau 1997 m. Europos Sąjungos *veiksmų plane skatinant saugesnį interneto naudojimą*, taip pat ir 2003 m. paskelbtoje JAV *nacionalinėje skaitmeninės erdvės saugumo strategijoje* matyti, kad vien valstybinės valdžios pastangos teisiškai reguliuoti internetą negali būti pakankamos, reikalingas glaudus valstybės valdymo bei teisėsaugos institucijų, interneto paslaugų teikėjų, kompiuterinės ir programinės įrangos gamintojų, nevyriausybinių visuomeninių organizacijų bei interneto vartotojų **bendradarbiavimas**.

C. Wallker ir *Y. Akdeniz*[34] kalbėdami apie nelegalaus turinio internete valdymo galimybes Europoje pateikė tokį galimą daugiasluoksnio reguliavimo modelį:

- tokių organizacijų kaip OECD ar Jungtinės Tautos pasauliniai tarptautinio reguliavimo sprendimai;
- regioninis tarptautinis teisinis reguliavimas, pvz., Europos Sąjungos lygmenyje;
- atskirų vyriausybių nacionalinio lygmens reguliavimas, pvz., specialūs policijos padaliniai;
- interneto paslaugų teikėjų vykdomas reguliavimas remiantis jų pačių nustatytais ir visuotinai priimtais šios srities elgesio kodeksais;
- interneto vartotojams atstovaujančios tarptautinio ir nacionalinio lygmens aktyvistų grupės;

[33] UN split on cybercrime conventions // OUT-LAW News, 2010 04 16. Prieiga per internetą: http://out-law.com/page-10923.

[34] *Walker C. P., Akdeniz Y.* The governance of the Internet in Europe with special reference to illegal and harmful content // Criminal Law Review, December Special Edition: Crime, Criminal Justice and the Internet, p. 9.

- interneto turinio reitingavimo sistemų įdiegimas;
- savarankiškas interneto vartotojų atliekamas reguliavimas naudojantis interneto turinio filtrais ar vadovaujantis internetinių bendruomenių vidaus taisyklėmis;
- organizacijos ar pranešimų centrai, kuriems būtų galima pranešti apie nelegalų turinį internete.

Autoriai teigia, kad toks daugelio lygių modelis atspindi ne tik reguliacinių galių pasiskirstymą skirtinguose lygmenyse, bet ir tam tikrą ribų tarp viešo ir privataus sektoriaus išsitrynimą, pastarajam suteikiant pakankamai svarų vaidmenį.

Panašus modelis aptariamas ir minėtame ACMA (angl. *Australian Communication and Media Authority*) pranešime.[35] Atsakomybės bei skirtingų vienas kitą papildančių vaidmenų tarp įvairių suinteresuotų pusių pasiskirstymas čia schemiškai vaizduojamas šešių lygių piramidės pavidalu. Šios piramidės pagrindas – **interneto paslaugų vartotojai**. Jie turi prisiimti atsakomybę už savo pačių elgesį elektroninėje erdvėje, taip pat siekti, kad paslaugų teikėjai atsižvelgtų į jų poreikius internetinio saugumo srityje. Kaip vienas iš tokio vartotojų spaudimo paslaugų teikėjams pavyzdžių pateikiamas vartotojų bendruomenės susirūpinimas savo privačių duomenų panaudojimu,[36] privertęs *Facebook* kompaniją pakoreguoti savo socialinio tinklo vartotojų duomenų privatumo politiką.[37] Antrasis lygmuo – **nevyriausybinės organizacijos**. Jų veiklos sritis – siūlymų dėl galimų priemonių, skirtų pavojų elektroninėje erdvėje mažinimui, teikimas, aktyvus interneto paslaugų teikėjų skatinimas rūpintis vartotojų saugumu bei informavimu. Trečias lygmuo – **interneto paslaugų industrijai atstovaujančios įmonės**. Šios įmonės, teikdamos paslaugas, turėtų diegti bei taikyti kon-

[35] ACMA (angl. *Australian Communications and Media Authority*). Online risk and safety in the digital economy: Third annual report to the Minister for Broadband, Communications and the Digital Economy on developments in internet filtering and other measures for promoting online safety, p. 5. Prieiga per internetą: http://www.acma.gov.au/webwr/_assets/main/lib310554/online%20risk_safety_report_2010.pdf.

[36] People Against the new Terms of Service (TOS). Prieiga per internetą: http://www.facebook.com/group.php?sid=a6cdf0abf38c1d67123c77fc196e546c&gid=77069107432.

[37] Facebook's Privacy Flap: What Really Went Down, and What's Next // PcWorld, 2009 02 18. Prieiga per internetą: http://www.pcworld.com/article/159743/facebooks_privacy_flap_what_really_went_down_and_whats_next.html.

krečias technologines bei kitas priemones, mažinančias galimą riziką, bei tiesiogiai informuoti vartotojus apie saugumą ir privatumą elektroninėje erdvėje. Ketvirtasis lygmuo – vadinamieji „reguliuotojai“. Tai – įvairios **valstybinės tarnybos**, užsiimančios, pavyzdžiui, duomenų apsaugos klausimais, ryšių infrastruktūros reglamentavimu ir pan. Jos taip pat turėtų informuoti vartotojus įvairiais saugumo bei privatumo elektroninėje erdvėje klausimais, bei imtis tam tikrų reguliuojančių intervencinių veiksmų, kai kyla pavojus, kad nustatyti saugumo ar privatumo standartai gali būti pažeidžiami. Penktajame, vyriausybiniame lygmenyje turėtų būti formuluojamos **nacionalinio masto strategijos**, skirtos grėsmių elektroninėje erdvėje mažinimui, nustatomi bendri standartizuoti reikalavimai šalyje veikiantiems interneto paslaugų teikėjams, atliekami instituciniai patvarkymai, reikalingi nustatytų standartų ir reikalavimų įgyvendinimo užtikrinimui. Paskutinis, aukščiausias piramidės lygmuo – **tarptautinis reguliavimas**. Jame tarptautinės organizacijos (tokios kaip OECD, ITU ir kt.) rūpinasi bendrais skaitmeninės ekonomikos reguliavimo principais, susijusiais su elektroninės erdvės, kaip saugios ir patikimos aplinkos kūrimu.

Dar vieną sisteminio požiūrio į skaitmeninės erdvės reguliavimą modelį pateikia *S. Schjølberg* ir S. *Ghernaouti-Hélie*.[38] Jie teigia, kad elektroninės erdvės saugumas yra varomoji skaitmeninės ekonomikos jėga ir todėl kritiškai svarbus, norint sukurti patrauklią verslui ir vartotojams aplinką. Tam būtinas visų dalyvaujančių veikėjų – nuo atskirų individų iki organizacijų bei valstybių – įsitraukimas ir bendradarbiavimas. Nepakanka vien techninių saugumo sprendimų, greta turi egzistuoti ir atitinkamos teisinio reguliavimo priemonės. Skaitmeninė ekonomika yra globali, todėl ypač svarbu, kad besivystančios šalys, investuojančios į IT infrastruktūrą bei siekiančios sumažinti savo technologinį atsilikimą (vadinamąją skaitmeninę atskirtį) nepaliktų nuošalyje šios infrastruktūros saugumo klausimų ir neatsidurtų dar gilesnėje „saugumo atskirtyje“. Autoriai išskiria penkias saugumo skaitmeninėje erdvėje dimensijas: politinę, teisinę, organizacinę, technologinę ir socialinę. Šiose veiklos srityse turėtų būti sprendžiami atitinkami skaitmeninės erdvės reguliavimo klausimai. Ypač pabrėžiama **švietimo reikšmė**. Nuolatinis švietimas ir sąmoningumo kėlimas būtinas tam, kad visi informacinės visuomenės dalyviai (nuo eilinių piliečių iki

[38] *Schjøberg S., Ghernaouti-Hélie S.* A Global Protocol on Cybersecurity and Cybercrime. Oslo: Edit, 2009, p. 8–13.

sprendimų priėmėjų) suprastų ir saugumo internetinėje erdvėje svarbą, ir iš to kylančią atsakomybę konkrečiose savo veiklos srityse. Tokio švietimo pasekmė ilgalaikėje perspektyvoje turėtų būti tam tikros visuotinės „kibersaugumo kultūros“ susiformavimas.

Pakankamai radikalų požiūrį į vartotojų bei IT kompanijų atsakomybę, susijusią su saugumu internetinėje erdvėje, išsako JAV tyrinėtoja *S. Brenner*.[39] Kritikuodama esamus, teisėsaugos institucijų naudojamus kovos su nusikaltimais elektroninėje erdvėje būdus kaip reaktyvius, orientuotus į pasekmes ir nepakankamai efektyvius, ji siūlo alternatyvią, prevencija ir paskirstyta atsakomybe paremtą strategiją. Jos esmė – tam tikrų teisinių įpareigojimų bei sankcijų už šių įpareigojimų nevykdymo sukeltas pasekmes nustatymas eiliniams interneto vartotojams. Jeigu vartotojas prisijungia prie interneto, nenaudodamas jokių kompiuterio apsaugos nuo kenksmingos programinės įrangos ar neteisėto prisijungimo priemonių, jis elgiasi analogiškai, lyg išeidamas iš namų paliktų praviras duris ir langus. Esminis skirtumas tas, kad neapsaugodamas kompiuterio vartotojas gali ne tik nukentėti pats, bet sukuria ir potencialią grėsmę kitų interneto vartotojų bei visos sistemos saugumui. Nustačius interneto vartotojams pareigą imtis prevencinių priemonių, kad jų kompiuteris netaptų lengva kompiuterinių nusikaltimų auka ir potencialia grėsme kitų vartotojų kompiuteriams, būtų galima taikyti ir tam tikras sankcijas už šios pareigos nevykdymą. Žinoma, sankcijos negalėtų būti taikomos vien už tai, kad neapsaugojęs savo kompiuterio vartotojas tapo internetinio nusikaltimo auka, nes tai prieštarautų ne tik teisinei, bet ir apskritai bet kokiai racionaliai logikai. Šiuo atveju, autorės nuomone, galėtų būti laikomasi „prisiimtos rizikos“ principo, kai laikoma, kad nevykdydamas pareigos imtis reikalingų apsaugos priemonių vartotojas suprato ir prisiėmė su tuo susijusią viktimizacijos riziką, todėl neturėtų tikėtis su tuo susijusios teisėsaugos institucijų reakcijos. Sankcijų taikymo pagrindas atsirastų tuo atveju, jeigu nesiimdamas reikalingų apsaugos priemonių, vartotojas suprato ir prisiėmė viktimizacijos riziką *ir* tai prisidėjo prie to, kad nukentėjo kiti interneto vartotojai.[40]

---

[39] *Brenner S. W.* Cybercrime: re-thinking crime control strategines. Iš: Jewkes Y. (ed.). Crime Online. Portland: Willan Publishing, 2007, p. 20–27.

[40] Autorė įžvelgia ir daugiau teisinių keblumų, kurie galėtų kilti įgyvendinant jos siūlomą atsakomybės vartotojams nustatymo modelį. Jie šiame straipsnyje nenagrinėjami, platesnę analizę žr. originaliame tekste.

S. Brenner siūlymai neapsiriboja vien atsakomybės interneto vartotojams nustatymu. Jos nuomone, reikėtų galvoti ir apie skaitmeninės erdvės „architektų“ – kompanijų, kuriančių programinę bei aparatinę kompiuterinę įrangą, – atsakomybę.[41] Šių kompanijų kuriami produktai daro tiesioginę įtaką tiek atskirų interneto vartotojų, tiek visos IT infrastruktūros saugumui, todėl reikia reikalauti atitinkamo jų patikimumo ir saugumo. Galima diskutuoti dėl konkrečių tokios atsakomybės formų, įgyvendinimo galimybių ir būdų, tačiau tikrai nereikėtų pasikliauti vien savireguliaciniais rinkos mechanizmais.

Taigi jau iš šios nedidelės apžvalgos galima matyti, kad idėjų ir siūlymų, skirtų interneto reguliavimo problemoms spręsti, netrūksta. Tokio reguliavimo poreikis nėra savitikslis, jis kyla iš vis aiškiau (ypač technologiškai labiau pažengusiose valstybėse) suvokiamų interesų apsaugoti nacionalinės svarbos kritinės infrastruktūros objektus, skatinti skaitmeninės ekonomikos raidą bei ginti interneto vartotojus nuo galimų grėsmių, kad jie galėtų saugiai ir pasitikėdami naudotis visomis informacinių technologijų atveriamomis galimybėmis. Darosi aišku, kad atskirų šalių vyriausybių taikomos lokalios priemonės, bandant suvaldyti skaitmeninę erdvę, kuri savo prigimtimi nėra nei lokali, nei pavaldi kokiai nors konkrečios šalies jurisdikcijai, dažniausiai nėra ir negali būti pakankamai efektyvios. Todėl, viena vertus, tebevyksta platesnių tarptautinių bendradarbiavimo galimybių paieška, kita vertus, bandomi kurti nauji reguliavimo modeliai, paremti tiek reguliacinių galių, tiek atitinkamos atsakomybės paskirstymu tarp visų informacinės visuomenės narių, globalios skaitmeninės ekonomikos dalyvių.

IŠVADOS

1. Pastarąjį dešimtmetį Lietuvoje (kaip ir kitose šalyse) matoma sparti interneto infrastruktūros ir informacinių technologijų pritaikymo sričių plėtra bei vartotojų skaičiaus didėjimas. Elektroninėje erdvėje atsiranda vis naujų galimybių tiek viešajam sektoriui, tiek verslui, tiek eiliniams vartotojams, formuojasi skaitmeninė ekonomika.

[41] *Brenner S. W.* Cybercrime: re-thinking crime control strategines. Iš: Jewkes Y. (ed.). Crime Online. Portland: Willan Publishing, 2007, p. 24.

2. Didėjant visuomenės priklausomybei nuo sklandaus IT infrastruktūros funkcionavimo, vis aiškesnis darosi skaitmeninės erdvės reguliavimo poreikis, susijęs su nacionalinio saugumo interesais (kritinės infrastruktūros objektų apsauga), saugios aplinkos vartotojams kūrimu.

3. Dėl skaitmeninės erdvės transnacionalumo, technologinio komplikuotumo, atviros tinklinės architektūros tik teisinis, nacionaline jurisdikcija paremtas, jos reguliavimas dažnai sunkiai įgyvendinamas ar nepakankamai efektyvus. Vien valstybės (valdžios) pastangų bei formalių administracinių priemonių nepakanka, reikalingas ir nuolatinis, sąmoningas visų dalyvaujančių veikėjų bendradarbiavimas tiek tarptautiniame tiek vietiniame lygmenyse.

4. Viena pagrindinių tokio bendradarbiavimo prielaidų – sisteminis požiūris, paskirstantis vaidmenis ir atsakomybę skirtinguose skaitmeninės erdvės saugumo užtikrinimo lygmenyse. Nuolatinė IT raida bei su tuo susijusių grėsmių kaita gali reikalauti ir skubių *ad hoc* pobūdžio sprendimų, tačiau jie neturėtų dominuoti.

5. Itin svarbus veiksnys – interneto vartotojų švietimas, sąmoningumo kėlimas, saugaus elgesio elektroninėje erdvėje propagavimas ir skatinimas. Kadangi vartotojų bazė plečiasi, švietimas neturėtų apsiriboti tik kuria nors jos dalimi (pvz., vaikais ir jaunimu), o stengtis pasiekti įvairius visuomenės sluoksnius. Ilgalaikėje perspektyvoje turėtų būti siekiama formuoti internalizuotas saugaus elgesio elektroninėje erdvėje normas, vadinamąją „kibersaugumo kultūrą“.

6. Kalbant apie elektroninės erdvės reguliavimo strategines kryptis, svarbu skirti du aspektus: a) nusikaltimų elektroninėje erdvėje tyrimas ir juos padariusių asmenų persekiojimas; b) galimybių nusikaltimams elektroninėje erdvėje mažinimas, saugumo didinimas, galimos žalos minimizavimas, t. y. prevencija. Dėl tam tikrų skaitmeninės erdvės ypatumų, pirmoji kryptis, reikalaujanti didelių techninių ir žmonių išteklių, neretai pasirodo esanti mažai efektyvi. Manytina, kad tam tikras prioritetų poslinkis nuo represinių link prevencinių priemonių ilgalaikėje perspektyvoje galėtų būti labiau naudingas.

7. Išlaikyti pusiausvyrą tarp informacinių technologijų teikiamų galimybių ir jų saugumo užtikrinimui skirtų reguliacinių priemonių – vienas svarbiausių virtualios elektroninės erdvės reguliavimo uždavinių. Visuomet išlieka pavojus, kad savitikslis ar perteklinis reguliavimas, apribojantis ar stipriai apsunkinantis vartotojų galimybes naudotis IT teikiamais privalumais, ne priartins, o veikiau atitolins nuo siekiamo tikslo – saugios ir patrauklios vartotojams aplinkos, skatinančios skaitmeninės ekonomikos raidą, sukūrimo.

LITERATŪRA

I. Mokslinės publikacijos

1. *Aas K. F.* Beyond „the deserto f the real“: crime control in a virtual(ised) reality. Iš: Jewkes Y. (ed.). Crime Online. Portland: Willan Publishing, 2007.

2. *Brenner S. W.* Cybercrime: re-thinking crime control strategines. Iš: Jewkes Y. (ed.). Crime Online. Portland: Willan Publishing, 2007.

3. *Brenner S. W.* Toward a Criminal Law for Cyberspace: Distributed Security. Boston University, 2004.

4. *Kalpokas V.* Nusikaltimai elektroninėje erdvėje: kriminologinės sampratos dilemos // Teisės problemos, 2009, Nr. 1.

5. *Kalpokas V.* Nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui. Knygoje: Sakalauskas G., Dobrynina M., Justickaja S. [et al.]. Registruotas ir latentinis nusikalstamumas Lietuvoje: tendencijos, lyginamieji aspektai ir aplinkos veiksniai. Teisės instituto mokslo tyrimai. 7 tomas. Vilnius: Eugrimas, 2011, p. 168–183.

6. *Schjølberg S., Ghernaouti-Hélie S.* A Global Protocol on Cybersecurity and Cybercrime. Oslo: E-dit, 2009.

7. *Walker C. P., Akdeniz Y.* The governance of the Internet in Europe with special reference to illegal and harmful content // Criminal Law Review, December Special Edition: Crime, Criminal Justice and the Internet, p. 5–19.

8. *Williams M.* Virtualy Criminal. London: Routledge, 2006.

II. Šaltiniai internete

9. ACMA (Australian Communications and Media Authority). Online risk and safety in the digital economy: Third annual report to the Minister for Broadband, Communications and the Digital Economy on developments in internet filtering and other measures for promoting online safety. http://www.acma.gov.au/webwr/_assets/main/lib310554/online%20risk_safety_report_2010.pdf.

10. ACMA (Australian Comunications and Media Authority). Australian Internet Security Initiative. http://www.acma.gov.au/WEB/STANDARD/pc=PC_310317.

11. Action plan for a Safer Internet 1999–2004. http://europa.eu/legislation_summaries/information_society/l24190_en.htm.

12. Action Plan on promoting safe use of the Internet: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/97/1041.

13. An even safer internet for children. http://europa.eu/rapid/pressReleasesAction.do?reference=IP/08/310&format=HTML&aged=0&language=EN&guiLanguage=en.

14. CCC (Cyber Clean Center). What is Cyber Crime Center. https://www.ccc.go.jp/en_ccc/index.html.

15. CCC (Cyber Crime Center). Attention Rousing Activity. https://www.ccc.go.jp/en_activity/index.html.

16. Council of the European Union. Council conclusions concerning an Action Plan to implement the concerted strategy to combat cybercrime. http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/114028.pdf.

17. *Danchev D.* Coordinated Russia vs Georgia cyber attack in progress // ZDNet, 2008 08 11. http://www.zdnet.com/blog/security/coordinated-russia-vs-georgia-cyber-attack-in-progress/1670.

18. DHS (Departament of Homeland Security). The National Strategy of Secure Cyberspace. http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf.

19. Europos Sąjungos naujokės ir toliau pirmauja pagal FTTH plėtrą. FTTH Council Europe pranešimas spaudai. http://www.ftthcouncil.eu/documents/press_release/2010/PR2010_EU_Ranking_mid_2010_Final_LI.pdf.

20. Eurostat. Individuals frequently using the Internet. http://epp.eurostat.ec.europa.eu/tgm/table.do?tab=table&init=1&plugin=1&language=en&pcode=tin00092.

21. Eurostat. Households who have Internet access at home. http://epp.eurostat.ec.europa.eu/tgm/table.do?tab=table&init=1&plugin=1&language=en&pcode=tin00088.

22. Facebook's Privacy Flap: What Really Went Down, and What's Next // PcWorld, 2009 02 18. http://www.pcworld.com/article/159743/facebooks_privacy_flap_what_really_went_down_and_whats_next.html.

23. FBI (Federal Bureau of Investigation). What We Investigate. http://www.fbi.gov/about-us/investigate/what_we_investigate.

24. German ISPs team up with gov agency to clean up malware // The Register, 2009 12 09. http://www.theregister.co.uk/2009/12/09/german_botnet_blitz/.

25. Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime. Standing Committee on Communications report on the inquiry into Cyber Crime. http://www.aph.gov.au/house/committee/coms/cybercrime/report.htm.

26. ITU (International Telecommunication Union). Global Cybersecurity Agenda. http://www.itu.int/osg/csd/cybersecurity/gca/.

27. Kaimiškųjų vietovių informacinių technologijų plačiajuostis tinklas RAIN. http://www.rain.lt/.

28. Konvencija dėl elektroninių nusikaltimų. http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=228195&p_query=&p_tr2=.

29. *Molis A., Molytė R.* Kibernetinės grėsmės – tarp mito ir realybės // Geopolitika, 2010 01 22. http://www.geopolitika.lt/?artc=3796.

30. NATO (North Atlantic Treaty Organization). NATO opens new centre of excellence on cyber defence. http://www.nato.int/docu/update/2008/05-may/e0514a.html.

31. Netiquette Guidelines RFC 1885. http://tools.ietf.org/html/rfc1855.

32. OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. http://www.oecd.org/document/42/0,3343,en_2649_34255_15582250_1_1_1_1,00.html.

33. People Against the new Terms of Service (TOS). http://www.facebook.com/group.php?sid=a6cdf0abf38c1d67123c77fc196e546c&gid=77069107432.

34. RIAA (Recording Industry Association of America). Piracy: Online and on the Street. http://www.riaa.com/physicalpiracy.php.

35. Safer Internet Programme 2005–2008 (Safer Internet Plus). http://europa.eu/legislation_summaries/information_society/l24190b_en.htm.

36. *Salama S.* UAE ti create cybercrime courts. // Gulfnews, 2010 01 05. http://gulfnews.com/news/gulf/uae/crime/uae-to-create-cybercrime-courts-1.562337.

37. *Simonavičius G.* Prekyba keliasi į internetą // LTV „Šiandien“, 2009 07 27. http://lrt.lt/news.php?strid=31489&id=5252379.

38. Statistikos departamentas prie Lietuvos Respublikos Vyriausybės. Informacinių technologijų naudojimo namų ūkiuose statistinio tyrimo duomenys. http://www.stat.gov.lt/lt/pages/view/?id=1584.

39. Statistikos departamentas prie Lietuvos Respublikos Vyriausybės. Informacinių technologijų naudojimo įmonėse bei valstybės ir savivaldybių valdymo įstaigose tyrimų duomenys. http://www.stat.gov.lt/lt/pages/view/?id=1584.

40. The cyber raiders hitting Estonia // BBC News, 2007 05 17. http://news.bbc.co.uk/2/hi/europe/6665195.stm.

41. UN split on cybercrime conventions // OUT-LAW News, 2010 04 16. http://out-law.com/page-10923.

Vaidas KALPOKAS
Law Institute

REGULATION AND CONTROL OF DIGITAL SPACE: ASPECTS OF SECURITY

Summary

Information technologies have opened the new dimension of human existence – digital space. In the beginning of the 2011 there will be more than 2 billion inhabitants using it. Nevertheless these tempting possibilities that attract more and more new settlers inevitably relate to certain threats and dangers. What kind of dangers are these? Are the mechanisms sustaining inner order and inevitably used for survival of any other community needed in this special space? Who or what and in what ways could warrant the working of these mechanisms in the extraterritorial decentralized derivative – internet? These are the questions that are partially faced in this article.

The growing society's dependence upon fluent functioning of IT infrastructure shows the need to regulate digital space. It is also related to the interests of national security (protection of objects of critical infrastructure) and to the creation of safer environment for users. The author of the article draws attention to the need of constant and conscious communication among all the players at the international and local levels. The systemic approach while the roles and responsibilities are distributed among the different levels of security is the main premise of such communication.

Straipsnis redakcijai įteiktas 2010 m. lapkričio 17 d.