MYKOLO ROMERIO UNIVERSITETAS

SOCIALINĖS INFORMATIKOS FAKULTETAS

ELEKTRONINIO VERSLO KATEDRA

PAULIUS SARTATAVIČIUS

(Naujų technologijų teisė, NTTmns1-01)

INTERNETO PASLAUGŲ TEIKĖJŲ VAIDMUO KOVOJANT SU NETEISĖTU INTELEKTINĖS NUOSAVYBĖS PLATINIMU INTERNETE

Magistro baigiamasis darbas

Darbo vadovas –

Prof. dr. Mindaugas Kiškis

Vilnius, 2012

TURINYS

ĮVADAS 3

1. INTELEKTINĖS NUOSAVYBĖS ELEKTRONINĖJE ERDVĖJE PAŽEIDIMAI IR APSAUGOS MECHANIZMAI 7

2. TECHNINIAI INTELEKTINĖS NUOSAVYBĖS ELEKTRONINĖJE ERDVĖJE APSAUGOS BŪDAI 15

2.1. Filtravimas 16

2.2. Blokavimas 20

2.3. „Deep Packet Inspection“ 24

2.3.1. Intelektinės nuosavybės apsauga – tikslas taikyti „DPI“ 26

3. INTERNETO PASLAUGŲ TEIKĖJŲ NAUDOJAMŲ TECHNINIŲ INTELEKTINĖS NUOSAVYBĖS APSAUGOS BŪDŲ TEISĖTUMAS BEI INTERNETO PASLAUGŲ TEIKĖJŲ ATSAKOMYBĖS RIBOS 30

4. INTERNETO PASLAUGŲ TEIKĖJŲ VAIDMENS REGLAMENTAVIMAS LIETUVOJE 43

5. TEISMŲ PRAKTIKA REZONANCINĖS BYLOS 46

IŠVADOS 54

LITERATŪROS SĄRAŠAS 56

SANTRAUKA 62

SUMMARY 63

ĮVADAS

Temos aktualumas

Šių dienų žinių visuomenėje tiek verslo, tiek ir kituose sektoriuose pagrindinę vertę kuria žmonės ir nematerialusis turtas – intelektinė nuosavybė. Intelektinės nuosavybės teisė savo ruožtu atlieka labai svarbią funkciją, užtikrindama inovacijų ir informacijos teisinę apsaugą. Tačiau dėl nepaliaujamo technologijų vystymosi ir kaitos, intelektinės nuosavybės apsaugos būdai ypač sparčiai sensta ir tampa nebetinkami įgyvendinti savo funkciją. Prieš kelis metus išreikštas susirūpinimas dėl naujo apsaugos mechanizmo, išeinančio už teisės mokslo ribų, atsiradimo šiandien yra jau pasenęs, nes dabar tokie mechanizmai yra įprasti.

Informacinių technologijų panaudojimas intelektinės nuosavybės apsaugai kasdien vis didėja. Tačiau nerimą kelia tai, kad intelektinės nusavybės pažeidėjai vis greičiau randa apsaugos mechanizmų apėjimo būdus, ypač kai internetas dabar yra užėmęs pagrindinį vaidmenį informacijos sklaidos bei kituose globaliniuose procesuose (visuomeninių santykių raiškos terpėje, komercinių-prekybinių santykių arenoje). Įvertinant šių procesų bei santykių išplitimą reikia pažymėti, jog intelektinės nuosavybės pažeidimai tapo pagrindine teisės pažeidimų internete forma, nekreipiančia dėmesio į valstybių sienas bei laiko barjerus.

Piratinė produkcija platinama akimirksniu, o patys pažeidėjai turi galimybę išlikti anonimiški, dėl ko šie pažeidimai yra dar sunkesni.

Neteisėtas kūrinių, vaizdų ar kompiuterių programų kopijavimas iš esmės laikomas vagyste ir moraliai netinkamu elgesiu. Visuotinės žmogaus teisių deklaracijos 27 straipsnio 2 dalyje pažymima jog „kiekvienas žmogus turi teisę į apsaugą jo dvasinių ir materialinių interesų, atsirandančių ryšium su mokslo, literatūros ar meno kūrinių, kurių jis yra autorius, sukūrimu“[1]. Diskusijoje apie intelektinę nuosavybę linkstama sutelkti dėmesį ties žala, kuri padaroma neteisėtai atgaminant kūrinius, ir ties teisiniais bei techniniais būdais, kurie galėtų arba apsunkinti šį neteisėtą atgaminimą, arba visiškai užkirsti jam kelią.[2] Išsiaiškinus tai, kad elektroninėje erdvėje intlektinė nuosavybė vaidina tokį pat ar net svarbesnį vaidmenį nei įprastai ir įvertinus vis tobulesnių apsaugos mechanizmų poreikį bei intelektinės nuosavybės pažeidimų mastą, iškyla dar vienas klausimas: kas turėtų imtis priemonių užkirsti kelią pažeidimams, ar apsaugos mechanizmai turėtų būti automatizuoti ir svarbiausia, koks vaidmuo tenka tarpiniai grandžiai – interneto paslaugų teikėjams, kurių dėka atsiranda galimybė veikti elektroninėje erdvėje (tiek teisėtai, tiek neteisėtai)?

[1] *Human rights manual, Guidelines for Implementing a Human Rights Based Approach in ADC.* Austrian Development Agency. Vienna 2010. 141.
[2] Bagdonavičiūtė, I. *Intelektinės nuosavybės pažeidimai internete: specifika ir problemos*. Magistro baigiamasis darbas. Vilnius: Mykolo Romerio universitetas, 2007.

Interneto tarpininkų vaidmens neužtikrintumas paminėtas ir Europos Komisijos 2012 01 11 komunikate „COM (2011) 942 final“. Nepaisant garantijų, kurias nelegalų turinį pasyviai talpinančioms ar perduodančioms įmonėms suteikia Elektroninės komercijos direktyva, tarpinius interneto paslaugų teikėjus kausto teisinis netikrumas dėl to, kad jiems sužinojus apie nelegalų turinį savo interneto svetainėse, iš jų reikalaujama taikyti visoje Europos Sąjungoje skirtingas taisykles ar praktiką.[3] Interneto paslaugų teikėjai suteikia interneto prieigą ir sujungia pagrindinius tinklus, prieglobos svetaines ir serverius. Būdami tarpininkai tarp visų interneto vartotojų ir teisių turėtojų, dėl neteisėtų klientų veiksmų jie dažnai atsiduria kompromituojančioje padėtyje. Dėl šios priežasties ES teisėje jau esama konkrečių nuostatų, kuriomis apribojama interneto paslaugų teikėjų, kurių paslaugomis naudojamasi vykdant intelektinės nuosavybės teisių pažeidimus, atsakomybė.[4] Taip pat ir teisminė praktika diktuoja savo iniciatyvas, dėl ko šiandien požiūris į interneto tarpininkų vaidmenį intelektinės nuosavybės platinime internete keičiasi ir reikalauja konkretesnio reglamentavimo ir aptarimo.

Tiek Europos Sąjungos institucijos, tiek pavieniai mokslininkai bei praktikai, taip pat teisės studentai nagrinėja šią temą. Lietuvoje bendrai intelektinės nusavybės apsaugai elektroninėje erdvėje daugiausiai dėmesio skiria Mykolo Romerio universiteto Socialinės informatikos fakulteto Elektroninio verslo katedros mokslininkai prof. dr. Mindaugas Kiškis ir prof. dr. Rimantas Petrauskas. Bendras intelektinės nuosavybės problematikos elektroninėje erdvėje gaires yra aptarinėję ir Lietuvos universitetų magistrantai.[5] Temos aktualumą taip pat lemia ir naujausia teismų praktika, kuri iš esmės keičia požiūrį į interneto paslaugų teikėjų vaidmenį intelektinės nuosavybės platinime internete bei iškelia tvirtesnio reglamentavimo poreikio koncepciją.[6]

Problema

1) Interneto paslaugų teikėjų turinio (intelektinės nuosavybės) filtravimo ir blokavimo teisėtumas ir jo ribos.
2) Interneto paslaugų teikėjų teisinio netikrumo dėl reikalavimų visoje Europos Sąjungoje taikyti skirtingas taisykles buvimas.
3) Teismų praktikos bei teisinio reglamentavimo nesutapimai.

[3] Europos komisijos komunikatas Darni sistema, kuria siekiama padidinti pasitikėjimą bendrąja skaitmenine elektroninės prekybos ir internetu teikiamų paslaugų rinka; COM(2011)0942 final.
[4] 2004 m. balandžio 29 d. Europos Parlamento ir Tarybos direktyvos 2004/48/EB dėl intelektinės nuosavybės teisių gynimo taikymas; KOM/2010/0779 galutinis.
[5] Jonelis, A. Autorių teisių ir gretutinių teisių realizavimas internete. Magistro baigiamasis darbas. Vilnius: Mykolo Romerio universitetas, 2005; Bagdonavičiūtė, I., *Intelektinės nuosavybės pažeidimai internete: specifika ir problemos, supra* note 2.
[6] Byla C-70/10, *SA prieš Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2011]; Byla C-360/10, *Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) prieš Netlog NV* [2012].

4) Techninių būdų ir teisinių įpareigojimų santykio problema.

Objektas

Darbo objektas – interneto paslaugų teikėjų vaidmuo kovojant su neteisėtu intelektinės nuosavybės platinimu internete bei techninių apsaugos mechanizmų reglamentavimo galimybės.

Tyrimo tikslas ir uždaviniai

Atsižvelgiant į pasirinktą tyrimo objektą, tiesioginis darbo tikslas yra išanalizuoti ir įvertinti interneto paslaugų teikėjų vaidmens kovojant su neteisėtu intelektinės nuosavybės platinimu internete problematiką bei atsakomybės ribas.

Siekiant minėto magistro baigiamojo darbo tikslo, keliami tokie tyrimo uždaviniai:

1) Išanalizuoti ir apibendrinti esamą teoriją bei reglamentavimą interneto tarpininkų atžvilgiu;
2) Išanalizuoti teismų praktiką bylose dėl interneto paslaugų teikėjų vaidmens intelektinės nuosavybės pažeidimų elektroninėje erdvėje atvejais.
3) Pateikti techninių bei teisinių apsaugos priemonių visumos analizę ir aptarti jų efektyvumą praktikoje.
4) Apibendrinti interneto paslaugų teikėjų taikomas ir galimas prevencines intelektinės nuosavybės platinimo priemones.

Tyrimo metodai

Tiriamų reiškinių analizei naudotasi tokiais teoriniais ir empiriniais metodais:

a) dokumentų moksline analize;
b) lyginamąja analize;
c) lingvistiniu metodu (atskleisti sąvokų turinį);
d) logine analize (įvertinti tiriamus teisės aktus);
e) sistemine analize (tiriant nacionalinį ir užsienio valstybių teisinį reguliavimą).

Svarbios sąvokos

Elektroninė erdvė; interneto paslaugų teikėjas; tinklai (kompiuteriniai); intelektinė nuosavybė.

***Elektroninė erdvė*:** tai kompiuterių ir kompiuterinių tinklų erdvė, kurioje saugomi elektroniniai duomenys ir vyksta elektroninė komunikacija.

***Interneto paslaugų teikėjas*:** Interneto paslaugų teikėjai (ISP) yra įmonė, kuri teikia prieigą prie interneto, paprastai už mokestį. Dažniausiai prisijungiama prie ISP naudojant telefono arba plačiajuostį ryšį (kabelis arba DSL). Daug ISP teikia papildomas paslaugas, pvz., el. pašto abonementus, žiniatinklio naršykles ir vietą, kurioje galima kurti svetainę.

***Tinklai (kompiuteriniai)*:** Kompiuterinis tinklas — tai informacijos keitimosi sistema, jungianti darbo stotis, terminalus ir autonomiškai funkcionuojančius asmeninius kompiuterius, spausdintuvus ir pan. Tinklams būdingi bendri komponentai:

- serveriai (ang. *servers*) – kompiuteriai, kurių resursai yra prieinami tinklo vartotojams;
- klientai (ang. *clients*) – kompiuteriai, kurie naudojasi tinklo resursais;
- ryšio terpė (ang. *media*) – kompiuterių sujungimo būdas;
- resursai (ang. *resources*) – spausdintuvai, duomenys, programos, CD-ROM bibliotekos ir pan.

Intelektinė nuosavybė: tai nematerialioji nuosavybė, žmogaus dvasinės kūrybos bei protinio darbo rezultatas, proto (intelekto, mąstymo, minties) produktas, kuris yra saugomas įstatymo kaip ir bet kuri kita nuosavybės forma.

Darbo struktūra

Darbą sudaro įvadas, keturi skyriai, išvados ir rekomendacijos, naudotos literatūros sąrašas bei santrauka. Pirmoje dalyje analizuojami intelektinės nuosavybės pažeidimų būdai. Antroje dalyje išsamiai aptariami interneto paslaugų teikėjų taikomi bei galimi techniniai intelektinės nuosavybės elektroninėje erdvėje apsaugos metodai. Trečiojoje dalyje vertinamas aptartų techninių apsaugos metodų taikymo teisėtumas bei interneto paslaugų teikėjų atsakomybės ribos. Ketvirtoje dalyje analizuojami įpareigojimai interneto paslaugų teikėjams nacionaliniu ir tarptautiniu mastu, analizuojama teismų praktika bylose, susijusiose su interneto paslaugų teikėjų atsakomybės intelektinės nuosavybės pažeidimų atvejais nustatymu. Paskutinėje darbo dalyje pateikiamos išvados bei rekomendacijos interneto paslaugų teikėjų vaidmens intelektinės nuosavybės pažeidimų atvejais nustatymui ir reglamentavimo galimybėms.

1. INTELEKTINĖS NUOSAVYBĖS ELEKTRONINĖJE ERDVĖJE PAŽEIDIMAI IR APSAUGOS MECHANIZMAI

„Intelektinės nuosavybės pažeidimu laikomas intelektinės nuosavybės produktų atgaminimas, platinimas, naudojimas, laikymas ir gabenimas be teisių turėtojo sutikimo ar sutarties su teisių turėtoju (ar jo atstovu). Pažeidimu laikytinas ir bet koks intelektinės nuosavybės įstatymų pažeidimas, įskaitant neturtinių teisių pažeidimus.“[7]

Šnekant apie intelektinės nuosavybės pažeidimus elektroninėje erdvėje, visų pirma turime galvoje internetą. Pastaruoju metu grubūs intelektinės nuosavybės, o tiksliau autorių teisėmis apsaugotos medžiagos pažeidimai internete sutinkami labai dažnai. Kopijavimo ir įklijavimo funkcija sudaro visas galimybes paimti skaitmeninę medžiagą – tekstą, nuotraukas, video ar audio medžiagą – iš tinklalapio ar kitų elektroninių (skaitmeninių) šaltinių ir visa apimtimi nukopijuoti (padauginti) į kitą vietą. Internetas bei visa elektroninė erdvė, kaip terpė atsirasti intelektinės nuosavybės pažeidimams kelia daug naujų teisinių klausimų, tokių kaip:

ar paieškos sistemos padaro neteisėtas kopijas indeksuodamos tinklapius?

ar nuoroda į autorių teisėmis saugomą medžiagą yra autorių teisių pažeidimas?

ar autorių teisių įstatymai taikomi ir elektroniniams laiškams?

ar interneto paslaugų teikėjai yra atsakingi už kitų asmenų talpinamos medžiagos teisėtumą?

etc.

Nors interneto pagalba vartotojai gali lengviau vykdyti savo veiklą ir keistis idėjomis, intelektinė nuosavybė tampa labiau pažeidžiama. Interneto aplinkoje, pažeidėjas iš esmės gali lengvai suklaidinti vartotojus ir juos nuvesti į savo svetainę naudodamas kitą prekės ženklą kaip meta-žymą (angl. *meta-tag)* ir taip pat, kaip jau minėta, labai lengva neteisėtai atgaminti autorių teisių objektus.[8] Taip pat, dėl globalios interneto prigimties intelektinės nuosavybės pažeidimai elektroninėje erdvėje yra dažniausiai padaromi ne vienoje valstybėje, bet kertant valstybių sienas. Visa tai iškėlė daug problemų teritoriniams intelektinės nuosavybės įstatymams.

Pačius intelektinės nuosavybės pažeidimus elektroninėje erdvėje galima būtų suskirstyti į:

a) „tradicinius intelektinės teisės pažeidimus, kurie atliekami elektroninėje erdvėje arba kurie yra pasitelkus informacines technologijas.
b) specifinius pažeidimus padaromus tik elektroninėje erdvėje:

[7] Kiškis, M. Intelektinės nuosavybės teisinė apsauga elektroninėje erdvėje. Vilnius: Mykolo Romerio universiteto Leidybos centras, 2011. p. 34.
[8] *Intellectual property on the internet: A Survey of Issues (WIPO/INT/02).* World Intellectual Property Organisation. Geneva, 2002. 20-23, 104.

a. nuorodų į neteisėtas intelektinės nuosavybės kopijas talpinimas ir platinimas;
b. intelektinės nuosavybės neteisėtų kopijų talpinimas ir platinimas kompiuterių tinklais;
c. techninių apsaugos priemonių ir teisių valdymo informacijos pažeidimai;
d. priemonių, skirtų intelektinės nuosavybės pažeidimams elektroninėje erdvėje, platinimas.“[9]

Atsiradus galimybei reklamuotis ir teikti paslaugas elektroninėje erdvėje daugelis įmonių talpino internete savo prekių ženklus, siekdamos tokiu būdu reklamuoti savo prekes ir paslaugas ne tik fizinėje erdvėje.[10] Autorių teisių srityje daugelis literatūros darbų, filmų bei meno kūrinių buvo ir yra perkeliami internetu.[11] Patentų sistema taip pat jau migravo į elektroninę erdvę ir internetą, o įmonės vis dažniau patentuoja savo internetinio verslo metodus.[12]

„Pažeidimus komerciniais tikslais praktikoje įprasta vadinti intelektinės nuosavybės „piratavimu“.“[13] Elektroninėje erdvėje ši savoka ypatingai tinka būtent dėl to, jog vadinamieji „piratai“ išnaudoja svetimą intelektinės veiklos rezultatą savo tikslams be jokių įdėtų pastangų tam rezultatui pasiekti. Piratavimo atvejai šiandien labiausiai yra siejami su video bei audio kūriniais ir taip pat kompiuteriniais žaidimais. Šie autorių teisių objektai yra piratinės produkcijos pagrindas.

Pasak dr. Mindaugo Kiškio, iš esmės intelektinės nuosavybės pažeidimai elektroninėje erdvėje turėtų būti kvalifikuojami taip, kaip ir tradiciniai intelektinės nuosavybės pažeidimai. Kai kuriais atvejais šiuos pažeidimus vertėtų kvalifikuoti net kaip pavojingesnius. Daugelyje valstybių minimi pažeidimai yra įtraukti į baudžiamuosius bei administracinius kodeksus. Žinoma, visose vasltybėse šie pažeidimai taip pat laikomi ir civilinių teisių pažeidimu.[14]

Dėl intelektinės nuosavybės pažeidimų dar 2010 metais socialiniai tinklapiai, tokie kaip *MySpace* ir video dalijimosi svetainė *YouTube* sulaukė didžiulių autorių teisių pažeidimo ieškinių. *Universal Music Group* (UMG) padavė ieškinį dėl autorių teisių pažeidimų *MySpace* už tai, kad tinklapyje buvo sudaryta galimybė vartotojams įkelti bei parsisiųsti dainas ir muzikinius klipus. UMG reikalavo 150 000 dolerių kompensacijos už vieną paskelbtą dainą ar vaizdo įrašą teigdami, kad milijonai dainų ir vaizdo įrašų *MySpace* tinklapyje galimai pažeidžia autorių teises. Visuomenės informavimo priemonių įmonė *Viacom* pateikė ieškinį prieš *YouTube* ir pagrindinę

[9] Kiškis M., *supra* note 7, p. 34.
[10] WIPO, *supra* note 8.
[11] *Ibid*.
[12] *Ibid.*
[13] Kiškis, M., *op. cit., p.* 34-38.
[14] Kiškis, M., *ibid*.

įmonę *Google* siekdami prisiteisti vieną milijardą JAV dolerių žalos atlyginimo. *Viacom* teigė, jog *YouTube* sąmoningai naudojo technologijas stambaus masto autorių teisių pažeidimams vykdyti.[15]

Intelektinės nuosavybės pažeidimai elektroninėje ervėje yra ypač pavojingi dėl lengvo įgyvendinamumo. Išskirtini intelektinės nuosavybės elektroninėje erdvėje (konkrečiau interneto aplinkoje):

1) Prekių ženklai:
    a. Svetimo prekės ženklo kaip domeno vardo panaudojimas;
    b. Svetimo prekės ženklo panaudojimas savo tinklapyje;
    c. Prekės ženklo kaip meta-žymos panaudojimas;
2) Autorių teisės:
    a. Nuorodos ir „rėmeliai“;
    b. Autorių teisėmis saugomų objektų įkėlimas;
    c. Autorių teisėmis saugomų objektų parsisiuntimas;
3) Patentai:
    a. Verslo metodų patentai;
    b. Programinės įrangos patentai.

Svetimo prekės ženklo kaip domeno vardo panaudojimas:

Interneto vystymasis atnešė naujus iššūkius prekių ženklų teisei (įstatymams). Šioje vietoje svarbiausia tema yra prekių ženklų ir domenų vardų santykis. D. Rowland ir E. Macdonald pateikia tokį apibrėžimą: „Domeno vardas gali būti sulyginamas su pasauliniame kompiuterių tinkle esančiu adresu, kurie abu identifikuoja ir pateikia informaciją apie konkrečią interneto svetainę."[16] Šiuo atveju neverta šnekėti apie situaciją, kada egzistuoja dvi (ar daugiau) įmonių tokiu pačiu pavadinimu ir prekės ženklu (tačiau skirtingoms prekėms ir paslaugoms ženklinti) ir abi įmonės nori naudoti tą patį domeno vardą. Šiuo atveju kyla ginčas kurį turi spręsti arbitražinės institucijos ar teismas. Tačiau realaus pažeidimo tokiu atveju kaip ir nėra. Išskirti reikia atvejus, kada prekių ženklai registruojami kaip domeno vardai siekiant pasipelnyti juos pardavus prekių ženklų savininkams. Tokia situacija kyla pakankamai dažnai ir pavyzdžių toli ieškoti nereikia. „Pieno žvaigždžių“ byloje būtent ir buvo bandoma tai padaryti, tačiau teismas aiškiai pasisakė, kad domeno

[15] *Intellectual property and the internet: Copyright infringement liability in the digital era*. [interaktyvus]. Advisen special report, 2010. [žiūrėta 2012-06-03]. <https://www.advisen.com/downloads/Intellectual_Property.pdf>.
[16] Rowland, D. and Macdonald, E., *Information Technology Law*, London: Cavendish, 2nd ed., 2000, at 520.

vardas priklauso prekės ženklo savininkui, ypač atkreipiant dėmesį, kad registravęs domeno vardą asmuo turėjo komercinių siekių – pasipelnyti iš domeno vardo pardavimo.[17]

Svetimo prekės ženklo panaudojimas savo tinklapyje:

Prekių ženklų teritorinė apsauga leidžia vienodus prekės ženklus naudoti ne vienam produktui ar paslaugai skirtingose šalyse žymėti. Tačiau dėl globalaus interneto pobūdžio jame nėra sienų, todėl ir vieną kartą panaudojus prekės ženklą internete, jis yra pasiekiamas visur.[18] Todėl patalpintas prekės ženklas ar žymuo internete, kelia riziką pažeisti kitoje jurisdikcijoje esančio asmens teises į tapatų prekės ženklą fizinėje erdvėje.

Svetimo prekės ženklo kaip meta-žymos naudojimas:

Meta-žyma yra žodis, parašomas tinklapyje skaitmenine kalba, kaip pavyzdžiui HTML kalba. Toks žodis pridedamas prie tinklapio yra nematomas vartotojui, tačiau paieškos programos jį mato ir meta paieškos rezultatuose.[19] Taigi tokiu būdu svetimas prekės ženklas gali būti naudojamas savo tinklapio reklamai – pelnomasi iš svetimo intelektinės veiklos rezultato.

Nuorodos ir rėmeliai:

Viena iš svarbiausių techninių savybių išskiriančių internetą iš kitų komunikacijos priemonių yra galimybė dinamiškai sujungti kelis dokumentus ir elementus. Šios sąsajos dažnai pasireiškia „nuorodomis“ bei „rėmeliais“.

Tai yra atvejai, kada asmuo kurdamas tinklalapį į jį įdeda nuorodas į kitiems asmenims priklausančius tinklapius (dažniausiai ne į pagrindinį tinklapio puslapį) taip sukurdamas iliuziją, kad antrasis tinklapis yra pirmojo dalis.

Viena pirmųjų bylų susijusių su nuorodų naudojimu buvo nagrinėta Didžiojoje Britanijoje, *Shetland Times Ltd v Wills*. Ieškovui priklausė laikraštis ir jo atitikmuo internete. Atsakovas administravo tinklalapį *Shetland news,* kuriame panaudojo ieškovo tinklapyje skelbiamas antraštes. Paspaudus ant antraščių vartotojas buvo nukreipiamas į ieškovo tinklapį tiesiogiai į norimą tekstą, taip apeinant pagrindinį ieškovo tinklapio puslapį.[20]

Pastebėtina, jog nuorodos būna dviejų tipų – paprastos ir giluminės. Paprastos nuorodos nuveda vartotoją į tinklapio pagrindinį puslapį, o giluminės (angl. *Deep linking)* nukreipia į

[17] Vilniaus apygardos teismo 2008 m. spalio 1 d. nutartis civilinėje byloje *AB "Pieno žvaigždės" prieš E.K.* (bylos Nr. 2-1061-623/08).
[18] Bainbridge, D., *Intellectual Property*, Pearson: Longman, 6th ed., 2007, at 680.
[19] Phillips, J., *Trade Mark Law-A Practical Anatomy*, Oxford University Press, 2003, at 593.
[20] *Shetland Times, Ltd. v. Jonathan Wills and Another*, 1997 F.S.R. (Ct. Sess. O.H.).

konkrečią tinklapio dalį, taip apeinant pagrindinį puslapį ir sudarant iliuziją jog tai yra to paties, pirminio tinklapio dalis.

Kitas panašaus veikimo nuorodų variantas yra „rėmeliai“. Rėmeliais yra sudaroma galimybė į tinklapį įterpti informaciją iš kito tinklapio taip, kad atrodo, jog tai yra to paties tinklapio dalis. Tarsi į teksto kūrimo failą (*Word*) įterpti lentelę, ar paveiksliuką. Tokiu būdu, iš vartotojo nėra reikalaujama jokio aktyvaus veiksmo norint pamatyti turinį.

Viena pirmųjų bylų susijusių su „rėmelių“ naudojimu buvo nagrinėjama JAV, *Washington Post Co. v Total News, Inc.*[21] Atsakovas administravo tinklapį, kuriame buvo dedamos nuorodos į kitus įvairius tinklapius. Paspaudus ant nuorodų, tinklapiai buvo atidaromi „rėmeliuose“, kuriuose buvo matyti atsakovo logotipai, URL adresas bei reklamos. Dauguma naujienų portalų prieštaravo tokiam jų medžiagos naudojimui ir pateikė ieškinius dėl autorių teisių pažeidimų. Teismas, žinoma, priėmė sprendimą uždrausti atsakovui naudoti „rėmelius“.

Autorių teisėmis saugomų objektų įkėlimas:

Kadangi techniškai nėra sudėtinga ir jau įprasta autorių teisėmis saugomus objektus perkelti interneto pagalba, dauguma vartotojų mano, jog vien ta sąlyga, kad medžiaga yra prieinama elektroniniu būdu, suteikia jiems teisę įkelti tą medžiagą į savo tinklapius.[22] Iš esmės tai yra tie atvejai, kada panaudojami autorių teisėmis saugomi objektai be leidimo ir net be nuorodų į šaltinį ar autoriaus vardą.

Autorių teisėmis saugomų objektų atsisiuntimas:

Kai autorių teisėmis saugoma medžiaga yra be leidimo patalpinama internete ir padaroma viešai prieinama, daugeliu atvejų visiškai tikėtina, kad vartotojai tokią medžiagą atsisiųs. Beveik nėra abejonių, jog vartotojai neteisėtai atsisiųsdami autorių teisėmis saugomą medžiagą yra atsakingi už autorių teisių pažeidimus, tačiau autorių teisių savininkai yra realiai bejėgiai imtis kokių nors veiksmų prieš milijonus tokių pažeidėjų. Daug dėmesio buvo skirta išnagrinėti galimybę, kad atsakinga šalimi turėtų būti laikomi tie asmenys, kurie suteikia įrangą ir įrenginius, naudojamus tokiems pažeidimams atlikti

A & M Records, Inc. v Napster, Inc.[23] byloje buvo nustatyta, jog *Napster* palengvino Mp3 failų apsikeitimą tarp vartotojų. Įmonė per savo tinklapį išplatino nemokamą failų keitimosi

[21] United States District Court Southern District of New York case *Washington post v. TotalNews,* No. 97 Civ. 1190 (PKL), [1997].
[22] Reed, C., *Internet Law: Text and Materials*, Cambridge University Press, 2nd ed., 2004, at 101.
[23] *A & M Records, Inc. v Napster, Inc.*, 239 F. 3d 1004 (9th Cir. 2001).

programą. Proceso, kuris vadinamas *peer-to-peer* (P2P) failų keitimusi, metu vartotojai galėjo ieškoti ir dalintis Mp3 muzikos failais, kurie buvo sistemiškai kataloguojami *Napster* serveryje. Šie failai yra iš vartotojų kompiuterių tačiau per centrinį serverį naudojantis internetu. Kitaip sakant *Napster* pateikė tarsi žemėlapį, o programa pagal tą žemėlapį randa vartotojų kompiuteriuose konkrečiai ieškomus failus ir tada inicijuoja siuntimą. *A&M records Inc*. ir kitos įrašų kompanijos kreipėsi į teismą dėl autorių teisių pažeidimų.

Kalifornijos šiaurės apygardos teismas nustatė, kad *Napster* vartotojai, kurie siuntėsi autorių teisėmis saugomą produkciją, tiesiogiai pažeidė ieškovų teisę į atgaminimą.[24] Taip pat buvo nustatyta, kad be *Napster* sudarytų sąlygų, toks atgaminimas nebūtų vykdomas, todėl tai reiškia, jog Napster suteikė vietą ir įrangą tiesioginiam autorių teisių pažeidimui.[25]

Be to, teismas nurodė, jog *Napster* iš šių pažeidimų gavo komercinę naudą, kadangi tyrimas parodė, jog *Napster* pelningumas priklauso nuo vartotojų bazės didinimo.

Napster byla, paskatino sukūrimą naujų sistemų, kurios būtų nepriklausomos nuo centrinio serverio. Viena iš tokių – *Grokster*. Jos veikimui nereikalingas centrinis serveris, o pati programa sudaro eilę konkrečių kompiuterių, kuriuose yra ieškomas duomuo ir pradeda tiesioginį siuntimą. Toks necentralizuotas tinklas reiškė, jog vartotojas yra susijęs su konkrečiu serveriu tik tol, kol atsisiunčia pačią programą, ir vos tik toks siuntimas yra baigiamas, jokios sąsajos su centriniu serveriu nebelieka.

Paminėtina byla *Metro-Goldwyn-Mayer Studios, Inc*.[26] *(MGM) v Grokster Ltd. Grokster Ltd*. ir kiti atsakovai sukūrė minėtą P2P principu veikiančią programą, kuria naudodamiesi vartotojai galėjo siųstis filmus, muziką ir kitus autorių teisių objektus. MGM ir kiti autorių teisių turėtojai padavė atsakovus į teismą dėl autorių teisių pažeidimo. Šiuo atveju, skirtingai nei *Napster* byloje, nebuvo tiesioginių įrodymų, kad vartotojai siuntėsi konkrečią produkciją, kadangi šiuo atveju nebuvo jokio centrinio serverio.

Teismo sprendimas šiame ginče buvo palankus atsakovams, tačiau apeliacinėje instancijoje teismas nuomonę pakeitė ir nurodė, jog tokiais atvejais, kai programinės įrangos kūrėjas ar platintojas vartotojams suteikia programinę įrangą, kurios dėka šie gali keistis autorių teisėmis saugomais objektais be atitinkamų leidimų yra autorių teisių pažeidimas.[27] Taip pat reikšminga byla buvo *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd,*[28] kurioje buvo kalbama apie tuo pačiu P2P principu veikiančią programą *Kazaa*. Šioje byloje teismas siekdamas nustatyti ar

[24] *A & M Records, Inc. v Napster, Inc.*, *supra* note 23.
[25] Ibid.
[26] United States Supreme Court , 545 U.S. 913 (2005), *MGM Studios, Inc. v. Grokster, Ltd*
[27] *Ibid.*
[28] Federal Court of Australia,[2005] FCA 1242 *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd.*

atsakovai sudarė sąlygas vartotojams siųstis autorių teisėmis saugomą produkciją. Teismas įvertino tris kriterijus pagal Australijos autorių teisių įstatymą:

1) ar asmuo turėjo galimybę užkirsti kelią pažeidimui;
2) asmens leidžiančio vykdyti pažeidimą ir pažeidimą vykdančio asmens santykių kilmę;
3) ar asmuo, tariamai sudarantis sąlygas vykdyti pažeidimą, ėmėsi kokių nors veiksmų, kad užkirstų kelią pažeidimui vykdyti.

Įvertinęs šiuo principus teismas pripažino, kad atsakovai pažeidė ieškovų teises leisdami *Kazaa* vartotojams dalintis autorių teisėmis saugomais objektais. Teismo nuomone konkreti situacija atitiko visus tris principus, t.y. atsakovai turėjo technines galimybes neleisti kilti pažeidimams, bet to nedarė bei yra aišku, kad jeigu *Kazaa* nebūtų suteikusi įrangos duomenų keitimuisi, tai iš viso nebūtų *Kazaa* failų keitimosi.

Patentai ir internetas:

Patentų sistema suvaidino svarbų vaidmenį skatinant pagrindinės techninės interneto infrastruktūros plėtrą. Ši, per efektyvią patentų apsaugą įdiegta infrastruktūra suteikė didelę naujų idėjų, inovacijų bei technologinių išradimų rinką. Tačiau naujos technologijos iškėlė naujus iššūkius įprastoms teisinėms patentų sistemos schemoms.[29] Kai šnekama apie patentus ir internetą, išskiriame verslo modelių patentus bei programinės įrangos patentus. Šiuo atveju galioja tie patys patentų pažeidimai ir fizinėje erdvėje. Paminėtina *Amazon.com, Inc. v Barnesandnoble.com, Inc.* byla, kurioje *Amazon* padavė į teismą savo konkurentą dėl to, kad šis panaudojo ieškovo užpatentuotą vieno paspaudimo užsakymą. Galiausiai šalys susitarė šioje byloje, tačiau pirmos ir apeliacinės instancijų teismų nuomonės buvo prieštaringos.

Tokia pati situacija galima ir kalbant apie programinės įrangos patentus. Byloje *Eolas Technologies, Inc. v Microsoft Corp*[30] kilo ginčas dėl to, kad atsakovas naudojo ieškovo užpatentuotą programinės interneto naršymo įrangos funkciją, kuria automatiškai yra atsiunčiamos tam tikros HTML kalbos žymos. Byla nukeliavo iki apeliacinės instancijos ir ten buvo išspręsta. Be to, reikėtų pažymėti, jog šiuo atveju nekilo klausimas dėl jurisdikcijos ir taikytinos teisės, tačiau, jeigu bylos šalys būtų iš skirtingų valstybių arba pažeidžiantis patentą produktas būtų parduodamas internetu, kiltų klausimas dėl taikytinos teisės ir jurisdikcijos.

Šnekant apie intelektinės nuosavybės apsaugą elektroninėje erdvėje galima pasakyti, kad reikėtų išskirti du apsaugos mechanizmus, kurie darbe bus detalizuoti vėliau:

[29] WIPO, *supra* note 8.
[30] United States District Court of Illinois, 457 F. 3d 1279, C.A. Fed. (Ill.), 2006, *Eolas Technologies, Inc. v Microsoft Corp.*

- Techniniai apsaugos mechanizmai
- Teisiniai apsaugos mechanizmai

Taip pat dar galima išskirti ir moralinį apsaugos mechanizmą (švietimas), kurį galima apibrėžti kaip tam tikro visuomenės supratimo suformavimą, pradedant jaunimo ir vaikų auklėjimu mokyklose ir namuose.

Teisiniai apsaugos mechanizmai yra orientuojami į teisinės bazės tobulinimą ir harmonizavimą. Pastoviai tobulėjančios technologijos siūlo būdus, kaip galima valdyti disponavimą intelektinės nuosavybės objektais naudojantis ne tik intelektinės nuosavybės naudojimą reglamentuojančiais teisės aktais bei teisinėmis priemonėmis. Reikia turėti omenyje, kad siūlomi būdai negali pakeisti teisinio intelektinės nuosavybės reglamentavimo, tačiau šie metodai jau dabar papildo teisinius apsaugos būdus.[31] Tokie techniniai sprendimai, kaip filtravimas, blokavimas, skaitmeninio vandens ženklo naudojimas ir kitos priemonės sukuria galimybę įgyvendinti intelektinės nuosavybės apsaugą.

Taigi, visapusiška intelektinės nuosavybės apsauga turėtų apimti tiek teisines priemones, tiek ir technologinius sprendimus. Reikia pažymėti, jog teisinės priemonės intelektinės nuosavybės apsaugai elektroninėje erdvėje nesibaigia gavus patentą ar žinant, kad produkcija yra saugoma autorių teisėmis. Licencijavimo ir perlicencijavimo veikla yra reikalinga dinamiškame interneto pasaulyje. Po jų seka technologijų valdymo sprendimai. Išmanant intelektinės nuosavybės topografiją yra lengviau pasirinkti informacines technologijas bei valdymo sprendimus. Kaip ir minėjau, visi technologiniai sprendimai yra priedas prie teisinio reguliavimo.

Pagrindinis klausimas kyla dėl aptartinų apsaugos būdų-mechanizmų naudojimo teisėtumo bei apimties. Būtent tai ir siekiama aptarti toliau darbe.

[31] „Intelektinės nuosavybės pažeidimai internete: specifika ir problemos“, I. Bagdanavičiūtė, Magistro baigiamasis darbas, Mykolo Romerio universitetas, 2007, p. 47.

2. TECHNINIAI INTELEKTINĖS NUOSAVYBĖS ELEKTRONINĖJE ERDVĖJE APSAUGOS BŪDAI

Intelektinei nuosavybei elektroninėje erdvėje apsaugoti yra būtinas nuolatinis techninių būdų progresas. Informacinių technologijų srityje pokyčiai vyksta labai greitai. Pažeidimų padarymo būdai progresuoja taip pat sparčiai, kadangi yra kuriami vis nauji apsaugos mechanizmų apėjimo variantai. Šioje srityje, galima sakyti, verda nuolatinė kova tarp apsaugos technologijų kūrėjų bei asmenų, darančių pažeidimus. Internetiniai intelektinės nuosavybės pažeidimai iškėlė naujų sunkumų intelektinės nuosavybės teisei. Reikia sutikti su tuo, kad vien teisinėmis priemonėmis sėkmingai išspręsti intelektinės nuosavybės pažeidimų problemas nėra realu. Taip pat patebėtina, kad nacionalinė teisė nėra pajėgi išspręsti šią problemą, kadangi pažeidimai daromi pasauliniu mastu.[32]

Šiame skyriuje bus siekiama koncentruotis į pagrindinius techninės apsaugos būdus – filtravimą, blokavimą bei turinio kontrolės vykdymo ypatumus. Tačiau taip pat reikia trumpai aptarti kitus intelektinės nuosavybės elektroninėje erdvėje techninius apsaugos būdus.

Vienas iš tokių būdų yra Serijinių kopijų valdymo sistema (angl. *Serial Copy Management System – SCMS*). Šią sistemą sukūrė įrašų kompanijos ir ji leidžia daryti tik originalias, bet ne antros kartos garsų, įkeltų į audio laikmeną kopijas. Ši sistema naudoja tam tikras žymas, kurios nurodo ar inicijuotas atgaminimo procesas yra leistinas.

Kodavimas taip pat naudojamas iškraipyti turinį, kad šis būtų nesuprantamas iki kol bus atkoduotas. Kai turinys yra užkoduojamas, atgaminimas nebetenka prasmės, kadangi net ir nukopijavus medžiagą, jos turinys tampa prieinamas tik jį atkodavus. Plačiai naudojama kodavimo sistema vadinama viešo rakto sistema. Sistemoje naudojami du „raktai“ – viešas ir privatus. Viešas raktas yra platinimas visiems, tačiau privatų raktą turi tik konkretus asmuo. Taigi, turinys yra užkoduojamas viešuoju gavėjo raktu, tačiau atkoduoti jį galima tik gavėjo asmeniniu-privačiu raktu (kitaip tariant, užkoduoti informaciją galima konkretaus asmens viešu raktu, kadangi jis yra prieinamas viešai, tačiau atkoduoti galima tik to konkretaus asmens asmeniniu raktu). Šią technologiją galima naudoti ir intelektinės nuosavybės apsaugai. Kai autorius siunčia užkoduotą intelektinę nuosavybę (pvz. Autorių teisių objektą) gavėjas pasinaudodamas savo asmeniniu raktu ją

[32] Yang, F. *Infringement of intellectual property rights over the internet and private international law.* Magistro baigiamasis darbas. [interaktyvus] Nottingham University, 2010. <http://etheses.nottingham.ac.uk/1197/> .

atkoduoja, tokiu būdų ji yra neįskaitoma tretiesiems asmenims net ir informacijos perėmimo atveju (srauto duomenų perėmimo).[33]

Be kodavimo egzistuoja dar vienas kriptografinis apsaugos būdas – elektroniniai parašai. Elektroninio parašo schema taip pat apima viešąjį ir asmeninį raktus. Siuntėjas laiko paslaptyje asmeninį raktą, o viešąjį padaro prieinamą gavėjui. Siuntėjas, naudodamas specialią programinę įrangą, sukuria tam tikrą informacijos aprašą, kurį pasirašo ir kuriame atsispindi esminės pasirašomos informacijos charakteristikos. Šį aprašą siuntėjas užkoduoja savo asmeniniu elektroninio parašo raktu, o gavėjas pasinaudoja viešuoju siuntėjo raktu, kad atkoduotų elektroninį parašą. Ta pačia programine įranga šis sukuria naują gautos informacijos aprašą ir palygina su pirminiu aprašu. Jeigu šie sutampa, reiškia informacija po pasirašymo nebuvo keista ar tvarkyta.[34]

„Vandens ženklas“ yra dar viena skaitmeninė informacijos apsaugos technologija. Ši technologija veikia kaip ir įprasti vandens ženklai. Jos esmė yra tai, kad į informaciją yra „įspaudžiama“ nematoma identifikacinė informacija. Šis ženklas-žyma gali būti matoma tik su konkrečia nustatymo įranga. Nuskaičius žymą yra aišku ar informacija-turinys yra autentiškas ir iš kur jis atsirado. Elektroniniuose vandens ženkluose gali būti nurodomas autoriaus vardas, pavardė, identifikacinis numeris, elektroninio pašto adresas ir t.t. Dažniausiai elektroniniuose vandens ženkluose būna pridėtas ieškinys ar pranešimas apie autorių teisių pažeidimą.[35]

2.1. Filtravimas

Kartu su informacinių technologijų pažanga interneto prieigose bei mobiliųjų komunikacijų tinklų sektoriuose nuolatos yra tobulinami ir technologiniai informacijos srauto kontrolės šiuose tinkluose sprendimai. Šių technologijų pažangą skatina siekis palaikyti ir gerinti paslaugų kokybę. Tiesioginės rinkodaros pranešimų ir virusų atskyrimas bei nepageidaujamo turinio blokavimas įvairių subjektų prašymu yra vieni pagrindinių techologinių sprendimų tikslų.[36] Interneto turinio reguliavimas yra įmanomas keliais būdais, kurie gali būti įgyvendinami keliais skirtingais lygiais.

1) **Interneto paslaugų teikėjo iniciatyva**: interneto paslaugų teikėją valdžios įgaliotos agentūros dažnai skatina filtruoti nelegalų bei amoralų turinį, ar blokuoti paieškos rezultatuose tam tikrus puslapius. Taip pat interneto paslaugų teikėjas filtruoja

[33] Lehman, B.A. *Intellectual Property and the National Information Infrastructure – The Report of the Working Group on Intellectual Property Rights.* [interaktyvus] 1995 [žiūrėta 2012-04-05]. <http://www.ladas.com/NII/NII_Technology.html#enc>.
[34] Taylor, M., *Uses of Encryption: Digital Signatures*. C.T.L.R. 2006. 92.
[35] Akester, P., „Authorship and Authenticity in Cyberspace“, *Computer Law & Security Report,* Vol. 20, No. 6, 2004, 436, 439.
[36] „Dutton, W.H. Dopatka, A. Hills, M. Law, G. Nash, V. *Freedom of connection – freedom of expression: the changing legal and regulatory ecology shaping the internet.* A report prepared for UNESCO‟s Division for Freedom of Expression, Democracy and Peace. University of Oxford, 2010. 28-44.

nepageidaujamą elektroninį paštą bei stengiasi apsaugoti vartotojus nuo žalingų programų poveikio sistemų stabilumui bei saugumui.

2) **Tinklų sąsaja prie interneto „stuburo**“: dažnai filtravimo schemos ir blokavimo technologijos taikomos interneto „stuburo“ lygmenyje, statant filtravimo sistemas prie nuorodų į interneto „stuburą“. Pvz.: prie tarptautinių tinklų sąsajų.
3) **Institucijos:** įmonės, mokyklos, bibliotekos gali filtruoti turinį pagal savo kriterijus arba valstybės institucijų vardu.
4) **Individualūs kompiuteriai:** filtravimo programinė įranga gali būti įdiegta individualiuose kompiuteriuose, kuri neleis prisijungti prie tam tikrų puslapių.
5) **Teisėsauga:** veiksmų imamasi prieš vartotojus, kurie neteisėtai dalijasi muzika, įsilaužinėja į sistemas, užsiima sukčiavimu ir t.t. [37]

Informacijai keliaujant internetu veikia įvairūs interneto protokolai ir paslaugos, o pati informacija pereina daugelį tinklo taškų. Dėl šios priežasties, filtravimo metodus galima taikyti įvairiuose tinklo taškuose. Daugiausia diskusijų susilaukia valdžios institucijų remiamas ar vykdomas filtravimas, bet net ir tokiu atveju jis yra įgyvendinamas skirtinguose lygiuose ir skirtingų subjektų (individų, institucijų ar paslaugų teikėjų).

Kai šalis nusprendžia filtruoti internetą, filtravimo įgyvendinimas apima tiek įstatyminės bazės pritaikymą, tiek ir techninių priemonių panaudojimą siekiant užkirsti kelią asmenims pasiekti tam tikrą informaciją internete. Reikia paminėti, jog įstatymiškai dažniausiai nėra nustatomas konkretus techninis filtravimo pobūdis ar būdai, o veikiau yra nustatoma tam tikra bazinė struktūra – pagrindas, koks interneto turinys yra draudžiamas. Taigi, būdai tą turinį padaryti neprieinamu lieka diskutuotina tema..

Techniniu požiūriu interneto filtravimas nėra tobulas bet kokioje valstybėje. Net ir pažangiausi techniniai filtravimo sprendimai negali šimtu procentų apsaugoti nuo tokių asmenų, kurie yra pasiryžę investuoti bei rizikuoti norėdami pasiekti ar paviešinti tam tikrą turinį internete. Kiekviena filtravimo sistema dažniausiai arba per griežtai filtruoja, arba per silpnai ir tokiais atvejais techniškai išprusę vartotojai gali rasti prieigą prie norimo turinio. Nors ir atsiranda vartotojų galinčių apeiti filtravimo sistemas, tačiau didžioji dalis vartotojų to nesugeba. Filtravimas kartais suprantamas kaip tam tikra žinutė visuomenei, kad ši imtųsi savireguliacijos.

Šią mintį gerai iliustruoja Singapūro pavyzdys. Plačiai reklamuojama ir skelbiama Singapūro filtravimo sistema iš tiesų yra tik išpūstas burbulas ir realiai blokuoja tik nedidelę dalį pornografinio turinio tinklapių, o iš tiesų ši sistema veikia kaip gąsdinimo priemonė, kad pati

[37] Dutton, W.H. Dopatka, A. Hills, M. Law, G. Nash, V. *supra* note 36.

visuomenė imtųsi savireguliacijos – savicenzūros. Tokiu atveju yra skiepijama mintis, kad net nereikia bandyti pasiekti tam tikro turinio, kuris skelbiamas kaip neteisėtas.[38]

Vienas iš drastiškiausių filtravimo technologijų taikymo pavyzdžių yra Kinija. Kinijoje yra labai platus diapazonas temų, kurias valdžia laiko jautriomis ar kontaversiškomis. Žiniasklaida yra stipriai kontroliuojama ir dažnai žurnalistai yra baudžiami už skelbiamą informaciją, kuri prieštarauja komunistų partijos doktrinai.[39]

Priešingai nei daugelyje kitų valstybių, Kinijoje filtravimas vykdomas įvairiuose lygmenyse. Būtent dėl to, jog Kinijoje filtravimas yra labai dinamiškas ir nuolat besikeičiantis yra labai sunku pasakyti kaip Kinijoje vykdomas interneto filtravimas. Nors Kinijoje filtravimas yra vykdomas nuo pamatinių tinklo lygių („stuburo“), tačiau tuo pačiu ir atskiri interneto paslaugų teikėjai vykdo filtravimą savo iniciatyva. Taip pat reikia paminėti, jog čia filtravimas vykdomas ir paieškos programose pagal raktinius žodžius – tam tikri raktiniai žodžiai yra neleistini ir tinklapių su jais napateikia paieškos rezultatuose. Kinijoje yra ypač populiarios interneto kavinės, ir netgi jos yra įpareigotos sekti naršančius vartotojus ir srauto duomenis saugoti šešiasdešimt dienų. [40]

Taip pat reikia pasakyti, jog sudėtinga filtravimo sistema žengia koja kojon su nė ką sudėtingumu nenusileidžiančiu teisiniu reglamentavimu. Nors ir neegzistuoja vienas harmonizuotas teisės aktas, kuriame būtų įtvirtintas nacionalinio lygmens filtravimo vykdymas, tačiau daugelyje įstatymų, tokių kaip internetinės reklamos, valstybės paslapčių, interneto paslaugų ir turinio teikėjų kontrolės, interneto kavinių įstatymuose yra numatyta didelė parama ir leidimai filtruoti turinį valstybiniu lygmeniu. Privatumo apsaugos – asmens susižinojimo ar informacinio bei komunikacinio privatumo įtvirtinimas įstatymais, o tiksliau – konstitucija, Kinijoje yra labai miglotas bei, valstybės institucijų nuomone, šiuo – interneto aplinkos – atveju netaikomas.[41]

Grįžtant prie interneto filtravimo tikslų reikėtų išskirti tris motyvus:

1) Politika ir valdžia;
2) Socialinės normos ir moralė;
3) Saugumo sumetimai.[42]

Atsižvelgiant į tai daugiausiai yra filtruojamas politinis, socialinis turinys bei turinys, susijęs su saugumu. Filtravimo motyvai tiesiogiai koreliuoja su filtruojamu turiniu. Intelektinės nuosavybės

[38] Deibert, R. Palfrey, J. Rohozinski, R. Zittrain, J. *Access Denied – The Practice and Policy of Global Internet Filtering.* Cambridge: MIT Press, 2008. 9, 34.
[39] Qinglian, H. *Media control in China.* [interaktyvus] 2004. [žiūrėta 2012-05-15]. <http://www.hrichina.org/public/contents/8991>.
[40] Baumbauer, D.E. Deibert, R.J. Palfrey jr., J.G. Rohozinski, R. Villeneuve, N. Zittrain, J. *Internet filtering in china in 2004-2005: a country study.* Harward Law School Research Publication No. 2005-10, 2005. 3-4.
[41] *Ibid.*
[42] Deibert, R. Palfrey, J. Rohozinski, R. Zittrain, J. *Access Denied – The Practice and Policy of Global Internet Filtering.* Cambridge: MIT Press, 2008. 9.

apsauga yra dar viena svarbi paskata interneto turinio kontrolei. Siekiant apsaugoti intelektinę nuosavybę nuo neteisėto panaudojimo (atgaminimo, platinimo, autorystės pasisavinimo ir t.t.), dažnai yra blokuojami tam tikri interneto tinklapiai. Dažnai tinklapiai, pažeidžiantys intelektinės nuosavybės teises arba tinklapiai, kuriuose randasi turinys, netinkantis tam tikrai amžiaus grupei, ar prieštaraujantis socialinėms normoms bei moralei, yra įtraukiami į taip vadinamus juoduosius sąrašus. Šiuose sąrašuose esančius tinklapius interneto paslaugų teikėjai išima iš paieškos rezultatų arba padaro neprieinamais (puikiausias pavyzdys – Kinijos interneto filtravimas). Kitaip tariant, tokie tinklapiai yra blokuojami.

Kinijos interneto filtravimas yra, galbūt, drastiškas pavyzdys ir šiuo atveju interneto cenzūros suvokimas tampa iškreiptu ir formuojančiu tokią savimonę bei politinį ir bet kokį kitą požiūrį, kokį nori suformuoti vadžia. Negalima teigti, jog apskritai interneto filtravimas – cenzūra yra blogai ar gerai. Kiekvienu atveju reikia vertinti kokiu tikslu ši cenzūrą yra vykdoma. Apie tai šnekėsiu kitame skyriuje, tačiau dabar trumpai paminėsiu. Dauguma šalių tokį turinį kaip vaikų pornografija ar rasinę, tautinę ar bet kokią kitą neapykantą kurstančias kalbas laiko pakankamai nepriimtina informacija ir siekia jos platinimą panaikinti. Kadangi net demokratinės valstybės nepasisako vienareikšmiškai dėl nepritarimo atitinkamam turiniui, tai taip pat negalima vienareikšmiškai pasisakyti apie cenzūros teisėtumą vien tik įvertinus koks turinys yra blokuojamas.[43] E. Bambauer teigimu, interneto cenzūra yra teisėta ir visapusiškai priimtina, kai yra skaidri.[44] Tai reiškia, kad valstybė viešai ir atvirai paskelbia, kokį turinį ji ruošiasi blokuoti (fitruoti), filtravimą taiko tik konkrečiam neleistinam turiniui ir apie savo sprendimus informuoja visuomenę.

Pastebėtina, jog tokios sąlygos turėtų būti įgyvendintos dėl to, kad net gilias demokratines šaknis turinčiose valstybėse formaliai cenzūrai, įgyvendinamai pasitelkiant teisės normas, vis dažniau yra pasipriešinama. Vokietijoje federalinė valdžia 2009 metais išleido įstatymo projektą, kuriuo būtų privaloma filtruoti turinį, susijusį su vaikų pornografija.[45] Tačiau šis projektas susilaukė pasipriešinimo, ir, nors ir buvo pasirašytas paties Vokietijos prezidento, liko neįgyvendintas. Jungtinės Amerikos Valstijose panašus tinklapių, galimai pažeidžiančių intelektinės nuosavybės teises, cenzūros įstatyminis įtvirtinimas buvo pasiūlytas kongrese. Nors nei *Stop Online Piracy Act* (SOPA), nei *Protect Intellectual Property Act* (PIPA) nebuvo pateikti balsavimui, PIPA buvo priimtas Senato komiteto (*Senate Judiciary Comitee*), o SOPA buvo jau įtrauktas į darbotvarkę kai

[43] Baumbauer, D.E. *Censorship V3.1*. Discussion paper No. 12-28, University of Arizona, 2012. 3-4.
[44] *Ibid.*
[45] *Germany's President Signs an Internet Bill Against His Own Party.* [interaktyvus] EDRI 2010. [žiūrėta 2012-12-16]. <http://www.edri.org/edrigram/number8.4/german-president-adopts-internet-childporn-law>.

prasidėjo protestai ir teko jo svartymą sustabdyti.[46] Konkrečiai SOPA lėmė greitą koalicijos prieš interneto cenzūrą susiformavimą iš technologijų kompanijų, tokių kaip *Google*, civilines teises ginančių grupių, žiniasklaidos atstovų, ir vartotojų.[47] PIPA ir SOPA išėmimas iš Kongreso darbotvarkės simbolizuoja naujosios koalicijos pergalę. Šios koalicijos stipriausi argumentai buvo tai, kad naujieji įstatymai JAV prilygintų Kinijai bei Iranui (kuriuose cenzūra vykdoma drastiškiausiai) ir galiausiai naujas reguliavimas tiesiog padarytų internetą nebefunkcionalų.[48] Iš esmės PIPA ir SOPA „kova“ iliustravo demokratinės visuomenės vertybes, kur kiekvienas gali teisėtai kovoti už savo teises ir laisvai reikšti savo nuomonę.

2.2. Blokavimas

Ką iš tiesų reiškia filtravimas? Filtruoti – tai pagal nustatytus kriterijus atrinkti tik tam tikrus rezultatus. Iš esmės, filtravimas – tai tam tikro turinio išėmimas iš paieškos rezultatų arba padarymas konkretaus tinklapio neprieinamu. Blokavimas ir filtravimas iš esmės reiškia tą patį. Dažnai kalbant apie blokavimą ar filtravimą susidaro toks įspūdis, jog tai yra labai lengvas sprendimas, tiesiog reikia pasirinkti vieną iš dviejų funkcijų – „įjungti“ arba „išjungti“. Toks suvokimas yra toliausiai nuo tiesos. Interneto turinio blokavimas yra labai sudėtingas procesas, paremtas sudėtingomis technologijomis ir, negana to, gana lengvai apeinamas. Tam yra daugybė priežasčių, tačiau viena pagrindinių yra tai, kad internetas buvo sukurtas kaip decentralizuota aplinka su įdiegta laisvo duomenų judėjimo funkcija.

Blokavimas, kaip procesas, atsirado prieš porą dešimtmečių ir buvo skirtas grynai nepageidaujamiems elektroniniams pranešimams blokuoti. Ši technologija tobulėjo kartu su jos apėjimo būdais. Šiuo atveju tokio elektroninio pašto blokavimas yra kur kas lengviau įgyvendinamas nei tinklalapio blokavimas. Taip yra dėl vieno pagrindinio skirtumo:

a) Elektroninis laiškas yra siunčiamas iš konkretaus žinomo serverio ir tėra vienas kelias laiškui pasiekti adresatą (kadangi šis yra nurodomas);
b) Konkretaus interneto tinklapio blokavimas yra kur kas sudėtingesnis. Patekti į konkretų interneto tinklapį yra daugybė interneto kelių, todėl šiuo atveju interneto paslaugų teikėjams yra sunkiau užkirsti visus tuos kelius.[49]

---

[46] *Eric Goldman, Celebrating (?) the Six-Month Anniversary of SOPA's Demise.* [interaktyvus] Forbes 2012. [žiūrėta 2012-08-09]. <http://www.forbes.com/sites/ericgoldman/2012/07/18/celebrating-the-six-month-anniversary-of-sopas-demise/>.

[47] Tsukuyama, H. Kang, Cecilia. *SOPA opposition goes viral.* [interaktyvus] Washington POST 2011. [žiūrėta 2012-08-13]. <http://www.washingtonpost.com/business/economy/sopa-opposition-goes-viral/2011/11/22/gIQAZX7OmN_story.html> .

[48] Bambauer, D.E. *Censorship V3.1, supra* note 43,p. 4.

[49] Callanan, C. Gercke, M. Marco, E.D. Ziekenheiner, E.D. *Internet blocking balancing cybercrime responses in democratic societies.* Aconite internet solutions, Ireland, 2009. 43.

Egzistuoja du blokavimo būdai – privatus ir viešas. Paties vartotojo pasirenkamas blokavimas leidžia vartotojui pasirinkti, kokį turinį jis nori blokuoti, pavyzdžiui, apsaugoti vaikus („saugus internetas“ – Lietuvoje). Taigi blokavimas yra individualaus pobūdžio. Tačiau čia išlieka ta problema, kad jeigu vartotojas norės atsisiųsti ar pamatyti turinį, kuris yra neteisėtas, jis tą vis tiek galės padaryti.

Kitas blokavimo būdas, yra tinklo pagrindu veikiantis blokavimas. Šiuo atveju interneto paslaugų teikėjas nusprendžia, kokį turinį reikia blokuoti ir šis turinys tampa neprieinamas visiems paslaugų gavėjams.

Žinoma, yra skirtumas kai interneto paslaugos yra gaunamos tiesiai iš interneto paslaugų teikėjo ir kai šias paslaugas perteikia, pavyzdžiui, mokymo įstaigos ar darbdavys. Tokiu atveju yra pasitelkiama papildoma programinė įranga, kurios dėka yra griežčiau žiūrima į blokavimą. Tai reiškia, kad šiais atvejais interneto prieiga gali būti labiau suvaržoma išskiriant tam tikrus tinklapius. Taigi tokiu atveju prie blokavimo prisideda ir suinteresuoti paslaugų gavėjai.

Blokavimas (filtravimas) skirtingose šalyse yra nustatomas skirtingais tikslais ir atsakomybe. Pavyzdžiui, Australijoje juoduosius sąrašus sudaro Australijos komunikacijų ir žiniasklaidos priemonių institucija (*Australian Communications and Media Authority – ACMA).* Planuojama, jog šie sąrašai taps privalomi viesiems interneto paslaugų teikėjams. Didžiojoje Britanijoje tokius sąrašus sudaro Interneto priežiūros fondas (*Internet Watch Foundation*) ir šie sąrašai yra prieinami visiems interneto paslaugų teikėjams. Danijoje sąrašus sudarinėja Nacionalinės danų policijos nacionalinis aukštųjų technologijų nusikaltimų centras (*The National High Tech Crime Centre of the Danish National Police*) ir „Gelbėkit vaikus Danija” (*Save the Children Denmark*), o tuo tarpu Suomijoje blokavimas atliekamas pagal domeno vardų sąrašą, kurį pateikia Suomijos policija.[50]

Iš techninės pusės blokavimas gali būti vykdomas keliais pagrindais – būdais:

1) Interneto protokolų (IP) blokavimas. Šis blokavimas vykdomas atrenkant (filtruojant) konrečius IP adresus;
2) Blokavimas arba pakeitimas DNS informacijos – tai reiškia yra klastojamas DNS serverio atsakymas;
3) Universalaus nuorodos identifikatoriaus (*Universal Reference Identifyer* (URI) arba *Uniform Resource Identifyer*) blokavimas. Šio tipo blokavimo atveju yra išskiriamas konkretus tinklapio turinys (nuoroda).

[50] Callanan, C. Gercke, M. Marco, E.D. Ziekenheiner, E.D. *Supra* note 49, p. 16.

4) Raktažodžių blokavimas. Šio blokavimo atvejais yra blokuojami tinklapiai pagal juose esančius žodžius arba blokuojami paieškos rezultatai, kurie yra įtraukti į atitinkamus juoduosius sąrašus.[51]

Bandymas blokuoti – padaryti neprieinamą tam tikrą turinį nereiškia, jog tas turinys bus pašalintas. Techniniai trūkumai, tokie, kaip nepakankamas blokavimo lygis, per didelis blokavimo lygis, įstatymų kolizija ir faktas, kad blokuojamas turinys nėra pašalinamas iš interneto aplinkos, reiškia, jog klausimas yra ne tik ar reikia blokuoti, ar ne, tačiau, ir kokiomis priemonėmis tai geriausiai įgyvendinti demokratinėje visuomenėje nepažeidžiant pamatinių normų ir prigimtinių laisvių. Iš tiesų yra labai svarbu nustatyti, kokios pagrindinės teisės ir laisvės iš esmės prieštarauja interneto blokavimui ir kokios palaiko arba sudaro sąlygas įgyvendinti šį blokavimą. Interneto paslaugų teikėjų vaidmuo yra esminis taikant interneto turinio blokavimo priemones, tačiau jų veiklą riboja neaiškus teisinis reglamentavimas bei nevienodi jų veiklai keliami reikalavimai. Iš teisės pusės, interneto blokavimas yra priemonė, kuri suteiktų teisę blokuoti, teisę pasirinkti technines priemones bei teisę pasirinkti turinį, siekiant apginti konkretų interesą, tokiu būdu paneigiant kai kurių piliečių teisę pasiekti tam tikrą turinį ar padaryti jį prieinamu. Galima sakyti, kad interneto turinio blokavimas yra vykdomas siekiant apsaugoti vienas pagrindines laisves ir teises, tačiau tuo pačiu paneigiant kitas.

Reikia atskirti teises ir laisves, kurios prieštarauja interneto blokavimui iš savo prigimties – tai išraiškos teisė bei teisė į privatų ir šeimos gyvenimą. Taip pat reikia išskirti, kurios pagrindinės teisės ir laisvės blokavimą palaiko, kaip pavyzdžiui vaiko teisė būti apsaugotam nuo smurto ir išnaudojimo.[52] Interneto blokavimas iš dalies paneigia tokias žmogaus pagrindines teises ir laisves kaip:

1) Išraiškos laisvė – neleidžiant žmonėms pasiekti internete esančios informacijos arba neleidžiant jos skelbti. Blokavimas daro neigiamą poveikį transliavimui, komunikacijai bei ryšiui. Į šią laisvę įeina teisė gauti informaciją, įskaitant internetą, kaip šaltinį. Bet kokia blokavimo priemonė trukdanti asmeniui pasiekti norimą turinį internete galėtų būti traktuojama kaip šios laisvės paneigimas. Pastebėtina, jog 2009 metų gegužės 6 dienos telekomunikacijų teisinio reglamentavimo reformos projekte Europos parlamentas teigė, jog negali būti taikomas joks galutinių vartotojų pagrindinių teisių ir laisvių suvaržymas be išankstinio teismo sprendimo, išskyrus visuomenės saugumui užtikrinti. Kai kurie autoriai teigia, jog šia nuostata interneto prieiga buvo pripažinta viena iš pagrindinių žmogaus teisių ir laisvių. Kiekvienas bandymas blokuoti interneto turinį yra šios laisvės

[51] „Dutton, W.H. Dopatka, A. Hills, M. Law, G. Nash, V. *supra* note 36, p. 30.
[52] Callanan, C. Gercke, M. Marco, E.D. Ziekenheiner, E.D. *supra* note 49, p. 22-23.

apribojimas, ir nesvarbu ar traktuosime prieigą prie interneto kaip vieną pagrindinių žmogaus laisvių ar ne.

2) Interneto blokavimas taip pat gali pažeisti specialias teises, suteiktas kai kurioms žmonių kategorijoms, pavyzdžiui, teisė neįgaliems asmenims naudotis elektroninėmis ryšio priemonėmis.[53]

Iš kitos pusės ne visos pagrindinės teisės savo prigimtimi yra prieš bet kokią informacijos kontrolę. Kai kurios jų kaip tik turėtų antrinti pačiai filtravimo-blokavimo idėjai. Pavyzdžiui:

1) Vaikų teisė būti apsaugotiems nuo smurto;
2) Žmonių nediskriminavimo teisė;
3) Intelektinės nuosavybės teisės.

Šnekant apie vaikų teisę būti apsaugotiems nuo smurto pagrindinė nuoroda interneto aplinkoje būtų vaikų pornografija bei bet kokia seksualinio turinio ar smurtinio turinio informacija. Dažnai siekis apsaugoti vaikus nuo minėtos informacijos tampa pretekstu įgyvendinti galbūt griežtesnę turinio kontrolę ir neretai tampa vieninteliu valdžios ar privačių asmenų, vykdančių blokavimą, argumentu.

Pagrindinės žmogaus teisės ir laisvės yra garantuojamos kiekvienam asmeniui be išimčių. Viena iš tokių teisių yra nebūti diskriminuojamam. Taigi šios teisės apsauga taip pat gali būti paskata interneto turinio kontrolei. Iš interneto perspektyvos, į šios teisės apimtį įeina ne tik tekstai kurstantys diskriminaciją, tačiau ir kankinimo bei žmogžudysčių iš rasinės neapykantos paskatų vaizdiniai. Toks turinys taip pat yra viena iš paskatų imtis turinio kontrolės.

Intelektinės nuosavybės teisės yra saugomos ne vienos tarptautinės sutarties bei nacionalinių teisės aktų. Bendru suvokimu intelektinės nuosavybės teisės internete labiausiai susijusios su autorių teisėmis. Intelektinės nuosavybės apsauga taip pat yra vienas pagrindinių akstinų vykdyti interneto blokavimą (filtravimą).[54]

Europoje taikomos blokavimo priemonės turi atitikti ir elektroninių ryšių reguliavimui keliamus reikalavimus. Šie reikalavimai apima interneto paslaugų teikėjų įsipareigojimą dėl paslaugų kokybės, universalių paslaugų įsipareigojimus bei interneto paslaugų teikėjų neutralumo įsipareigojimą. Į universaliųjų paslaugų apimtį įeina pagrindinės komunikacinės paslaugos, įskaitant balso komunikaciją bei prieigą prie interneto. Bet kokios blokavimo priemonės, kurios neleistų asmeniui pasinaudoti viešu telefono tinklu, prieštarautų universaliųjų paslaugų teikimo įpareigojimui.

[53] Callanan, C. Gercke, M. Marco, E.D. Ziekenheiner, E.D. *supra* note 49, p. 26.
[54] *Ibid.*, p. 26-27.

Iš esmės vieši kompiuterių tinklai yra labai sudėtingas darinys ir todėl blokavimo priemonių taikymas tik padidina riziką atsirasti tam tikriems nesklandumams, pavyzdžiui, nestabilus ryšys ar nuolatiniai ryšio trūkinėjimai. Žiūrint iš šios pusės, tarp turinio blokavimo ir elektroninių ryšių paslaugų teikimo atsiranda priešprieša. Kitaip tariant, įpareigojant interneto paslaugų teikėją taikyti blokavimo priemones paslaugų teikėjui atsiranda dviguba atsakomybė. Iš vienos pusės jis turi teikti nustatytos kokybės paslaugas, o iš kitos turi taikyti priemones, dėl kurių išlaikyti paslaugų kokybę pasidaro ypač sunku.[55]

Interneto paslaugų teikėjai turi laikytis įsipareigojimo išlikti neutraliais turinio perdavimo internetu atžvilgiu (pagal kitų tarpininkų pavyzdžius: tradicinės telefonijos bei pašto paslaugų atvejais). Atsižvelgiant į šį įsipareigojimą, interneto paslaugų teikėjas negali pasirinkti perduoti ar neperduoti konkrečios „žinutės“ (pranešimo, informacijos) priklausomai nuo jos turinio, išskyrus atvejus kai yra gautas subjekto sutikimas arba kai to reikalauja teisinis reglamentavimas.

Interneto paslaugų teikėjas negali vykdyti tiesioginės turinio kontrolės – monitoringo, išskyrus atvejus, kai to reikalauja teisės aktai ar teisėsaugos institucijos. Bet kokia turinio kontrolės priemonė, kuria galima pasiekti konkretų siunčiamos informacijos turinį (pvz. elektroninio laiško) yra negalima, nebent toks įgalinimas yra reglamentuotas teisės aktuose atitinkamoms situacijoms. Be atitinkamų teisės aktų, kurie įpareigotų interneto paslaugų teikėją blokuoti konkretų turinį, paslaugų teikėjas neturi teisės stebėti ar blokuoti tinklo turinio nepažeisdami savo apsaugos nuo atsakomybės salygų. [56]

2.3. „Deep Packet Inspection“

Kas yra „deep packet inspection“? Tai yra į tinklą integruota funkcija, kuri leidžia tinklo savininkui (paslaugų teikėjui) realiu laiku analizuoti srauto duomenis ir atskirti juos pagal turinį. Tai padaryti galima tik pasitelkus specialią programinę įrangą. „Deep packet inspection“ yra toks kompiuterinių sistemų naudojimas, kuris leidžia trečiai šaliai identifikuoti tam tikrus komunikacijos aspektus. Pavyzdžiui, šią technologiją gali naudoti interneto paslaugų teikėjas teisėtam pranešimo viešuose tinkluose perėmimui, siekdamas nustatyti ar vartotojai naudojasi tinklu neteisėtais tikslais arba tikslais, kurie pažeidžia vartojimo sutartį. Vyriausybės Šiaurės Amerikoje, Azijoje bei Afrikoje naudoja DPI įvairiems tikslams, tokiems kaip sekimas ar cenzūra. DPI gali tarnauti kaip pagrindinis įrankis komunikacijų ir srautų stebėjimui bei reguliavimui. Taip pat DPI gali tarnauti įvairių tarpininkų interesams:

1) Politinė kontrolė – valstybinės agentūros ir turinio tiekėjai, kurie yra suinteresuoti informacijos srautų filtravimu ir monitoringu;

[55] Callanan, C. Gercke, M. Marco, E.D. Ziekenheiner, E.D. *supra* note 49, p. 27.
[56] *Ibid., p.* 28.

2) Technologinis našumas – tinklo darbuotojai, kurie dirba su žalingomis programomis.
3) Ekonominiai interesai – interneto paslaugų teikėjai, norintys sukurti papildomų pajamų arba jas apsaugoti.[57]

Pati technologija yra trijų lygių. Išskiriama *Shallow inspection, Medium inspection* ir *Deep packet inspection*. Pirmasis lygmuo yra technologija, kurią naudoja net ir paprasti vartotojai to net nežinodami. Tai yra ta technologija, kurios pagrindu veikia elementarios (sąlyginai) „ugniasienės“. Jos neleidžia konkrečiam vartotojo nurodytam informacijos paketo (turinio) tipui patekti į kompiuterį ar išeiti iš jo. Ši sistema veikia tokiu pagrindu.

Kai iš serverio į vartotojo kompiuterį atkeliauja informacijos paketas, SPI (*Shallow packet inspection*) technologija, nuskaičiusi paketo pavadinimą (angl. *header*), sulygina jį su turimu juoduoju sąrašu ir sprendžia, ar tokį paketą praleisti, ar ne. Šiuo atveju egzistuoja įvairūs juodųjų sąrašų sudarymo variantai, juos gali sudaryti tiek tinklo administratorius, tiek vartotojas, o taip pat gali būti palikti baziniai ugniasienės nustatymai pagal gamintojo iš anksto sudarytą sąrašą.

SPI technologija negali nuskaityti paketo turinio esančio giliau, nei jo pavadinimas. Galima sakyti ši situacija yra panaši į atvejus, kada kompiuteryje norite atidaryti tam tikrą failą su puikiai matomu pavadinimu, tačiau neturite reikiamos programinės įrangos, kad galėtumėte jį atidaryti. SPI technologija nuskaito siuntėjo ir gavėjo IP adresus, paketų skaičių (į kuriuos informacija yra išskaidoma) bei sinchronizavimui reikalingą informaciją, kuri paketus vėl sujungia į vieną. Taigi, ši technologija nėra pajėgi analizuoti paketo turinio.

Antras šios technologijos lygmuo yra *Medium packet inspection*. Šiuo atveju technologija veikia jau ne vartotojo galiniame įrenginyje (kompiuteryje), o tarpinėje stotelėje tarp vartotojo kompiuterio ir interneto paslaugų teikėjo – *proxy* serveryje. Dažniausiai ši technologija yra diegiama tinklo „proxy“ serveriuose ties maršrutizuojančia įranga.[58]

Kai informacijos paketas patenka į *proxy* serverį, jis yra analizuojamas pagal „apdorojimo“ sąrašą (angl. *parse-list*), kurį tinklo administratorius gali lengvai papildyti ar pakeisti. Šis sąrašas yra šiek tiek subtilesnis nei juodojo sąrašo variantas. Priešingai nei pastarajame, „apdorojimo“ sąraše galima numatyti konkrečius duomenų tipus, kuriuos norėsime praleisti arba užblokuoti atsižvelgiant į duomenų formatą, jų vietą internete, o ne tik pagal IP adresą. Naudodamiesi MPI technologija tinklo administratoriai galėtų neleisti vartotojams matyti *Flash* tipo video failų (kurių pagrindu veikia tinklapis *YouTube*), ar socialiniuose tinkluose talpinamų nuotraukų. Vienas iš MPI minusų yra tai, kad ši technologija negali tikrinti didelio kiekio paketų iš karto, dėl ko labai sulėtėja

[57] Dutton, W.H. Dopatka, A. Hills, M. Law, G. Nash, V. *supra* note 36, p. 29.
[58] Parson, C. *Deep packet inspection in perspective: tracing it's lineage and surveillance potentials.* Working paper, doctoral studies. University of Victoria's Political Science department, Canada, 2009. 7.

paketų pristatymo greitis. Dėl tokių trūkumų, MPI dažniausiai nėra taikomas didelių tinkle priežiūrai, ir būtent dėl to interneto paslaugų teikėjams nėra naudingas.

Deep packet inspection yra labiausiai išvystyta technologija iš minėtų trijų. Šis kontrolės būdas apima tiek duomenų tipo, išeities taško, IP adresų ir t.t. nustatymą, tiek ir paties turinio analizę. Kaip minėjau MPI savo pobūdžiu negali peržiūrėti didelio kiekio informacijos paketų, o DPI yra sukurtas būtent tam, kad galėtų vienu metu skanuoti tūkstančius vykstančių perdavimų, nustatant, kokia programinė įranga sugeneravo paketą. Kartais DPI negali tuoj pat nustatyti kokia programinė įranga sugeneravo tam tikrą paketą. Tokiais atvejais į pagalbą ateina *Deep packet capture* (DPC) technologija, kuri leidžia paketą išsaugoti ir tada pasitelkiant DPI jį pilnai išanalizuoti.[59]

Pirminis DPI kūrimo tikslas buvo saugumo sumetimai. DPI buvo naudojama apsaugoti interneto vartotojus nuo kenkėjiškų programų, kurios keliauja internetu. DPI tikslas buvo jas atpažinti ir dar nepasiekusias vartotojo galinio įrenginio. Nors dabar ši technologijos funkcija dar egzistuoja, bet kartu DPI pradėta naudoti ir kitais tikslais, tokiais kaip tinklo valdymas, stebėjimo, reklaminių pranešimų atskyrimui bei autorių teisių pažeidimams išaiškinti.[60] Du tikslai, į kuriuos labiausiai reikėtų atkreipti dėmesį (nešnekant apie stebėjimo vykdymą) – tai yra tinklo valdymas ir kova su autorių teisių pažeidimais.

Taip pat interneto paslaugų teikėjai naudoja DPI tinklo valdymo tikslu, į kurį įeina daugybė funkcijų, tokių kaip užtikrinti galiniam vartotojui teikiamų paslaugų kokybę. R. Bendrath tokį DPI naudojimą charakterizuoja kaip technologinio našumo ir ekonominių interesų kombinaciją.[61] Toks DPI naudojimas iš tiesų kelia tam tikrų neaiškumų ir teisėtumo klausimą. Kaip ir minėjau, bet koks filtravimas savo prigimtimi iš dalies kertasi su žmogaus teisėmis. Taigi interneto paslaugų teikėjų DPI naudojimas kelia klausimų. Apie interneto paslaugų teikėjų filtravimo galimybę bei praktiką išsamiai bus kalbama kituose skyriuose.

2.3.1. Intelektinės nuosavybės apsauga – tikslas taikyti „DPI“

Autorių teisių turėtojai tiek JAV, tiek Europoje reikalauja, kad interneto paslaugų teikėjai naudotų DPI autorių teisių pažeidimams išvengti ir ginti autorių teises. Pavyzdžiui, Belgijoje ir Airijoje buvo bandymų, siekiančių nustatyti atsakomybę interneto paslaugų teikėjams už vartotojų padarytus autorių teisių pažeidimus. Belgijoje šalys susitarė be teismo sprendimo, dėl to, jog

[59] Parson, C. *supra* note 58, p. 8.
[60] Daly, A. *The legality of deep packet inspection. First interdisciplinary Workshop on Communications Policy and Regulation 'Communications and Competition Law and Policy – Challenges of the New Decade'.* University of Glasgow, 2010. 4.
[61] *Ibid.*

nepavyko efektyviai nustatyti pažeidimų, o Airijoje šalys susitarė, jog nustačius, kad vartotojai daro autorių teisių pažeidimus (esant tam tikroms sąlygoms), tokiems vartotojams bus atjungtas interneto ryšys.

Pati DPI sistema dėl savo dinamiškumo gali būti programuojama įvairiems tikslams, pavyzdžiui, nustatyti, kada yra siunčiamas duomuo veikiant *torrent* protokolams.

DPI naudojimas siekiant apsaugoti intelektinės nuosavybės teises (o tiksliau autorių teises) yra sudėtingiausias ir unikaliausias procesas. Ar autorių teisių apsauga tokių sistemų taikymui yra pakankama priežastis bus matyti kitame skyriuje.

DPI sistema autorių teisių apsaugai veikia „pirštų antspaudų“ modeliu. Autorių teisių subjektai pasinaudoję sistemų kūrėjų programine įranga, kad sugeneruotų unikalų parašą kiekvienam saugomam objektui. Visi tokie „pirštų antspaudai“ yra saugomi registre. Iš esmės DPI sistema pagauna perduodamos informacijos fragmentus, iš kurių ši nusprendžia, ar tai saugomas objektas ir, jeigu pasitvirtina, kad tai saugomas objektas, sistema padaro šio objekto „pirštų antspaudą“ – skaitmeninį įspaudą, kopiją. Tada sistema sutikrina padarytą įspaudą su registre registruotais parašais ir taip nusprendžia ar padarytas pažeidimas.[62]

Taip pat yra ir alternatyvus modelis autorių teisių ir jų apsaugos stebėjimui. Tokiais atvejais teisių subjektų atstovai ar samdyti darbuotojai patys vykdo stebėseną. Tokia stebėsena pavyzdžiui gali būti vykdoma per P2P tinklus valdant *torrent* failus (duomenis). Iš esmės šie asmenys renka neteisėtai platinamus objektus kaip paprasti vartotojai ir naudodami prieš tai minėtą „pirštų antspaudų“ atitikmenų paieškos metodą atpažįsta ir renka IP adresus tų vartotojų, kurie kaip nors susiję su autorių teisių objektų neteisėtu platinimu. Tada yra kreipiamasi į interneto paslaugų teikėjus, kad šie susietų IP adresus su konkrečiais vartotojais, kad pastarieji galėtų būti patraukti atsakomybėn. Nors toks metodas ir nereikalauja, kad interneto paslaugų teikėjai taikytų DPI sistemas, tačiau vis tiek yra reikalingas jų bendradarbiavimas, kadangi tik interneto paslaugų teikėjas gali susieti konkretų IP adresą su konkrečiu vartotoju. [63]

Reikia pabrėžti, kad skirtingos šalys turi skirtingus požiūrius į interneto turinio cenzūrą (kontrolę), kaip ir į priemones kuriomis yra vykdoma kontrolė. Taip pat skirtingai traktuojama piliečių dalyvavimas priimant sprendimus, susijusius su interneto turinio filtravimu. Šiuo atveju visuomenės atsakingumas priklauso nuo vykdomų veiksmų skaidrumo. Skaidrumas reiškia žinojimą, kas yra filtruojama, kas filtruoja, kokiu tikslu filtruoja, kokia apimtimi yra vykdomas filtravimas. Būtent skaidrumas yra tas veiksnys, kuris galėtų sudaryti sąlygas visuomenei būti

[62] Mueller, M. Kuehn, A. Santoso, S.M. *Policing the Network: Using DPI for Copyright Enforcement.* Surveilance and society, 2012. 351.
[63] *Ibid.*

aktyvesnei bei dalyvauti sprendimų, susijusių su filtravimo sistemomis, priėmime. Tačiau iškyla ir problema – yra sunku užtikrinti skaidrumą, kai filtruojamas turinys savo prigimtimi prieštarauja socialinėms normoms bei moralei ir teisėtai yra nepasiekiamas ar neturėtų būti pasiekiamas (pavyzdžiui vaikų išnaudojimo vaizdai ir pan.)[64].

Įtampą tarp filtravimo skaidrumo ir visuomenės dalyvavimo gerai atsispindi 2008 metų byloje Didžiojoje Britanijoje. Interneto priežiūros fondas (*Internet Watch Foundation*), nepriklausoma, veikianti savireguliacijos principu institucija, turėdama tikslą sumažinti neteisėto turinio kiekį internete, įtraukė į juodąjį sąrašą vieną *Wikipedia* straipsnį, kaip galimai pažeidžiantį Didžiosios Britanijos vaikų apsaugos įstatymą. Buvo nuspręsta, jog minimame straipsnyje apie roko grupės „Scorpions“ albumą *Virgin Killer* įdėta albumo viršelio nuotrauka yra nepadori asmenų iki 18 metų atžvilgiu. Dėl šios priežasties buvo užblokuotas minimas straipsnis. Žinoma, toks interneto priežiūros fondo sprendimas susilaukė įvairių komentarų, tuo labiau, kad padarius neprieinamą konkretų straipsnį įvyko blokavimo sistemų konfliktas tarp *BT Cleanfeed Technology* ir *Wikipedia Vandalism Blacklist*. Šis konfliktas iškilo dėl to, kad *BT Cleanfeed technology* filtravimo sistema yra tiesiogiai susijusi su Interneto priežiūros fondo juodaisiais sąrašais. Jeigu norimas tinklapis yra juodajame sąraše, sistema nukreipia užklausą į mažesnius *proxy* (tarpinius) serverius ir iš ten dar kartą sutikrinusi konkrečią užklausą arba leidžia prisijungimą, arba ne. Kadangi konkretus *Wikipedia* straipsnis pateko į minėtą juodąjį sąrašą, dėl to visos *Wikipedia* užklausos buvo peradresuojamos į mažus *proxy* serverius (iš kurių yra tikrinamas konkretus adresas). Dėl to visos užklausos, kurios nebuvo nukreiptos konkrečiai į užblokuotą tinklapio dalį – straipsnį, buvo praleidžiamos. *Wikipedia* apsauga kiekvieno prisijungimo prie tinklapio metu identifikuoja IP adresą, siekiant apsaugoti tinklapį nuo vandalizmo (kad pažeidimo atveju galima būtų užblokuoti prieigą konkrečiam IP adresui). Kadangi *BT Cleanfeed technology* sistema po antros patikros (nukreipimo į *proxy* serverius) leisdama patekti varototojams į *Wikipedia* tinklapį praleisdavo juos ne su orginaliais IP adresais, bet su *proxy* serverių adresais, *Wikipedia* sistema nebegalėjo nustatyti kiekvieno vartotojo IP adreso, todėl sistema buvo suklaidinta ir galiausiai užblokavo visus prisijungimus iš *proxy* serverių IP adresų. Dėl to dauguma vartotojų neteko galimybės redaguoti *Wikipedia* straipsnių.[65] Vėliau Interneto priežiūros fondas savo sprendimą pakeitė, teigdami, kad: „išnagrinėjus konkrečios situacijos kontekstą, bei įvertinus kiek laiko šis atvaizdas egsistuoja bei yra prieinamas, nusprendėme pašalinti šį tinklapį iš savo sąrašo“[66].

[64] Dutton, W.H. Dopatka, A. Hills, M. Law, G. Nash, V. *supra* note 36, p. 42-43.
[65] Dutton, W.H. Dopatka, A. Hills, M. Law, G. Nash, V. *supra* note 36, p. 43-44.
[66] Internet Watch Foundation statement *regarding Wikipedia webpage*. [interaktyvus] 2008. [žiūrėta 2012-10-10]. <http://www.iwf.org.uk/about-iwf/news/post/251-iwf-statement-regarding-wikipedia-webpage>.

Apibendrinant turinio kontrolės arba, kitaip tariant, interneto kontrolės priemones, reikia pasakyti, kad visos aptartos technologinės galimybės ir jų naudojimas priklauso tik nuo to, kokią poziciją užima konkrečios valstybės valdžia. Kitaip tariant, technologinės galimybės leidžia kontroliuoti internetą, kuris savo prigimtimi yra laisvas ir globalus, bei kontroliuoti jį įvairiais lygmenimis. Tačiau čia iškyla klausimas, kas yra teisėta kontrolė ir kiek ją galima taikyti. Tai įvertinus iškyla kitas klausimas – kokias kontrolės priemones gali taikyti tas, kas sukuria vartotojams galimybę pasiekti internetą – interneto paslaugų teikėjas. Taip pat, kiek galima jį įpareigoti vykdyti kontrolę ir kiek toks įpareigojimas būtų teisėtas globaliame kontekste, kai pagrindinės žmogaus teisės ir laisvės yra iškeliamos į pirmą vietą? Kitame skyriuje bus apžvelgta kokias iš aptartų kontrolės priemonių gali taikyti interneto paslaugų teikėjai bei kokios yra jų atsakomybės ribos, taip pat bus įvertinama, kokiu tikslu gali būti taikomos kontrolės priemonės.

3. INTERNETO PASLAUGŲ TEIKĖJŲ NAUDOJAMŲ TECHNINIŲ INTELEKTINĖS NUOSAVYBĖS APSAUGOS BŪDŲ TEISĖTUMAS BEI INTERNETO PASLAUGŲ TEIKĖJŲ ATSAKOMYBĖS RIBOS

Intelektinės nuosavybės gamintojai bei platintojai, siekdami užkirsti kelią nuolatiniams intelektinės nuosavybės teisių pažeidimams greta įprastų teisinių priemonių (kurios bus aptartos toliau darbe) naudoja taip pat ir techninius apsaugos būdus, priemones. Iš esmės, dažnai techninės apsaugos priemonės būna kur kas veiksmingesnės nei bet koks teisinis reglamentavimas (draudimai bei apribojimai). Techninės apsaugos priemonės suprantamos kaip technologija, įrenginiai 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."[67] Tokios techninės apsaugos priemonės skirtos tam, kad teisių turėtojai galėtų kontroliuoti autorių teisių, gretutinių teisių bei *sui generis* teisių objektų naudojimą. Tokios priemonės gali būti kodavimas, elementų perskirstymas ar bet koks kitoks intelektinės nuosavybės objekto transformavimas. Reikia pastebėti, jog įsipareigojimai užtikrinti techninių priemonių ir informacijos apie autorių ir gretutinių teisių valdymą teisinę apsaugą įtraukti į TRIPS bei WIPO sutartis[68].

Vienas iš apsaugos būdų yra skaitmeninėse garso ir vaizdo laikmenose naudojamas techninis apribojimas informaciją atkurti skaitmeniniu formatu. Kitaip tariant, šis apribojimas reiškia, kad turimą laikmenoje informaciją galima naudoti tik toje laikmenoje ir bet koks atgaminimas yra techniškai apribojamas. [69]

Kiti techniniai metodai apima informacijos šifravimą, programinius ir aparatinius kodus, specialias apsaugos sistemas, kurios neleidžia atgaminti kompaktinių diskų bei DVD laikmenų (neleidžia padaryti šių laikmenų kopijų). Šios ir kitos techninės apsaugos priemonės pakankamai patikimai apsaugo intelektinės nuosavybės objektus nuo neteisėto atgaminimo ir naudojimo, ypač nuo tokio, kuris yra pavienis individualus bei nekomercinio pobūdžio.[70]

Kita vertus, taikant minėtas technines apsaugos priemones, atsirado ir toliau vystosi naujos neteisėtos veiklos formos. Ši veikla yra susijusi su įrenginių, skirtų apeiti ar pašalinti minėtas apsaugos priemones gamyba ir platinimu. Iš esmės ši veikla nedaro tiesioginių autorių teisių ar gretutinių teisių pažeidimų ir dėl to techninėms apsaugos priemonėms buvo nustatyta savarankiška

[67] Kiškis, M. *supra* note 7, p. 65.
[68] Kiškis, M. *Ibid.*
[69] Kiškis, M. *Ibid*.
[70] Kiškis, M. *Ibid*.

teisinė apsauga. „Visose išsivysčiusiose valstybėse draudžiama pašalinti bet kokias autorių teisių ir gretutinių teisių objekto techninės apsaugos priemones, taip pat gaminti ir platinti prietaisus ar kitokias priemones, skirtas minėtoms techninėms priemonėms pašalinti.“[71] Reikia taip pat pastebėti, kad kai kuriais atvejais toks apsaugos priemonių pašalinimas ar apėjimas yra būtinas suderinamumui užtikrinti ar atsarginės kopijos atgaminimui, ką įstatymai ir leidžia. Dėl to iki šiol kyla tiek teorinių, tiek ir praktinių problemų susijusių su techninių apsaugos priemonių taikymu bei teisine apsauga.[72]

Jeigu asmuo tyčia šalina ar vengia techninių apsaugos priemonių, tokie atvejai yra laikomi techninių apsaugos priemonių pažeidimu. Techninių apsaugos priemonių apsauga įtvirtinta tiek Europos Sąjungos teisės aktuose, tiek ir nacionaliniuose.[73] Lietuvoje tehninių priemonių apsauga įtvirtinta Lietuvos Respublikos baudžiamojo kodekso nuostatomis, kurios nustato baudžiamąją atsakomybę už informacijos apie autorių teisių ar gretutinių teisių valdymą, sunaikinimą ar pakeitimą,[74] taip pat neteisėtą autorių ar gretutinių teisių techninių apsaugos priemonių pašalinimą[75].

Šiuo atveju problema išlieka ta, kad iš esmės vartotojas negali įgyvendinti savo teisių, susijusių autorių teisių ar gretutinių teisių objektų atgaminimu švietimo ir mokslo tikslais arba asmeniniais tikslais, ką numato autorių teisių ir gretutinių teisių įstatymai. Baudžiamasis kodeksas tokių išimčių nenumato ir tai aiškiai sąlygoja intelektinės nuosavybės naudotojo teisių ir intelektinės nuosavybės teisių pažeidimų koliziją.[76]

Interneto tarpininkų vaidmens nustatymas pagal jų teisinę atsakomybę daugeliu atveju yra vienas pagrindinių elektroninės erdvės teisės tikslų. Teisiniai iššūkiai, kurie elektroninės erdvės teisėje yra unikalūs ir diferencijuoja šią teisės sritį nuo kitų, kyla iš to, kokiais būdais ir apimtimi įstatymų leidėjai ir teismai yra pasirengę taikyti atsakomybę interneto paslaugų teikėjams už trečiųjų asmenų elgesį elektroninėje erdvėje bei talpinamą turinį. Interneto tarpininkų vaidmens svarbą pabrėžia ir galia, kurią jie turi vartotojų atžvilgiu ir kuri pasireiškia galimybe kontroliuoti programinės įrangos kodą, kuris suteikia galimybę veikti pasauliniame tinkle ir taip pat jų galimybė stebėti internete vykdomą veiklą. Interneto tarpininkai yra efektyviausia vykdymo grandis norimų

[71] Kiškis, M. *supra* note 7, p. 65-66.
[72] Kiškis, M. Ibid.
[73] Kiškis, M Ibid. p. 67.
[74] Lietuvos Respublikos baudžiamasis kodeksas. *Valstybės žinios.* 2000, Nr. 89-2741. 193 str.
[75] Ibid. 194 str.
[76] Kiškis, M. *op. cit.*, p. 67.

elgesio normų nustatymui internete per pačių tarpininkų nuostatus ar per teisines taisykles, arba abiejų kombinaciją.[77]

Iš esmės teisinis reikalavimas nukreiptas į interneto paslaugų teikėjus yra žymiai efektyvesnis nei, tarkim, toks reikalavimas nukreiptas į informacijos skleidėjus, kurie dažniausiai yra išsibarstę po visą pasaulį ir nebekontroliuoja paskleistos informacijos nuo to momento, kai patalpina ją internete.[78] Svarbiausia, kad tarpininkai nebūtų per daug sukaustyti reguliavimo, kad nebūtų sustabdytas inovacijų atsiradimas ir progresas. Įstatymų leidėjai vis dažniau susiduria su sudėtingu klausimu, kaip reglamentuoti stiprių ir labai inovatyvių interneto tarpininkų veiklą. Vienas iš tokių klausimų yra kada interneto paslaugų teikėjas turėtų būti laikomas atsakingu už žalingą turinį patalpintą internete trečiojo asmens.[79]

Interneto tarpininkai esant tam tikroms sąlygoms vis tik yra atsakingi už trečiųjų asmenų – interneto vartotojų – talpinamą informaciją (turinį). Kalbant apie interneto paslaugų teikėjų atsakomybę bei vaidmenį turinio kontrolės mechanizme, reikia pastebėti, jog europinis reglamentavimas aiškiai pasako, jog interneto paslaugų teikėjų atsakomybė yra pagrįsta žinojimo principu[80]. Šis principas iš esmės reiškia tai, kad interneto paslaugų teikėjai, žinodami apie bet kokį neteisėtą turinį, esantį internete, privalo jį pašalinti. Ilgą laiką vyksta diskusijos dėl interneto paslaugų teikėjų vaidmens turinio kontrolėje. Dažnai yra siūloma priskirti interneto tarpininkams pareigas vertinti turinio teisėtumą. Iš esmės dažnai užduodamas klausimas, ar interneto paslaugų teikėjai neturėtų imtis aktyvios kontrolės veiksmų – monitoringo. Toks klausimas buvo iškeltas byloje SABAM prieš Tiscali (interneto paslaugų teikėją bylos eigoje persivadinusį į Scarlet). Šioje byloje Belgijos muzikos autorių kolektyvinio administravimo asociacija (atitikmuo Lietuvoje būtų LATGA-A) kreipėsi į teismą pastebėjusi, jog daugeliu autorių kūrinių yra keičiamasi peer-to-peer tinklais ir savo kreipimęsi nurodė, jog interneto paslaugų teikėjas turėtų imtis aktyvių veiksmų identifikuoti tokius pažeidimus (intelektinės nuosavybės neteisėto platinimo veiksmus) ir užkirsti jiems kelią. Byla pasiekė Europos Teisingumo Teismą, kur galiausiai buvo priimtas sprendimas, kuriame teismas pasisakė, jog:

„...draudžiama nustatyti interneto prieigos paslaugų teikėjui įpareigojimą įdiegti filtravimo sistemą:
– visiems naudojantis jo paslaugomis gaunamiems ir siunčiamiems elektroniniams pranešimams, pasinaudojant, be kita ko, „peer-to-peer“ programine įranga,

[77] Lipton, J.D. *law of the intermediated information exchange.* case western reserve university school of law, USA, 2012. 8-9.
[78] Lipton, J.D. *Combating Cyber-Victimization.* 26 BERKELEY TECH. L. J. 1103, 1139 USA, 2011.
[79] Lipton, J.D. *supra* note 77.
[80] 2000 m. birželio 8 d. Europos Parlamento ir Tarybos Direktyva 2000/31/EB dėl kai kurių informacinės visuomenės paslaugų, ypač elektroninės komercijos, teisinių aspektų vidaus rinkoje (Elektroninės komercijos direktyva). [2000], OL L178.

– visų jo klientų atžvilgiu,

– prevenciškai,

– tik jo sąskaita,

– neterminuotai,

leidžiančią nustatyti tokio teikėjo tinklu siunčiamas muzikos, kinematografijos ar audiovizualinių kūrinių, kurių intelektinės nuosavybės teisės tariamai priklauso ieškovui, elektronines rinkmenas, kad būtų galima užblokuoti rinkmenų, kuriomis keičiantis pažeidžiamos autorių teisės, persiuntimą."[81]

Atsižvelgiant į tokį autorių teisių kolektyvinio administravimo asociacijos prašymą, galima tikėtis, jog ir kitų sričių atstovai galėtų savo iniciatyva reikalauti privalomo interneto paslaugų teikėjų turinio kontrolės vykdymo. Kai tik interneto paslaugų teikėjas būtų įpareigotas vykdyti kokio nors pobūdžio „monitoringą" (stebėjimą), nuo to momento prasidėtų grandininė reakcija. Pavyzdžiui, įpareigojus interneto paslaugų teikėją vykdyti aktyvų „monitoringą" turinio, susijusio su šmeižtu, ar reputacijos menkinimu bei garbės ir orumo įžeidimu, tuoj pat atsirastų reikalavimai iš autorių teisių savininkų, prekių ženklų savininkų, duomenų bazių kūrėjų, filmų industrijos atstovų, fotografų ir daugelio kitų, vykdyti atitinkamą aktyvų filtravimą, „monitoringą" dėl jų teisių pažeidimų. Tokia „lavina" galiausiai paverstų interneto paslaugų teikėją tapti tiesioginiu turinio kontrolės vykdytoju bei turinio vertintoju, nes būtent jam tektų atsakomybė atskirti, koks turinys yra priimtinas ir teisėtas, ir kokio turinio internete negali būti dėl trečiųjų asmenų teisių pažeidimų. Galiausiai interneto paslaugų teikėjas bijodamas atsakomybės taptų privačios cenzūros vykdytoju.[82]

Informacinės visuomenės paslaugų teikėjų atsakomybės sąlygos ir ribos Europos Sąjungoje buvo harmonizuotos Europos Parlamento ir Tarybos Direktyva 2000/31/EB „Dėl kai kurių informacinės visuomenės paslaugų, ypač elektroninės komercijos, teisinių aspektų vidaus rinkoje" (Elektroninės komercijos Direktyva). Direktyva numato visišką ryšio (kanalo) teikėjo atleidimą nuo atsakomybės. Interneto prieigos teikėjas būtent ir yra priskiriamas ryšio (kanalo) teikėjui[83], taigi šiuo atveju šis be išlygų yra atleidžiamas nuo bet kokios galimos atsakomybės. Kita vertus prieglobos paslaugų teikėjas yra atleidžiamas nuo atsakomybės tik tol, kol nežino apie pažeidimą, tačiau jeigu jam yra žinoma apie talpinamą turinį, pažeidžiantį intelektinės nuosavybės ar kitas

[81] Europos Teisingumo Teismo sprendimas byloje C-70/10, *supra* note 7.

[82] Schellekens, M. *liability of internet intermediaries:aslippery slope? SCRIPTed, Volume 8, Issue 2, Tilburg Insitute for Law, Technology and Society*. Netherlands, 2011. 156-161.

[83] Order of the Court (Eighth Chamber) of 19 February 2009 (reference for a preliminary ruling from the Oberster Gerichtshof (Austria)): *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v Tele2 Telecommunication GmbH*, Case C-557/07, [2009] C 113/28.

teises, šis privalo jį tučtuojau pašalinti arba uždrausti prieigą prie tokio turinio. To nepadarius prieglobos paslaugų teikėjui iškyla grėsmė prarasti savo taip vadinamą „neliečiamybę“.[84]

Prieš tęsiant atsakomybės ribų nustatymo problematikos nagrinėjimą reikėtų trumpam grįžti ir pažiūrėti, kas yra interneto paslaugų teikėjas. Pagal Europos Teisingumo Teismo praktiką, terminas „tarpininkai“ gali būti suprantamas kaip elektroninių ryšių tinklų ir paslaugų operatoriai, prieigos prie telekomunikacijų tiklų teikėjai bei duomenų saugojimo paslaugų teikėjai ir t.t.[85]. Pagal Lietuvos Respublikos autorių teisių ir gretutinių teisių įstatymą tarpininku laikomas fizinis arba juridinis asmuo, įskaitant Lietuvos Respublikoje įregistruotus užsienio juridinio asmens filialą ar atstovybę, teikiantis elektroninių ryšių tinklais paslaugas, kurias sudaro trečiųjų asmenų pateiktos informacijos perdavimas elektroninių ryšių tinklais arba galimybės naudotis elektroninių ryšių tinklais suteikimas ir (arba) pateiktos informacijos saugojimas.[86]

Kaip jau buvo minėta prieš tai, interneto tarpininkai nėra atsakingi už pažeidimus išskyrus atvejus kai jie:

a) patys inicijuoja ryšį;
b) atrenka ryšio adresatą;
c) parenka ar keičia informaciją konkretaus ryšio metu (t.y. perduodamą informaciją);
d) žino apie jų tinklapiuose, tinkluose ar serveriuose esantį turinį, kuris pažeidžia kitų asmenų teises ir iš prigimties yra neteisėtas, įskaitant autorių teises pažeidžiančias kūrinių kopijas bei nuorodas.[87]

Taigi interneto paslaugų teikėjų atsakomybės nustatymo pareiga yra pagrįsta jų kaltės egzistavimu (ketinimu ar dideliu neatsargumu). Nors bendra pareiga vykdyti interneto turinio „monitoringą“ nėra įtvirtinta Elektroninės komercijos direktyvoje[88], tačiau interneto tarpininkai gali būti prašomi kontroliuoti turinį, susijusį su suinteresuotomis šalimis (pavyzdžiui, intelektinės nuosavybės teisių turėtojais) ir apie tokį turinį pranešti. Toks susitarimas buvo įgyvendintas Lietuvoje 2003 metais, kai memorandumą pasirašė IT įmonės bei intelektinės nuosavybės teisių turėtojų asociacija[89]. Nors ES valstybėse narėse tokie reikalavimai nėra reglamentuoti, tačiau

[84] Schellekens, M. *supra* note 82.
[85] Byla C-275/06, *Productores de Música de España (Promusicae) prieš Telefónica de España S.A.U.* [2008] ECR I-271.
[86] Lietuvos Respublikos autorių teisių ir gretutinių teisių įstatymas. *Valstybės žinios.* 1999, Nr. 50-1598.78 str. 2 d.
[87] Europos Parlamento ir Tarybos Direktyva 2000/31/EB, *supra* note 80.
[88] Byla C-275/06, *op. cit.*
[89] Janušauskaitė, K. *Regulation of the internet service providers' liability: does ir really work? Lithuanian legislation and court practice*. Research papers from the WIPO-WTO colloquium for teachers of intellectual property law. Geneve, 2011. 108-111.

intelektinės nuosavybės teisių turėtojų prašymai gali būti svarstomi atsižvelgiant į reikalavimus nepažeisti konfidencialios informacijos ir asmens duomenų neliečiamumo.[90]

Kalbant apie autorių teisių pažeidimus, reikia pastebėti, jog „teigiami“ įpareigojimai, kurie valstybėms narėms suteikia galimybę taikyti draudimus (įsakymus) yra išdėstyti 2001 m. gegužės 22 d. Europos Parlamento ir Tarybos Direktyvoje 2001/29/EB dėl autorių teisių ir gretutinių teisių informacinėje visuomenėje tam tikrų aspektų suderinimo 8 straipsnio 3 dalyje: „Valstybės narės užtikrina, kad teisių turėtojai turėtų galimybes prašyti teismo draudimo tarpininkams, kurių paslaugomis tretieji asmenys naudojasi autorių teisėms ar gretutinėms teisėms pažeisti.“[91]

Taip pat, pasak dr. K. Janušauskaitės, reikėtų pastebėti, kad skirtingose šalyse praktika susijusi su interneto paslaugų teikėjų atsakomybe, ypač su draudimų taikymais, gali skirtis. Šiuo klausimu taip pat svarbų vaidmenį vaidina Europos Teisingumo Teismo praktika. *L'Oréal* v. *eBay* byloje[92] buvo priimtas sprendimas dėl internetinių parduotuvių-aukcionų administratorių atsakomybės dėl vartotojų padaromų prekių ženklų pažeidimų ir galimų draudimų taikymo tokiems administratoriams. Taip pat buvo paminėtas poreikis tokiais atvejais didinti tarpininkų atsakomybę.[93]

Minėtoje byloje teismas konstatavo, kad internetinio aukciono administratorius aktyviai dalyvavo tinklapio veikloje, žinojo ir teikė informaciją apie pardavimų pasiūlymus. Teismas priėmė tokį sprendimą, kadangi administratorius teikė pagalbą optimizuodamas ir pateikdamas konkrečius pasiūlymus bei juos reklamuodamas, taigi akivaizdžiai vykdė aktyvius veiksmus. Kai tarpininkas vykdo aktyvius veiksmus, tokius kaip šioje byloje, šis negali tikėtis visiško atleidimo nuo atsakomybės, kurį garantuoja Europos Sąjungos teisės aktai elektroninių ryšių paslaugų teikėjams, tokiems, kaip internetinių parduotuvių administratoriams, atsižvelgiant į Elektroninės komercijos direktyvos 14 straipsnį.[94] Negana to, Europos Teisingumo teismas pasisakė, kad Europos Sąjungos teisė reikalauja iš valstybių narių užtikrinti, kad nacionaliniai teismai būtų pajėgūs įpareigoti tinklų operatorius, administratorius imtis efektyvių, proporcingų ir atgrąsančių priemonių užkirsti kelią tokiems pažeidimams.[95]

Elektroninės komercijos direktyva, kaip jau minėta, išskiria atvejus, kada interneto tarpininkai vis tik gali būti atsakingi už trečiųjų asmenų talpinamą informaciją, bet taip pat paminėtina, jog priverstinis kontrolės vykdymas nėra galimas..

[90] Janušauskaitė, K. *supra* note 89.
[91] 2001 m. gegužės 22d. Europos Parlamento ir Tarybos Direktyva 2001/29/EB dėl autorių teisių ir gretutinių teisių informacinėje visuomenėje tam tikrų aspektų suderinimo. [2001], OL L0029.
[92] Byla C-324/09, *L'Oréal* v. *eBay* [2011] ECJ,
[93] Janušauskaitė, K. *op. cit.*
[94] *Ibid*.
[95] Byla C-324/09, *supra* note 92.

Savanoriškas kontrolės vykdymas (monitoringas):

Interneto tarpininkas gali vykdyti stebėjimą (monitoringą) savanoriškai. Taip pat, jis tai gali daryti teikdamas paslaugas vartotojams ar valdžios prašymu. Kaip pavyzdį galima paminėti pirmoje darbo dalyje minėtą *Cleanfeed* filtravimo sistemą. Iš pradžių šią sistemą naudojo tik vienas interneto paslaugų teikėjas, tačiau įsikišus vyriausybei, šią sistemą pradėjo naudoti ir kiti Didžiosios Britanijos interneto paslaugų teikėjai. „Monitoringo“, stebėjimo veikla, pradėta savanoriškai, nebūtinai tokia ir išliks. Kitaip tariant nebūtinai tokia veikla liks be įsipareigojimų. Interneto paslaugų teikėjas, kuris inkorporuoja tam tikrą stebėjimo, filtravimo formą į sutartis su vartotojais, pavyzdžiui, įsipareigoja filtruoti turinį tam, kad būtų sudaroma „draugiška“, morali interneto aplinka, tai tokio filtravimo nevykdymas gali sąlygoti sutarties bei vartotojų teisių pažeidimų atsiradimą. Jeigu tokį savo pasižadėjimą interneto tarpininkas reklamuoja, tai toks pasižadėjimas gali virsti teisiniu įsipareigojimu vartotojams. Apskritai savanoriškas kontrolės vykdymas yra įtvirtintas elektroninės komercijos direktyvoje. [96]

Interneto paslaugų teikėjų atsakomybės ribas nustato elektroninės komercijos direktyva, kurioje išskiriamas žinojimo apie neteisėtą veiklą reikalavimas. Įdomu tai, kad redaktoriams bei leidėjams daugelyje šalių yra taikomi gerokai griežtesni apribojimai. Nors iš pirmo žvilgsnio interneto paslaugų teikėjo ir redaktoriaus ar leidėjo veiklos kardinaliai skiriasi, tačiau praktikoje yra kilę neaiškumų. Tokios situacijos pavyzdys būtų JAV byla *Stratton Oakmont v Prodigy*[97]. Šioje byloje paslaugų teikėjas *Prodigy* sukūrė savo vartotojams tam tikras turinio taisykles, dėl ko JAV aukščiausiasis teismas nusprendė, kad *Prodigy* vykdė redaktoriaus funkcijas ir dėl to yra atsakingas už talpinamą turinį.[98]

Stebėjimas pagrįstas žinojimo sąlyga

Vokietijoje federalinis teismas interneto paslaugų teikėjui nustatė pareigą vykdyti „monitoringą“ dėl žalingo turinio vaikų atžvilgiu. Teismas nusprendė, kad toks reikalavimas yra atitinkantis Direktyvos nuostatas, interneto paslaugų teikėjas yra įpareigojamas po to kai, sužino apie tokį turinį. [99] Stebėjimo („monitoringo“) prievolė *eBay* šiuo sprendimu buvo gana plati. Tai yra, *eBay* turėjo ne tik stebėti, kad tas pats turinio tiekėjas nepateiktų tokio paties žalingo turinio, tačiau taip pat turėjo stebėti, ar kiti turinio tiekėjai nepateikia tokio pačio turinio. Be to *eBay* buvo

[96] Schellekens, M. *supra* note 82.
[97] Supreme Court of New York, case *Stratton Oakmont, Inc. v Prodigy Services Co*. [1995] WL 323710 (NY Sup Ct 1995).
[98] Schellekens, M. *op. cit.*
[99] BGH, *Urteil v 12.07.2007, Az. I ZR 18/04.*

įpareigotas stebėti, ar tas pats turinio tiekėjas neįkėlė panašaus pobūdžio turinio.[100] Kitaip tariant, toks teismo įpareigojimas buvo gana plačios apimties.

Stebėjimas pagrįstas draudimu

Kaip jau minėta prieš tai, tiek 2001 m. gegužės 22 d. Europos Parlamento ir Tarybos Direktyva 2001/29/EC „Dėl autorių teisių ir gretutinių teisių informacinėje visuomenėje tam tikrų aspektų suderinimo“, tiek ir nacionaliniai autorių teisių apsaugą reglamentuojantys teisės aktai numato tam tikrus draudimus interneto paslaugų teikėjams. Tačiau Direktyva nenustato tokių draudimų turinio, taigi lieka daug erdvės interpretavimui. *SABAM v. Tiscali (Scarlet)* byla yra geras to pavyzdys. Briuselio apeliacinis teismas pateikė du klausimus Europos Teisingumo Teismui. Pirmasis buvo ar esamas europinis reglamentavimas (Direktyvos bei Europos pagrindinių žmogaus laisvių ir teisių konvencija) numato galimybę nacionaliniams teismams įsakyti interneto paslaugų teikėjui filtruoti visus elektroninius perdavimus (komunikacijas) kurie vykdomi konkretaus paslaugų teikėjo paslaugų apimtyje. Konkrečiai filtruoti visus perdavimus, vykstančius *peer-to-peer* programa turint tikslą nustatyti, kuriuose informacijos paketuose yra perduodami darbai, į kuriuos teises turi tretieji asmenys (kitaip tariant nustatyti autorių teisių pažeidimus) ir tokius perdavimus sustabdyti. Jei į šį klausimą Europos Teisingumo Teismas atsakytų teigiamai, tada iškyla kitas klausimas, ar Direktyva reikalauja, kad nacionaliniai teismai taikytų proporcingumo principą kai iškyla klausimas dėl tokių priemonių efektyvumo vertinimo.

Šiuo atveju aiškiai matoma, kad teisių turėtojas neprašo draudimo konkretaus pažeidimo atveju (pavyzdžiui pranešti tinklapio administratoriui apie tai, kad tinklapyje neteisėtai talpinamas autorinis darbas), tačiau yra prašoma draudimo apsaugoti jo darbus apimant nekonkretintą pažeidimą ir galimus ateities pažeidimus ir tikimasi, kad paslaugų teikėjas imsis stebėti, kad konkretus turinys – autorinis darbas – nebūtų neteisėtai perduodamas.[101] Šiuo atveju yra prašoma labai plataus filtravimo, arba kaip tik konkretaus saugomo turinio stebėjimo. Kaip bus matyti šios bylos analizėje (paskutiniame darbo skyriuje) toks prašymas yra per platus, ir akivaizdu, kad žymiai siauresnės apimties filtravimo įpareigojimai gali būti taikomi. Pavyzdžiui, Prancūzijos teismas nusprendė interneto paslaugų teikėjui skirti pareigą neleisti konkrečiam turiniui vėl atsirasti internete (žinoma tik per konkretaus paslaugų teikėjo tinklą) dvejų metų laikotarpyje.[102]

Įdomu yra tai, kad teismas norėdamas įpareigoti interneto tarpininką užkirsti kelią intelektinės nuosavybės teisių pažeidimui turi laikytis proporcingumo principo. Tais atvejais, kai

[100] Schellekens, M. *supra* note 82.
[101] *Ibid.*
[102] Cour d'Appel de Paris Pôle 1, Chambre 4 Arrêt du 26 Mars 2010, *Youtube v Magdane et Autres* [2010].

teismo yra prašoma įsakyti interneto tarpininkui taikyti filtravimo ar blokavimo sistemas tinklapiuose, kuriuose galimai yra pažeidžiamos intelektinės nuosavybės teisės, teisių turėtojai iš esmės tokį prašymą argumentuoja tuo, kad reikia sustiprinti intelektinės nuosavybės apsaugą. Paminėtinos pagrindinės nuostatos, kuriomis dažniausiai ir remiasi filtravimo ir blokavimo taikymo šalininkai:[103]

- pagal Europos Parlamento ir Tarybos Direktyvos 2004/48 3 straipsnį valstybės narės „privalo nustatyti priemones, procedūras bei teisių gynimo priemones tam, kad būtų užtikrinta intelektinės nuosavybės teisių apsauga...".
- tos pačios Direktyvos 11 straipsnis sukuria prievolę valstybei narei prižiūrėti, kad „teisių turėtojai turėtų galimybę prašyti teismo draudimo tarpininkams, kurių paslaugomis naudojasi tretieji asmenys, pažeisdami intelektinės nuosavybės teises".
- Europos Parlamento ir Tarybos Direktyva 2000/31 (elektroninės komercijos direktyva) 14 straipsnyje dėl prieglobos paslaugų nustato „galimybę valstybėms narėms nusistatyti procedūras, reguliuojančias neteisėto turinio pašalinimą arba prieigos panaikinimą".
- Tos pačios direktyvos 18 straipsnis nustato pareigą valstybės narėms užtikrinti, kad nacionalinių teismų procesas „leistų greitai imtis priemonių, įskaitant laikinųjų apsaugos priemonių, skirtų nutraukti bet kokį įtariamą pažeidimą bei užkirsti kelią bet kokiam interesų konfliktui".[104]

Tačiau tuo pačiu metu šios direktyvos diktuoja svarbius apribojimus draudimų, kuriuos iš tiesų gali taikyti teismai, apimčiai. Pavyzdžiui, pagal Direktyvos 2004/48 3 straipsnį „Priemonės, procedūros ir teisių gynimo būdai (valstybių narių), turi būti teisingi ir negali būti bereikalingai komplikuoti ir brangūs, ar taikomi per nepagrįstai ilgą laiko tarpą." To paties straipsnio antroje dalyje teigiama, kad taip pat priemonės turi būti „taikomos taip, kad nesukurtų kliūčių teisėtai prekybai".

Kitaip tariant, kaip buvo minėta, nors Direktyva reikalauja, kad valstybės narės taikytų priemones efektyviai intelektinės nuosavybės apsaugai, tačiau tuo pačiu reikalauja, kad nebūtų pažeistas proporcingumo principas.

Proporcingumo reikalavimas, kaip bendra taisyklė, yra reikalingas tam, kad nebūtų pažeidžiamos pagrindinės teisės ir laisvės, o ypač informacijos laisvė. Kaip yra išdėstyta Europos Pagrindinių žmogaus teisių ir laisvių konvencijoje, 10 straipsnyje, informacijos laisvės apribojimai gali būti toleruojami tik konkrečiose situacijose, tuomet, kai jie reikalingi „Demokratinėje

[103] Neri, A. *Ordering intermediaries to implement filtering mechanisms: a controversial measure with dreadful consequences.* France, 2011. 2-5.
[104] *Ibid.*

visuomenėje“. Kaip dažnai pabrėžia Europos Žmogaus Teisių Teismas, minėti apribojimai turi būti „įtikinami“ kaip atsakas į „neatidėliotiną visuomenės poreikį“[105] ir taip pat „pagrįstai proporcingi siekiamiems teisėtiems tikslams“[106]

Prieš tai minėtos direktyvos 2004/48 11 straipsnis, leidžiantis taikyti draudimus arba, kitaip tariant, įsakymus paslaugų teikėjams, iš esmės turėtų būti skaitomas kartu su to paties straipsnio pirmu sakiniu, kuriame pasakyta: „Valstybės narės užtikrina, kad tais atvejais, kai teismo sprendimu yra nustatytas intelektinės nuosavybės teisių pažeidimas, institucijos gali taikyti draudimus prieš pažeidėją, turint tikslą nutraukti pažeidimą“. Tai reiškia, kad draudimas (įsakymas) gali būti taikomas tik prieš pažeidėją, ir tik po to kai teismo sprendimas, kuriame nustatytas pažeidimas yra priimtas, bet tik tam konkrečiam pažeidimui sustabdyti. Jeigu būtų vadovaujamasi tokia taisykle, kad konkretūs draudimai yra taikomi tik prieš pažeidėją konkrečiu atveju, tai bet koks platesnis interneto paslaugų teikėjų įpareigojimas būtų nelogiškas, tuo labiau, kad paslaugų teikėjas nėra pats atsakingas už padarytus pažeidimus naudojantis jo paslaugomis.[107]

Pagal 2004/48 direktyvos 2 straipsnio 3 dalį: „Ši direktyva neturi poveikio: a) Bendrijos nuostatoms, reglamentuojančioms materialinę intelektinės nuosavybės teisę, Direktyvai 95/46/EB, Direktyvai 1999/93/EB ar Direktyvai 2000/31/EB bendrai ir, ypač, Direktyvos 2000/31/EB 12-15 straipsniams.“[108]. Tačiau elektroninės komercijos Direktyvos (2000/31) nuostatos teigia, kad: „Valstybės narės nenustato teikėjams nei bendros prievolės teikiant 12, 13 ir 14 straipsnių reglamentuojamas paslaugas stebėti informaciją, kurią jie perduoda arba saugo, nei bendros prievolės aktyviai domėtis faktais arba aplinkybėmis, rodančiomis nelegalią veiklą.“[109] Siekis užtikrinti intelektinės nuosavybės teisių apsaugą negali tapti pateisinimu įsakyti taikyti filtravimo ir blokavimo priemones, kadangi tokiu atveju būtų vykdomas per platus bendras filtravimas.

Labai svarbu atkreipti dėmesį į Direktyvos 2000/31 įžangos 47 punktą, kuriame teigiama, kad: „Valstybėms narėms draudžiama paslaugų teikėjams nustatyti priežiūros prievolę tik bendro pobūdžio prievolių atžvilgiu; tai netaikoma priežiūros prievolėms konkrečiu atveju ir ypač neturi įtakos nacionalinės valdžios institucijų sprendimams, išleistiems vadovaujantis nacionaliniais įstatymais.“[110] Atsižvelgiant į tai, gana painų sąvokos „konkrečiu atveju“ aiškinimą pateikė Europos

[105] Didžiosios kolegijos sprendimas iš esmės: *Fressoz and Roire v. France*, no. 29183/95, ECHR 1999-I.
[106] Didžiosios kolegijos sprendimas iš esmės: *Lehideux and Isorni v. France*, no. 92, ECHR 1998-VII; Kolegijos sprendimas iš esmės: *Du Roy and Malaurie v. France*, no. 34000/96, ECHR 2000-X.
[107] Neri, A. *supra* note 103.
[108] 2004 m. balandžio 29 d. Europos Parlamento ir Tarybos Direktyva 2004/48/EB dėl intelektinės nuosavybės teisių gynimo. [2004], OL L157/45., 2str, 3d.
[109] Europos parlamento ir tarybos direktyva 2000/31/EB, *supra* note 80, 15 str.
[110] Europos parlamento ir tarybos direktyva 2000/31/EB, *supra* note 80, įžanga, 47 punktas.

Komisija 2003 metais savo pranešime Europos Parlamentui, Tarybai bei Ekonominiam ir Socialiniam komitetui.[111]

Komisija pranešime išryškino tai, kad valstybės narės gali reikalauti, kad interneto paslaugų teikėjai imtųsi stebėjimo (monitoringo) tik „išskirtiniais, pavieniais ir aiškiai apibrėžtais atvejais“[112]. Pagal tokį aiškinimą, Direktyvoje numatytas įpareigojimas saugojimo paslaugų teikėjams (iš esmės interneto paslaugų teikėjams, kurie patys netalpina informacijos) pašalinti arba padaryti neprieinamą informaciją, kuri, suinteresuotos šalies teigimu yra neteisėta arba neteisėtai talpinama, turi būti siejamas su tiksliai nustatytu faktu. Tokiu atveju reikalavimas pašalinti ar padaryti neprieinamą informaciją turi būti siejamas su konkrečiu failu – duomeniu, kuris talpina neteisėtai atgamintą kūrinį ir, kuris konkretaus vartotojo yra patalpintas internete, tačiau bet koks vėlesnis kūrinio atgaminimas jau neįeina į šį konkretų individualų atvejį.[113] Taigi iš esmės, jeigu neteisėtai paskelbtas kurinys yra pašalinamas, tačiau kitas vartotojas jį jau yra atgaminęs ir paskelbęs internete savo iniciatyva, šis atgaminimas ir paskelbimas jau neįeina į konkretų nurodytą atvejį ir toks pažeidimas negali būti tuo pačiu nutrauktas.

Atsižvelgiant į paskutinę teismų praktiką bei priimtus sprendimus, pastaruoju metu teisių turėtojai pradėjo žiūrėti į interneto paslaugų teikėjus kaip į pagalbininkus. Kadangi pagal teisinį reglamentavimą interneto paslaugų teikėjai negali būti priversti vykdyti pastovų filtravimą ir stebėjimą, tai intelektinės nuosavybės teisių turėtojai pradėjo derėtis su interneto tarpininkais ir tikėtis iš pastarųjų savanoriško kai kurio turinio filtravimo bei blokavimo. Vienas iš tokios savanoriškos iniciatyvos pavyzdžių galėtų būti kai kurių tarpininkų taikoma įspėjimų sistema. Šiuo atveju, jeigu interneto paslaugų teikėjas gauna pranešimą arba pats pastebi intelektinės nuosavybės teisių pažeidimą, savo iniciatyva išsiunčia konkrečiam vartotojui įspėjimą, kad iš vartotojo pusės buvo pasinaudota teikiama paslauga padaryti pažeidimui. Griežtesnių priemonių imamasi po trijų tokių pranešimų. Minimos griežtesnės priemonės apsiriboja interneto prieigos apribojimais arba netgi interneto paslaugos sustabdymu. Bet kokiu atveju tokių priemonių taikymas yra interneto paslaugų teikėjo diskrecija.

Tačiau jau yra buvę bandymų tokią įspėjimų sistemą padaryti privalomą. Pirmasis toks bandymas buvo Prancūzijoje kai buvo priimtas ‘*Loi favorisant la diffusion et la protection de la*

[111] Neri, A. *supra* note 103.
[112] Commission of European Communities. *First Report on the application of Directive 2000/31/EC of the European Parliament and of the Council no.* COM(2003) 702 final. [interaktyvus] Brussels 2003 § 4.6. [žiūrėta 2012-10-16]. < http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2003:0702:FIN:EN:PDF>.
[113] Neri, A. *op. cit.*

creation sur Internet'[114] aktas. Nauja šiame akte buvo tai, kad juo buvo siūloma ne tik nutraukti interneto paslaugų teikimą kaip bausmę pažeidėjams, bet ir įsteigti nepriklausomą instituciją, kurios pagrindinis uždavinys būtų siųsti pranešimus pažeidėjams ir vėliau nuspręsti, ar tokiems pažeidėjams reikia nutraukti interneto paslaugų teikimą. Po ilgų diskusijų ir Prancūzijos Konstitucinio teismo verdikto, buvo priimtas pakoreguotas aktas. Pagal jį buvo įsteigta nepriklausoma institucija HADOPI, kurios vykdomos procedūros buvo išskirtos į dvi dalis:

- *Pirma, įspėjimų procedūra.* Institucija nagrinėja teisių turėtojų (subjektų) skundus dėl galimų pažeidimų ir pažeidėjų ir išsiuntinėja įspėjimus;
- *Antra, paslaugų nutraukimo procedūra*. Sprendimą nutraukti interneto paslaugų teikimą konkrečiam pažeidėjui gali priimti tik teismas, tačiau HADOPI suteikiama teisė turėti vartotojų, kuriems nutrauktas paslaugos teikimas dėl padarytų pažeidimų sąrašą turint tikslą, kad tokiems vartotojams paslaugų neteiktų ir kiti interneto paslaugų teikėjai.[115]

Prancūzijos pavyzdžiu taip pat pasekė kitos šalys. Pavyzdžiui Korėjoje 2009 metais priimtas aktas leidžia Korėjos Autorių teisių komisijai įsakyti vietiniams interneto paslaugų teikėjams nutraukti paslaugų teikimą vartotojams už pakartotinį autorių teisių pažeidimą.[116]

Naujesnis pavyzdys yra Didžiosios Britanijos Skaitmeninės ekonomikos įstatymas.[117] Kaip ir prieš tai minėti aktai, šis aktas taip pat nustato interneto paslaugų teikėjams tam tikrus bendrus įpareigojimus, pagal kuriuos šie privalo siųsti pranešimus tiems vartotojams, kurių IP adresai yra susiję su intelektinės nuosavybės pažeidimais. Vėliau atskira institucija svarsto, ar tokiems pažeidėjams reikia taikyti tam tikras technines priemones, tokias kaip filtravimas ar net interneto paslaugų nutraukimas.[118] Taip pat pastebėtina, kad po teisinės įstatymo peržiūros D. Britanijos didžiausio interneto paslaugų teikėjo prašymu, Aukščiausiasis D. Britanijos teisingumo teismas nustatė, kad jokios įstatyme numatytos priemonės ir įpareigojimai nepažeidžia proporcingumo principo ir yra teisėti.[119] Čia paminėti atvejai, kai interneto paslaugų teikėjai yra įpareigojami taikyti

---

[114] Loi nº 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet (Law No. 2009-669 of June 12, 2009 promoting the Dissemination and Protection of Creation on the Internet), [interaktyvus]. [žiūrėta 2012-11-02]. <http://www.wipo.int/wipolex/en/details.jsp?id=5613>.

[115] Giannopoulou, A. *Copyright enforcement measures: the role of the ISPs and the respect of the principle of proportionality.* European Journal for Law and Technology, Vol. 3, No. 1, 2012. [interaktyvus] [žiūrėta 2012-11-14]. < http://ejlt.org/article/viewArticle/122/204>.

[116] Korėjos autorių teisių įstatymas [interaktyvus]. [žiūrėta 2012-11-10] <http://www.moleg.go.kr/english/korLawEng?pstSeq=52683&pageIndex=23>.

[117] Didžiosios Britanijos skaitmeninės ekonomikos įstatymas [interaktyvus]. [žiūrėta 2012-11-10] < http://www.legislation.gov.uk/ukpga/2010/24/contents?view=plain>.

[118] *Ibid.,* 124G str.

[119] The High Court of Justice Queen's Bench Division Administrative Court, case *BT & Talk Talk v The Secretary of State for BIS,* No. CO/7354/2010, [2011] EWHC 1021 (admin).

įspėjimų sistemą, tačiau daugelyje valstybių tai vis tiek yra susitarimo reikalas tarp tarpininko ir teisių turėtojų ar jiems atstovaujančių institucijų.

Žinoma, daugelis interneto paslaugų teikėjų prieštarauja tokiems prašymams savanoriškai vykdyti stebėjimą ir netgi atskleisti vartotojų duomenis be teismo sprendimo. Dėl tokių nesutarimų teisių turėtojai mėgino patraukti atsakomybėn paslaugų teikėjus. Tokios bylos kaip *Scarlet extended v Societé Belge des Auteurs* bei kitos bus aptariamos paskutiniame darbo skyriuje.

Šnekant apie interneto paslaugų teikėjų atsakomybę ir įpareigojimus reikia trumpai paminėti ir europinio lygmens teisės aktą, kuris sukėlė daug diskusijų. Tai prekybos susitarimas dėl kovos su klastojimu – ACTA (ang. *Anti Counterfeiting Trade Agreement*). Neaptarinėjant šio akto smulkiau tikslinga būtų atkreipti dėmesį į interneto paslaugų teikėjų vaidmenį.

Visų pirma ACTA numatė galimybę prašyti įsakymo, kuriuo būtų galima išreikalauti iš interneto paslaugų teikėjo informacijos, susijusios su konkretaus vartotojo, kurio paskyra galimai panaudota padaryti pažeidimą, tapatybe. Pagal ACTA, toks įsakymas turėtų būti išduotas „kompetentingos institucijos“, ir šiuo atveju tai nebūtinai teismas.[120]

Antra, ACTA buvo išdėstytas reikalavimas, kad būtų imamasi „efektyvių veiksmų“ prieš pažeidimus elektroninėje erdvėje, įskaitant priemones, skirtas sustabdyti ir užkirsti kelią pažeidimams, įskaitant draudimus (įsakymus). Tai taikyta interneto paslaugų teikėjams.[121]

Trečia, ACTA išdėstytas reikalavimas šį susitarimą pasirašiusioms šalims, kad šios „skatintų verslo bendruomenės bendradarbiavimą“ kovoje su pažeidimais, konkrečiai turint omenyje bendradarbiavimą tarp paslaugų teikėjų bei teisių turėtojų. Toks reikalavimas buvo išdėstytas pirmame ACTA teksto variante taip bandant padaryti privalomą jau minėtą savanorišką filtravimą, o konkrečiai – aptartą trijų įspėjimų metodą. Tačiau po Europos Parlamento neigiamos pozicijos šiuo klausimu išdėstymo toks įpareigojimas buvo panaikintas.[122]

Šnekant apie interneto paslaugų teikėjų vaidmenį neteisėto intelektinės nuosavybės platinimo atvejais reikia paminėti *peer-to-peer* pagrindu daromus pažeidimus.

Visų pirma apie *peer-to-peer* (P2P) duomenų keitimosi pobūdį. P2P programinė įranga leidžia vartotojams prisijungti prie duomenų dalijimosi tinklo, padaro duomenis prieinamus bei taip pat aptinka kitus duomenis, kurie yra prieinami parsisiuntimui. Nepaisant to, kad P2P tinklai iš esmės yra decentralizuoti, tačiau trečioji šalis vis vien atlieka tam tikrą vaidmenį, nors ir nebūdama griežtai šio tinklo dalimi. Tokių šalių pavyzdžiai yra programinės įrangos kūrėjai bei duomenų

[120] Baraliuc, I. Depreeuw, S. Gutwirth, S. *Copyright enforcement in Europe after ACTA: what now?*. Netherlands journal of legal philosophy,Vol. 41/2, 99-104, 2012. 3-4.
[121] *Ibid.*
[122] *Ibid.*

indeksavimo ir paieškos tinklapiai.[123] Šiuo atveju tarpininkai yra būtent prieigos suteikėjai, tinklapiai, kuriuose arba galima talpinti duomenis (šiuo atveju nereikia P2P technologijos) arba kurie suranda duomenis, kurių ieško vartotojas ir leidžia jam tuos duomenis atsisiųsti P2P programinės įrangos pagalba.

Duomenų keitimosi veikla P2P pagrindu nebūtinai yra neteisėta. Pavyzdžiui, kai asmenys savanoriškai dalijasi savo intelektinės veiklos rezultatais arba kai kūrėjai naudoja atvirąsias licencijas. Tačiau kai duomenimis yra dalijamasi neturint teisių turėtojo leidimo, tikėtina, kad duomenimis besikeičiantys asmenys pažeidžia autorių teises.[124]

Įdomus faktas yra tai, kad kai kuriose Europos šalyse (pvz. Šveicarija, Nyderlandai) duomenų parsisiuntimas nėra neteisėtas, tačiau jų įkėlimas jau yra laikomas neteisėtu. Tokiu atveju pats parsisiuntimas radus duomenis internete nėra neteisėtas, tačiau tokių duomenų įkėlimas užtraukia atsakomybę.

Taip pat pastebėtina, kad neturtinės teisės gali būti pažeidžiamos ir tais atvejais kada yra pašalinama arba kaip nors pakeičiama informacija apie kūrinio autorių. Tokiai informacijai priskiriama informacija apie patį autorių, ar gretutinių teisių subjektą bei kūrinio naudojimo sąlygas. Tokios informacijos panaikinimas ar pakeitimas gali klaidinti vartotoją ir sudaryti galimybę neteisėtoms veikoms.[125]

4. INTERNETO PASLAUGŲ TEIKĖJŲ VAIDMENS REGLAMENTAVIMAS LIETUVOJE

Pagal Europos Parlamento ir Tarybos direktyvą 2004/48 (Intelektinės nuosavybės teisių įgyvendinimo Direktyva) nacionaliniams teismams yra suteikiama teisė nustatyti interneto paslaugų teikėjams įpareigojimus (tiek laikinus, tiek ir ilgalaikius). Pagal minėtą Direktyvą laikini įpareigojimai gali būti nustatomi tiems interneto tarpininkams, kurių paslaugomis naudojasi trečioji šalis (vartotojas), kuri pažeidžia intelektinės nuosavybės teises. Konkrečiai tai atvejai, kai trečiosios šalies veiksmai pažeidžia autorių ar gretutines teises, kurios aptartos direktyvoje dėl autorių teisių ir gretutinių teisių informacinėje visuomenėje tam tikrų aspektų suderinimo.

Nuostatos, susijusios su įpareigojimų interneto paslaugų teikėjams nustatymu dar prieš įgyvendinant direktyvą 2004/48, jau buvo perkeltos iš direktyvos dėl autorių teisių ir gretutinių

[123] Muir, A. *Online copyright enforcement by internet service providers.* Journal of Information Science XX (X) pp. 1-15. Loughborough University, UK, 2012.
[124] *Ibid.*
[125] Kiškis, M. *supra* note 7, p. 66.

teisių informacinėje visuomenėje tam tikrų aspektų suderinimo į Lietuvos Respublikos autorių teisių ir gretutinių teisių įstatymą.

Lietuvos Respublikos Autorių teisių ir gretutinių teisių įstatymo 78 straipsnio 1 dalyje nustatyta, kad autorių teisių, gretutinių teisių ir *sui generis* teisių (pvz. Duomenų bazių savininkų teisės) subjektai, gindami savo teises, turi teisę kreiptis į teismą ir reikalauti uždrausti tarpininkui teikti elektroninių ryšių tinklais paslaugas tretiesiems asmenims, kurie šiomis paslaugomis naudojasi pažeisdami autorių teises, gretutines teises ar *sui generis* teises.[126] Tokios pačios nuostatos yra įtrauktos ir į Lietuvos Respublikos pramoninę nuosavybę reglamentuojančius teisės aktus[127].

Lietuvoje teismai gali taikyti trijų tipų ilgalaikius įpareigojimus (draudimus) tarpininkams, kurie teikia paslaugas tretiesiems asmenims, pažeidžiantiems intelektinės nuosavybės teises:

- informacijos, susijusios su teisių pažeidimu, perdavimo sustabdymas;
- tokios informacijos pašalinimas, jeigu tarpininkas techniškai gali tai atlikti;
- prieigos prie autorių teises, gretutines teises ar *sui generis* teises pažeidžiančios informacijos panaikinimą, kaip tai numatoma nacionaliniuose autorių teisių įstatymuose.[128]

Be to, teismai gali nurodyti laikinuosius įpareigojimus (tarsi laikinąsias apsaugos priemones) siekdami minėtų tikslų. Draudimas (įpareigojimai) gali būti taikomi ir suinteresuotos šalies prašymu, kuri turi pateikti bet kokią žinomą informaciją (įrodymus) apie tarpininko tinkle, tinklapiuose ar serveriuose esantį turinį, kuris pažeidžia suinteresuotos šalies teises. Taip pat: „Teismas turi teisę įpareigoti asmenį, kuris prašo taikyti laikinąsias apsaugos priemones, pateikti visus pagrįstai turimus įrodymus, galinčius pakankamai įtikinti, kad jis ar asmuo, kurio interesais prašoma taikyti laikinąsias apsaugos priemones, yra pagal šį Įstatymą saugomų teisių subjektas ar naudotojas ir kad pareiškėjo teisė pažeidžiama arba kad gresia toks pažeidimas.“[129]

Analizuojant nacionalinius teisės aktus, kuriuose nustatomi įpareigojimai (draudimai) tarpininkams, galima įžvelgti, kad norint įpareigojimus taikyti praktikoje galima susidurti su sunkumais dėl dviejų priežasčių. Pirma, susiduriama su sunkumais norint pateikti „pagrįstai turimus įrodymus“, susijusius su galimai pažeidžiančiu teises turiniu. Kadangi informacija tarpininkų serveriuose ar tinklapiuose gali būti talpinama tik laikinai, dėl to teisių turėtojai iš esmės turi turėti tam tikrą sistemą, pagal kurią galėtų reguliariai rinkti pažeidimų įrodymus, kas užima labai daug

[126] Lietuvos Respublikos Autorių teisių ir gretutinių teisių įstatymas, *supra* note 86, 78 str. 1 d.
[127] Lietuvos Respublikos patentų įstatymas. *Valstybės žinios.* 1994, Nr. 8-120, 41 str. 4 d.; Lietuvos Respublikos prekių ženklų įstatymas. *Valstybės žinios.* 2000, Nr. 92-2844, 50 str. 4 d.; Lietuvos Respublikos dizaino įstatymas. *Valstybės žinios.* 2002, Nr. 112-4980, 47 str. 4d.
[128] Lietuvos Respublikos Autorių teisių ir gretutinių teisių įstatymas, *supra* note 86, 78 str. 1 d.
[129] Lietuvos Respublikos Autorių teisių ir gretutinių teisių įstatymas, *supra* note 86, 81 str. 4 d.

laiko. Daroma prielaida, kad prašymas nustatyti įpareigojimus (draudimus) tarpininkams gali būti paduodamas teismui iš karto, kai tik teisių turėtojas surenka pakankamai informacijos apie teisių pažeidimą ir tą informaciją pateikia raštu (atspausdintą, kopijuotą ar kitaip atgamintą). [130]

Teisių turėtojams taip pat gali prireikti turimus įrodymus išsaugoti. Įrodymų saugojimo priemonės yra suderintos Europos Parlamento ir Tarybos Direktyvoje 2004/48[131] ir įgyvendintos Lietuvoje. Lietuvos Respublikos Autorių teisių ir gretutinių teisių įstatymo 81 str. 5 dalis numato: „Teismas asmens, pateikusio visus pagrįstai turimus ir jo reikalavimus pagrindžiančius įrodymus, kad buvo pažeistos arba gresia, kad bus pažeistos, jo pagal šį įstatymą saugomos teisės, prašymu gali taikyti su įtariamu pažeidimu susijusių įrodymų užtikrinimo priemones, tai yra:

1) išsamiai aprašyti pagal šį Įstatymą saugomas teises pažeidžiančių kūrinių, kitų saugomų teisių objektų kopijas ir prekes ir jas sulaikyti arba tik aprašyti;

2) areštuoti ir paimti pagal šį Įstatymą saugomas teises pažeidžiančias kūrinių ir kitų saugomų teisių objektų kopijas, prekes, o prireikus – medžiagas ir priemones, kurios naudojamos jų gamybai ir (arba) platinimui bei su jomis susijusius dokumentus;

3) taikyti kitas laikinąsias priemones, numatytas Civilinio proceso kodekse“[132].

Antra, dėl praktinių sunkumų renkant įrodymus, kurie savaime būtų pakankamai pagrįsti ir įtikintų teismą pažeidimo buvimu, yra labai sunku suformuoti nacionalinę teismų praktiką šiuo klausimu, tuo labiau, kai Lietuvoje šis klausimas yra labai mažai nagrinėtas.[133] Dėl tokios teismų praktikos stokos yra labai sunku numatyti, kaip nacionaliniai teismai vertintų informaciją bei įrodymus, susijusius su galimu pažeidimu. Taip pat reikėtų atsižvelgti į tai, kad įrodymų forma, pavyzdžiui, būtų atspausdinti elektroniniai laiškai ar *peer-to-peer* failų sąrašai ir panašiai. Nors teorija ir sako, kad elektroniniams dokumentams bei visiems santykiams elektroninėje erdvėje turi būti taikomas lygiavertiškumo principas (bet koks elektroninis dokumentas turi būti vertinamas tapačiai popieriniam dokumentui), tačiau nėra galima vienareikšmiškai nuspėti, koks teismų požiūris būtų į tokių įrodymų patikimumą.

[130] Janušauskaitė, K. *supra* note 89.
[131] 2004 m. balandžio 29 d. Europos Parlamento ir Tarybos Direktyva 2004/48/EB dėl intelektinės nuosavybės teisių gynimo. [2004], OL L157/45.
[132] Lietuvos Respublikos Autorių teisių ir gretutinių teisių įstatymas, *supra* note 86, 81 str. 5 d.
[133] Janušauskaitė, K. *op. cit.*

5. TEISMŲ PRAKTIKA REZONANCINĖS BYLOS

Scarlet prieš SABAM

Visų pirma reikėtų aptarti vieną naujausių ir, turbūt svarbiausią bylą Europoje, kurios baigtis galima sakyti nustatė praktikos gaires ir davė suprasti, jog intelektinės nuosavybės, o tiksliau, autorių teisių subjektai negali vienareikšmiškai reikalauti interneto paslaugų teikėjų filtruoti visą tinklą.

Ši byla yra *Scarlet (buvusi Tiscali) v. SABAM*[134]. Trumpai apibendrinant patį sprendimą ir jo motyvaciją reikia pasakyti, kad Europos Teisingumo Teismas pasisakė, jog plataus masto priemonių, kurios apima visišką interneto vartotojų veiksmų stebėjimą, taikymas bei P2P tinklapių, kurių pagalba autorių teisėmis saugomas turinys gali būti neteisėtai pasiekiamas, blokavimas neribotą laiką yra neproporcingos apsaugos priemonės. Taip pat teismas pabrėžė, jog intelektinės nuosavybės teisės nėra absoliučios, o turi būti derinamos su kitomis teisėmis, tokiomis kaip išraiškos laisvė bei teisė į privatumą.

Šioje byloje *Société d'Auteurs Belge – Belgische Auteurs Maatschappij* (Autorių, kompozitorių ir leidėjų sąjunga – SABAM) kreipėsi į teismą dėl to, kad Belgijos interneto paslaugų teikėjas (interneto prieigos teikėjas) *Scarlet* (buvęs *Tiscali*), manomai žinodamas leido savo tinklu *peer-to-peer* programinės įrangos pagalba siųstis SABAM saugomus autorių darbus. SABAM reikalavo interneto paslaugų teikėjui nustatyti įpareigojimus imtis aktyvių veiksmų, kad užkirstų kelią neteisėtam saugomo turinio platinimui ir keitimuisi tarp paslaugų teikėjo vartotojų.

Tribunal de Première Instance de Bruxelles (Briuselio pirmos instancijos teismas) priėmė sprendimą, kad Interneto paslaugų teikėjas turi taikyti filtravimo priemones, kad būtų užkirstas kelias intelektinės nuosavybės pažeidimams.

Byla pasiekė Europos Teisingumo Teismą ir nacionalinio teismo sprendimas buvo panaikintas. Nacionalinis Belgijos teismas iš esmės klausė Europos Teisingumo Teismo išvados, ar gali nacionalinis teismas įpareigoti interneto paslaugų teikėją įdiegti (pradėti naudoti) filtravimo sistemą, kuri įgalintų interneto paslaugų teikėją stebėti (vykdyti pastovų monitoring) visų vartotojų visas komunikacijas (perdavimus) neribotą laiką bei savo sąskaita, kaip prevencinę priemonę prieš intelektinės nuosavybės pažeidimus.

Europos Teisingumo teismo sprendimas susideda iš kelių dalių. Visų pirma, įpareigojimas interneto paslaugų teikėjui įdiegti tokią filtravimo sistemą, reikštų, kad šis visą laiką aktyviai

[134] Europos Teisingumo Teismo sprendimas byloje C-70/10, *supra* note 7.

stebėtų visą informaciją, susijusią su jo klientais – vartotojais, o tai yra uždrausta ES elektroninės komercijos direktyvos[135].

Antra, teismas taip pat vertino, ar toks interneto paslaugų teikėjo įpareigojimas neprieštarauja pagrindinėms žmogaus teisėms ir laisvėms. Šiuo klausimu teismas pripažino, kad intelektinės nuosavybės apsauga yra viena iš pagrindinių žmogaus teisių[136], tačiau ši teisė nėra neliečiama bei nėra absoliuti ir turi būti derinama su kitomis teisėmis ir laisvėmis. Šiuo atveju kitos aktualios teisės apima interneto paslaugų teikėjo laisvę vykdyti verslą[137], taip pat kaip ir interneto paslaugų teikėjo vartotojų teisė į asmens duomenų apsaugą bei laisvė teikti ir gauti informaciją.[138]

Teismas nusprendė, kad privalomas filtravimo sistemos diegimas būtų rimtas interneto paslaugų teikėjo teisės užsiimti verslu pažeidimas, kadangi interneto paslaugų teikėjas būtų priverstas įdiegti sudėtingą ir brangią kompiuterinę sistemą savo sąskaita. Be to tokios sistemos naudojimas reikštų, kad ši sistemiškai analizuotų informaciją, susijusią su vartotojais, įskaitant IP adresus, kurie yra asmeninė informacija ir saugomi kaip asmens duomenys. Dar vienas pažymėtinas tokios sistemos minusas yra tai, kad greičiausiai tokia sistema adekvačiai neatskirtų, kuri interneto paslaugų teikėjo tinkle skleidžiama informacija yra teisėta ir kuri ne, ir dėl to būtų blokuojami taip pat ir teisėti perdavimai.[139]

Europos Teisingumo Teismas nurodė, kad tarp minimų teisių nebuvo nustatytas lygiavertis balansas, todėl Belgijos teismo įsakymas *Scarlet* įdiegti filtravimo sistemą negali būti patvirtintas ir laikomas pagrįstu.

Šiuo sprendimu iš esmės teismas vadovavosi ir pritarė generalinio advokato pateiktai išvadai.[140] Genaralinis advokatas pasisakė, kad filtravimo įpareigojimas apribotų komunikacijų privatumo laisvę, asmens duomenų apsaugos teisę bei informacijos laisvės principą. Tiesa, generalinis advokatas pasisakė plačiau nei teismas, nurodydamas, kad toks įpareigojimas būtų galimas tik tokiu atveju, jeigu nacionalinė teisinė bazė tai nustatytų aiškiai, nedviprasmiškai ir konkrečiai numatytomis aplinkybėmis. Šiuo atveju tokio reglamentavimo nebuvo.

Sprendimas šioje byloje yra svarbus dėl kelių aspektų. Iš esmės šis sprendimas simbolizuoja tam tikrą "srovių" pasikeitimą, sietiną su autorių teisių (ir apskritai intelektinės nuosavybės) apsaugos ir įgyvendinimo absoliutizmo pabaiga ir vartotojų interesų bei teisių iškėlimu į dienos šviesą. Tačiau, šis sprendimas nėra aiškus tokios filtravimo sistemos, skirtos aptikti intelektinės

[135] Europos Parlamento ir Tarybos Direktyva 2000/31/EB, *supra* note 80.
[136] 2012 m. spalio 26 d. Europos Sąjungos Pagrindinių Teisių Chartija 2012/C 326/02. [2012]. 17 str. 2 d.
[137] *Ibid.*, 16 str.
[138] *Ibid.*, 8 str., 11 str.
[139] Daly, A. Farrand, B. *Scarlet v SABAM: evidence of an emerging backlash against corporate copyrights lobbies in Europe?* European University Institute – Department of Law, 2012. 2-4.
[140] Europos Teisingumo Teismo sprendimas byloje C-70/10, *supra* note 7.

nuosavybės pažeidimus, draudimas. Tiesą sakant, atrodo, kad kitokio pobūdžio filtravimo sistemos gali būti taikomos tol, kol atitinka reikalavimus, iškeltus Europos Teisingumo Teismo sprendime, bei tokius, apie kuriuos šnekėjo generalinis advokatas savo išvadoje, teikiamoje teismui. Šie reikalavimai apima proporcingumą, visų dalyvių teisių suderinimą, teisinį skaidrumą ir galbūt išlaidų, susijusių su filtravimo sistemos diegimu bei palaikymu, pasidalijimą tarp paslaugų teikėjo ir intelektinės nuosavybės teisių subjektų.[141]

Ši byla, galima sakyti, nurodė tai, kad intelektinės nuosavybės teisės nėra absoliučios ir visada turi būti atsižvelgiama į bendrą teisių balansą.

The Pirate Bay byla

Šnekant apie P2P pagrindu daromus pažeidimus ir juose dalyvaujančias trečias šalis reikia paminėti 2012 metų pradžioje Olandijos teismo priimtą sprendimą. Teismas, nepaisydamas pareiškimų, kad išraiškos laisvei yra iškilęs pavojus, savo sprendimu įpareigojo porą Olandijos interneto paslaugų teikėjų blokuoti tinklapį *The Pirate Bay*. Šis tinklapis yra vienas žinomiausių tinklapių, veikiančių paieškos P2P tinkle principu. *The Pirate Bay* tinklapio pagalba yra randami prieinami duomenys – failai ir P2P programinės įrangos pagalba šie duomenys yra atsisiunčiami tiesiai į vartotojo kompiuterį. Šio tinklapio pagalba daugiausiai yra daromi intelektinės nuosavybės pažeidimai, kadangi, kaip buvo minėta prieš tai, P2P tinklais dažnai atliekami intelektinės nuosavybės pažeidimai (kai intelektinės nuosavybės objektai perduodami šiais tinklais be autorių leidimo.)[142]

Olandijos antipiratinės organizacijos BREIN reikalavimu Hagos teismas nusprendė, kad du didžiausi Olandijos interneto paslaugų teikėjai turi blokuoti savo vartotojams prieigą prie žinomiausio pasaulyje *torrent* (P2P tipo failas) failų tinklapio. 2010 metais BREIN kreipėsi į teismą siekdama, kad būtų blokuojamas jau minėtas *torrent* tinklapis. Pirmasis Hagos teismo sprendimas buvo palankus interneto paslaugų teikėjams. Šis pasisakė, jog tinklapio padarymas neprieinamu visiems vartotojams yra per daug griežtas sprendimas. Tačiau BREIN nesusitaikė su tokiu sprendimu ir bylinėjosi toliau.

Teismas nustatė, jog maždaug 34,5 procentų abiejų interneto paslaugų teikėjų vartotojų naudojasi *The Pirate Bay* tinklapiu ir per jį neteisėtai dalijasi autorių teisių objektais. Teismas taip pat nurodė, kad nors ir *The Pirate Bay* blokavimas užkirs kelią vartotojams įgyvendinti savo teisėtus interesus (turima omenyje teisėtą dalinimasi duomenimis), tačiau atsižvelgiant į pažeidimų

[141] Daly, A. Farrand, B. *supra* note 139.
[142] *Dutch ISPs Ordered To Block The Pirate Bay.* [interaktyvus] 2012. [žiūrėta 2012-11-17]. <http://torrentfreak.com/dutch-isps-ordered-to-block-the-pirate-bay-120111/>.

mastus ir neteisėtos informacijos, prieinamos per šį tinklapį, kiekį yra aišku, kad bus apginta daugiau teisėtų interesų (turima omenyje intelektinės nuosavybės subjektų interesų) nei pažeista.

Be to, teismas pabrėžė, jog įpareigojimų nustatymas neleis pasiekti tik konkretaus tinklapio, kuris ir taip jau turėtų būti neprieinamas pagal ankstesnį teismo sprendimą, kuriuo tinklapio valdytojai turėjo neleisti tinklapio pasiekti vartotojams, esantiems Nyderlanduose. Toks sprendimas buvo priimtas Amsterdamo teisme, tačiau tinklapio valdytojų buvo ignoruojamas.[143]

Taip pat pastebėtina, kad *The Pirate Bay* valdytojai norėdami apeiti įpareigojimus numatytus jau minėtiems interneto paslaugų teikėjams, techniškai tinklapį padarė prieinamą per naują IP adresą bei papildomą *proxy* serverį.

Kaip atsaką į tai, BREIN nurodė interneto paslaugų teikėjams blokuoti ir naująjį IP adresą. Teismas tuo pačiu įpareigojo dar penkis interneto paslaugų teikėjus blokuoti du *The Pirate Bay* IP adresus bei 20 domeno vardų. Tačiau, teismo manymu, toks sprendimas nuėjo per toli, todėl jis nurodė, jog BREIN nebegalės savo iniciatyva pridėti naujų IP adresų (jeigu jie atsirastų).[144]

Grįžtant prie teismo sprendimo, įdomu tai, kad teismas nustatė, jog pagrindinis sprendimo motyvas yra tai, kad „*The Pirate Bay"* pažeidė autorių teises, o interneto paslaugų teikėjai, tiksliau prieigos teikėjai, prisidėjo prie šio pažeidimo (tapo bendrininkais) perduodami saugomą turinį savo tinklais. Taip pat prieigos teikėjai įvykdė ir savarankišką autorių teisių pažeidimą dėl to, kad perdavimo metu automatiškai turinys trumpą laiką buvo saugomas prieigos teikėjo sistemoje.

Toks teismo sprendimas kelia daug klausimų, kadangi tiek pats tinklapio valdytojas autorių teisių objektų nei saugo, nei įkelia į internetą, tiek, tuo labiau, prieigos teikėjas to nedaro. Taigi toks teismo sprendimas iš dalies yra sunkiai suprantamas.

Minėtas pavyzdys nėra vienintelis atvejis, kada praktikoje interneto paslaugų tiekėjai yra įpareigojami taikyti filtravimo ar blokavimo priemones. Iš esmės galima teigti, jog šiuo aspektu yra stengiamasi apginti intelektinės nuosavybės teisių subjektų interesus, tačiau taip pat nepažeidžiant informacijos laisvės principo. Iš minėto pavyzdžio matyti, jog yra svarbus veikos neteisėtumas, kitaip tariant, turi būti nustatytas pažeidimas, tokiu būdu įgyvendinant Europinio lygmens reglamentavimą, kuris buvo nagrinėtas anksčiau. Nors ir susiduriama su kitų asmenų interesų nepaisymu (kada asmenys naudojasi P2P tinklais teisėtais veiksmais), tačiau apimties prasme tokiais atvejais yra svarbiau sustabdyti daromus pažeidimus bei apginti intelektinės nuosavybės subjektų teises.

[143] *Dutch ISPs Ordered To Block The Pirate Bay.* [interaktyvus] 2012. [žiūrėta 2012-11-17]. <http://torrentfreak.com/dutch-isps-ordered-to-block-the-pirate-bay-120111/>.
[144] *ISPs Refuse to Block New Pirate Bay IP-Address.* [interaktyvus] 2012. [žiūrėta 2012-11-17]. < http://torrentfreak.com/isps-refuse-to-block-new-pirate-bay-ip-address-120524/>.

MySpace byla

2007 metais Prancūzijos aukščiausiasis pirmos instancijos teismas nesutiko su socialinio tinklo *MySpace* klasifikavimu kaip prieglobos paslaugų teikėjo. Pasak teismo, paruoštų tinklapių priskyrimas konkrečiam vartotojui asmeniniam naudojimui, kartu su pajamas generuojančiais reklaminiais pranešimais, kurie matomi kiekvieno apsilankymo tinklapyje metu, įtvirtina *MySpace* kaip turinio tiekėjo statusą. Panašių sprendimų Prancūzijoje buvo priimta ir anksčiau, ir šiais metais.[145]

Atkreiptinas dėmesys į tai, kad atsakomybės "režimas" turinio tiekėjams yra kur kas griežtesnis nei prieglobos ar prieigos paslaugų teikėjams, kuriems taikomos išimtys minimos elektroninės komercijos direktyvoje. Taigi *MySpace* pripažinimas turinio tiekėju leidžia tinklapio valdytojui įdiegti automatinę filtravimo sistemą, kuri filtruotų visą teikiamą turinį.

Bendrai darytina išvada, jei informacinės visuomenės paslaugų teikėjas nepatenka į elektroninės komercijos direktyvoje numatytas atsakomybės išimtis, tai šio atsakomybę reglamentuoja nacionaliniai teisės aktai, numatantys atsakomybę už tiesioginį ar netiesioginį intelektinės nuosavybės pažeidimą.[146]

Viacom prieš Youtube

Tai yra viena naujausių JAV bylų dėl interneto tarpininkų atsakomybės. Nors sprendimas šioje byloje ir neturi įtakos Europos teismų praktikai, tačiau iš šio sprendimo matomas bendras požiūris į interneto tarpininkus.

Šioje byloje intelektinės nuosavybės teisių subjektai (*Viacom*, futbolo asociacija bei nemažai kino studijų bei TV kompanijų) kreipėsi į teismą, dėl to, kad *YouTube* tinklapyje laikotarpyje nuo 2005 iki 2008 metų buvo atgaminta bei peržiūrėta daugmaž 79 000 audiovizualinių kūrinių (klipų) ir taip pažeistos intelektinės nuosavybės subjektų teisės.

Pirmos instancijos teismas pripažino, kad *YouTube* neturėjo pakankamai informacijos apie daromus pažeidimus ir dėl to šiam paslaugų teikėjui taikoma atsakomybės išimtis numatyta JAV Digital Millennium Copyright Act.[147]

Apeliacinis teismas, nors ir iš esmės sutiko su pirmos instancijos teismo sprendimu, tačiau vis tiek perdavė bylą pirmos instancijos teismui nagrinėti iš naujo. Toks sprendimas buvo priimtas

[145] Angelopoulous, C. *Filtering the internet for copyrighted content in Europe.* Amsterdam Law School Legal Studies Research Paper No. 2012-04, 2012.
[146] *Ibid.*
[147] 1998 m spalio 28 d. USA Digital Millenium Copyright Act. Public Law 105-304.

dėl to, kad nors *YouTube* trys iš keturių funkcijų atitinka *Digital Millennium Copyright Act* keliamus reikalavimus, kad būtų taikoma atsakomybės išimtis, tačiau dėl ketvirtos nėra aišku. Teismas pasisako, jog pirmos instancijos teismas suklydo interpretuodamas, kad "teisė ir galimybė kontroliuoti" reikalauja žinių apie "konkretų pažeidimą" (*item specific knowledge*), t.y. konkretų objektą ir subjektą. Taigi byla perduota nagrinėti pirmosios instancijos teismui ir taip toliau tęsiama kova tarp interneto paslaugų teikėjų bei intelektinės nuosavybės teisių subjektų kaip Europoje taip ir JAV.[148]

"Orakulas", "Top sportas", asociacija "Lažybų organizatorių aljansas" prieš "Unibet (International) Ltd", "Spread Your Wings Ltd.", "bwin International Ltd.", Hillside (New Media) ltd, "Nordic Gaming Group Ltd."

Paminėtina ir Lietuvoje nagrinėta byla 2-2534/2011[149], kurioje buvo sprendžiamas ginčas, susijęs su veiklos teisėtumu organizuojant lažybas. Pagal atskiruosius skundus nagrinėjami klausimai, susiję su laikinųjų apsaugos priemonių taikymu, pakeitimu ir panaikinimu. Kadangi atsakovai lažybų paslaugas teikė internetu, ieškovų prašymu buvo taikytos laikinosios apsaugos priemonės. Ieškovai prašė: "Uždrausti visas galimas prieigas per Lietuvos Respublikoje veikiantį viešo naudojimo kompiuterių tinklą prie interneto portalų *bwin.com, unibet.com, triobet.com, sportingbet.com, bet365.com*. Nurodė, kad ginčo suma yra didelė, prašomos taikyti laikinosios apsaugos priemonės yra tikslingos, jų nepritaikius, ieškovų patiriama žala tik didėtų"[150].

Pirmos instancijos teismas tenkino laikinųjų apsaugos priemonių prašymą. Tačiau ieškovai kreipėsi į teismą su prašymu taikyti papildomas laikinąsias apsaugos priemones – areštuoti atsakovams priklausančius domeno vardus ir įpareigoti registratorius (šiuo atveju užsienio registratorius) pakeisti tų pačių domenų nukreipimo įrašus, nukreipiant į Lietuvos Respublikos valstybinės lošimų priežiūros komisijos interneto tinklapį.

Šiuo klausimu yra svarbus Lietuvos Respublikos ryšių reguliavimo tarnybos vadovo atsakymas į Apeliacinio teismo užklausimą dėl galimybės techniškai įgyvendinti ieškovų prašymą dėl papildomų laikinųjų apsaugos priemonių. Atsakyme vadovas nurodo, jog: "techniškai yra neįmanoma įgyvendinti įpareigojimą užsienio valstybėse registruotoms įmonėms uždrausti visas galimas prieigas per Lietuvos Respublikoje veikiantį viešo naudojimo kompiuterių tinklą prie

[148] United States Court of Appeals for the Second Circuit, case *Viacom Int'l, Inc., Football Ass'n Premier League Ltd. V. YouTube, Inc*, 10-3270, 10-3342, [2012].
[149] Lietuvos apeliacinio teismo 2011 m. gruodžio 27 d. sprendimas civilinėje byloje *"TopSport", "Orakulas", Asociacija Lažybų organizatorių aljansas, prieš "Unibet (International) Ltd.", "Spread Your Wings Ltd.", "bwin International Ltd.", Hillside (New Media) ltd, "Nordic Gaming Group Ltd."* (bylos nr. 2-2534/2011).
[150] *Ibid.*

konkrečių interneto portalų *bwin.com; unibet.com; triobet.com; sportingbet.com; bet365.com.*"[151] (tai atsakovų tinklapiai, dėl kurių prašoma taikyti laikinąsias apsaugos priemones ir neleisti prie jų prieiti vartotojams). „Rašte paaiškinta, jog domenams *bwin.com; unibet.com; triobet.com; sportingbet.com; bet365.com* yra taikoma didesnės apimties apsauga ir dėl ribojimų įgyvendinimo reikėtų kreiptis į korporaciją *Verisign Inc*., kuri pagal Registracijos sutartį su ICANN organizacija vykdo aukščiausio lygio domeno *com* registro valdytojo funkcijas. Įgyvendinus šį įpareigojimą, būtų panaikinta prieiga prie atsakovų lažybų portalų ne tik vartotojams iš Lietuvos, bet ir visiems interneto vartotojams."[152]

Taigi, ką ir konstatavo teismas bei LR ryšių reguliavimo tarnybos vadovas atsakyme į minėtą teismo užklausimą, toks domeno vardų prašomas areštas bei įpareigojimų nustatymas yra visiškai nepagrįstas. Tokių priemonių taikymo prašymas yra peržengiantis pareikštų reikalavimų ribas, kadangi draudimas prisijungti galiotų visiems vartotojams, o ne tik tiems, kurie prisijunginėja iš Lietuvos teritorijos. Taip pat tai pažeistų vartotojų ne iš Lietuvos teisėtus interesus gauti jų valstybėse teisėtai teikiamas paslaugas. Be to, pastebėtina, jog ieškovų prašymas areštuoti konkrečius domenus, galėtų nebent užtikrinti reikalavimų dėl daiktinių teisių į domenus vykdymą, tačiau negali būti reiškiamas ir tenkinamas, kai kalbama apie neturtinio pobūdžio reikalavimus.[153]

Iš esmės teismas apgynė tiek Europos lygmens reglamentavime (direktyvose), tiek ir LR nacionaliniuose teisės aktuose įtvirtintus proporcingumo principus bei teisių balansą. Iš ankstesnių darbo dalių matyti, kad nacionaliniai teismai kai kuriais atvejais gali įpareigoti interneto paslaugų teikėjus taikyti tam tikras priemones, kitaip sakant, nustatyti jiems įpareigojimus. Tačiau toks įpareigojimų nustatymas turi būti pagrįstas konkrečiais pažeidimais bei negali išeiti už konkrečių pažeidimų ribų. Kaip ir nurodė teismas bei LR ryšių reguliavimo tarnybos vadovas, negalima įpareigoti interneto paslaugų teikėją blokuoti konkretų domeną viesiems vartotojams, todėl, kad būtų pažeidžiami teisėti kitų vartotojų interesai. Konkrečiu atveju būtų peržengtos pareikštų reikalavimų ribos. Nors, kaip ir buvo matyti anksčiau minėtos teisminės praktikos apžvalgoje, kai kada gali būti nepaisoma kitų vartotojų teisėtų interesų, tačiau turi būti aiškiai nustatyta, kad apgintų interesų mastas yra kur kas didesnis nei tokiu sprendimu pažeistų. Labiausiai tai susiję su intelektinės nuosavybės teisių pažeidimais, kada iš esmės padaroma žala, pats pažeidimo pobūdis ir ginamos teisės yra galima sakyti "svarbesnės" už galimai pažeidžiamus teisėtus kitų vartotojų interesus (duomenų keitimosi P2P tinkle atvejais tai labai keliantis klausimą kriterijus, kadangi nustatyti teisėto ir neteisėto naudojimosi santykį yra sunku).

[151] *Ibid.*
[152] Lietuvos apeliacinio teismo sprendimas c.b. 2-2534/2011, *supra* note.
[153] Ibid.

Bendrai kalbant apie įpareigojimų nustatymus interneto paslaugų teikėjams dėl trečiųjų asmenų padarytų pažeidimų reikia vertinti tiek reikalavimų apimtį, tiek pažeidimo mastą bei santykį su ginamais interesais. Šioje byloje būtent buvo įvertintas teisių ir interesų santykis ir techninių galimybių taikymas.

IŠVADOS

1. Iš esmės tradiciniai intelektinės nuosavybės pažeidimai kartu su technologijų raida persikelia į elektroninę erdvę. Tokių pažeidimų objektai dažniausiai yra autorių teisės bei gretutinės teisės, prekių ženklų savininkų teisės bei patentų savininkų teisės.

2. Naujesnės ir nebūdingos tradiciniams intelektinės nuosavybės pažeidimams yra duomenų bazių savininkų bei autorių teisių pažeidimų formos. Taip pat pastebėtina, kad turbūt daugiausia intelektinės nuosavybės pažeidimų vykdoma *peer-to-peer* tinklų ir programinės įrangos pagalba, kas išskiria šių pažeidimų padarymo būdus kaip specifinius ir egzistuojančius tik elektroninėje erdvėje.

3. Išanalizavus technines interneto paslaugų teikėjų intelektinės nuosavybės apsaugos ir bendrai turinio kontrolės galimybes bei kai kurių valstybių pavyzdžius, darytina išvada, kad interneto paslaugų teikėjai turi technines galimybes įgyvendinti beveik bet kokį įsivaizduojamą prevencinį filtravimą ar stebėjimą.

4. Klausimas, kokia apimtimi techninės priemonės turėtų būti taikomos, kad interneto tarpininkai netaptų cenzūros vykdytojais bei taip pat kiek tokios prevencinės priemonės būtų teisėtos globaliame kontekste, kai pagrindinės žmogaus teisės ir laisvės yra iškeliamos į pirmą vietą, išlieka Europos Sąjungos lygmens reglamentavime bei nacionalinio reglamentavimo diskrecijoje (kalbant apie Europos Sąjungos valstybes nares).

5. Išanalizavus interneto paslaugų teikėjų veiklos reglamentavimą Europos Sąjungos lygmeniu matoma, kad Europos Parlamento ir Tarybos Direktyva 2000/31/EB „Dėl kai kurių informacinės visuomenės paslaugų, ypač elektroninės komercijos, teisinių aspektų vidaus rinkoje“ įtvirtina principus, pagal kuriuos interneto paslaugų teikėjai yra atsakingi už informaciją ar duomenis, kurie yra patalpinti jų serveriuose ar tinklapiuose, tik tokiu atveju, kai interneto paslaugų teikėjai apie tokią informaciją žino ir ją kontroliuoja.

6. Iš teisės aktų analizės matoma, kad pastovus filtravimo vykdymas nesant konkrečiam intelektinės nuosavybės teisių pažeidimui ar tuo labiau nesant teismo sprendimui negali būti vykdomas. Tuo labiau nesant konkrečioms aplinkybėms (pažeidimui, teismo sprendimui) interneto paslaugų teikėjas negali būti įpareigotas vykdyti bet kokią turinio kontrolę. Toje pačioje Europos Parlamento ir Tarybos Direktyvoje 2000/31EB „Dėl kai kurių informacinės visuomenės paslaugų, ypač elektroninės komercijos, teisinių aspektų vidaus rinkoje“, nustatyta, jog valstybės narės nenustato teikėjams nei bendros prievolės stebėti informaciją, kurią jie perduoda arba saugo, nei bendros prievolės aktyviai domėtis faktais arba aplinkybėmis, rodančiomis nelegalią veiklą.

7. Teismų praktikos analizė iš esmės parodė tendenciją, kad interneto paslaugų teikėjai negali būti lengvai įpareigojami taikyti filtravimo ir kitų apsaugos priemonių esant bet kokiam intelektinės nuosavybės subjekto reikalavimui. Iš naujausios teismų praktikos matoma, kad šiuo metu vyksta tam tikras pasikeitimas požiūryje į interneto paslaugų teikėjų veiklą bei teisių balansą. Nagrinėtose bylose jaučiamas proporcingumo principo aktyvinimas bei intelektinės nuosavybės teisių absoliutizmo naikinimas, kadangi šios teisės, nors ir įtvirtintos Europos žmogaus teisių chartijoje, tačiau jos nėra absoliučios ir turi būti ginamos santykyje su kitomis teisėmis.

8. Vertinant interneto paslaugų teikėjų vaidmenį neteisėtame intelektinės nuosavybės platinime reikia pasakyti, jog iš teismų praktikos ir nuolatinių diskusijų yra matomas šioks toks poslinkis link to, kad interneto paslaugų teikėjai neturėtų būti įpareigojami imtis tam tikrų prevencinių priemonių nesant konkretaus teisių pažeidimo. Tiek iš tarptautinės, tiek ir iš Lietuvos teismų praktikos matyti, kad teismai atsižvelgia į pažeidimo mastą, pobūdį bei į paslaugų gavėjų teisėtų interesų pažeidimą įpareigojant interneto paslaugų teikėjus imtis techninių intelektinės nuosavybės apsaugos priemonių.

PASIŪLYMAI

1. Galimos korekcijos Lietuvos Respublikos autorių teisių ir gretutinių teisių įstatyme.

Siūlytina patikslinti pagrįstai turimų įrodymų formuluotę LR Autorių teisių ir gretutinių teisių įstatymo 80 straipsnio 1 dalyje:

1.1. Lietuvos Respublikos autorių teisių ir gretutinių teisių įstatymo 80 straipsnyje pridėti 3 dalį ir ją išdėstyti taip:

„3. Šio straipsnio pirmoje dalyje minimi pagrįstai turimi įrodymai apima bet kokią informaciją, įrodančią vykdomą arba galimai vyksiantį autorių teisių, gretutinių teisių ar sui generis teisių pažeidimą, įskaitant, bet neapsiribojant tinklapių su matomai neteisėtai talpinamais autorių teisių, gretutinių teisių ar sui generis teisių objektais spausdintomis patvirtintomis kopijomis bei „peer-to-peer“ tinklais neteisėtai prieinamų duomenų išklotinėmis (sąrašais).“

Pastebėtina, kad harmonizuotos korekcijos turėtų būti daromos Europos Sąjungos lygmeniu, daugiausia elektroninės komercijos Direktyvoje (2000/31/EB), kadangi šios direktyvos nuostatos įgyvendinamos ir Lietuvos Respublikos nacionaliniuose teisės aktuose.

LITERATŪROS SĄRAŠAS

Norminiai teisės aktai:

1. Europos komisijos komunikatas „Darni sistema, kuria siekiama padidinti pasitikėjimą bendrąja skaitmenine elektroninės prekybos ir internetu teikiamų paslaugų rinka“; COM(2011)0942 final.
2. Lietuvos Respublikos baudžiamasis kodeksas. *Valstybės žinios.* 2000, Nr. 89-2741. 193-194 str.
3. 2000 m. birželio 8 d. Europos Parlamento ir Tarybos Direktyva 2000/31/EB dėl kai kurių informacinės visuomenės paslaugų, ypač elektroninės komercijos, teisinių aspektų vidaus rinkoje (Elektroninės komercijos direktyva). [2000], OL L178.
4. Lietuvos Respublikos autorių teisių ir gretutinių teisių įstatymas. *Valstybės žinios.* 1999, Nr. 50-1598.
5. 2001 m. gegužės 22d. Europos Parlamento ir Tarybos Direktyva 2001/29/EB dėl autorių teisių ir gretutinių teisių informacinėje visuomenėje tam tikrų aspektų suderinimo. [2001], OL L0029.
6. 2004 m. balandžio 29 d. Europos Parlamento ir Tarybos Direktyva 2004/48/EB dėl intelektinės nuosavybės teisių gynimo. [2004], OL L157/45.
7. Loi nº 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet (Law No. 2009-669 of June 12, 2009 promoting the Dissemination and Protection of Creation on the Internet), [interaktyvus]. [žiūrėta 2012-11-02]. <http://www.wipo.int/wipolex/en/details.jsp?id=5613>.
8. Korėjos autorių teisių įstatymas [interaktyvus]. [žiūrėta 2012-11-10] < http://www.moleg.go.kr/english/korLawEng?pstSeq=52683&pageIndex=23>.
9. Didžiosios Britanijos skaitmeninės ekonomikos įstatymas [interaktyvus]. [žiūrėta 2012-11-10] < http://www.legislation.gov.uk/ukpga/2010/24/contents?view=plain>.
10. Lietuvos Respublikos patentų įstatymas. *Valstybės žinios.* 1994, Nr. 8-120.
11. Lietuvos Respublikos prekių ženklų įstatymas. *Valstybės žinios.* 2000, Nr. 92-2844.
12. Lietuvos Respublikos dizaino įstatymas. *Valstybės žinios.* 2002, Nr. 112-4980.
13. 2012 m. spalio 26 d. Europos Sąjungos Pagrindinių Teisių Chartija 2012/C 326/02. [2012].
14. 1998 m spalio 28 d. USA Digital Millenium Copyright Act. Public Law 105-304.

Vadovėliai, monografijos, moksliniai straipsniai:

1. Bagdonavičiūtė, I. *Intelektinės nuosavybės pažeidimai internete: specifika ir problemos*. Magistro baigiamasis darbas. Vilnius: Mykolo Romerio universitetas, 2007.
2. Jonelis, A. Autorių teisių ir gretutinių teisių realizavimas internete. Magistro baigiamasis darbas. Vilnius: Mykolo Romerio universitetas, 2005.
3. Kiškis, M. Intelektinės nuosavybės teisinė apsauga elektroninėje erdvėje. Vilnius: Mykolo Romerio universiteto Leidybos centras, 2011.
4. Rowland, D. and Macdonald, E., *Information Technology Law*. London: Cavendish, 2nd ed., 2000. 520.
5. Bainbridge, D., *Intellectual Property*. Pearson: Longman, 6th ed., 2007. 680.
6. Phillips, J., *Trade Mark Law-A Practical Anatomy*. Oxford University Press, 2003. 593.
7. Reed, C., *Internet Law: Text and Materials*. Cambridge University Press, 2nd ed., 2004. 101.
8. Yang, F. *Infringement of intellectual property rights over the internet and private international law*. Magistro baigiamasis darbas. [interaktyvus] Nottingham University, 2010. <http://etheses.nottingham.ac.uk/1197/>
9. Taylor, M., *Uses of Encryption: Digital Signatures*. C.T.L.R. 2006. 92.
10. Akester, P., „Authorship and Authenticity in Cyberspace", *Computer Law & Security Report*, Vol. 20, No. 6, 2004, 436, at 439.
11. Dutton, W.H. Dopatka, A. Hills, M. Law, G. Nash, V. *Freedom of connection – freedom of expression: the changing legal and regulatory ecology shaping the internet*. A report prepared for UNESCO"s Division for Freedom of Expression, Democracy and Peace. University of Oxford, 2010. 28-44.
12. Deibert, R. Palfrey, J. Rohozinski, R. Zittrain, J. *Access Denied – The Practice and Policy of Global Internet Filtering*. Cambridge: MIT Press, 2008. 9, 34.
13. Baumbauer, D.E. Deibert, R.J. Palfrey jr., J.G. Rohozinski, R. Villeneuve, N. Zittrain, J. *Internet filtering in china in 2004-2005: a country study*. Harward Law School Research Publication No. 2005-10, 2005. 3-4.
14. Baumbauer, D.E. *Censorship V3.1*. Discussion paper No. 12-28, University of Arizona, 2012. 3-4.

15. Callanan, C. Gercke, M. Marco, E.D. Ziekenheiner, E.D. *Internet blocking balancing cybercrime responses in democratic societies.* Aconite internet solutions, Ireland, 2009. 16-43.
16. Parson, C. *Deep packet inspection in perspective: tracing it's lineage and surveillance potentials.* Working paper, doctoral studies. University of Victoria's Political Science department, Canada, 2009. 7-8.
17. Daly, A. *The legality of deep packet inspection. First interdisciplinary Workshop on Communications Policy and Regulation 'Communications and Competition Law and Policy – Challenges of the New Decade'.* University of Glasgow, 2010. 4.
18. Mueller, M. Kuehn, A. Santoso, S.M. *Policing the Network: Using DPI for Copyright Enforcement.* Surveilance and society, 2012. 351.
19. Lipton, J.D. *Law of the intermediated information exchange.* Case Western Reserve University School of Law, USA, 2012. 8-9.
20. Lipton, J.D. *Combating Cyber-Victimization.* 26 BERKELEY TECH. L. J. 1103, 1139 USA, 2011.
21. Schellekens, M. *Liability of internet intermediaries:aslippery slope? SCRIPTed, Volume 8, Issue 2, Tilburg Insitute for Law, Technology and Society*. Netherlands, 2011. 156-161.
22. Janušauskaitė, K. *Regulation of the internet service providers' liability: does ir really work? Lithuanian legislation and court practice*. Research papers from the WIPO-WTO colloquium for teachers of intellectual property law. Geneve, 2011. 108-111.
23. Neri, A. *Ordering intermediaries to implement filtering mechanisms: a controversial measure with dreadful consequences.* France, 2011. 2-5.
24. Giannopoulou, A. *Copyright enforcement measures: the role of the ISPs and the respect of the principle of proportionality.* European Journal for Law and Technology, Vol. 3, No. 1, 2012. [interaktyvus] [žiūrėta 2012-11-14]. < http://ejlt.org/article/viewArticle/122/204>.
25. Baraliuc, I. Depreeuw, S. Gutwirth, S. *Copyright enforcement in Europe after ACTA: what now?*. Netherlands journal of legal philosophy,Vol. 41/2, 99-104, 2012. 3-4.
26. Muir, A. *Online copyright enforcement by internet service providers.* Journal of Information Science XX (X) pp. 1-15. Loughborough University, UK, 2012.
27. Daly, A. Farrand, B. *Scarlet v SABAM: evidence of an emerging backlash against corporate copyrights lobbies in Europe?* European University Institute – Department of Law, 2012. 2-4.

28. Angelopoulous, C. *Filtering the internet for copyrighted content in Europe.* Amsterdam Law School Legal Studies Research Paper No. 2012-04, 2012.

Teismų praktika:

1. Byla C-70/10, *Scarlet Extended SA prieš Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2011].
2. Byla C-360/10, *Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) prieš Netlog NV* [2012].
3. Vilniaus apygardos teismo 2008 m. spalio 1 d. nutartis civilinėje byloje *AB "Pieno žvaigždės" prieš E.K.* (bylos Nr. 2-1061-623/08).
4. *Shetland Times, Ltd. v. Jonathan Wills and Another*, 1997 F.S.R. (Ct. Sess. O.H.).
5. United States District Court Southern District of New York case *Washington post v. TotalNews,* No. 97 Civ. 1190 (PKL), [1997].
6. *A & M Records, Inc. v Napster, Inc.*, 239 F. 3d 1004 (9th Cir. 2001).
7. United States Supreme Court , 545 U.S. 913 (2005), *MGM Studios, Inc. v. Grokster, Ltd*.
8. Federal Court of Australia,[2005] FCA 1242 *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd.*
9. United States District Court of Illinois, 457 F. 3d 1279, C.A. Fed. (Ill.), 2006, *Eolas Technologies, Inc. v Microsoft Corp.*
10. Order of the Court (Eighth Chamber) of 19 February 2009 (reference for a preliminary ruling from the Oberster Gerichtshof (Austria)): *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v Tele2 Telecommunication GmbH*, Case C-557/07, [2009] C 113/28.
11. Byla C-275/06, *Productores de Música de España (Promusicae) prieš Telefónica de España S.A.U.* [2008] ECR I-271.
12. Byla C-324/09, *L'Oréal prieš eBay* [2011] ECJ.
13. Supreme Court of New York, case *Stratton Oakmont, Inc. v Prodigy Services Co*. [1995] WL 323710 (NY Sup Ct 1995).
14. BGH, *Urteil v 12.07.2007, Az. I ZR 18/04.*
15. Cour d'Appel de Paris Pôle 1, Chambre 4 Arrêt du 26 Mars 2010, *Youtube v Magdane et Autres* [2010].
16. Didžiosios kolegijos sprendimas iš esmės:
    Fressoz and Roire v. France, no. 29183/95, ECHR 1999-I.

17. Didžiosios kolegijos sprendimas iš esmės:
Lehideux and Isorni v. France, no. 92, ECHR 1998-VII.
18. Kolegijos sprendimas iš esmės:
Du Roy and Malaurie v. France, no. 34000/96, ECHR 2000-X.
19. The High Court of Justice Queen's Bench Division Administrative Court, case *BT & Talk Talk v The Secretary of State for BIS*, No. CO/7354/2010, [2011] EWHC 1021 (admin).
20. United States Court of Appeals for the Second Circuit, case *Viacom Int'l, Inc., Football Ass'n Premier League Ltd. V. YouTube, Inc,* 10-3270, 10-3342, [2012].
21. Lietuvos apeliacinio teismo 2011 m. gruodžio 27 d. sprendimas civilinėje byloje *"TopSport", "Orakulas", Asociacija Lažybų organizatorių aljansas, prieš "Unibet (International) Ltd.", "Spread Your Wings Ltd.", "bwin International Ltd.", Hillside (New Media) ltd, "Nordic Gaming Group Ltd."* (bylos nr. 2-2534/2011).

Kiti šaltiniai:

1. *Human rights manual, Guidelines for Implementing a Human Rights Based Approach in ADC.* Austrian Development Agency. Vienna 2010. 141.
2. *Intellectual property on the internet: A Survey of Issues (WIPO/INT/02).* World Intellectual Property Organisation. Geneva, 2002. 20-23, 104.
3. *Intellectual property and the internet: Copyright infringement liability in the digital era*. [interaktyvus]. Advisen special report, 2010. [žiūrėta 2012-06-03]. <https://www.advisen.com/downloads/Intellectual_Property.pdf>
4. Lehman, B.A. *Intellectual Property and the National Information Infrastructure – The Report of the Working Group on Intellectual Property Rights*. [interaktyvus] 1995 [žiūrėta 2012-04-05]. <http://www.ladas.com/NII/NII_Technology.html#enc>.
5. Qinglian, H. *Media control in China.* [interaktyvus] 2004. [žiūrėta 2012-05-15]. <http://www.hrichina.org/public/contents/8991>.
6. *Germany's President Signs an Internet Bill Against His Own Party*. [interaktyvus] EDRI 2010. [žiūrėta 2012-12-16]. <http://www.edri.org/edrigram/number8.4/german-president-adopts-internet-childporn-law>.
7. *Eric Goldman, Celebrating (?) the Six-Month Anniversary of SOPA's Demise.* [interaktyvus] Forbes 2012. [žiūrėta 2012-08-09]. <http://www.forbes.com/sites/ericgoldman/2012/07/18/celebrating-the-six-month-anniversary-of-sopas-demise/>.

8. Tsukuyama, H. Kang, Cecilia. *SOPA opposition goes viral.* [interaktyvus] Washington POST 2011. [žiūrėta 2012-08-13]. <http://www.washingtonpost.com/business/economy/sopa-opposition-goes-viral/2011/11/22/gIQAZX7OmN_story.html>
9. Internet Watch Foundation statement *regarding Wikipedia webpage.* [interaktyvus] 2008. [žiūrėta 2012-10-10]. <http://www.iwf.org.uk/about-iwf/news/post/251-iwf-statement-regarding-wikipedia-webpage>.
10. Commission of European Communities. *First Report on the application of Directive 2000/31/EC of the European Parliament and of the Council no.* COM(2003) 702 final. [interaktyvus] Brussels 2003. [žiūrėta 2012-10-16]. < http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2003:0702:FIN:EN:PDF>.
11. *Dutch ISPs Ordered To Block The Pirate Bay.* [interaktyvus] 2012. [žiūrėta 2012-11-17]. <http://torrentfreak.com/dutch-isps-ordered-to-block-the-pirate-bay-120111/>.
12. *ISPs Refuse to Block New Pirate Bay IP-Address.* [interaktyvus] 2012. [žiūrėta 2012-11-17]. < http://torrentfreak.com/isps-refuse-to-block-new-pirate-bay-ip-address-120524/>.

SANTRAUKA

Darbe nagrinėjama tema yra aktuali, kadangi toliau besivystanti informacinė visuomenė bei informacijos pateikimo būdai elektroninėje erdvėje sąlygoja pažeidimų vykdymą vis naujomis formomis. Pagrindiniai kylantys klausimai yra susiję su tokių pažeidimų darymo sustabdymu bei prevencijos galimybėmis.

Pagrindinis darbo tikslas yra atskleisti interneto paslaugų teikėjų vaidmenį kovoje su neteisėtu intelektinės nuosavybės platinimu, išanalizuoti jų atsakomybės bei galimybių ribas. Darbe yra aptariami pažeidimai, kurie atsiranda elektroninėje erdvėje ir ypač išskiriama intelektinės nuosavybės pažeidimų specifika ir problematika. Taip pat aptariami intelektinės nuosavybės apsaugos elektroninėje erdvėje techniniai būdai ir jų pritaikomumas. Atsižvelgiant į išskirtus pažeidimus bei aptartus apsaugos būdus, darbe analizuojamas interneto paslaugų teikėjų vaidmuo šių apsaugos priemonių taikyme bei analizuojamas atsakomybės ribų nustatymas.

Darbe yra supažindinama su nacionaline bei Europos Sąjungos teismų praktika situacijose, kada reikia nustatyti interneto paslaugų teikėjų atsakomybę bei įpareigojimų jiems nustatymo teisėtumą. Analizuojamas esamas reglamentavimas tiek Europos lygmeniu, tiek ir atskirų valstybių nacionalinės teisės lygmeniu bei taip pat paminima ir ne Europos Sąjungos valstybių praktika ir reglamentavimas.

Apibendrinus ir išanalizavus tyrimo metu surinktą medžiagą, darytina išvada, kad interneto paslaugų teikėjai neturėtų būti įpareigojami vykdyti turinio kontrolės tol, kol nėra konkretaus pažeidimo, o imantis tam tikrų techninių priemonių intelektinei nuosavybei apsaugoti visada turi būti atsižvelgiama į pažeidimo apimtį ir suinteresuotų trečiųjų šalių teises. Interneto paslaugų teikėjų statuso klausimas dar nėra išspręstas, tačiau jau yra daromi žingsniai, kad būtų suderintos suinteresuotų asmenų teisės su įpareigojimais interneto paslaugų teikėjams.

SUMMARY

The topic of the work is of great interest, since further development of information society and information presentation techniques in cyberspace leads to new forms of violations. Main questions that arise are related to stopping such violations and preventive measures that can be applied.

The main goal of the work is to expose the role of the internet service providers in the fight against illegal distribution of intellectual property, to analize the limits of their liability and preventive possibilities. The paper dicusses the violations that occur in cyberspace and especialy infringements of intellectual property rights. Also the paper discusses the technical methods of intellectual property protection in cyberspace and their application. Given the analyzed infringements and protection measures, the paper also analyzes the role of internet sevice providers in applying these protective measures and the liability limits.

The paper introduces the national and European Union case law relating situations in which it requires to establish internet service providers liability and established obligations legitimacy. The work analyzes the existing regulation on European level and on individual national levels, as well as regulation in non-European Union countries law.

Summarizing and analyzing the material collected during preparation of this paper, it must be concluded that internet service providers shoul not be obliged to excercise content control, as long as there are no specific violations and applying certain technical measures for the protection of intellectual property must always take into account the extent of damage, and interested third partie‘ rights.