MYKOLO ROMERIO UNIVERSITETO
EKONOMIKOS IR FINANSŲ VALDYMO FAKULTETO
INFORMATIKOS IR STATISTIKOS KATEDRA

MARIUS KALINAUSKAS
DIENINIO SKYRIAUS INFORMATIKOS TEISĖS STUDIJŲ PROGRAMOS STUDENTAS,
II KURSAS, ITMD07 – 01

PRIVATUMO IR ASMENS DUOMENŲ APSAUGOS REGULIAVIMAS TARPTAUTINIU MASTU

Magistro baigiamasis darbas

Darbo vadovas -
Doc. Dr. D. Štitilis

Vilnius, 2008

TURINYS

Įvadas 4
1. TARPTAUTINIŲ TEISĖS AKTŲ, REGLAMENTUOJANČIŲ PRIVATUMĄ BEI ASMENS DUOMENŲ APSAUGĄ APŽVALGA BEI ANALIZĖ 8
1.1. 1948 m Visuotinės žmogaus teisių deklaracijos apžvalga bei analizė asmens privatumo aspektu 9
1.2. Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos apžvalga ir analizė teisės į asmens privatumą aspektu 10
1.3. 1980 m. EBPO gairių dėl privatumo apsaugos ir asmens duomenų judėjimo tarp valstybių narių apžvalga 12
1.4. 1981 m. Konvencijos dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu apžvalga 15
1.5. 1990 m. Jungtinių Tautų Ekonominių ir Socialinių reikalų Tarybos Kompiuterizuotų asmens duomenų bylų gairių apžvalga 21
1.6. Skyriaus apibendrinimas 21
2. REGIONINIAI PRIVATUMO BEI ASMENS DUOMENŲ APSAUGOS REGULIAVIMO MODELIAI KAIP ALTERNATYVA PASAULINIAM REGULIAVIMUI 23
2.1. Regioninis asmens duomenų apsaugos reguliavimas, bei jo įtaka formuojant pasaulinę privatumo bei asmens duomenų apsaugos politiką 23
2.2. Europos Sąjungos asmens duomenų apsaugos reguliavimo modelis 24
2.2.1. Europos Parlamento ir Tarybos direktyvos dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (95/46/EB) apžvalga 25
2.2.2. Europos Parlamento ir Tarybos direktyvos dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (2002/58/EB) apžvalga 30
2.2.3. Europos parlamento ir tarybos direktyvos dėl duomenų, generuojamų arba tvarkomų teikiant viešai prieinamas elektroninių ryšių paslaugas arba viešuosius ryšių tinklus, saugojimo (2006/24/EB) apžvalga asmens duomenų apsaugos aspektu 32
2.2.4 Ministrų komiteto rekomendacijų valstybėms narėms apžvalga privatumo bei asmens duomenų apsaugos aspektu 33
2.3. Jungtinių Amerikos Valstijų privatumo apsaugos reguliavimo modelis 35
2.4. Regioninio reguliavimo skirtumai bei tendencijos privatumo bei asmens duomenų apsaugos aspektu 37

2.5. Skyriaus apibendrinimas 39
3. GRĖSMES PRIVATUMUI IR ASMENS DUOMENIMS ŠIANDIENINIAME PASAULYJE 41
3.1. Grėsmių privatumui šaltiniai bei asmens duomenų apsaugos poreikis šiandieniniame pasaulyje 41
3.2. Netinkamas asmens duomenų naudojimas ir tvarkymas bei su tuo susiję teisės pažeidimai 44
3.3. Skyriaus apibendrinimas 46
4. NAUJOS KARTOS TARPTAUTINIS PRIVATUMO BEI ASMENS DUOMENŲ APSAUGOS REGULIAVIMAS. BŪTINA, BEPRASMIŠKA AR NEIŠVENGIAMA? 47
4.1. Dabartinis privatumo bei asmens duomenų apsaugos reguliavimo efektyvumas 47
4.2. Problemų, kylančių dėl naujos kartos teisinio reguliavimo nebuvimo privatumo bei asmens duomenų apsaugos srityje, analizė 51
4.3. Naujų privatumo bei asmens duomenų apsaugos reguliavimo modelių privalumai bei trūkumai 54
4.3.1. Naujo tarptautinės teisės akto, reglamentuojančio privatumą bei asmens duomenų apsaugą, privalumai bei trūkumai teisės į privatumą aspektu 54
4.3.2. Probleminiai privatumo bei asmens duomenų apsaugos savireguliacijos aspektai 58
4.3.3. Techninė asmens duomenų apsauga 59
4.4. Skyriaus apibendrinimas 60
Išvados 61
Literatūros sąrašas 64
Santrauka 69
Summary 70

ĮVADAS

Privatumas bei asmens duomenų apsauga – sąvokos, žinomos nuo XIX a. pabaigos. Teisinės privatumo šaknys glūdi Jungtinėse Amerikos Valstijose (toliau – JAV). 1890 metais JAV teisininkai [1]Samuel Warren ir Louis Brandeis parašė darbą apie asmens teisę į privatumą teisės pažeidimų prasme ir apibrėžė ją kaip *"teisę būti paliktam ramybėje"* (ang. *The right to be left alone*). Jie pirmieji šią teisę išreiškė kaip didžiulę socialinę vertybę. Šis darbas sukėlė daug diskusijų, o teisės mokslininkai pradėjo aktyviau gilintis į asmens privatumo problematiką. Tačiau tarptautiniu lygiu ši teisė buvo pripažinta tik 1948 metais Jungtinių Tautų (toliau – JT) Visuotinėje žmogaus teisių deklaracijoje. Tuo metu dar nebuvo įmanoma numatyti civilizacijos vystymosi greičio bei masto, o teisė į privatumą nebuvo išskiriama iš kitų žmogaus teisių.

Darbo problematika išvedama iš temos pavadinimo – tai tarptautinio reguliavimo nebuvimo, ar pasenusio reguliavimo problema taikant jį elektroninėje erdvėje. Tobulėjant kompiuteriams bei su jais susijusioms technologijoms atsirado nauji duomenų tvarkymo būdai bei formos. Pagreitį įgavo automatizuotas duomenų tvarkymas, todėl padidėjo rizika pažeisti teisę į privatumą. Atskiros šalys ėmė rengti įstatymus, turėjusius padėti teisiškai sureguliuoti vykstančius procesus bei apsaugoti asmenis nuo galimų jų interesų pažeidimų. Svarbų vaidmenį reguliuojant pasaulinę privatumo bei asmens duomenų apsaugą suvaidino Ekonominio bendradarbiavimo ir plėtros organizacija (toliau – EBPO), 1980 metais nustačiusi privatumo apsaugos ir asmens duomenų judėjimo tarp valstybių narių gaires. Jos atspindėjo neoficialų tarptautinį susitarimą dėl asmens duomenų apsaugos principų. 1981 metų Strasbūro konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu buvo pagrindinis tokio pobūdžio tarptautinis privalomasis aktas visoms Europos Tarybos valstybėms narėms. Gana stabiliai teisės į privatumą buvo ginamos iki 1997-ųjų, kai išaugo interneto vartotojų skaičius ir grėsmės privatumui atgijo naujomis formomis.

Asmeninės informacijos srautų didėjimas virtualioje erdvėje sukuria naujų teisinių problemų privatumo bei asmens duomenų apsaugos srityje. Dėl tinklinių technologijų specifiškumo jų naudojimas teisiniu požiūriu tampa problematiškas. Elektroninei erdvei negalioja valstybių sienos, ji yra dinamiška bei skverbiasi į įvairias kasdieninio gyvenimo sritis. Asmens duomenų naudojimas elektroninėje erdvėje nuolat didėja, tad dabar galiojantis tarptautinio lygio asmens duomenų apsaugos reglamentavimas yra tik iš dalies veiksmingas, o tarptautinių konvencijų bei rekomendacijų taikymo sritys, atsižvelgiant į dabartinį asmens duomenų naudojimo pobūdį bei dažnumą, nepakankamos.

[1] The right to be left alone, 1890, http://www-swiss.ai.mit.edu/6805/articles/privacy/Privacy_brand_warr2.html [2008-05-20, 20:10]

Tarptautinė bendruomenė dar nesiima spręsti šios problemos pasauliniu lygiu, todėl didžiausia našta bandant sureguliuoti naujai atsiradusius procesus tenka nacionalinei ar regioninei teisei. Toks reguliavimo pobūdis turi ir privalumų, ir trūkumų. Nacionalinės teisėkūros institucijos nevienodai interpretuoja teisines problemas bei taiko skirtingo pobūdžio ar griežtumo reguliavimo priemones. Informacijų technologijų specifika nesikeičia priklausomai nuo valstybės sienų ir vidaus įstatymų, nes šioms technologijoms teritorijos ribojimų nėra. Europos Sąjunga (toliau - ES) pirmoji pradėjo rūpintis teisinės bazės šalyse narėse suvienodinimu ir priėmė keletą direktyvų dėl privatumo bei asmens duomenų apsaugos. Toks problemos sprendimas neperžengė regiono ribų, o direktyvų nuostatos tik iš dalies atitiko technologines realijas. ES keitimosi asmens duomenimis politika yra griežta ir įsakmi kitų valstybių atžvilgiu. Už bendrijos ribų nuostatos ir principai dėl virtualios erdvės yra skirtingos. JAV pasikliaujama sektoriniu reguliavimu bei savikontrole, skiriasi požiūris į privatumą kaip vertybę. Egzistuoja ir trečioji šalių grupė. Tai valstybės, kuriose privatumo bei asmens duomenų apsauga yra deklaratyvi arba jos būtinumas apskritai neigiamas. Tokia „priešingų stovyklų“ konkurencija vertintina prieštaringai, kadangi technologijos pasauliniu lygmeniu daugmaž vienodos, o teisinis reguliavimas – skiriasi. Nesvarbu, kuris reguliavimo modelis būtų taikomas, naujųjų technologijų kontekste išryškėja kiekvieno iš jų spragos.

Pavojų privatumui kelia ne tik verslo subjektai ar pavieniai fiziniai bei juridiniai asmenys, bet ir valstybė. Būdama galios monopolininke ji gali lemti šios teisės ribojimą ar vystymą. Po 2001 m. rugsėjo 11-osios įvykių JAV demokratinių valstybių piliečiams teko paaukoti dalį privatumo dėl nacionalinių interesų. Atsakymo, ar šios aukos nauda atpirko jos kainą, dar nėra.

Kalbant apie privačių subjektų vykdomus privatumo bei asmens duomenų apsaugos pažeidimus, dera paminėti, jog iš pažiūros menko pobūdžio nusikalstamos veikos, tokios kaip neteisėtas asmens duomenų tvarkymas ar tokio tvarkymo tikslų nepaisymas, gali peraugti į kur kas sudėtingesnius kriminalinius nusikaltimus, darančius žalą ne tik virtualiame, bet ir realiame pasaulyje.

Probleminių aspektų šioje srityje netrūksta, nes tuo pačiu metu stengiamasi apsaugoti asmenų teisę į privatumą ir vengiama per griežtais ribojimais stabdyti ekonomikos bei technologijų pažangą. Didžiausia problema, jog nesutariama, kuri iš šių dviejų vertybių svarbesnė.

Mokslininkai privatumo bei asmens duomenų apsaugos srityje mažai nagrinėja naujo tarptautinio šių vertybių gynimo reglamentavimo klausimą, nors ir įvardija problemas, kylančias dėl reguliavimo spragų. Harvardo universiteto profesorius Viktor‘as Mayer-Schönberger‘is [2]išsakė nuomonę, jog antrosios kartos asmens duomenų apsaugos teisinis reguliavimas yra iš esmės

[2] Philip E. Agre, Mark Rotenberg. Technology and privacy: the new landscape. Mit Press, 1998. P. 219 – 236.

neveiksmingas, todėl reikalingi nauji globalių problemų sprendimo būdai. Mokslininkai Daniel‘is Solove‘as, Paul‘as M. Schwartz‘as, Marc‘as Rotenberg‘as, pripažinti autoritetai privatumo apsaugos srityje, gilinasi į regioninio ir nacionalinio reguliavimo privalumus bei trukumus bei nagrinėja bendrąsias privatumo problemas. Jie pastebi, jog grėsmių šiai vertybei daugėja, teisinis reguliavimas atsilieka nuo technologijų, o idėjinė bei juridinė priešprieša tarp ES ir JAV klampina problemų sprendimo procesą į gilią privatumo apsaugos krizę**.**

Tema aktuali, nes yra glaudžiai susijusi su pagrindinėmis žmogaus teisėmis bei laisvėmis. Be to, informacinių technologijų specifika verčia ieškoti išeičių iš susidariusios situacijos, kai skirtingas atskirų valstybių asmens duomenų apsaugos teisinis reglamentavimas užkerta kelią šalių piliečiams naudotis informacinių technologijų teikiamomis galimybėmis įvairiose gyvenimo srityse. Privatumo apsauga aktuali dideliam subjektų ratui, kadangi interneto bei telekomunikacinių technologijų suteikiamos galimybės ne tik palengvina bendravimą ar informacijos keitimąsi, bet ir sukuria iššūkius, susietus asmeninės informacijos apsauga.

Tema nauja, nes šis klausimas mažai nagrinėtas Lietuvos ir užsienio šalių literatūroje. Mokslininkų atliekama problemų analizė apima vieną arba kitą konkrečią sritį, susietą su asmens duomenų apsauga bei jos pažeidimais, siekiama įvardinti bei atskleisti atskirų elementų sąveiką, aplenkiant globalesnį probleminių aspektų nagrinėjimą. Su privatumo apsauga susiję procesai yra dinamiški ir nulemti globalių technologinių veiksnių. Duomenų saugos klausimas yra įvairiapusis ir apima tiek socialinius, tiek politinius, tiek ekonominius aspektus, todėl universalų, visiems priimtiną sprendimą rasti sudėtinga.

Magistrinio darbo tyrimo objektas – tarptautinis privatumo bei asmens duomenų apsaugos reguliavimas bei su juo susiję probleminiai reiškiniai.

Magistrinio darbo tyrimo dalykas – tarptautinės bei regioninio pobūdžio teisės normos, reglamentuojančios privatumą bei asmens duomenų apsaugą. Nacionalinės teisės normos kaip dalykas vertinamos tik tada, kai nagrinėjamus klausimus susieja su privatumo bei asmens duomenų apsaugos teisiniu reglamentavimu tarptautiniu mastu. Taip pat nagrinėjama mokslinė literatūra bei kiti šaltiniai.

Darbo tikslas - išnagrinėti privatumo ir asmens duomenų apsaugos reguliavimo aspektus tarptautiniu mastu. Šiam tikslui įgyvendinti keliami tokie **uždaviniai**:

1. Apžvelgti ir išnagrinėti tarptautinius teisės aktus, reglamentuojančius privatumą bei asmens duomenų apsaugą bei atskleisti jų veikimo ypatumus;
2. Apžvelgti regioninius privatumo ir asmens duomenų apsaugos reguliavimo modelius kaip alternatyvą tarptautiniam reguliavimui;

3. Atsižvelgiant į technologines bei socialines šiandienos realijas išskirti galimas grėsmes privatumui bei asmens duomenų apsaugai dabartinio tarptautinio teisinio reguliavimo aspektu;
4. Ištirti tarptautinių teisės aktų poveikį sprendžiant šiuolaikines privatumo ir asmens duomenų apsaugos problemas bei aptarti galimas tokio reguliavimo alternatyvas ir naujos kartos reguliavimo reikalingumą privatumo ir asmens duomenų apsaugos srityje, elektroninėje erdvėje;

Hipotezė: Dėl globalių technologinių bei ekonominių veiksnių dabartinis pasaulinis privatumo bei asmens duomenų apsaugos reguliavimas nėra pakankamas, todėl būtina ieškoti naujų šios problemos sprendimo būdų bei formų.

Magistrinio darbo metodologinis pagrindas: lingvistinis (analizuojamas tarptautinių, regioninių bei nacionalinių teisės aktų nuostatų turinys), loginis (atskleidžiamos kylančios problemos, pateikiami jų sprendimo būdai), lyginamasis (analizuojami bei lyginami tarptautiniai, regioniniai bei nacionaliniai teisės aktai), sisteminės analizės metodas (atskleidžiami tyrimo objekto ir jį determinuojančių veiksnių struktūriniai ryšiai. Ši tarpusavio sąveika fiksuojama parodant sisteminį priklausomumą ir sąveikos dėsningumus).

Šiame darbe siekiama apsvarstyti įvairius asmens duomenų apsaugos reguliavimo tarptautiniu mastu variantus bei tikimasi atskleisti jų stipriąsias ir silpnąsias puses globaliame bei dinamiškame pasaulyje. Keliami klausimai dėl vienodo teisinio reguliavimo reikalingumo, atskirų valstybių ar regionų teigiamo ar neigiamo poveikio globaliam technologijų bei ekonomikos vystymuisi. Atkreipiamas dėmesys į grėsmių privatumui šaltinius bei su šios vertybės pažeidimais susijusias nusikalstamas veikas. Nagrinėjamos alternatyvos dabartinei duomenų saugai, analizuojamos privatumo reguliavimo tendencijos, ieškoma reguliavimo spragų priežasčių, pateikiami galimi probleminių klausimų sprendimo variantai.

1. TARPTAUTINIŲ TEISĖS AKTŲ, REGLAMENTUOJANČIŲ PRIVATUMĄ BEI ASMENS DUOMENŲ APSAUGĄ APŽVALGA BEI ANALIZĖ

Tarptautinis privatumo bei asmens duomenų apsaugos reguliavimas nėra gausus. Negana to, atskiros valstybės (ar regionai) vadovaujasi skirtingomis nuostatomis asmens duomenų apsaugos srityje. Požiūris į privatumą bei būtinybę jį apginti tolygiai evoliucionavo su žmonijos socialiniu, ekonominiu bei technologiniu progresu. Šiame skyriuje nebus nagrinėjamos privatumo koncepcijos ištakos. Šia tema yra parašyta pakankamai daug darbų tiek lietuvių, tiek užsienio kalbomis. Dėmesys bus kreipiamas į dabar esantį teisinį reguliavimą privatumo bei asmens duomenų apsaugos srityje.

Asmenims, kurie nėra nuodugniai susipažinę su privatumo problematika gali kilti klausimas, kodėl apie šį reiškinį aktyviai pradėta kalbėti tik prieš kelis dešimtmečius? Negi anksčiau nebuvo privatumo pažeidimo problemos? Į šiuos klausimus negalima žiūrėti vienpusiškai, norint juos tinkamai atsakyti būtina kompleksiškai nagrinėti ryšius tarp skirtingų kategorijų, juk apie privatumą bei būtinybę jį saugoti prabilo JAV teisininkai [3]Samuel Warren ir Louis Brandeis dar 1890 metais, tuo tarpu pirmasis tarptautinis dokumentas, kuriame privatumas išskiriamas kaip vertybė atsirado tik 1948 metais, t.y. beveik po 60 metų nuo to momento, kai pasirodė minėtų JAV teisininkų darbas „*The right to be left alone*“. Tuomet gali kilti kitas klausimas, gal paprasčiausiai nebuvo būtinybės spręsti asmens privatumo problemos, kadangi šiuo laikotarpiu minėtoji problema neegzistavo? Deja, realybė buvo visiškai priešinga. XX a. pirmojoje pusėje tiek Europoje, tiek kituose žemynuose klestėte klestėjo totalitariniai režimai, kurie kaip įmanydami varžė asmens laisves bei privatų gyvenimą. Tik po antrojo pasaulinio karo, vakarų Europoje įsitvirtinus demokratijoms (o kartu ir visiškai naujai vertybių sistemai) atsirado galimybė bei poreikis viešai iškelti privatumo interesą. Privatumas yra neatsiejamas nuo laisvės bei demokratinių gyvenimo principų. Būtent palaipsninis demokratijos įsigalėjimas sudarė sąlygas kitaip pažvelgti į asmens privatumą bei įteisinti jį oficialiai kaip visuotinę vertybę.

Kitas svarbus privatumo aktualizavimo aspektas buvo ir tebėra ekonomikos globalizacija bei technologijų pažangos sukurta terpė, sudaranti sąlygas greitam ir efektyviam informacijos keitimuisi. Tokioms technologijoms plintant bei tobulėjant atsirado ir poreikis teisiškai sureguliuoti šią sferą. Siekiant tai padaryti buvo priimta keletas tarptautinių teisės aktų, kurie ir bus aptariami pirmajame skyriuje. Taigi, šio skyriaus tikslas – apžvelgti tarptautinius teisės aktus, reglamentuojančius privatumą bei asmens duomenų apsaugą, bei įvertinti jų reikšmę sprendžiant privatumo problemas.

[3] The right to be left alone, 1890, http://www-swiss.ai.mit.edu/6805/articles/privacy/Privacy_brand_warr2.html [2008-05-20, 20:10]

1.1. 1948 m Visuotinės žmogaus teisių deklaracijos apžvalga bei analizė asmens privatumo aspektu

Asmens privatumas, kaip tarptautinės bendruomenės oficialiai pripažinta žmogaus teisė, atsirado visai neseniai. Sulig teisės į asmens privatumą įtvirtinimu buvo žengtas naujas žingsnis žmogaus teisių apsaugos srityje. Pats 1948 m. Visuotinės žmogaus teisių deklaracijos priėmimo laikas bei šioje deklaracijoje išdėstytos nuostatos byloja apie sunkią Europos bei viso pasaulio patirtį. Deklaracijos preambulėje skelbiama: „...žmogaus teisių nepaisymas ir niekinimas pastūmėjo vykdyti barbariškus aktus, kurie papiktino žmonijos sąžinę, ir didžiausiu paprastų žmonių siekiu buvo paskelbtas pasaulio, kuriame žmonės turi žodžio bei įsitikinimų laisvę ir yra išlaisvinti iš baimės ir skurdo, sukūrimas.“ Pasaulis visai neseniai buvo pergyvenęs vienus tamsiausių ir daugiausiai aukų pareikalavusių periodų savo istorijoje. Laikotarpis nuo 1914 iki 1945 vakarų Europoje pažymėtas baimės, nepasitikėjimo bei tironijos viešpatavimo ženklais (rytų Europoje ši situacija tęsėsi dar 50 metų). Du pasauliniai karai, kraštutinių politinių jėgų sustiprėjimas, demokratijos krizė bei didžiuliai žmogiškieji nuostoliai išvargino ne tik Europą, bet ir visą pasaulį. 1948 m Visuotinės žmogaus teisių deklaracija buvo tarsi atsvara tiems neigiamiems reiškiniams, kurie dar visai neseniai viešpatavo senajame žemyne. Ja siekta iš naujo priminti pasauliui apie pamatines vertybes bei nuostatas, kurios turėtų būti sektinos bei gerbtinos. Nors apie asmens privatumą buvo diskutuojama ir anksčiau, ši teisė 1948 m. Deklaracijoje įgyvendinta atsižvelgiant į beveik 50 metų trukusią absoliučią privataus gyvenimo kontrolę visomis prasmėmis. Nors 1948 m. Visuotinės žmogaus teisių deklaracijos 12 straipsnyje ir neišskiriamas informacinio privatumo elementas, pati privatumo koncepcija jau tampa teisinė realybe. Tokiu būdu sudaromos galimybės šios teisės plėtojimui bei aiškinimui.

1948 m Visuotinės žmogaus teisių deklaracijos 12 straipsnyje skelbiama, jog: [4]„Niekas neturi patirti savavališko kišimosi į jo privatumą, šeimos gyvenimą, buitį ar susirašinėjimą arba kėsinimosi į jo garbę ir reputaciją. Kiekvienas turi teisę į įstatymo apsaugą nuo tokio kišimosi arba kėsinimosi.“ Šiame straipsnyje naudojamas sąvokas derėtų panagrinėti atidžiau. Čia išskiriamas [5]skirtingų formų privatumas kaip vertybė, ir garbės bei reputacijos sąvokos. [6]Dabartinės lietuvių kalbos žodynas privatumą apibrėžia kaip kažką „nuosavo“, priklausančio tik konkrečiam asmeniui, o savavališką kišimąsi įvardija kaip nepageidaujamą lindimą nesilaikant taisyklių ar įstatymų. Taigi, privatumo pažeidimas šiuo atveju apibrėžiamas kaip neteisėtas, nepageidaujamas brovimasis į asmeninę erdvę. Tačiau šiame straipsnyje privatumas siejamas su dar dviem kategorijom – garbe bei reputacija. Minėtų

[4] 1948 m. Visuotinė žmogaus teisių deklaracija // Valstybės žinios, 2006-06-17, Nr. 68-2497
[5] Išskiriamas teritorinis bei komunikacinis privatumas.
[6] Internetinis Dabartinės lietuvių kalbos žodynas
http://www.autoinfa.lt/webdic/, [2008-08-24, 10:10];

sąvokų kilmė yra priešinga privatumui (vertinant socialinės kilmės aspektu). Tiek Privatumas, tiek garbė ir reputacija neabejotinai apibrėžiamos kaip vertybės, tačiau jei asmens privatumas kildinamas iš individo, tai garbė bei reputacija apibrėžiamos kaip visuomeninės kategorijos, kitaip tariant, tai visuomenės požiūrio į individą rodiklis. Šios sąvokos yra tiesiogiai susiję, kadangi teisės į privatumą pažeidimas gali įtakoti viešąją nuomonę apie asmenį bei pakenkti jo garbei bei reputacijai. Apibendrinant galima teigti, jog asmens privatumo pažeidimas 1948 m Visuotinės žmogaus teisių deklaracijos kontekste gali sąlygoti ne tik vidinį (moralinį) diskomfortą, bet ir pakeisti visuomenės požiūrį į individą bei taip daryti neigiamą įtaką jo padėčiai visuomenėje.

Pirminė deklaracijos vizija buvo ta, jog ji bus tarsi pareiškimas, kuriame išdėstyti pamatiniai žmogaus teisių principai, o šalių vyriausybės vadovausis šiomis nuostatomis kaip rekomendacinėmis gairėmis. Todėl 1948 m. Deklaracija nėra įpareigojantis tarptautinės teisės dokumentas. Nepaisant to, šis teisės aktas turi didelę įtaką ir juo remiantis daromas diplomatinis bei moralinis spaudimas šalims, kurios nesilaiko dokumente išdėstytų principų. [7]1968 Jungtinių Tautų tarptautinėje žmogaus teisių konferencijoje Teherane buvo sutarta, jog valstybės, esančios tarptautinės bendruomenės narėmis, privalo ginti bei saugoti savo piliečių teises ir laisves.

Kadangi deklaracija kaip dokumentas nėra techniškai privaloma, negali būti ir jos tiesioginių signatarių. Tačiau Visuotinė žmogaus teisių deklaracija buvo patvirtinta per Generalinės Asamblėjos atsišaukimą 1948 gruodžio 10 dieną. 48 valstybės balsavo už Deklaracijos priėmimą ir tik 8 šalys susilaikė. Balsavusiųjų prieš nebuvo. Šis įvykis laikomas triumfu, kadangi balsavime dalyvavo labai skirtingų politinių režimų atstovai, o kai kurios šalys konfliktavo tarpusavyje.

1948 m. Deklaracija – rekomendacinio pobūdžio dokumentas, nepaisant to, ji padarė didžiulę įtaką žmogaus teisių vystymuisi pasaulyje. Šis dokumentas tapo pagrindu daugybės tarptautinių sutarčių sudarymui bei tarptautinių ir nacionalinių teisės aktų priėmimui. Be to jame pirmą kartą oficialiai įtvirtinta teisė į privatumą.

1.2. Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos apžvalga ir analizė teisės į asmens privatumą aspektu;

1950 m. buvo priimta Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija, kurioje teisė į asmens privatumą įgyvendinama priverstine tvarka regioniniu lygmeniu. Teisės aktas buvo parengtas pasirašymui Romoje ir įsigaliojo 1953 m. Konvencijos pagrindu laikyta 1948 m.

[7] Proclamation of Teheran, Final Act of the International Conference on Human Rights http://www.arabhumanrights.org/publications/unconf/wchr/teheran-proclamation68e.html [2008-11-22, 16:20],

Visuotinė žmogaus teisių deklaracija. Dokumento rengėjai matė Europos Tarybos veiklos viziją per tolesnį žmogaus teisių bei laisvių principų realizavimą bei plėtojimą. Konvencija padėjo pamatus kolektyvinei žmogaus teisių [8]gynybai.

Aštuntajame Konvencijos straipsnyje apibrėžiama teisė į privatumą. Straipsnis susideda iš dviejų dalių, kiekviena iš jų siekiama skirtingų tikslų. Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos (toliau – EŽTK) 8 straipsnio pirmojoje dalyje skelbiama: [9]„Kiekvienas turi teisę į tai, kad būtų gerbiamas jo asmeninis ir jo šeimos gyvenimas, buto neliečiamybė ir susirašinėjimo slaptumas.“ Šios straipsnio dalies formuluotė iš dalies sutampa su 1948 m Visuotinės žmogaus teisių deklaracijos 12 straipsniu, tačiau, šiuo atveju, neminimas kėsinimasis į garbę bei reputaciją. EŽTK įvardijamas teritorinis bei komunikacinis privatumas, tačiau vis dar nėra nuorodos į informacinį asmens privatumą.

Antrojoje 12 straipsnio dalyje kalbama apie teisės į privatumą suvaržymo pagrindus: „Valdžios pareigūnai neturi teisės kištis į naudojimąsi šia teise, išskyrus įstatymo numatytus atvejus ir kai tai būtina demokratinėje visuomenėje valstybės saugumo, viešosios tvarkos ar šalies ekonominės gerovės interesams, siekiant užkirsti kelią teisės pažeidimams ar nusikaltimams, taip pat gyventojų sveikatai ar dorovei arba kitų žmonių teisėms ir laisvėms apsaugoti.“ Tuo pačiu valstybės, ratifikavusios Konvenciją, privalo imtis veiksmų ir apibrėžti teisės į privatumą ribojimo pagrindus. Kitaip tariant, dokumentą priėmusioms šalims yra imperatyviai nurodoma, jog jos turi įstatymais nustatyti šios teisės galiojimo apimtį bei ribas. Antrojoje 12 straipsnio dalyje nurodoma, kad tesė į privatumą nėra absoliuti ir tam tikrais atvejais gali būti ribojama. Kitas šio klausimo aspektas – santykis su kitomis asmens teisėmis. Iš to, kaip formuluojamas straipsnio tekstas, galima daryti išvadą, jog asmens privatumas yra mažesnė vertybė už viešąjį interesą ir gali būti apribotas, siekiant užtikrinti minėtojo intereso apsaugą bei gynimą. Taip pat akcentuojama nuostata, jog vieno individo teisės neturi pažeisti kito asmens teisių bei kad šių teisių užtikrinimas įmanomas tik demokratinėje visuomenėje.

Europos bendrijos kompetentingos institucijos bei Europos Žmogaus Teisių Teismas (toliau – EŽTT) nuo pat pradžių rodė didelę iniciatyvą privatumo apsaugos srityje. [10]Teismas peržiūrėjo valstybių narių nacionalinius teisės aktus ir nubaudė kai kurias už tai, kad šios tinkamai nesureguliavo valstybinių institucijų ir privačių asmenų vykdomo telefoninių pokalbių pasiklausymo. EŽTT 8 str.

[8] Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijoje numatytas mechanizmas, padedantis užtikrinti reikalavimų vykdymą tarp šalių signatarių. Šių reikalavimų vykdymo priežiūra buvo patikėta trims institucijoms: Europos žmogaus teisių komisijai (įsteigta 1954), Europos žmogaus teisių teismui (įsteigtas 1959) bei Europos tarybos ministrų komitetui.

[9] Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija // Valstybės žinios, 2000, Nr. 96-3016 (su papildomais protokolais);

[10] Mindaugas Civilka. Asmens duomenų apsauga tarptautinėje ir EB teisėje. Vilnius, 2001;

taikymo ribas išplėtė už valstybinių institucijų neteisėtų veiksmų ir pritaikė privatiems asmenims, jeigu valstybė privalėjo uždrausti tokius veiksmus. EŽTK atvertė naują puslapį privatumo apsaugos srityje, negana to, Konvencijos nuostatos tapo privalomomis, todėl jų turėjo būti paisoma Europos regione.

Šiuo metu dokumentą yra pasirašiusios bei ratifikavusios visos 47 Europos tarybos valstybės narės. Šio teisės akto pagrindu vyksta žmogaus teisių gynyba senajame žemyne. Nepaisant to, kai kurios šalys, pasirašiusios bei ratifikavusios Konvenciją ir pasižadėjusios gerbti bei ginti žmogaus teises, ne visada paiso šių įsipareigojimų. Nevyriausybinė žmogaus teisių gynimo organizacija [11]Amnesty International 2008 m. pasaulinio žmogaus teisių apsaugos būklės raporte akcentuoja vienokio ar kitokio pobūdžio pažeidimus daugumoje pasaulio valstybių, neišskiriant ir Lietuvos, tačiau ypač rimta grėsmė žmogaus teisėms kyla tokiose šalyse kaip Rusija ar Baltarusija, susirūpinimas išreikštas dėl Turkijos pozicijos kai kuriais žmogaus teisių apsaugos aspektais. Šiuo atveju Baltarusija nėra Europos tarybos narė ir nėra prisijungusi prie EŽTK, tuo tarpu Rusija bei Turkija yra ratifikavę minėtą teisės aktą, tačiau šis faktas vis vien neužkerta kelio žmogaus teisių pažeidimams dėl nenoro veikti, nesugebėjimo to daryti ar kitų aplinkybių. Šios valstybės tėra pavyzdys, kadangi su žmogaus teisių apsaugos problemomis susiduria daugmaž visos šalys. Amnesty International taip pat pažymi, jog minint 60 metų sukaktį nuo tos dienos, kai buvo priimta 1948 m Visuotinė žmogaus teisių deklaracija, vis dar yra labai daug žmogaus teisių pažeidimų pasauliniu mastu, o idėjinės Deklaracijos nuostatos toli gražu ne visada įgyvendinamos realybėje. Nepaisant to, padėtis yra geresnė nei prieš 60 metų, kai nebuvo įtakingų institucijų ar organizacijų, padedančių ginti žmogaus teises bei laisves.

1.3. 1980 m. EBPO gairių dėl privatumo apsaugos ir asmens duomenų judėjimo tarp valstybių narių apžvalga

Kaip jau minėta, 1950 m. EŽTK buvo pirmasis imperatyvaus pobūdžio dokumentas privatumo apsaugos srityje. Deja, šios Konvencijos nuostatos veikė tik Europos tarybos šalių narių teritorijoje, tuo tarpu kiti regionai (JAV, Azija, Australija) vis dar neturėjo privalomo pobūdžio privatumą reguliuojančių teisės aktų. Tiesa, Amerikos žmogaus teisių konvencijos 11 straipsnyje teisė į privatumą įtvirtinama panašiai kaip ir 1948 m. Visuotinėje žmogaus teisių deklaracijoje. 1965 m. Amerikos Valstybių Organizacija paskelbė Amerikos Žmogaus teisių ir pareigų deklaraciją, kurios devintajame bei dešimtajame straipsniuose kalbama apie teisę į privatumą, tačiau privalomojo pobūdžio privatumą apibrėžiančių teisės aktų neturėjo nei JAV nei Australija nei kiti regionai, išskyrus Europą. Situacija

[11] Amnesty International svetainė,
http://www.amnesty.org [2008-11-23];

liko nepakitusi tol, kol nebuvo pradėta kalbėti apie naują privatumo rūšį – informacinį privatumą. Asmens duomenų apsaugos įstatymai yra palyginti nauja teisinio reguliavimo sritis, atsiradusi 1970-ųjų pradžioje, susikūrus pirmiesiems duomenų bankams. Šie, dideliuose kompiuteriuose, milžiniškuose duomenų tvarkymo centruose sukaupti duomenų bankai, valdomi naudojant tam pritaikytą programinę įrangą, saugojo tiek asmeninius, tiek su darbu susijusius duomenis. Didžiausios įmonės pradėjo diegti personalo informacines sistemas, o mokesčių institucijos ir socialinio draudimo įmonės kaupė didžiulius duomenų kiekius apie piliečius. Vis pasigirsdavo nuogąstavimų, jog toks valstybės bei didelių korporacijų duomenų kontrolės monopolis gali kelti grėsmę asmenų teisėms bei laisvėms, tačiau tuo metu ekonominė duomenų kaupimo bei jų panaudojimo nauda laikinai nutildė sistemos kritikus.

Tuo tarpu valstybinės institucijos neabejotinai turėjo teisėtų interesų, susijusių su tam tikrų asmens duomenų tvarkymu, todėl buvo priimti nauji arba atitinkamai aiškinami senieji įstatymai, padedantys viešosioms administracijoms vykdyti jų užduotis. Pirmieji asmens duomenų apsaugą reglamentuojantys teisės aktai buvo priimti [12]Vokietijoje (1970 m.), vėliau sekė nacionalinis Švedijos asmens duomenų apsaugos įstatymas (1973 m.), Jungtinėse Amerikos Valstijose asmens duomenų apsaugos įstatymai buvo labiau nukreipti į tam tikrus specifinius sektorius, tačiau 1974 m. visgi buvo priimtas Asmens privatumo įstatymas, kuriame apibrėžiamas informacinis privatumas. Prancūzija asmens duomenų apsaugos sritį reglamentuojantį įstatymą priėmė 1978 m. Tačiau tarptautiniu lygiu nebuvo nei vieno dokumento, kuris apibrėžtų informacinio privatumo sąvoką. Taip pat nebuvo susitarimų, kaip elgtis su kitų valstybių piliečių asmens duomenimis ar kokios šalies įstatymus taikyti keičiantis privačia informacija tarp skirtingų šalių. Šią problemą bent iš dalies bandė išspręsti dar vienas rekomendacinio pobūdžio tarptautinis dokumentas, kuris buvo priimtas 1980 m. Ekonominio bendradarbiavimo ir plėtros organizacijos (toliau - EBPO) iniciatyva. 1980 m. EBPO gairės dėl privatumo apsaugos ir asmens duomenų judėjimo tarp valstybių narių atspindi neoficialų tarptautinį susitarimą dėl asmens duomenų apsaugos principų. Šis dokumentas stipriai įtakojo asmens duomenų apsaugos reguliavimą tarptautiniu lygiu. Gairėse akcentuojama, jog skirtingas asmens duomenų apsaugos reglamentavimas gali užkirsti kelią laisvam šių duomenų judėjimui tarp valstybių, o tai sukeltų trikdžius svarbiuose ekonominiuose sektoriuose, tokiuose kaip bankininkystė ar draudimo paslaugų sektorius.

[12] World Legal Information Institute svetainė, http://www.worldlii.org/int/journals/EPICPrivHR/2006/PHR2006-The-2.html#fn38 [2008-07-22, 20:30];

[13]1980 m. EBPO gairės apibrėžia, kas yra duomenų valdytojas, asmens duomenys bei tarptautiniai duomenų srautai. Duomenų valdytoju laikoma šalis, kuri pagal nacionalinės teisės aktus yra kompetentinga priimti sprendimą dėl automatizuotos duomenų rinkmenos paskirties, kokie asmens duomenys turėtų būti saugomi ir kaip jie turėtų būti tvarkomi. Asmens duomenimis laikoma bet kokia informacija, susijusi su identifikuotu ar identifikuotinu individu (asmens duomenų subjektu). Tarptautiniai asmens duomenų srautai apibrėžiami kaip asmens duomenų judėjimas tarp valstybių.

Nepaisant to, jog 1980 m. EBPO gairės dėl privatumo apsaugos ir asmens duomenų judėjimo tarp valstybių narių yra deklaratyvaus pobūdžio dokumentas, jo reikšmė formuojant privatumo bei asmens duomenų apsaugos teisinę bazę yra nenuginčijama. Dokumente suformuluoti pagrindiniai asmens duomenų apsaugos principai išlaikė laiko išbandymus bei nustatė minimalius asmens duomenų apsaugos standartus, kuriais vadovaujasi šalys, nesusaistytos privalomo pobūdžio tarptautiniais susitarimais. Šie principai yra:

- Duomenų rinkimo ribojimas – rinkti duomenis galima tik vadovaujantis įstatymais bei su asmens duomenų subjekto sutikimu;
- Duomenų kokybė – duomenys turi būti tikslūs, surinkti tik griežtai apibrėžtais tikslais bei nuolat atnaujinami jei tai būtina;
- Tikslo nurodymas – asmens duomenų rinkimo tikslai turi būti aiškiai nurodyti bei apibrėžti nuo pat jų rinkimo pradžios;
- Asmens duomenų naudojimo apribojimas – duomenys gali būti naudojami tik tuo tikslu, kuriuo yra surinkti;
- Apsaugos principas – duomenys turi būti renkami bei laikomi saugiai, siekiant išvengti šios informacijos vagysčių, praradimo ar pakeitimo;
- Atvirumo principas – Duomenų naudojimo tikslas bei jų naudojimo politika turi būti atvira asmens duomenų subjektui;
- Individualus dalyvavimas – asmens duomenų subjektas turi turėti teisę susipažinti bei turėti priėjimą prie savo asmens duomenų;
- Atskaitomybės principas – duomenų valdytojai bei tvarkytojai turi laikytis aukščiau nurodytų principų;

Principai puikiai išlaikė laiko išbandymus ir buvo atspindėti keliuose tarptautinio pobūdžio dokumentuose, tokiuose kaip 1981 m. Konvencijoje dėl asmenų apsaugos ryšium su asmens duomenų

[13] 1980 m. EBPO gairės, http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html [2008-07-23, 15:30];

automatizuotu tvarkymu bei 1990 m. Jungtinių Tautų kompiuterizuotų asmens duomenų bylų gairėse. JT Generalinė asamblėja pabrėžė, jog šalys rengdamos nacionalinius teisės aktus privatumo bei asmens duomenų apsaugos srityje turėtų atsižvelgti į minėtuosius principus, tačiau jų įgyvendinimas buvo paliktas valstybių valioje. [14]Gairės turi ypač didelę reikšmę pasauliniu mastu, kadangi Australijoje, Naujojoje Zelandijoje, Azijos šalyse, Kanadoje ir kitose valstybėse, šis dokumentas įtakojo asmens duomenų apsaugos įstatymų atsiradimą bei suderinimą su EBPO bendraisiais asmens duomenų apsaugos principais.

Aštuntajame – devintajame XX a. dešimtmetyje asmens duomenų apsaugą užtikrino pakankamai dideli informacijos perdavimo kaštai, tačiau atsiradus globaliam informaciniam tinklui keitimasis duomenimis tapo itin pigus bei paprastas. Nepaisant to, 1998 m. vykusioje EBPO ministrų konferencijoje buvo pripažinta, jog 1980 m. gairių nuostatos bei principai ir toliau taikomi kaip bendras susitarimas, reguliuojantis asmens duomenų apsaugą tarptautiniu lygiu. Taip pat pastebėta, jog tuometinės nuostatos šiuolaikinių technologijų kontekste yra labiau deklaratyvaus pobūdžio ir jokios reikšmingos įtakos neturi. Šiuo metu technologija yra gerokai pažengusi į priekį lyginant su 1998 m. Internetas, tinklinės bei telekomunikacinės technologijos tampa neatsiejama kasdieninio gyvenimo dalimi. Tinkle juda didžiuliai duomenų srautai. Atsiradę nauji internetinių svetainių formatai (socialiniai tinklai, video peržiūros tinklapiai ir pan.) dar labiau paspartina keitimosi duomenimis tempą bei mastą. Pavyzdžiui, 2006 m. į video peržiūros tinklapį *www.youtube.com* buvo įkeliama vidutiniškai 15 milijonų filmų per dieną, tačiau 2008 m. šis skaičius jau siekė 40 milijonų ir nuolat [15]augo. 1980 m. net nebuvo galima numatyti tokio technologinių pokyčių masto, nekalbant apie teisines problemas atsirandančias dėl minėtų veiksnių. Todėl nauji reiškiniai, atsiradę sulig informacinių technologijų vystymusi, reguliuojami pagal senus standartus ne todėl, kad jų universalumas visiškai atitinka šiandienos realijas, o todėl, kad paprasčiausiai nėra rimtos alternatyvos tokiam teisiniam reguliavimui.

1.4. 1981 m. Konvencijos dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu apžvalga

1980 m. EBPO gairių principai buvo perkelti į pagrindinį tarptautinio pobūdžio privalomąjį teisės aktą – 1981 m. Strasbūro konvenciją dėl asmenų apsaugos ryšium su asmens duomenų

[14] Lee A. Bygrave. Privacy Protection in a Global Context – A Comparative Overview // Published in Scandinavian Studies in Law, 2004, vol. 47, p. 319–348

[15] Kaip pastebi vienas belgų žiniatinklininkas (*blogger*) , jei vieno filmuko trukmė yra vidutiniškai 2-3 minutės, tai per dieną įkeliamos informacijos peržiūrėjimas užtruktų 100 milijonų minučių, arba 19 metų. http://blog.forret.com/2006/05/youtube-bandwidth-terabytes-per-day [2008-11-23];

automatizuotu tvarkymu. Šiame dokumente asmens duomenų apsauga išskiriama kaip atskira kategorija, kaip privatumo dalis ir vertybė, kurią būtina ginti naujų technologijų priešaušryje. Konvencijos preambulėje kalbama apie tai, jog: [16]„...pageidautina garantuoti kiekvieno žmogaus teises ir pagrindines laisves, o svarbiausia, teisę į privatų gyvenimą, atsižvelgiant į didėjantį automatizuotai tvarkomų asmens duomenų srautą, kuris kerta sienas“. Strasbūro konvencijoje dar kartą pabrėžiama būtinybė ginti teisę į privataus gyvenimo neliečiamumą. Šiuo atveju kalbama apie asmens duomenis – informacinio privatumo elementą – ir jų apsaugą. Ši privatumo forma nebuvo minima nei 1948 m. Visuotinėje žmogaus teisių deklaracijoje, nei EŽTK. Pokyčiai, lėmę būtent tokios krypties privatumo gynimo poreikį, šioje srityje atsirado dėl technologijų pažangos ir naujų techninių galimybių, kurių pagalba buvo galima valdyti didelius asmens duomenų srautus, juos tvarkyti bei perduoti nepaisant valstybių teritorijos ribojimo. 1981 m . Strasbūro konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu priskiriama pirmosios kartos teisės aktams, reguliuojantiems privatumą bei asmens duomenų apsaugą tarptautiniu lygiu. Asmens duomenų apsaugos svarbos iškilimas nėra atsitiktinis. Dar 1950 m., kai buvo priimta EŽTK, asmens duomenų tvarkytojų bei naudotojų ratas buvo siauras, aiškiai apibrėžtas, o patys duomenys nebuvo glaudžiai susieti tarpusavyje. Pagrindinis duomenų tvarkytojas buvo valstybė, o duomenys buvo dažniausiai kaupiami kaip įvairių registrų informacija., be to, tokių duomenų apdorojimas bei tvarkymas nebuvo automatizuotas, todėl reikalavo didelių laiko bei finansinių sąnaudų. Tuo metu didžioji dalis demokratinių valstybių piliečių nemanė, jog jų teisė į asmeninį informacinį privatumą yra labiau pažeidžiama, nei teisė į fizinį ar komunikacijos privatumą. Situaciją iš esmės pakeitė informacinės revoliucijos pradžioje (septintas – aštuntas XX a. dešimtmetis) atsiradusi galimybė tvarkyti asmens duomenis automatiniu būdu, bei perkelti juos iš vienos vietos į kitą mažomis laiko ir investicijų sąnaudomis. Prasidedanti kompiuterių naudojimo era privertė pasaulį atkreipti dėmesį į naujas grėsmes asmens duomenų saugumui. Tačiau pirmosios kartos teisės aktais, reglamentuojančiais privatumą bei asmens duomenų apsaugą, buvo siekiama apsaugoti asmens duomenų subjektus ne nuo kitų subjektų neteisėto pasinaudojimo jų asmens duomenimis, bet nuo pačios valstybės per didelio kišimosi į privatų gyvenimą. XX a. aštuntajame – devintajame dešimtmetyje kompiuterius turėjo retas namų ūkis. Juos pagrinde naudojo valstybės institucijos bei verslininkai. Atsiradus galimybei tvarkyti duomenis automatizuotai bei pagerėjus duomenų suderinamumui buvo baiminamasi, jog valstybė sukaups

[16] 1981 m. Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu, Pagrindinės Europos Tarybos sutartys. - Vilnius: Europos Tarybos informacijos ir dokumentacijos centras, 2000;

didžiulius kiekius asmeninio pobūdžio informacijos apie savo piliečius ir įgis viršenybę jų atžvilgiu. Šis nuogąstavimas nebuvo nepagrįstas. Patogumo tikslais vis daugiau valstybių įvairių registrų duomenis laikydavo vienoje vietoje. Šie duomenys buvo tarpusavyje suderinti, todėl atskleisti duomenų subjekto tapatybę nebuvo sudėtinga. Kita vertus, nebuvo norima per griežtais ribojimais stabdyti elektroninių technologijų vystymosi bei neigiamai įtakoti verslo sektoriaus. Ši situacija ir sudarė terpę naujam tarptautiniam teisės aktui, reglamentuojančiam teisę į informacinį privatumą (asmens duomenų apsaugą), atsirasti.

1981 m. Strasbūro konvencijos 2 straipsnyje apibrėžiamos asmens duomenų, asmens duomenų automatizuoto tvarkymo, duomenų valdytojo sąvokos. Asmens duomenų bei duomenų valdytojo sąvokos iš esmės atkartoja apibrėžtąsias 1980 EBPO gairėse. Automatizuotas tvarkymas Strasbūro konvencijoje apibrėžiamas kaip: „visiškai arba iš dalies atliekamos operacijos šiomis automatinėmis priemonėmis: duomenų saugojimas, loginės ir (arba) aritmetinės operacijos, jų keitimas, ištrynimas, paieška arba platinimas.“ Taigi, buvo apibrėžti pagrindiniai veiksmai,atliekami su asmens duomenimis. Tokiu būdu buvo konkretizuota teisės taikymo sritis asmens duomenims kaip visumai. Kalbant apie asmens duomenų apsaugos spektro išplėtimą dera paminėti 3 Konvencijos straipsnio 2 dalies „b“ ir „c“ punktus. B punktu valstybės, ratifikavusios Konvenciją, įsipareigoja jos nuostatas taikyti ir informacijai apie asmenų grupes, asociacijas, fondus, bendroves, korporacijas ir kitas institucijas, kurios tiesiogiai ar netiesiogiai sudarytos iš asmenų, nepaisant to, ar šie asmenys turi juridinį statusą, ar ne. 3 straipsnio 2 dalies c punkte skelbiama, jog Strasbūro konvencijos nuostatas būtina taikyti ir toms asmens duomenų rinkmenoms, kurios nėra apdorojamos automatizuotai. Tokiu būdu išplečiama teisės taikymo sritis asmens duomenų apsaugos atžvilgiu. Šis punktas įtvirtina apsaugą tokiems asmeninio pobūdžio duomenims, kurie nėra tvarkomi automatizuotai (pvz.: asmeninei informacijai bibliotekų kortelėse).

Antrajame Strasbūro konvencijos skyriuje išskiriami principai taikytini asmens duomenis. Dalis jų taip pat sutampa su 1980 m. EBPO gairėse išdėstytais asmens duomenų apsaugos principais. Tačiau papildomai atsiranda straipsnis, apibrėžiantis ypatingų duomenų sąvoką. Šiems duomenims suteikiama išskirtinė svarba. Dokumentas aiškiai pabrėžia draudimą tvarkyti ypatingus duomenis automatizuotai, jei jiems nėra taikomos papildomos apsaugos garantijos. Ši nuostata į Konvenciją įtraukta atsižvelgiant į tokių duomenų pobūdį, nes šio tipo asmeninio pobūdžio informacija yra „jautresnė“. [17]Jos

[17] Nutekėjus jautriai informacijai apie asmens teistumą, religiją, seksualinę orientaciją ir pan. gali kilti neigiamų padarinių, susijusių su darbo praradimu (darbdavys atleidžia darbuotoją sužinojęs apie jo teistumą), garbės ar reputacijos sumenkinimu, socialiniais konfliktais (įžeidžiantis ar smerkiantis elgesys su kitatikiais vienos dominuojančios religinės grupės aplinkoje). Asmeniui gali kilti socialinės izoliacijos, neapykantos kurstymo aktų grėsmė. 1997 m. Didžiojoje Britanijoje priėmus Seksualinių pažeidėjų įstatymą (Sex Offenders Act 1997, Sexual Offences Act 2003), asmenims, padariusiems seksualinio pobūdžio nusikaltimą ir atlikusiems bausmę būtina nuolat registruotis policijos įstaigoje, informuoti apie savo judėjimą ar planus keisti vardą, pavardę. Šio reikalavimo nepaisymas užtraukia baudžiamąją

atskleidimas trečiosioms šalims gali turėti didesnių neigiamų pasekmių asmens duomenų subjektui nei paprastos asmeninio pobūdžio informacijos atskleidimas.

Aštuntajame Konvencijos straipsnyje kalbama apie papildomas duomenų subjektų garantijas bei numatoma teisė gauti informaciją apie duomenų tvarkytoją, duomenų tvarkymo tikslą bei pobūdį. Remiantis Konvencija, duomenų valdytojai bei tvarkytojai yra savotiškai atskaitingi duomenų subjektui ir privalo informuoti asmenį ne tik apie duomenų subjekto privačius duomenis, bet ir atskleisti savo tapatybę bei disponavimo duomenimis tikslus. Šia nuostata siekiama subalansuoti duomenų subjekto bei duomenų valdytojo ar tvarkytojo teises, kadangi jie nėra lygiateisiai savaime. Duomenų tvarkytojas (valdytojas) turi daugiau galimybių pakenkti asmeniui netinkamai atlikdamas operacijas su jo duomenimis. Šiuo atveju duomenų subjektas yra silpnesnioji šalis ir todėl, kad [18]duomenų praradimo, iškraipymo ar sunaikinimo atveju didžiausią žalą patirs būtent tas asmuo, kurio duomenimis buvo disponuojama. Tuo tarpu duomenų tvarkytojui ar valdytojui šis praradimas gali būti menkavertis, ypač jei duomenų bazėje konkretaus individo duomenų praradimas neturi didelės įtakos tinkamam duomenų tvarkymo tikslų įgyvendinimui. Tiesa, Konvencijoje siekiama apsaugoti ne tik duomenų subjekto, bet ir duomenų valdytojo ar tvarkytojo interesus. Kad duomenų subjektas nepiktnaudžiautų teise gauti informaciją apie asmens duomenų tvarkymą, turi būti nustatyti tam tikri laiko intervalai, po kurių vėl leidžiama teikti užklausas iš duomenų subjekto pusės. Konvencijoje taip pat pabrėžiama teisė į neteisingų duomenų koregavimą ar ištrynimą duomenų subjekto iniciatyva, o šio prašymo nevykdant, numatytas skundo institutas.

Strasbūro konvencija numato teisių į privatumą ribojimo pagrindus, tačiau šie ribojimai turi būti išimtiniai bei taikomi tada, kai tokie atvejai nurodomi nacionaliniuose teisės aktuose ir yra būtina demokratinės visuomenės priemonė, kuri:

- saugo valstybės saugumą, visuomenės saugumą, valstybės finansinius interesus arba siekia stabdyti nusikalstamumą;
- apsaugo duomenų subjektą arba kitų asmenų teises ir laisves;

---

atsakomybę. Tuo tarpu JAV ši asmens privatumą ribojanti norma, kitaip dar vadinama „Megan's law“ taikoma siekiant registruoti už pedofiliją teistų asmenų buvimo vietą, rinkti jų asmens duomenis, atvaizdus ir pan. Yra netgi oficialios valstijų seksualinių nusikaltėlių registrų svetainės, kuriose galima rasti ne tik už tokio pobūdžio nusikaltimus teistų asmenų vardus, pavardes, buvimo vietą, bet ir jų nuotraukas. Tokios sistemos kritikai atkreipia dėmesį, kad pagal minėtuosius įstatymus (Didžiojoje Britanijoje) asmenų ratas, privalantis registruotis yra labai platus ir į jį patenka per daug asmenų (įskaitant nepilnamečius). Šiuo klausimu nėra vieningos nuomonės, kadangi viena prieš kitą statomos dvi vertybės: visuomenės saugumas bei sveikata prieš asmens teisę į privatumą ir šių vertybių santykį (apribojimus) sprendžia kiekviena šalis atskirai.

[18] Pavyzdžiui: išnykus medicinos įrašų duomenims asmuo gali negauti tinkamo gydymo ar nutekėjus duomenims į internetą duomenų subjektas gauna brukalų į savo elektroninio pašto dėžutę, o tai kenkia jo verslui.

Taigi, dokumentas numato, jog tam tikros išlygos visgi įmanomos. Nors valstybės, ratifikavusios Konvenciją, negali išbraukti 5, 6 arba 8 straipsnio, jos visgi gali jo netaikyti. Svarbi netaikymo sąlyga yra ta, jog bendroje Konvencijos normų taikymo praktikoje tai būtų traktuojama kaip išimtis, o ne kaip taisyklė bei šia išimties galimybe būtų naudojamasi tik siekiant apginti kitus, svarbesnius valstybės interesus. Remiantis antrąja devintojo straipsnio dalimi galima teigti, jog Konvencijos tekste netiesiogiai nurodoma vertybinė asmens privatumo vieta santykyje su kitomis šalies vertybėmis. Šiuo atveju kaip aukštesnis gėris yra įvardijamas valstybės (kaip politinio, teritorinio, socialinio darinio) saugumas, taip pat visuomenės saugumas. Visuomenę galima būtų apibrėžti kaip išskirtinį bei valstybei gyvybiškai svarbų darinį, be kurio jos teritoriniai bei politiniai elementai netenka [19]prasmės. Vėliau išskiriami finansiniai valstybės interesai (valstybės finansų sistema yra viena kertinių siekiant užtikrinti normalų šalies funkcionavimą, prekių bei paslaugų apyvartą ir efektyvią šalies kontrolę bei valdymą). Paskutinė galimų teisių į privatumą apribojimų priežastis - nusikalstamumo stabdymas. Nuo anksčiau minėtų kategorijų ši skiriasi tuo, jog yra ne interesas, o reiškinys, galintis pakenkti aukščiau nurodytiems teisiniams gėriams. Kitaip tariant, nusikalstamumas gali turėti neigiamos įtakos tiek valstybės bei visuomenės saugumui tiek finansiniams jos interesams. Taip pat, minėtųjų teisių ribojimai išimtys gali būti taikomi pačio duomenų subjekto saugumui užtikrinti, o taip pat, kai iškyla pavojus, jog bus pažeistos [20]trečiųjų asmenų teisės bei laisvės.

Tarptautinės teisės požiūriu svarbus duomenų statusas jiems keliaujant iš vienos valstybės į kitą, t.y., kokie reikalavimai keliami šalims gaunančioms bei teikiančioms asmens duomenis siekiant apsaugoti duomenų subjektų privačią informaciją. Trečiojo 1981 m. Strasbūro konvencijos skyriaus nuostatos taikomos asmens duomenims, kurie automatiškai tvarkomi ar renkami siekiant juos automatizuotai tvarkyti, bei perduoti bet kuriuo būdu per valstybines sienas. Skyriuje išdėstyta nuostata, jog vienintelis šalies tikslas stebint bei kontroliuojant duomenų srautus tarp valstybių turėtų būti duomenų subjekto privatumo apsauga. Jokie kiti papildomi reikalavimai nekeliami.

Pati 1981 m. Strasbūro konvencija buvo atsakas į sparčiai plintantį bei technologinio progreso pagimdytą automatizuotą duomenų rinkimą bei tvarkymą. Perteklinis duomenų srautų tarp valstybių suvaržymas galėjo neigiamai atsiliepti ne tik šalims atskirai, bet ir viso pasaulio ekonomikai, kadangi pramoninės, intelektualinės bei informacinės globalizacijos era jau buvo prasidėjusi. Pirmiausiai būtų

[19] "Tauta yra pirminis valstybės elementas. Jei nėra su valstybe susijusios žmonių bendrijos, nebus ir valstybės. Valstybės valdžią galima įgyvendinti tik žmonių bendruomenėje."
Toma Birmontienė, Egidijus Jarašiūnas, Egidijus Kūris ir k.t. Lietuvos konstitucinė teisė. Vilnius: : Lietuvos teisės universiteto Leidybos centras, 2002. P. 486.;

[20] Pavyzdys – ypatingi asmens duomenys apie žmogaus sveikatą gali būti atskleisti tada, jei asmuo serga užkrečiama liga ir yra tikimybė, kad jis gali ligą platinti (sąmoningai arba ne). Siekiant išvengti pavojaus visuomenės narių sveikatai, galimas tokio asmens ypatingų duomenų atskleidimas.

nukentėjęs finansų sektorius, kadangi būtent šioje srityje reikalingas dažnas bei operatyvus keitimasis duomenimis tarp skirtingų valstybių. Per griežtas reguliavimas būtų neigiamai paveikęs ir technologinį progresą, kadangi išaugus duomenų apsikeitimo kaštams būtų kuriama bei diegiama mažiau inovatyvių technologijų, o investicijos šioje srityje būtų gerokai kuklesnės. Todėl Konvencijos rengėjų liberalesnis požiūris į duomenų srautų kontrolę pasiteisino ir suteikė galimybę suderinti dviejų skirtingų grupių interesus.

Tačiau 1981 m. Strasbūro konvencijos galiojimas Europos mastu nėra toks visa apimantis kaip kad EŽTK, kurią pasirašė bei ratifikavo visos Europos tarybos narės. Tokios šalys kaip Armėnija, Azerbaidžanas ar San Marinas apskritai nėra pasirašę Konvencijos, tuo tarpu Monakas, Rusija, Turkija bei Ukraina šio dokumento nėra ratifikavusios. Turkija buvo pasižadėjusi priimti asmens duomenų apsaugos įstatymus dar iki 2004 m., tačiau įstatymo projektas įstrigo. Šioje šalyje apie privatumą kalbama Turkijos Konstitucijos [21]20 straipsnyje bei [22]22 straipsnyje. Užuominų apie teisės į privatumą gynybą yra šios šalies civiliniame bei baudžiamajame kodeksuose. Nepaisant to, privatumas Turkijoje nėra deramai [23]apsaugotas.Tuo tarpu Rusija, kuri yra viena iš pirmaujančių valstybių pagal elektroninių nusikaltimų padarymo skaičių, jau yra priėmusi privatumą saugantį [24]įstatymą. Teisę į privatumą taip pat užtikrina šios šalies Konstitucijos 23, 24 ir 25 straipsniai , tačiau problemos asmens duomenų apsaugos srityje išlieka vienomis iš pagrindinių informacinių technologijų kontekste.

1981 m. Strasbūro konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu buvo savalaikis bei pažangus dokumentas, privaloma tvarka įtvirtinantis teisę į privatumo apsaugą Europos regione. Tačiau tai, jog technologijos, į kurias buvo atsižvelgiama kuriant šį teisės aktą, gerokai patobulėjo bei pasikeitė, o taip pat faktas, jog ne visos Europos Tarybos narės prisijungė prie Konvencijos, leidžia teigti, jog ši reguliavimo forma turi spragų, kurių panaikinimo galimybes derėtų panagrinėti atidžiau.

[21] „Kiekvienas turi teisę reikalauti pagarbos savo ir savo šeimos privačiam gyvenimui. Privatus individo bei jo šeimos gyvenimas negali būti pažeidžiamas.“

[22] “Komunikavimui negali būti trukdoma, o jo slaptumas negali būti pažeidžiamas, nebent egzistuoja teisėjo sprendimas, paremtas teisės normomis arba egzistuoja įstatymu įpareigotos įstaigos sprendimas tais atvejais, kai delsimas atlikti veiksmus gali būti žalingas teisei.“

[23] Internetinio tinklapio www.privacyinternational.org teigimu, Turkijoje dažni nesankcionuoto pokalbių įrašinėjimo ar pasiklausymo atvejai.
http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-83783 [2008-11-24];

[24] Федеральный закон Российской Федерации Об информации, информационных технологиях и о защите информации // Росийская газета (oficialus valstybinis leidinys). 2006 liepos 27 d.,. Nr. 149-ФЗ

1.5. 1990 m. Jungtinių Tautų Ekonominių ir Socialinių reikalų Tarybos Kompiuterizuotų asmens duomenų bylų gairių apžvalga

1990 m. gruodžio 14 dieną JT Generalinės asamblėja priėmė rezoliuciją 45/95, kurioje buvo išdėstyti pagrindiniai principai dėl kompiuterizuotų asmens duomenų bylų. 1990 m. JT Ekonominių ir Socialinių reikalų Tarybos Kompiuterizuotų asmens duomenų bylų gairės iš esmės atkartoja visus principus, suformuluotus 1980 m. EBPO gairėse dėl privatumo apsaugos ir asmens duomenų judėjimo tarp valstybių narių. Nuo EBPO gairių šis dokumentas skiriasi tuo, jog jame kalbama ir apie ypatingus asmens duomenis, o tiksliau apie jų kaupimo ribojimus. JT gairėse taip pat numatoma teisių į privatumą ribojimo galimybė jeigu reikia užtikrinti nacionalinį saugumą, viešąją tvarką, visuomenės sveikatą ar moralę ar siekiant kitų asmenų teisių užtikrinimo. Gairių kūrėjai atkreipia dėmesį į tuo metu buvusią padėtį asmens duomenų apsaugos srityje ir skatina valstybes įtraukti gairių nuostatas į nacionalinės teisės normas taip prisidedant prie žmogaus teisių gynimo bei stiprinimo.

Šiame dokumente savu laiku buvo surinktos pažangiausios tuo metu jau buvusių tarptautinių teisės aktų idėjos bei principai. Tokiu būdu tarptautinei bendruomenei buvo priminta žmogaus teisių apsaugos svarba labiausiai akcentuojant teisę į informacinį privatumą. Tuo tarpu tais pačiais 1990 m. prasidėjo diskusijos Europos regione dėl visai kitokio, naujo pobūdžio asmens duomenų apsaugos užtikrinimo. Šių diskusijų bei svarstymų rezultatas - Europos Parlamento ir Tarybos direktyva dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo.

1.6. Skyriaus apibendrinimas

Technologijų pažanga bei naujų teisinių reiškinių atskleidimas ir įtvirtinimas sudarė sąlygas keisti požiūrį į privatumą bei asmens duomenų apsaugą. XIX a. sąvoka „privatumas“ tebuvo kelių teisininkų svarstymo objektas, o iki XX a. antros pusės apie privatumo gynimą totalitarinių režimų pavėsyje negalėjo būti nei kalbos. Tik iš naujo „pertvarkius“ pasaulį, bei daug kur įsivyravus demokratiniams režimams atsirado galimybė ginti šią teisę. Visuotinės žmogaus teisių deklaracijos priėmimas bei pamatinių žmonijos vertybių bei principų iškėlimas atvertė naują puslapį pasaulio istorijoje. Čia buvo įtvirtinta teisė į privatumą ir nors dokumentas tebuvo rekomendacinio pobūdžio, jo reikšmė yra didžiulė. EŽTK Visuotinės žmogaus teisių deklaracijos principai įtvirtinami bei tampa privalomi valstybėms, prisijungusioms prie šio dokumento. Minėtame teisės akte taip pat išskiriama teisė į privatumą, tačiau nieko nekalbama apie asmens duomenų apsaugą. 1980 m. EBPO gairėse dėl privatumo apsaugos ir asmens duomenų judėjimo tarp valstybių narių informacinis privatumas buvo

išskirtas iš kitų, taip pat pirmą kartą buvo suformuluoti bei įtvirtinti asmens duomenų apsaugą užtikrinantys bendrieji principai. Nepaisant rekomendacinio gairių pobūdžio, laikas parodė, jog tai bene vienintelis plataus veikimo tarptautinis dokumentas, kuriuo vadovaujamasi keičiantis bei renkant asmens duomenis visame pasaulyje. Europos taryba nusprendė privaloma tvarka įtvirtintini minėtuosius principus asmens duomenų apsaugos atžvilgiu ir 1981 m. Strasbūre priėmė Konvenciją dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu. Šią Konvenciją, priešingai nei EŽTK, pasirašė ne visos Europos tarybos narės, o kai kurios pasirašiusios šio dokumento dar neratifikavo, taip iškeldamos klausimą ar privatumo apsauga išties yra pakankamai veiksminga. 1990 m. JT Ekonominių ir Socialinių reikalų Tarybos Kompiuterizuotų asmens duomenų bylų gairės iš esmės atkartoja 1980 m. EBPO gairių principus labiau akcentuojant ypatingų asmens duomenų svarbą. Tačiau nepaisant anksčiau minėtų dokumentų, asmens duomenų apsauga pasauliniu mastu vis dar nėra tinkamai įgyvendinta, kadangi technologijos, kurių pagrindu buvo kuriami teisės aktai, stipriai pasikeitė ir tai kas laikytina „universaliais principais“ 1990 m., šuo metu gali neatitikti teisinės bei techninės realybės. Globalizacija, „sienų išnykimas“ tarp valstybių elektroninėje erdvėje bei galimybė vykdyti asmens duomenų persiuntimo operacijas realiu laiku mažomis kapitalo sąnaudomis įvedė daugiau neaiškumo asmens duomenų apsaugos srityje. Apibendrinant šį skyrių, galima teigti jog:

- Teisės į privatumą pripažinimui bei vystymuisi didžiulę įtaką turėjo istorinės epochos aplinkybės, technologijų pažanga bei teisinio reguliavimo trūkumas šioje srityje;
- Visuotinė žmogaus teisių deklaracija bei Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija įtvirtina teisę į privatumą jo nedetalizuojant;
- 1980 m. EBPO gairėse dėl privatumo apsaugos ir asmens duomenų judėjimo tarp valstybių narių išskiriamas informacinis privatumas bei pirmą kartą pasaulio istorijoje nustatomi bendrieji asmens duomenų apsaugos principai. 1981 m. Strasbūro Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu įtvirtina šiuos principus privalomai tarp didžiosios dalies Europos Tarybos narių bei atkreipia dėmesį į ypatingus asmens duomenis, o 1990 m. JT Ekonominių ir Socialinių reikalų Tarybos Kompiuterizuotų asmens duomenų bylų gairės iš esmės atkartoja 1980 m. EBPO gairių principus bei papildomai akcentuoja ypatingų duomenų apsaugą;
- Informacinio privatumo teisės aktai reguliuoja dabartinius teisinius santykius, nors jų priėmimo metu reguliavimo specifika skyrėsi nuo dabartinės, o patys dokumentai, nors ir laikomi universaliais, nėra visapusiški.

2. REGIONINIAI PRIVATUMO BEI ASMENS DUOMENŲ APSAUGOS REGULIAVIMO MODELIAI KAIP ALTERNATYVA PASAULINIAM REGULIAVIMUI

Šiandienos pasaulis – sudėtingas multikulūrinis darinys, kuriame visi elementai yra labai skirtingi, bet neatsiejami vienas nuo kito. Globalizacija bei informacinė revoliucija prisidėjo prie valstybinių sienų „tirpimo“ informacinių technologijų kontekste. Globalios ekonomikos sąlygomis visa pasaulio prekyba bei finansų sistema yra susaistyta tarpusavyje ir pažeidžiama tarsi domino kaladėlių eilė. Neigiami ar teigiami procesai vienos arba kitos „stambiosios ekonomikos žaidėjos“ viduje tuoj pat aidu nuvilnija per pasaulį ir taip įtakoja globalias [25]rinkas. Tinklinių technologijų pagalba keitimasis asmens duomenimis tapo itin spartus, pigus bei kokybiškas. Kelių dešimtmečių pasaulinės konvencijos be rekomendacijos, apibrėžiančios privatumą kaip saugotiną vertybę naujųjų technologijų akivaizdoje, tampa vis labiau deklaratyvios. Kiekviena valstybė ar regionas pirmiausiai stengiasi apginti savo interesus ir tam pasitelkia įvairių priemonių, padedančių tuos tikslus įgyvendinti, arsenalą. Galiausiai naudojamų metodų visuma formuoja ir pačios valstybės (regiono) principinius įpročius bei skirtingą požiūrį į tuos pačius dalykus. Taip nutiko ir privatumo bei asmens duomenų apsaugos srityje. Negana to, jog ne visos šalys apskritai pripažįsta teisę į asmens privataus gyvenimo neliečiamumą, atskiros valstybės ar regionai, sutinkantys, jog privatumą būtina gerbti bei saugoti, taiko skirtingas teisines nuostatas identiškiems teisiniams reiškiniams reguliuoti. Šiame skyriuje kalbama ne apie tai, kuris reguliavimo modelis yra „geras“ arba „blogas“ (visi jie turi savų privalumų bei trūkumų), šiuo atveju tiesiog bandoma apžvelgti pagrindinius regioninio reguliavimo modelius bei jų įtaką pasauliniam privatumo bei asmens duomenų apsaugos reguliavimui.

2.1. Regioninis asmens duomenų apsaugos reguliavimas, bei jo įtaka formuojant pasaulinę privatumo bei asmens duomenų apsaugos politiką;

Per beveik 30 metų nuo 1980 m. EBPO gairių dėl privatumo apsaugos ir asmens duomenų judėjimo tarp valstybių narių priėmimo nebuvo priimta nei vieno solidaus bei novatoriško teisinio

[25] Globalizacijos sąlygomis prekių, paslaugų bei kapitalo apykaita yra dinamiška bei tarpusavyje susieta. Pavyzdžiui, JAV kompanija gamina prietaisų mikroschemas Kinijoje (dėl pigesnės darbo jėgos), o galutinį gaminį pardavinėja Europos rinkoje. Bent vienam iš šio ciklo elementų pradėjus „šlubuoti“ akimirksniu nukenčia ir likę subjektai. 2008 m. JAV prasidėjusi finansų krizė vos per kelias savaites išplito po visą pasaulį paskui save sukeldama ekonomikos nuosmukį. Globalios ekonomikos pranašumas tas, kad ji yra lanksti, sugebanti greitai reaguoti į pokyčius bei orientuota į konkurencingų produktų kūrimą prieinama kaina. Tačiau šios sistemos minusas, kad jos griūties atveju yra paveikiamos visos proceso dalyvės.

dokumento, reglamentuojančio privatumo bei asmens duomenų apsaugą tarptautiniu lygiu. Labiausiai tikėtina to priežastis – technologijų plėtros ir teisėkūros santykio netolygumas. Technologijos žengia gerokai priekyje lyginant su teisėkūros procesu. Europos Tarybos valstybių narių priimta 1981 m. Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu taip pat nukreipta į tuo metu vykdytą apsikeitimą duomenimis bei jų tvarkymą automatizuotomis sistemomis siekiant apsaugoti asmens duomenų subjektus. Europos Komisija ilgai delsė ir nesiėmė veiksmų siekdama harmonizuoti Europos Bendrijos teisinę bazę asmens duomenų apsaugos srityje, tačiau vėliau buvo pastebėta, jog skirtingas šio klausimo reguliavimas tarp valstybių narių daro žalą ES valstybių narių ekonomikai. Didžioji Britanija ypač priešinosi privatumo ir asmens duomenų apsaugos reglamentavimui Sąjungos lygiu, nepaisant to, šią sritį reguliuojanti Direktyva buvo priimta 1995 m. Tačiau tuo metu pasiūlytas iš pažiūros detalus bei pažangus asmens duomenų apsaugos reguliavimo modelis tik iš dalies atitiko laikmečio realijas. Po kelių metų interneto bei tinklinių technologijų bumas sukėlė tikrą perversmą informacijos apsikeitimo procese. Virtualioje erdvėje išnyko valstybių sienos, atstumai bei suvaržymai. Akivaizdu, jog priiminėjant direktyvas šis įvykių posūkis nebuvo numatytas. Taip technologinis progresas dar kartą aplenkė teisinį. Nepaisant to, ES laikėsi savo pozicijos asmens duomenų apsaugos klausimu, ir reikalavimais dėl adekvataus asmens duomenų apsaugos lygio sugebėjo paskui save patraukti nemažą dalį pasaulio valstybių, nepriklausančių bendrijai. ES direktyvos proteguoja individo, kaip „silpnesniosios šalies“ interesus. Tuo tarpu JAV nuėjo kitu keliu. Ši valstybė mažai tesikišo į informacinio privatumo apsaugą. Reguliavimas išliko sektorinio pobūdžio, o visuotinio federalinio teisės akto, išsamiai, griežtai bei aiškiai reglamentuojančio asmens duomenų apsaugą taip ir nebuvo. Negana to, kai kuriose šalyse privatumo bei asmens duomenų apsauga apskritai buvo mažai tikėtina dėl tų valstybių tradicijų, gyvenimo būdo ar politinės santvarkos. Taip pasaulyje susiformavo trys atskiri blokai, kurie visiškai skirtingai suvokė ne tik asmens duomenų apsaugos reikalingumą, bet ir privatumą kaip vertybę apskritai.

2.2. Europos Sąjungos asmens duomenų apsaugos reguliavimo modelis

ES pasirinko detalų asmens duomenų apsaugos reguliavimo modelį. Šio modelio rengėjai surinko tuo metu geriausias bei labiausiai individą ginančias asmens duomenų apsaugos idėjas bei parengė keltą direktyvų, kuriomis detaliai reglamentavo ne tik asmens duomenų subjekto bei valdytojo teises bei pareigas, bet ir numatė sąlygas dėl asmens duomenų keitimosi su trečiosiomis valstybėmis. Šiuo pavyzdžiu asmens duomenų apsaugos srityje pasekė ne viena pasaulio valstybė, tačiau vargu ar taip būtų įvykę, jei ES nebūtų numačiusi imperatyvaus reikalavimo trečiosioms šalims, jog jų asmens

duomenų apsaugos lygis privalo būti adekvatus lygiui, esančiam tarp valstybių narių, priešingu atveju, trečiajai šaliai nebus leista keistis asmens duomenimis su bendrijos teritorijoje veikiančiais subjektais. Taip iš dalies primesdama savo sąlygas Europa padėjo išjudinti asmens duomenų apsaugos klausimą iš mirties taško, bei stengėsi sukurti į asmenį orientuotą privatumo bei asmens duomenų apsaugos modelį.

2.2.1. Europos Parlamento ir Tarybos direktyvos dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (95/46/EB) apžvalga

ES yra priėmusi keletą direktyvų, kuriose kalbama apie asmens duomenų apsaugą, tačiau pirmoji ir pati svarbiausia iš jų yra [26]Europos Parlamento ir Tarybos direktyva dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (95/46/EB). Nors šis teisės aktas yra regioninio lygmens, jis daro didelę įtaką pasaulinei asmens duomenų apsaugos praktikai. Direktyva saisto ES valstybes nares bei trečiąsias šalis – Norvegiją, Islandiją bei Lichtenšteiną, kurios yra prisijungusios prie Europos ekonominės erdvės susitarimo 1992 m. Vienas svarbiausių ir ryškiausių reikalavimų 95/46/EB direktyvoje yra draudimas perduoti asmens duomenis trečiosioms šalims, nebent jos užtikrina adekvatų asmens duomenų apsaugos lygį tam, kuris yra tarp ES valstybių narių. Tokios šalys kaip Kanada, Rusija, Argentina suderino savo teisinę bazę su ES, siekdamos asmens duomenų apsaugos lygio atitikimo. Iš to galima daryti išvadą, jog nors Europos Parlamento ir Tarybos direktyva dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo yra regioninio pobūdžio teisės aktas, jo pasaulinė įtaka yra didžiulė, todėl būtina dokumentą panagrinėti atidžiau.

Direktyvos tikslas yra dvejopas. [27]Viena vertus Direktyva siekiama apsaugoti fizinių asmenų pagrindines teises bei laisves, ypač jų privatumo teisę tvarkant asmens duomenis. Kita vertus, Direktyva nevaržo ir nedraudžia laisvo asmens duomenų judėjimo tarp valstybių narių dėl priežasčių, susijusių su asmens duomenų apsauga. Teisės akte atkreipiamas dėmesys į technologijų pažangą. Taip pat pažymima jog norint sukurti veikiančią vidaus rinką, kurioje pagal ES steigimo sutarties [28]7a straipsnį užtikrinamas laisvas prekių, žmonių, paslaugų ir kapitalo judėjimas, būtina ne tik galimybė asmens duomenims laisvai judėti iš vienos valstybės narės į kitą, bet taip pat ir asmens pagrindinių teisių apsauga. Europos Sąjungos kompetentingos institucijos suvokė, jog nepagrįstas asmens duomenų

[26]Europos Parlamento ir Tarybos direktyva dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (95/46/EB),
http://www3.lrs.lt/pls/inter1/dokpaieska.showdoc_l?p_id=7879&p_query=&p_tr2=2 [2008-11-10, 15:30];
[27] Mindaugas Kiškis, Rimantas Petrauskas, Irmantas Rotomskis, Darius Štitilis. Teisės informatika ir informatikos teisė. Vilnius: Mykolo Romerio universitetas, 2006. P. 120
[28] Europos Sąjungos steigimo sutartis,
http://eur-lex.europa.eu/lt/treaties/dat/11992M/word/11992M.doc [2008-11-10, 15:59]

srautų ribojimas pakenktų Bendrijos ekonomikai bei technologiniam vystymuisi, nepaisant to, atkreipiamas dėmesys į tai, jog įmonių ir įstaigų, operuojančių asmens duomenimis, skaičius nuolat auga, o pats duomenų apdorojimo bei keitimosi procesas sparčiai tobulėja, taip atsiranda papildoma rizika pažeisti asmenų teises į informacinį privatumą, todėl išreiškiama būtinybė užtikrinti tiek duomenų srautų judėjimo tęstinumą tiek asmenų privatumo apsaugą. Direktyvoje pažymima, jog skirtingas asmenų teisių ir laisvių, ypač jų privatumo teisės, apsaugos lygis tvarkant asmens duomenis įvairiose valstybėse narėse gali trukdyti perduoti tokius duomenis iš vienos valstybės narės į kitą ir tai gali kliudyti užsiimti kai kuriomis ekonominės veiklos rūšimis Bendrijos lygiu, iškreipti konkurenciją ar trukdyti valdžios institucijoms vykdyti savo pareigas pagal Bendrijos teisę. Apsaugos lygio skirtumai savo ruožtu atsiranda dėl pernelyg didelės nacionalinių įstatymų ir kitų teisės aktų įvairovės ir tai įvardijama kaip neigiamą poveikį visai Bendrijai darantis veiksnys.

Skirtingų asmens duomenų apsaugos įstatymų egzistavimas bei veikimas stipriai padidina išlaidas, susijusias su tinkama duomenų apsauga bei sudaro kliūtis laisvam prekių, asmenų, paslaugų bei kapitalo judėjimui. Siekiant panaikinti šias kliūtis buvo galima pasirinkti du reguliavimo variantus:

1. panaikinti asmens duomenų apsaugos įstatymus visose valstybėse narėse;
2. harmonizuoti tuo metu buvusius nacionalinius asmens duomenų apsaugos įstatymus;

Pirmasis variantas buvo netinkamas, kadangi siekiant jį įgyvendinti atsirastų konfliktų tarp ES ir atskirų valstybių, kurios turėjo pakankamai gerai išvystytą asmens duomenų apsaugos mechanizmą, be to, toks sprendimas būtų kirtęsis su svarbiausių žmogaus teisių apsaugos klausimais. Todėl buvo pasirinktas antrasis kelias, kuriuo norėta suvienodinti teisinį reguliavimą asmens duomenų apsaugos srityje. Esant vieningam reguliavimui bei vieningai rinkai duomenų perdavimo kaina suvienodėja, todėl duomenų tvarkytojai galėjo laisviau ir efektyviau veikti visoje Bendrijos teritorijoje. Tačiau duomenų perdavimo kaštai į trečiąsias šalis, neturinčias asmens duomenų apsaugą reglamentuojančių įstatymų arba turinčias tokį apsaugos lygį, kuris neatitinka esančio tarp Bendrijos narių, galėjo neigiamai įtakoti (iškreipti) rinką. Todėl ES įvedė sudėtingą asmens duomenų srautų apsaugos mechanizmą, siunčiant duomenis į trečiąsias šalis.

Direktyva dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo taikoma tada, kai duomenys tvarkomi automatiniu arba dalinai automatiniu būdu, o taip pat kai kurioms mechaninio tvarkymo sistemoms. Direktyva taikoma tik tada, kai duomenys yra struktūrizuotos sistemos dalis.

ES narės yra sutarusios, jog šalies saugumo politika yra pačios valstybės kompetencijoje ir kad nacionaliniai interesai šiuo atveju gali būti ginami tokiomis priemonėmis, kurios atrodo tinkamos

kiekvienai valstybei narei, todėl šia Direktyva nesiekiama kontroliuoti ar įtakoti valstybių narių veiklos tvarkant asmens duomenis vidaus saugumo politikos tikslais.

ES direktyva, kaip specifinio pobūdžio dokumentas, palieka nemažą manevravimo laisvę šalimas narėms, kadangi teisės akto įgyvendinimo bei įtraukimo į nacionalinės teisės sistemą klausimas yra pačių valstybių narių kompetencijoje. Direktyva nustato minimalų asmens duomenų apsaugo lygį ES teritorijoje, todėl teisė įvesti papildomas asmens duomenų apsaugos priemones šalims nėra uždrausta. 95/46/EB nurodoma, jog asmens duomenys turi būti tvarkomi pagal [29]nacionalinius teisės aktus, kurie privalo būti suderinti su Direktyvos nuostatomis. Dokumente pabrėžiama, kad duomenų tvarkymas turi atitikti teisės aktų reikalavimus, o teisės aktai turi būti parengti taip, kad [30]apribojimai būtų taikomi tiek, kiek tai būtina iškeltiems tikslams pasiekti. Rinkimo tikslai taip pat turi būti aiškūs bei apibrėžti. Išskiriama, jog duomenų rinkimas turi atitikti adekvatumo principą (duomenų renkama tik tiek, kiek reikia tikslams įgyvendinti). Numatoma duomenų laikymo trukmė bei būtinybė tikslinti, atnaujinti, ištaisyti ar ištrinti duomenis.

Septintajame straipsnyje kalbama apie duomenų teisėto tvarkymo kriterijus. Iš to, kaip formuluojamas straipsnio [31]tekstas, galima daryti išvadą, jog direktyvoje pateikiamas baigtinis reikalavimų, būtinų leidimo gavimui tvarkyti duomenis, sąrašas. Šis leidimas suteikiamas tik tuo atveju jeigu:

- duomenų subjektas yra nedviprasmiškai davęs sutikimą;
- tvarkyti reikia vykdant sutartį, kurią duomenų subjektas yra sudaręs kaip viena iš šalių, arba duomenų subjekto reikalavimu norint imtis priemonių prieš sudarant sutartį;
- tvarkyti reikia vykdant teisinę prievolę, kuri privaloma duomenų valdytojui;
- tvarkyti reikia norint apsaugoti gyvybinius duomenų subjekto interesus;
- tvarkyti reikia vykdant užduotį, atliekamą visuomenės labui arba įgyvendinant oficialius įgaliojimus, suteiktus duomenų valdytojui arba trečiajai šaliai, kuriai atskleidžiami duomenys;

[29] Direktyvos ketvirto straipsnio pirmojoje dalyje sakoma jog: „Kiekviena valstybė narė taiko nacionalines nuostatas, kurias ji priima pagal šią direktyvą, kai tvarkomi asmens duomenys“. A, b ir c punktuose išdėstomos sąlygos, kuriomis remiantis minėtasis straipsnis galioja. Duomenų valdytojas turi vadovauti tos šalies teisės aktais, kurios teritorijoje jis veikia nepriklausomai nuo to ar jo filialai yra vienoje valstybėje narėje, ar keliose valstybėse narėse, ar jis tik naudojasi valstybės narės techniniais resursais, siekdamas vykdyti operacijas su asmens duomenimis.

[30] Teisingumo principas yra universalus principas, kuris, be kita ko, suponuoja ir tai, kad bet kokios valstybės taikomos poveikio priemonės turi būti proporcingos (adekvačios) teisės pažeidimui ir turi atitikti siekiamus teisėtus tikslus, neturi varžyti asmens akivaizdžiai labiau negu reikia šiems tikslams pasiekti, be to, teisingumas gali būti įgyvendinamas tik užtikrinant interesų pusiausvyrą bei išvengiant socialinio gyvenimo nestabilumo.
http://www.litlex.lt/scripts/sarasas2.dll?Tekstas=1&Id=57378&Zd=BANKROT [2008-11-12, 05:05]

[31] „Valstybės narės numato, kad asmens duomenis galima tvarkyti tik tuo atveju, jeigu;“

- tvarkyti reikia dėl teisėtų interesų, kurių siekia duomenų valdytojas arba trečioji šalis (šalys), kurioms atskleidžiami duomenys, išskyrus atvejus, kai duomenų subjekto, kuriam pagal 1 straipsnio 1 dalį reikalinga apsauga, teisės ir laisvės yra viršesnės nei šie interesai.

Direktyvoje 95/46/EB akcentuojamas draudimas tvarkyti ypatingus asmens duomenis su tam tikromis išimtimis. Šiuo atveju išimtys taikomos, kai ypatingi duomenys renkami bei tvarkomi duomenų subjektui vienareikšmiškai sutikus, visgi, valstybėms narėms paliekama teisė šio sutikimo nepaisyti ir įstatymais vienašališkai drausti tokių duomenų tvarkymą. Išimtis galioja ir tais atvejais, kai duomenys tvarkomi norint įgyvendinti duomenų valdytojo prievoles ir specifines teises darbo įstatymų srityje. Ši išlyga palikta todėl, kad pagal nacionalinius įstatymus kai kurių profesijų atstovai turi atitikti tam tikrus specifinius reikalavimus, kurių apimtyje gali būti ir ypatingieji asmens [32]duomenys. Ypatingų duomenų tvarkymas leidžiamas ir tada, kai siekiama apginti pačio duomenų subjekto interesus tais atvejais kai duomenų subjektas fiziškai neįgali arba yra juridiškai neveiksnus duoti sutikimą šiems duomenims tvarkyti. Ypatingus asmens duomenis taip pat gali tvarkyti įstaiga ar organizacija, kurios nariu tas asmuo yra, ir kai priklausymas šiai įstaigai asmenį padaro ypatingų asmens duomenų, susietų su duomenis tvarkančios organizacijos veiklos pobūdžiu, [33]subjektu. Paskutinė išimtis, kuria remiantis direktyva leidžia tvarkyti ypatingus asmens duomenis yra susijusi su subjektais, kurie yra akivaizdžiai paskelbę ypatingus duomenis viešai arba kai tokie duomenys yra reikalingi nustatant, įvykdant ar siekiant apginti teisinius ieškinius.

Kitas svarbus Direktyvoje aptariamas aspektas - automatizuoti individualūs sprendimai. Pagrindinė 15 Direktyvos straipsnio idėja yra ta, jog jei automatizuoto asmens duomenų tvarkymo metu gali būti pakenkta asmeniui, tuomet automatiniu būdu priimto sprendimo rezultatą turi peržiūrėti atsakingas asmuo, siekiant sumažinti riziką galinčią atsirasti dėl netinkamo sistemos faktų interpretavimo. Tačiau teisės akte taip pat nurodyti atvejai, kai automatinis sprendimas visgi gali būti priimamas. Tokiu atveju turi būti užtikrinamas tinkamas duomenų subjekto interesų gynimas bei įstatyminė bazė, įteisinanti automatinių sprendimų priėmimą.

---

[32] Pavyzdžiui: Lietuvos Respublikos teismų įstatymo 52 straipsnyje nurodyta, jog: „asmuo negali būti laikomas nepriekaištingos reputacijos ir skiriamas teisėju, jeigu jis įsiteisėjusiu teismo nuosprendžiu pripažintas padaręs nusikalstamą veiką“. Teistumas yra priskiriamas prie ypatingų asmens duomenų, tačiau šiuo atveju, duomenimis apie asmens teistumą galima disponuoti, kadangi ši informacija yra tiesiogiai susijusi su jo tinkamumu užimti pareigas valstybės institucijoje. Lietuvos Respublikos teismų įstatymo pakeitimo įstatymas // Valstybės žinios. 2002-02-20, Nr. 17-649;

[33] Pavyzdžiui: Bažnyčia tvarko duomenis apie asmenis, priklausančius jos religinei bendruomenei, daro tai tik vidinio administravimo tikslais bei neperduoda šių duomenų jokiai trečiajai šaliai, kuri nėra tiesiogiai susijusi su minėta organizacija.

Duomenų perdavimo saugumas neabejotinai prioritetinis duomenų saugos elementas, be kurio visi kiti apsaugos principai taptų labai sunkiai įgyvendinami arba iš viso neįmanomi. Direktyvoje 95/46/EB pabrėžiama, jog duomenų perdavimo saugumo priemonės turi būti savalaikės, ekonomiškai pagrįstos bei turėtų būti taikomos atsižvelgiant į riziką, kurią gali sukelti asmens duomenų tvarkymas. Tai ypač aktualu, kai duomenys perduodami virtualiais tinklais. Deja, tuo metu, kaip buvo svarstomas direktyvos tekstas buvo itin sunku numatyti, jog tinklinės technologijos pasieks tokį spartų vystymosi tempą. Dėl šios priežasties techninė duomenų apsauga įgauna didesnę reikšmę nei Direktyvos rengimo bei priėmimo metu.

Vienas esminių skirtumų tarp Direktyvos nuostatų bei anksčiau nagrinėtų tarptautinių privatumą reglamentuojančių dokumentų yra asmens duomenų apsaugos santykis tarp ES ir trečiųjų šalių. ES užėmė griežtą poziciją asmens duomenų perdavimo į trečiąsias šalis atžvilgiu. Viena iš sudėtingiausių Duomenų apsaugos direktyvos nuostatų numato, kad asmens duomenų perdavimas trečiai valstybei faktiškai galimas tik tada, kai pastaroji užtikrina adekvatų apsaugos lygį. Apsaugos lygio tinkamumas įvertinamas pagal daugelį kriterijų ir gali būti paremtas tuo, kad valdytojas pateikia privatumo apsaugos garantijas, kurių tikslas – užtikrinti jog nei duomenų keitimosi proceso metu nei po jo nebūtų pažeistos teisės į privatumą. Ši Direktyvos nuostata buvo vertinama kritiškai, kadangi jai įsigaliojus galėjo sutrikti duomenų srautai į trečiąsias šalis. Viena iš didžiausių šio sprendimo oponenčių buvo JAV. Jungtinės Valstijos taiko sektorinį asmens duomenų apsaugos reguliavimą, o pats privatumo apsaugos lygis skiriasi priklauso nuo konkrečios valstijos įstatymų. JAV, priešingai nei ES, nėra privatumą valstybiniu lygiu ginančių agentūrų. Skiriasi ir pats požiūris į šią vertybę. Kai kurie autoriai kritikavo tokią ES poziciją, nes anot jų: [34]„sunku numatyti, kaip Direktyvos centralizuoto kompiuterio modelis galėtų būti pritaikytas technologijoms, kurios decentralizuoja duomenų tvarkymą.“ Akivaizdu, jog Direktyvos rengėjai nenumatė tokios sparčios technologijų, įgalinančių keistis duomenimis nepaisant valstybių sienų, plėtros. Nepaisant to, po ilgų derybų, 2000 m. Europos Komisijos bei JAV atstovai susitarė, jog Jungtinių Valstijų verslo subjektai bus pripažinti užtikrinantys adekvatų ES asmens duomenų apsaugos lygį jei veiks tos valstijos teritorijoje, kurioje yra užtikrinamas adekvatus privatumo apsaugos lygis. Šis susitarimas dar vadinamas Saugaus uosto principu (*safe harbour*). Tai iš dalies išsprendė teisės normų suderinamumo problemą, kadangi ES tik dalinai pripažįsta JAV privatumo apsaugą tinkama. Apskritai mokslininkų ginčai dėl „adekvataus“ apsaugos lygio netyla. Manoma, jog tokie suvaržymai kenkia pačiai ES tokiose srityse kaip elektroninė prekyba. Tuo tarpu kompetentingi ES pareigūnai atsikerta, jog aukštas privatumo asmens duomenų apsaugos lygis padidins visuomenės

[34] Mindaugas Civilka. Asmens duomenų apsaugos reguliavimas interneto kontekste. Vilnius, 2001

pasitikėjimą elektronine komercija, o ši verslo šaka Europoje suklestės įgyto pasitikėjimo dėka. Tenka pripažinti, kad Jungtinės Valstijos netaikydamos tokių griežtų asmens duomenų apsaugos standartų šiuo metu gerokai lenkia ES elektroninės komercijos srityje. 95/46/EB direktyvos 26 straipsnyje numatytos duomenų perdavimo į trečiąsias šalis draudimo išimtys, kuriomis paprastai ir naudojasi duomenų valdytojai. Duomenų keitimasis patenka po 26 straipsnio 1 dalies [35]a arba b punktais. Jais vadovaujantis stengiamasi apeiti griežtus europinius duomenų saugos reikalavimus.

Europos Parlamento ir Tarybos direktyva dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo yra pažangus dokumentas, kuris atvertė naują puslapį asmens duomenų apsaugos istorijoje. Ši Direktyva, įtakojanti ir kitų regionų įstatymų leidybą, ne tik detalizavo bei naujai apibrėžė asmens duomenų apsaugos principus. Jos pagalba buvo stengiamasi užtikrinti geresnę žmogaus teisių gynybą, o taip pat padidinti pasitikėjimą automatizuotu asmens duomenų tvarkymu. Nors rengiant teisės aktą buvo siekiama įtakoti ir kitų šalių teisinį reguliavimą, neišvengta trumparegiškų nuostatų, kurių įvedimas ne tik nedavė naudos ES valstybėms narėms, bet ir iškėlė daugybė klausimų apie asmens duomenų apsaugos normų interpretavimą interneto bei tinklinių technologijų kontekste. Nepaisant to, suvienodindama šalių narių teisinę bazę ES panaikino trukdžius, kliudančius efektyviai keistis duomenimis, ir kylančius dėl skirtingo asmens duomenų apsaugos reguliavimo nacionaliniu mastu.

Taigi, direktyva 95/46/EB yra šiuo metu solidžiausias bei išsamiausias privatumą bei asmens duomenų apsaugą užtikrinantis dokumentas regioniniu lygiu. Tiesa, jame yra abejonių keliančių nuostatų, šiuo teisės aktu taip pat bandoma diktuoti ES sąlygas kitoms pasaulio valstybėms, o tai ne visada padeda siekiant glaudesnio politinio bei ekonominio bendradarbiavimo. Direktyva turi tiek savo užtarėjų, tiek oponentų abiejose Atlanto vandenyno pusėse bei kituose regionuose, nepaisant to, net ir kritikai pripažįsta svarų jos indėlį į žmogaus teisių apsaugos stiprinimą.

2.2.2. Europos Parlamento ir Tarybos direktyvos dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (2002/58/EB) apžvalga

Augant interneto socialinei, politinei bei ekonominei svarbai atsirado poreikis teisiškai reglamentuoti procesus, vykstančius elektroninėje erdvėje. Internetas, kaip technologija, susiduria ne

[35] Europos Parlamento ir Tarybos direktyvos dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo 26 straipsnio 1 dalies išimtys: „a) duomenų subjektas yra nedviprasmiškai davęs sutikimą perduoti siūlomu duomenis; arba
b) duomenis perduoti būtina, kad būtų įvykdyti sutarties tarp duomenų subjekto ir duomenų valdytojo reikalavimai, arba kad būtų įgyvendintos priemonės, kurių prieš pasirašant sutartį imamasi duomenų subjekto prašymu;

tik su techniniais tobulėjimo iššūkiais, bet ir tam tikrais socialiniais lūkesčiais, kuriuos iššaukia technologijų atnešamos naujovės. Suprasdama strateginę interneto vystymo svarbą Europos Komisija parengė [36]pranešimą Tarybai bei Europos Parlamentui dėl naujos kartos interneto bei prioritetinių veiksmų pereinant prie naujo interneto protokolo IPv6 bei naują [37]direktyvą dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (2002/58/EB). Direktyva dėl privatumo ir elektroninių ryšių yra dalis iniciatyvinių pasiūlymų paketo, kuris tapo pagrindu reguliuojant komunikacijų bei elektroninių ryšių sektorių ES teritorijoje. Šios direktyvos tikslas – adaptuoti bei atnaujinti jau buvusią direktyvą 97/66/EB bei pritaikyti ją prie technologinių realijų.

Aktualiausi direktyvos straipsniai asmens duomenų apsaugos aspektu yra 12, kuriame kalbama apie abonentų knygų sudarymą bei 13, kuriame kalbama apie automatinio skambinimo sistemas bei skambinimo automatus, faksus ar elektroninį paštą, kurie naudojami tiesioginės rinkodaros tikslais. Remiantis 12 straipsniu valstybės narės privalo užtikrinti, kad asmens duomenų subjektas būtų tinkamai informuotas apie abonentų sąrašų sudarymo tikslą, taip pat apie asmens duomenų naudojimą paieškos tikslais bei apie tokių duomenų prieinamumą kitiems asmenims. Direktyvoje nurodoma, jog asmuo pats gali apsispręsti ar jo duomenys gali būti viešai paskelbti, o taip pat reikalauti nemokamo jų pataisymo bei ištrynimo. Tryliktame Direktyvos straipsnyje akcentuojamas asmens duomenų naudojimas tiesioginės rinkodaros tikslais. Straipsnio esmė – norint siųsti reklaminius pranešimus asmens duomenų subjektui būtina gauti jo sutikimą. Tam tikros išimtys taikomos jeigu fiziniai ar juridiniai asmenys parduodami produktus ar teikdami paslaugas pagal Direktyvą 95/46/EB gauna iš savo klientų jų elektroninio pašto kontaktinius duomenis, šie fiziniai ar juridiniai asmenys gali pasinaudoti elektroniniais kontaktiniais duomenimis savo paties panašių prekių ar paslaugų tiesioginei rinkodarai su sąlyga, kad klientams yra suteikiama aiški ir lengvai įgyvendinama galimybė nemokamai ir paprastomis priemonėmis nesutikti su tokiu elektroninių kontaktinių duomenų naudojimu. Taip pat draudžiamas reklaminių pranešimų siuntimas elektroniniu paštu jei slepiama siuntėjo tapatybė.

Taigi, Europos Parlamento ir Tarybos direktyva 2002/58/EB papildo asmens duomenų apsaugos mechanizmą ES lygiu, bei nustato tam tikrus saugiklius prieš galimą netinkamų operacijų su asmens duomenimis vykdymą elektroninių ryšių sektoriuje.

---

[36] Communication from the Commission to the Council and the European parliament. Next Generation Internet - Priorities for Action in Migrating to the New Internet Protocol IPv6, ftp://ftp.cordis.lu/pub/ist/docs/ka4/mb_com_parlipv6.pdf [2008-11-20, 09:15];

[37]Europos Parlamento ir Tarybos direktyva dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje**,** http://www3.lrs.lt/pls/inter1/dokpaieska.showdoc_l?p_id=36605&p_query=&p_tr2=2 [2008-11-20, 09:15];

2.2.3. Europos parlamento ir tarybos direktyvos dėl duomenų, generuojamų arba tvarkomų teikiant viešai prieinamas elektroninių ryšių paslaugas arba viešuosius ryšių tinklus, saugojimo (2006/24/EB) apžvalga asmens duomenų apsaugos aspektu

[38]Direktyva dėl duomenų, generuojamų arba tvarkomų teikiant viešai prieinamas elektroninių ryšių paslaugas arba viešuosius ryšių tinklus, saugojimo, trumpiau dar vadinama Duomenų saugojimo direktyva, įvairiuose sluoksniuose vertinama prieštaringai. Kai kurios žmogaus teisių gynimo grupės išreiškė rimtą susirūpinimą dėl jos reikalavimų tam tikrą laiką saugoti srauto bei vietos nustatymo duomenis. Netrukus po šio teisės akto priėmimo tiek visuomenėje, tiek žiniasklaidoje dokumentas buvo pakrikštytas kaip „sekimo direktyva“. Baiminamasi, jog prisidengiant Direktyvos nuostatomis, valstybė žinos per daug privataus pobūdžio informacijos apie savo piliečius, o ir pats tokių duomenų laikymas yra perteklinis bei mažai padedantis nusikaltimų prevencijos tikslais. Tuo tarpu šalininkai tvirtina, jog nebus renkama informacija, susijusi su pranešimų turiniu, o pagal gautus srauto bei vietos nustatymo duomenis bus galima atsekti teroristinių grupuočių ryšius ir taip užtikrinti saugumą ES teritorijoje. Tokių duomenų rinkimas bei saugojimas be abejo yra naudingas valstybei, nes palengvėja nusikaltimų tyrimo procesai, tačiau tiek pavienių fizinių asmenų, tiek verslo subjektų, tiek interneto bei telekomunikacinių paslaugų teikėjų minėtieji reikalavimai nedžiugina.

2006/24/EB direktyvoje deklaruojama, jog teroro išpuolių grėsmė bei skirtingas srauto bei turinio duomenų laikymo intervalas kai kuriose šalyse veda prie būtinybės suderinti šį reguliavimą ir taip pasinaudojant EŽTK bei Privatumo direktyvos išimtimis nacionalinio saugumo atžvilgiu, įtvirtinti tokių duomenų rinkimą terorizmo bei organizuoto nusikalstamumo tyrimo tikslais. Duomenys gali būti saugomi nuo pusės, iki dviejų metų. Saugojimo trukmę nustato valstybės narės savo nuožiūra. Direktyvoje nenurodoma, kad turėtų mokėti už tokių duomenų saugojimą, todėl šis klausimas taip pat paliekamas valstybių narių atsakomybėje.

Nors Direktyvos būtinumas ir grindžiamas kova prieš terorizmą bei organizuotą nusikalstamumą, joje išlieka daugybė prieštaravimų dėl kaupiamų duomenų pobūdžio. Privacy International [39]skelbia, jog šios direktyvos priėmimas kertasi su EŽTK nuostatomis dėl privatumo apsaugos bei atima teisę iš piliečių koreguoti savo elgesį priklausomai nuo valstybės vykdomo

[38] Europos Parlamento ir Tarybos direktyva dėl duomenų, generuojamų arba tvarkomų teikiant viešai prieinamas elektroninių ryšių paslaugas arba viešuosius ryšių tinklus, saugojimo, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:LT:PDF [2008-11-27, 09:20];
[39] Privacy International svetainė, http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-57875 [2008-12-03]

[40]stebėjimo. Remiantis šiuo dokumentu, srauto duomenims priskiriama ir elektroninio laiško antraštė, o ji gali atskleisti nemažai informacijos apie duomenų siuntimo tikslą bei turinį. Kalbant apie telefoninių pokalbių srauto duomenis taip pat galima paminėti, jog skambučiai išsikviečiant taksi ir skambučiai į anoniminės pagalbos liniją Direktyvos požiūriu yra lygiaverčiai, nors antruoju atveju skambučio tikslas gali nemažai pasakyti apie skambinančiojo asmenybę ar pokalbio turinį, kuris, pagal EŽTK bei Privatumo direktyvą jau būtų priskiriamas ypatingų, t.y. griežčiau saugomų, duomenų kategorijai.

Tai tik keletas paradoksų, susijusių su Europos parlamento ir tarybos direktyva dėl duomenų, generuojamų arba tvarkomų teikiant viešai prieinamas elektroninių ryšių paslaugas arba viešuosius ryšių tinklus, saugojimo. Šis prieštaringai vertinamas teisės aktas parodė, jog Europos Sąjunga pradėjo grįžtis į kitą pusę privatumo bei asmens duomenų apsaugos srityje. Žinoma, nacionalinio saugumo užtikrinimas yra prioritetinis uždavinys, tačiau valstybė disponuodama tokiais dideliais informacijos kiekiais anksčiau ar vėliau gali neišlaikyti balanso tarp tiesėtų interesų apsaugos ir savavališko kišimosi į piliečių gyvenimą.

2.2.3. Ministrų komiteto rekomendacijų valstybėms narėms apžvalga privatumo bei asmens duomenų apsaugos aspektu

Ministrų komiteto rekomendacijos valstybėms narėms yra dokumentai, kuriuose pasisakoma vienu ar kitu aktualiu klausimu bei patariama kaip elgtis esant tam tikromis aplinkybėmis probleminių klausimų kontekste. Po Europos Parlamento ir Tarybos direktyvos dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo priėmimo netruko atsirasti naujų techninių bei teisinių reiškinių, kuriems reguliuoti nepakako šio teisės akto ar tarptautinių konvencijų. Vienos iš pagrindinių naujovių – internetas bei telekomunikacijų tinklai. Kompetentingos Europos Sąjungos institucijos priėmė keletą rekomendacijų, kurių tikslas buvo padėti interneto bei kitų tinklų naudotojams bei tiekėjams nustatyti teisingus privatumo apsaugos principus. Svarbiausia interneto ir kitų globaliųjų tinklų požiūriu yra [41]Ministrų komiteto rekomendacija Nr. R (99) 5 valstybėms narėms dėl privatumo apsaugos internete. Šios rekomendacijos tikslas – nustatyti duomenų apsaugos principus internete, tačiau dokumentas tuo neapsiriboja. Jame taip pat nurodoma,kaip elgtis virtualioje erdvėje siekiant iki minimumo sumažinti trečiųjų asmenų priėjimą prie interneto naudotojo asmens duomenų

[40] Pavyzdžiui, viešosiose erdvėse, kuriose įrengiamos stebėjimo kameros, taip pat pakabinami įspėjamieji pranešimai piliečiams, kad jie yra stebimi. Asmenys, atsižvelgdami į perspėjimą gali koreguoti savo elgesį ir taip riboti žinomumą apie save.

[41] Ministrų komiteto rekomendacija Nr. R (99) 5, http://www.ada.lt/images/cms/File/Rekomendacijos%20ministru%20tarybos/R_99_%205%20priv_aps_intern_rekom.pdf [2008-11-26, 00:35];

bei apskritai kokių saugumo priemonių imtis siekiant apsaugoti savo privatumą. Rekomendacijoje atkreipiamas dėmesys į dalinio anonimiškumo išlaikymą naršant, taip pat apie kodavimo priemonių bei slapyvardžių naudojimą, apie tinkamą paslaugų teikėjo pasirinkimą ir pan. Tuo tarpu interneto tiekėjai supažindinami su pareigomis vartotojų atžvilgiu asmens duomenų apsaugos aspektu. Nurodoma kaip paslaugų tiekėjas turi elgtis su klientų asmens duomenimis, kokie veiksmai draudžiami su privačia vartotojų informacija ir pan. Rekomendacijos tekstas suformuluotas gana aptakiai. Greičiausiai taip buvo pasielgta todėl, jog rengėjai tikėjosi, kad abstraktesnės formuluotės bus universalesnės ir pritaikomos bet kuriai situacijai, galinčiai atsirasti interneto erdvėje. Rekomendacija reikšminga ir tuo, kad joje išryškinamas duomenų subjekto savisaugos principas. Kitaip tariant, asmuo yra skatinamas pats tinkamai pasirūpinti saugumo priemonėmis, susijusiomis su jo privatumu, nes suvokiama, jog globalus interneto pobūdis iš esmės stipriai padidina galimybę susidurti su asmens duomenų tvarkymo pažeidimais, todėl duomenų subjektas turi nemaža dalimi prisidėti prie tokių duomenų saugojimo ar tinkamo naudojimo. Kitas privatumo aspektu svarbus rekomendacinio pobūdžio dokumentas yra [42]Ministrų komiteto rekomendacija Nr. R (95) 4 valstybėms narėms dėl privatumo apsaugos telekomunikacijų paslaugų srityje, ypač telefoninio ryšio paslaugose. Rekomendacijoje pabrėžiama automatizuoto duomenų tvarkymo telekomunikacijų srityje nauda, nepamirštant ir grėsmių asmens duomenų saugumui. Šiame dokumente apibrėžiami principai taikomi tinklo operatoriams ir paslaugų tiekėjams, kurie atlikdami savo funkcijas renka ir tvarko asmens duomenis. Į šį sąrašą patenka tiek privatūs, tiek valstybiniai subjektai. Rekomendacijoje aptariami tokie aspektai kaip pagarba privatumui,duomenų tvarkymas, rinkimas bei perdavimas, duomenų rinkimas tiesioginei rinkodarai, telefonų knygų sudarymas ir k.t. Iš esmės rekomendacijoje atspindimi privatumo bei asmens duomenų apsaugos principai, įtvirtinti 1981 m. Strasbūro konvencijoje bei direktyvose, susietose su asmens duomenų apsauga. Tačiau principų turinys šiuo atveju yra išplėstas ir pritaikytas telekomunikacijų sektoriui.

Apibendrinant galima teigti, jog Ministrų komiteto rekomendacijos valstybėms narėms yra tarsi bandymas atsigręžti į technologinę laikmečio realybę, bei užlopyti tas spragas, kurios liko priėmus direktyvas, reguliuojančias privatumą bei asmens duomenų apsaugą Europos Sąjungos lygiu. Kadangi šie dokumentai yra rekomendacinio pobūdžio, jų imperatyvus įgyvendinimas nėra privalomas valstybėms narėms, tačiau tinkamas patarimų bei nurodymų laikymasis bent jau Europos Sąjungos teritorijoje galėtų garantuoti geresnę asmens duomenų apsaugą.

[42] Ministrų komiteto rekomendacija Nr. R (95) 4, http://www.ada.lt/images/cms/File/Rekomendacija%20Nr.%20R%20(95)%204.pdf [2008-11-26, 00:40];

2.3. Jungtinių Amerikos Valstijų privatumo apsaugos reguliavimo modelis

JAV pasirinko visiškai kitokį modelį reguliuojant privatumo apsaugą. Nors pagrindiniai finansų srautai bei elektroninės komercijos iniciatyvos plaukia iš šios valstybės, čia, priešingai nei ES, privatumo bei asmens duomenų apsaugos reguliavimas nėra detalus. Iš esmes skiriasi ne tik pats reguliavimo pobūdis, bet ir požiūris į privatumą kaip vertybę. JAV privatumo apsaugos teisinė bazė yra tarsi įvairių reguliavimo formų mišinys, apjungiantis savireguliaciją, teismų precedentus, valstijų teisės aktus bei federalinius įstatymus. Istoriškai JAV dažnai remiamasi Konstitucijos pataisomis. [43]Pirmoji pataisa įteisina žodžio laisvės principą. Šis principas yra stipriai saugomas Jungtinėse Valstijose ir, žvelgiant iš Europos perspektyvos, kartais „konfliktuoja“ su teise į privatumą. [44]Ketvirtoji pataisa skelbia, jog asmuo turi jaustis saugus pats asmeniškai, taip pat savo namuose ar kitoje nuosavybėje bei jo saugumo neturi įtakoti paties asmens užrašai.. [45]Penktojoje pataisoje ginama piliečių teisė į laisvę bei nuosavybės neliečiamumą. Šiomis pataisomis vadovaujamasi siekiant atskleisti teisės į privatumą esmę. Amerikiečių požiūriu, pats reikšmingiausias dokumentas, reguliuojantis privatumo apsaugą JAV yra [46]Teisingų informacijos praktikų kodeksas, kuris buvo parengtas 1973 m. Nuo tada buvo daug bandymų parengti federalinį įstatymą, saugantį teisę į privatumą, tačiau realių rezultatų tokie bandymai nedavė. Šis dokumentas remiasi penkiais principais, apibrėžiančiais privatumo bei asmens duomenų apsaugą. Principai teigia, jog negali būti asmens duomenų kaupimo sistemų, kurių egzistavimo faktas yra slaptas; asmuo turi teisę sužinoti, kokia informacija apie jį laikoma bei naudojama; asmuo turi teisę užkirsti kelią asmeninės informacijos naudojimui arba tokios informacijos naudojimui ne pagal nurodytą tikslą; asmuo turi teisę į asmeninės informacijos ištaisymą; organizacijos, užsiimančios asmens duomenų pardavinėjimu turi užtikrinti jų kokybę bei užkirsti jų naudojimą ne pagal numatytą tikslą. Šie principai buvo perkelti į [47]1974 m. Privatumo įstatymą, taip suteikiant teisę piliečiams prieiti prie savo duomenų, kuriuos apie juos kaupė vyriausybė. [48]1974 m. Informacijos laisvės įstatymas suteikė galimybė prieiti prie duomenų, saugomų federalinėse agentūrose. 1991 m. Telefono vartotojų apsaugos įstatymas uždraudė siuntinėti nepageidaujamus pranešimus telefono ar faksimiliniais aparatais. Jungtinių Valstijų Senate būta mėginimų priimti griežtesnius privatumo apsaugos įstatymus,

[43] http://www.gpoaccess.gov/constitution/html/amdt1.html [2008-11-27, 04:30];
[44] http://www.gpoaccess.gov/constitution/html/amdt4.html [2008-11-27, 04:35];
[45] http://www.gpoaccess.gov/constitution/html/amdt5.html [2008-11-27, 04:35];
[46] Code of Fair Information Practices,
http://www.ftc.gov/reports/privacy3/fairinfo.shtm, [2008-12-01, 20:20];
[47] 1974 m. Privatumo įstatymo tekstas:
http://www.usdoj.gov/oip/privstat.htm [2008-11-27, 05:30]
[48] Įstatymo pataisos priimtos 2007 metais. 1974 m. Informacijos laisvės įstatymo tekstas:
http://www.usdoj.gov/oip/foiastat.htm [2008-11-27, 05:32]

ypač tokiose srityse, kur operuojama finansiniais ar ypatingais duomenimis, tačiau šioms iniciatyvoms vis pritrūkdavo palaikymo. [49]Federalinės prekybos komisijos nuomone, nauji įstatymai, reguliuojantys privatumą bei asmens duomenų apsaugą, nėra reikalingi, o duomenų saugumą galima užtikrinti esamų teisės aktų pagalba. Be to, norint priimti tokio pobūdžio teisės aktą būtina atlikti nuodugnius tyrimus dėl jo tikslingumo. Teigiama, jog privačios kompanijos pasiekė didelę pažangą gindamos vartotojų teises, o faktas, jog vartotojai pasirenka tas įmones, kurios geriausiai patenkina jų interesus savaime garantuoja geriausią privatumo apsaugą, kadangi įmonės nenori prarasti konkurencinio pranašumo sumažindamos asmens duomenų apsaugos lygį. Tiesa, pažymima ir tai, jog modernių technologijų epochoje keistis asmens duomenimis tapo ypač paprasta, todėl tiek privatūs asmenys, tiek verslo subjektai privalo rūpintis privatumo apsauga atsižvelgiant į galimas grėsmes virtualioje erdvėje. Svarbų vaidmenį saugant asmenų teisę į privatumą vaidina ir atskirų valstijų įstatymai. Remiantis jais taip pat taikomas „saugaus uosto“ susitarimas su ES.

JAV pasuko visiškai kitu keliu privatumo bei asmens duomenų apsaugos reguliavimo srityje. Šioje šalyje apskritai labiau atsižvelgiama į verslo interesus, o įteisintas lobizmas užtikrina verslo subjektų paramą politikams bei valstybės vadovams. Šie, savo ruožtu, nedrįsta papildomai varžyti verslininkų. Tačiau Jungtinių Valstijų savireguliacija grįsto privatumo apsaugos reglamentavimo toli gražu negalima pavadinti niekam tikusiu ar socialiai neatsakingu. JAV gerokai lenkia tiek ES, tiek kitus regionus pagal elektroninės komercijos apimtis bei pajamas, gaunamas iš šios verslo šakos. Kitas aspektas – valstybės atliekamas asmens duomenų rinkimas bei piliečių stebėjimas, kurio ekonominė naudą itin sunku pagrįsti. Jungtinių Valstijų pareigūnai tokias priemones vadina neišvengiamomis kovoje su terorizmu, tačiau ar terorizmo korta nesinaudojama per dažnai ir ar to kaina nėra per didelė žmonėms, kuriuos valstybė stengiasi apsaugoti? Vienareikšmiško atsakymo nėra, tačiau aišku viena, Jungtinių Valstijų gebėjimas uždirbti iš elektroninės komercijos bei apeliavimas į „saugumo užtikrinimą“ paminant teisę į privatumą sulaukia ne tik kritikos, bet ir nemažai palaikymo už JAV sienų. Tokiu būdu šalis „eksportuoja“ savo požiūrį į privatumą bei daro įtaką pasauliniam privatumo bei asmens duomenų apsaugos reguliavimui.

[49] Federalinė prekybos komisija yra nepriklausoma agentūra prie Jungtinių Amerikos Valstijų vyriausybės, įsteigta 1914 m. Federalinės prekybos komisijos įstatymu. Pagrindiniai jos uždaviniai – vartotojų teisių apsauga, bei reiškinių, susijusių su nesąžininga konkurencija atskleidimas bei šalinimas.

2.4. Regioninio reguliavimo skirtumai bei tendencijos privatumo bei asmens duomenų apsaugos aspektu;

Informacinė visuomenė yra globali ir atskiros jos grupės ganėtinai seniai iškėlė pasaulinio privatumo reguliavimo klausimą. Esminis šio klausimo aspektas – kokiu lygiu turėtų būti reguliuojama privatumo bei asmens duomenų apsauga, ar rinktis griežtą, biurokratiškai suvaržytą, bet asmenų teises labiausiai ginantį ES modelį, ar pasikliauti savireguliacija bei valstybės interesų ribų išplėtimu gyventojų privatumo sąskaita, kaip kad yra JAV?

Tarptautinė vartotojų organizacija (*Consumers International*) vienijanti daugiau nei 220 vartotojų teisių gynimo organizacijų 115 valstybių dar 2001 m. sausį atliko [50]tyrimą, kuriame lygino 751 elektroninės komercijos svetainę privatumo apsaugos internete aspektu. Rezultatai parodė, jog tiek ES, tiek JAV interneto svetainės neatitinka privatumo bei asmens duomenų apsaugos pasaulinių standartų. Tyrimas atskleidžia pagrindinių asmens duomenų apsaugos principų ignoravimą. Pastebėta, jog interneto puslapiai esantys ES ne ką geriau informuoja vartotojus apie asmens duomenų naudojimą nei JAV esančios svetainės nepaisant gerokai griežtesnės asmens duomenų apsaugos. Kai kurios geriausios svetainės privatumo aspektu buvo rastos būtent JAV ir jose būdavo dažniau pateikiama informacija apie galimybę būti įtrauktam į kompanijos tiesioginės rinkodaros adresatų sąrašus bei kaip to atsisakyti.

Verslo interesų grupės kritikuoja griežtesnį privatumo reguliavimą informaciniuose tinkluose, kadangi šie apribojimai duotų neigiamą efektą internetinei prekybai bei užkrautų verslui ant pečių sudėtingą biurokratinį mechanizmą. Toks sprendimas taip pat apribotų vartotojų pasirinkimo laisvę, kas galiausiai sąlygotų produktų kainų kilimą. Teisininkas, autorius bei patarėjas ES duomenų apsaugos bei elektroninės komercijos klausimais Lucas‘as Bergkamp‘as [51]teigia, kad duomenų apie asmenį nuosavybės klausimas yra išspęstas per greitai. Pasak jo, nėra pagrindo duomenų subjektui suteikti nuosavybės teises į duomenis vien todėl, kad tie duomenys yra apie jį patį. Jei kitas subjektas renka duomenis ir atlieka visą darbą bei eikvoja savo resursus, vadinasi, jis ir yra duomenų rinkmenos savininkas. Toks autoriaus požiūris yra kritikuotinas, kadangi resursų naudojimas bei laiko eikvojimas dar nesuteikia nuosavybės teisių į vieną ar kitą objektą. Šį L. Bergkamp‘o traktavimą būtų galima

[50] An international comparative study of consumer privacy on the internet; http://www.consumersinternational.org/Shared_ASP_Files/UploadedFiles/80732215-7329-4A22-A02A-9A8062C65BC7_Doc30.pdf [2008-11-27, 07:50]

[51] EU Data Protection Policy - The Privacy Fallacy: Adverse Effects of Europe’s Data Protection Policy in an Information-driven Economy Computer Law & Security Report Vol. 18 no. 1 (2002)

pritaikyti norint pateisinti turto ar resursų [52]pasisavinimą, todėl teisę į privatumą būtina laikyti prigimtine, o duomenų nuosavybė neabejotinai turėtų priklausyti asmens duomenų subjektui, nes yra tiesioginis bei stiprus ryšys tarp duomenų bei asmens, kurio tapatybę tie duomenys apibūdina.

Esminis skirtumas tarp JAV ir ES privatumo bei asmens duomenų apsaugos yra tas, jog ES privatumas reguliuojamas Bendrijos lygiu ir užtikrina minimalią privatumo apsaugą Sąjungos teritorijoje, tuo tarpu Jungtinėse Valstijose vadovaujamasi keliais federaliniais bei valstijų įstatymais, aprėpiančiais privatumo apsaugos reikalaujančias sritis. Tačiau skirtingai nuo ES, JAV piliečių apsaugos lygis priklauso nuo valstijos, kurioje gyvena asmuo, įstatymų. Tačiau žvelgiant bendrai, akivaizdu, jog bendras privatumo apsaugos lygis JAV yra žemesnis nei ES. Sunku nustatyti tikslias priežastis, kodėl taip atsitiko, tačiau aišku viena – politinis klimatas šiuose regionuose labai skiriasi. Jungtinėse Valstijose į privatumą žiūrima labiau iš ekonominės pusės, čia žodžio laisvės principas yra labai stipriai ginamas, o verslo grupių įtaka sprendimų priėmimui – didesnė, tuo tarpu ES privatumo sąvoka apibrėžiama per socialinę prizmę ir į pirmą vietą iškelia individo teisių gynybą. Dar vienas esminis skirtumas yra tas, jog JAV pieliečiams jų duomenys priklauso tik išskirtiniais atvejais. Juos galima rinkti, sudarinėti sąrašus bei pardavinėti be duomenų subjekto sutikimo. Tuo tarpu ES tai draudžiama.

Šie abu regionai formuoja pasaulinį privatumo bei asmens duomenų apsaugos veidą, tačiau šiuo atveju egzistuoja ir trečias žaidėjas – tai šalys, kurios nepripažįsta teisių į privatumą bei niekaip nesistengia jo apginti. Nepaisant to, tiek ES, tiek JAV lenktyniauja teisės į privatumą „eksporte“ pasauliniu mastu. ES priėmus direktyvą 95/46/EB ir įtvirtinus joje adekvataus duomenų apsaugos lygio reikalavimą, kitos pasaulio valstybės turėjo nusileisti Europos pozicijai. Tačiau ar toks sąlygų diktatas davė apčiuopiamos naudos žmogaus teisių apsaugos kontekste? Taip, nemažai valstybių pasekė Europos Sąjungos pavyzdžiu. Argentina, Rusija, Naujoji Zelandija, Kanada ir kitos šalys priėmė reikalingus teisės aktus, tačiau didžiausia „prekiautoja“ asmens duomenimis (JAV) taip ir liko „dalinai atitinkanti apsaugos lygį“. Nepaisant to, atrodė, jog visi koziriai yra europiečių rankose ir anksčiau ar vėliau Jungtinės Valstijos bus priverstos griežčiau reguliuoti privatumo apsaugą arba prisidėti prie grupės šalių, kurios apskritai neigia šią teisę, o tai nebūtų išmintinga nei politiškai, nei ekonomiškai, nei ideologiškai. Viską iš esmės pakeitė 2001 m. rugsėjo 11 atakos prieš Amerikos civilius objektus. Visas pasaulis nustėro, o amerikiečiai tvirtai stojo valstybės pusėn ir paaukojo savo asmens privatumo likučius vardan „nacionalinio saugumo“. Europa nors ir laikėsi savo pozicijos asmens duomenų

[52] Asmuo, kurio teritorijoje auga obelis gali be jokių papildomų išlaidų ar sąnaudų sulaukti gausaus obuolių derliaus. Tai, kad jis pats neskina vaisių dar nereiškia, jog juos rinkti leidžiama bet kam. Remiantis L. Bergkamp‘o pamąstymais, galima teigti, jog vagis, rinkęs obuolius, naudojęs savo laiką šiam procesui bei degalus obuolių išvežimui tampa teisėtu jų savininku.

apsaugos srityje galiausiai ir pati buvo paveikta „karo prieš terorizmą“ bei priėmė Europos parlamento ir tarybos direktyvą dėl duomenų, generuojamų arba tvarkomų teikiant viešai prieinamas elektroninių ryšių paslaugas arba viešuosius ryšių tinklus, saugojimo (2006/24/EB). Nors šios direktyvos priėmimas aiškinamas kaip būtinybė kovoje prieš terorizmą, kyla klausimas ar toks reguliavimas nepažeis teisės į privatumą ir ar srauto duomenų rinkimas bei saugojimas netaps pirmu žingsniu į [53]„Didžiojo brolio“ glėbį.

2.5. Skyriaus apibendrinimas

Natūralu, jog skirtingos valstybės turi savus teisės sistemų ypatumus, be to tam tikri visuomeniniai santykiai taip pat gali būti reglamentuojami skirtingai. Ši tendencija gyvavo nuo pačių pirmųjų teisės užuomazgų iki šių dienų. Nacionaliniai teisės aktai pakankamai gerai reguliavo visuomenės bei valstybės gyvenimą, tuo tarpu tarptautinės sutartys buvo pasitelkiamos siekiant sureguliuoti tarpvalstybinius santykius. Didžiąją dalį žmonijos egzistavimo laiko ši schema pasiteisindavo, kadangi kiekviena šalis žiūrėjo savo bei savo piliečių interesų, o su kitų valstybių teisėmis skaitėsi tiek, kiek tai buvo paranku ekonominiu, kariniu ar politiniu požiūriu. Padėtis iš esmės pradėjo keistis tik XX a. antrojoje pusėje, kai buvo suvokta, jog merkantilistinė politika yra žalinga tiek bendram pasaulio geopolitiniam stabilumui, tiek kiekvienai valstybei atskirai. Ekonominiai interesai atvėrė duris permainoms. Pasaulinė rinkų globalizacija, intensyvėjanti prekyba bei atskirų valstybių (ar jų blokų) susisaistymas bei ekonominė priklausomybė privertė šalis ieškoti tobulesnių bei naujesnių bendradarbiavimo formų bei būdų. Sparčiausiai tarpvalstybiniai santykiai buvo reglamentuojami srityse, susijusiose su prekyba materialiais objektais bei paslaugomis, kadangi vienodos veiklos taisyklės duodavo naudos visoms suinteresuotoms šalims. Tačiau privatumo bei asmens duomenų apsaugos srityje vieningos politikos nebuvo laikomasi, o tai neigiamai įtakojo finansų bei kitus ekonomiškai svarbius sektorius. Tarptautinėmis deklaracijomis bei konvencijomis buvo bandoma bent iš dalies sureguliuoti šią probleminę sritį, apginti pamatines teises į privatumą, numatyti kertinius šių teisių principus. Nepaisant to, dvi didžiulės pasaulio ekonomikos (ES bei JAV) pasuko skirtingais keliais asmens duomenų apsaugos reglamentavimo srityje.

Direktyva dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo iš dalies išsprendė asmens duomenų apsaugos problemas regioniniu lygiu. Vienodas

[53] 1984-ieji (angl. Nineteen Eighty-Four, kartais 1984) – anglų rašytojo Džordžo Orvelo antiutopinis romanas, kurio pagrindinis veikėjas Winston Smith, intelektualus Teisybės ministerijos biurokratas, gyvenantis diktatūroje 1984-aisiais. Išgalvotas personažas - Didysis brolis, esantis valdžios piramidės viršūnėje, šiuolaikinėje kultūroje tapo bendriniu terminu, kuriuo apibūdinamas per didelis valdžios ar atskirų asmenų siekis prižiūrėti ir kontroliuoti visuomenę.

informacinio privatumo traktavimas bei harmonizuotos įstatymų bazės valstybėse narėse užtikrina ne tik galimybę atlikti operacijas su asmens duomenimis, bet tuo pačiu ir saugo asmens duomenų subjektų teisę į privatumą. ES pavyzdžiu reguliuojant asmens duomenų apsaugą pasekė nemažai pasaulio valstybių. Tačiau ar toks reguliavimas yra pranašesnis už JAV savireguliacijos politiką? ES įstatymai direktyvos bei rekomendacijos toli gražu nėra tobulos. Jų reguliavimo sritis tik dalinai atitinka šiandienos technologines realijas, o piliečių asmens duomenų apsauga informacinių technologijų kontekste kartais kelia pagrįstų abejonių. Tuo tarpu JAV itin atlaidžiai žiūri į operacijas atliekamas su asmens duomenimis bei palieka didžiąją dalį privatumo apsaugos naštos savireguliacijai. Tai, galbūt, naudinga verslo subjektams, tačiau fiziniais asmenimis neabejotinai yra labiau manipuliuojama, o jų teisės mažiau saugomos. Kitas privatumo apsaugos reguliavimo aspektas – valstybinės stebėjimo sistemos, renkančios informacija ne tik apie savo šalies, bet ir viso pasaulio gyventojus. Taigi, apibendrinant šį skyrių galima teigti, jog:

- Regioninis privatumo bei asmens duomenų apsaugos reglamentavimas virto alternatyva pasauliniam šio reiškinio reguliavimui;
- Regioninio reguliavimo formos ne visiškai atitinka technologinę realybę;
- Reguliavimo skirtumai yra didžiuliai, akivaizdūs bei esminiai, o tai trukdo keitimuisi duomenimis tarp skirtingus apsaugos lygius turinčių valstybių;
- ES akcentuoja individo teisių apsaugą ir griežtą, centralizuotą privatumo bei asmens duomenų gynimą, tuo tarpu JAV taiko sektorinį reguliavimą bei pasikliauja savikontrole;
- Dabartinis privatumo bei asmens duomenų apsaugos reguliavimas yra krizėje, kadangi nei ES, nei JAV, nei trečiosios šalys nėra pasirengę privatumo apsaugai globalių informacinių technologijų veikimo erdvėje, o privatumo vystymosi tendencijos yra neaiškios;

3. GRĖSMES PRIVATUMUI IR ASMENS DUOMENIMS ŠIANDIENINIAME PASAULYJE

Grėsmės privatumui nėra naujas reiškinys. Dažniausiai jos nėra kriminalinio pobūdžio, bet gali į tokias peraugti. Kaip ir bet kuriuo aktualiu visuomenei klausimu, taip ir šiuo, yra daugybė nuomonių už ir prieš asmens duomenų apsaugos stiprinimą. Šiandieninėje situacijoje pastebima, kad piliečiai labiau linkę ginti teisę į informacinį privatumą tada, kai duomenis renka verslo subjektai, tačiau kai reikalai pasisuka link valstybės vedamo stebėjimo, tokių nuomonių skaičius gerokai sumažėja. Tačiau tiek viena tiek kita asmens duomenų rinkimo forma gali neigiamai paveikti asmens duomenų subjektą. Tiesa, verslininkai gali netinkamai naudoti duomenis, tačiau ir valstybės institucijos dėl ydingo informacijos tvarkymo gali ją prarasti, o tokiu atveju labiausiai kentės paprasti piliečiai, kurių asmens duomenys atsidurs elektroninių sukčių ar brukalų siuntinėtojų rankose. Taigi, grėsmės išlieka, todėl šiame skyriuje bus aptariamas ne tik privatumo teisės gynimo būtinumas, bet ir atskiros grėsmių rūšys, kurias sukelia asmens duomenų praradimas. Visos jos atsiranda kaip informacinių technologijų naudojimo išdava, todėl globalus šių grėsmių pobūdis akivaizdus.

3.1. Grėsmių privatumui šaltiniai bei asmens duomenų apsaugos poreikis šiandieniniame pasaulyje

Iki tinklinių technologijų atsiradimo visuomenės susirūpinimas privatumo apsauga buvo sąlyginai menkas, kadangi dideli informacijos rinkimo bei administravimo kaštai savaime veikė kaip saugiklis, nukreiptas prieš netinkamą disponavimą asmenine informacija. Tačiau atsiradus automatizuotai duomenų tvarkymo galimybei šis susirūpinimas tolygiai augo ir savo piką pasiekė įsigalėjus internetui bei mobiliesiems telekomunikacijų įrenginiams. EBPO organizacija [54]pastebi, jog asmens privatumas bus viena tų teisių, kurių išlikimas bei efektyvus realizavimas taps abejotinu XXI amžiuje. Jau dabar egzistuoja visuotinės stebėjimo sistemos, glaudus sekimo kamerų bei palydovų tinklas, galintis aptikti bei atpažinti asmenį pagal tam tikrus specifinius kriterijus. Taip pat plinta daugiafunkciniai įrenginiai, skirti garso bei vaizdo įrašymui. Šiuo metu aptikti žmogaus veiklos pėdsakus yra be galo paprasta, užtenka bent kartą pasinaudoti mobiliuoju telefonu, internetinės bankininkystės paslaugomis ar prisijungti prie duomenų bazės naudojant slapyvardį bei slaptažodį, o tai

[54] E Cornish, "The Cyber Future: 92 Ways Our Lives will Change by the Year 2025" (1996) 30(1) *The Futurist* 27 abstracted in OECD, above n 20, at 12.

sumažina individo privataus gyvenimo erdvę iki minimumo. [55]Tyrimai rodo, jog susirūpinimas privatumo bei asmens duomenų apsaugos problemomis vis didėja. Šiuo atveju kalbama ne vien tik apie asmens duomenų apsaugą, o apie privatumą kaip reiškinį apskritai. Iš esmės galima kalbėti apie du didžiausius pavojų privatumui šaltinius. Pirmasis – fiziniai bei juridiniai asmenys, užsiimantys neteisėtomis veikomis bei renkantys ir pardavinėjantys arba kitaip nelestinai disponuojantys asmeninio pobūdžio informacija. Antrasis šaltinis – valstybė bei jos institucijos, renkančios, tvarkančios bei naudojančios asmens duomenis „nacionalinių interesų“ vardan. Tradiciškai didesnį susirūpinimą visuomenei kelia privačių bei verslo subjektų vykdoma veikla asmeninės informacijos atžvilgiu, tačiau nederėtų nuvertinti ir valstybės, kaip galios monopolį turinčio subjekto, neigiamo poveikio individui ar visuomenei darymo galimybės pasinaudojus asmenine informacija. Daniel‘is Solove‘as, garsus JAV mokslininkas bei autorius privatumo ir asmens duomenų apsaugos srityje, pastebi, jog valstybės kišimasis į jos piliečių (ir ne tik) privatų gyvenimą dažnai pateisinamas „aš neturiu ką slėpti“ argumentu. Kitaip tariant, valstybė teigia, jog „jei jūs neturite ko slėpti, tai ko jums bijoti duomenų rinkimo bei apdorojimo“? Taip primetama nuomonė, jog valstybės institucijos visada yra „teisingas“ duomenų valdytojas bei tvarkytojas ir asmenims „neturintiems ko slėpti“ paprasčiausia nėra pagrindo nerimauti, jog jų asmenine informacija bus disponuojama netinkamai. Deja, valstybės aparatas tėra administracinius bei kitus įgalinimus turinčių žmonių grupė, deleguota ar kitaip paskirta atstovauti visos šalies piliečių [56]interesus. O žmonės – klysta, turi savų išskaičiavimų bei ambicijų, todėl „neabejotinai teisingos“ valstybės modelis yra mažų mažiausiai naivus. 2008 m. Didžiojoje Britanijoje dėl jos institucijų darbuotojų aplaidumo ir netinkamo požiūrio į asmens duomenų apsaugą vos per kelis mėnesius buvo prarastos didžiulės asmens duomenų bazės su privačia piliečių informacija. Gavę tokius duomenis sukčiai gali lengvai juos panaudoti nusikalstamų veikų vykdymui. Tokie ir panašūs atvejai įrodo, jog kai kurių visuomeninių organizacijų susirūpinimas valstybių vykdoma politika privatumo apsaugos aspektu yra pagrįstas. Solove‘as teigia, jog pats „neturiu ką slėpti“ argumentas yra formuojamas klaidingai, kadangi paslapčių neturėjimas nesuteikia teisės kitiems subjektams brautis į asmens privatų gyvenimą. Žinoma, valstybei yra labai patogu turėti kuo daugiau informacijos apie savo piliečius, nes taip yra lengviau surasti prievolių ar įsipareigojimų vengiančius asmenis, atskleisti nusikalstamas veikas ir pan. Tačiau didžiausia problema yra ta, jog šis teisių ir pareigų balansas labai

[55] Tyrimas dėl grėsmių privatumui
http://www.businessweek.com/2000/00_12/b3673010.htm [2008-11-23, 16:15];
Tyrimas dėl labiausiai stebimų visuomenių pasaulyje
http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-559597 [2008-11-23, 16:30];
[56] Ši taisyklė galioja tik toms valstybėms, kurios yra tvarkomos demokratiškai. Priešingu atveju gali nebūti ne tik atstovavimo piliečiams, bet ir teisių į privatumo apsaugą apskritai.

greitai gali būti pažeistas individo nenaudai, o iš to kyla totalaus stebėjimo bei vėliau sekantis neproporcingos valstybinės kontrolės pavojus.

Verslo subjektų ar kitų suinteresuotų asmenų veika, susijusi su netinkamu asmens duomenų rinkimu bei panaudojimu, kelia ne ką mažesnį pavojų nei valstybės vykdomas sekimas. Tiesą sakant, neleistinos operacijos su duomenimis yra labiau pavojingos atskiriems duomenų subjektams sąlyginai trumpu laikotarpiu, kadangi čia duomenys renkami bei naudojami siekiant komercinės naudos ar kitų siauro pobūdžio interesų.

Tiek atskirų fizinių bei juridinių asmenų netinkamas disponavimas privataus pobūdžio informacija, tiek valstybinių stebėjimo bei sekimo sistemų plėtra kartu su technologinėmis galimybėmis sukuria išties rimtas grėsmes privatumui ne tik šalių teritorijų ribose, bet ir pasauliniu mastu. JAV vykdomas [57]elektroninių laiškų bei telefoninių pokalbių turinio filtravimas ieškant kodinių su terorizmu sietinų žodžių įtakoja ne tik tos šalies gyventojus, kadangi didžioji dalis elektroninio pašto serverių įrengti Jungtinių Valstijų teritorijoje, čia taip pat sutelkti ir pasauliniai interneto paslaugų teikėjai, į šią šalį suplaukia pasaulio elektroniniai pranešimai, todėl nacionalinio saugumo agentūros gali skenuoti informacijos srautą neatsižvelgiant nei į asmenų amžių, nei tautybę, nei į pilietybę. Tokie ir panašūs pavyzdžiai rodo, jog technologijų įvairiapusiškumas bei globalumas panašių veiksmų galimybes ypač padidina, todėl pasaulinis privatumo bei asmens duomenų apsaugos reguliavimo klausimas anksčiau ar vėliau turės būti sprendžiamas. Dėl nusikaltėlių vykdomų neleistinų operacijų su asmens duomenimis kenčia tiek eiliniai žmonės, tiek verslo subjektai, tiek valstybė. Tuo tarpu žala, padaroma pasinaudojus tokia informacija, gali būti ne tik moralinė, bet ir materialinė. Nereikia pamiršti ir valstybės vykdomo sekimo, kuris yra gerokai platesnio pobūdžio. Jis nukreiptas ne prieš konkretų asmenį, o prieš visuomenę. Laikui bėgant tokia kontrolės rūšis gali padaryti gerokai didesnės žalos visiems sekamiems asmenims tuo pakirsdama demokratinės valstybės pamatus bei užgniaužda piliečių teisę turėti paslapčių. Šiuolaikinės demokratijos gyvavimo laikotarpis vis dar yra pakankamai trumpas, o šios valdymo formos suteikiama galimybė įvairioms interesų grupėms siekti valdžios taip pat atveria kelią radikaliems elementams, kurie pasitelkę visuotinio stebėjimo sistemas gali neigiamai įtakoti visuomenės raidos kursą. Apibendrinant galima teigti, jog pavojai privatumui šiandieniniame pasaulyje tikrai nėra menki ir turi tendenciją didėti. Jau ne kartą minėti technologiniai, socialiniai bei politiniai veiksniai tiesiogiai įtakoja privatumo sampratos metamorfozes šiuolaikiniame pasaulyje. Todėl tik subrandintais, apmąstytais, kryptingais bei subalansuotais veiksmais įmanoma bent dalinai

[57] Po 2001 m. rugsėjo 11 teroro aktų Federalinis tyrimų biuras (FTB) įdiegė prieštaringai vertinamą šnipinėjimo modulį DCS-1000 paprasčiau vadinamą *Carnivore* (mėsėdis).

sumažinti pažeidimų, galinčių atsirasti dėl netinkamos privatumo pasaugos, skaičių bei sušvelninti iš to kylančius padarinius.

3.2. Netinkamas asmens duomenų naudojimas ir tvarkymas bei su tuo susiję teisės pažeidimai

Kaip jau minėta šio skyriaus pirmojoje dalyje, grėsmės privatumui gali kilti tiek dėl fizinių bei juridinių asmenų, tiek dėl valstybinių institucijų ar įstaigų netinkamų veiksmų. Privatumo bei asmens duomenų apsaugos kraštutiniai reguliavimo oponentai gali ginčyti reglamentavimo griežtumo efektyvumą bei išryškinti neigiamus padarinius, kuriuos toks reglamentavimas sukelia, tačiau sunku paneigti tai, jog per didelė duomenų tvarkymo bei rinkimo laisvė taip pat turi nemažai neigiamų aspektų, kurie galiausiai priveda prie nusikalstamų veikų padarymo. Pats asmeninės informacijos rinkimas, apdorojimas bei keitimasis ja be duomenų subjekto sutikimo yra kriminalizuotas ne visose šalyse. Jungtinėse Valstijose tai legalu ir neužtraukia jokios atsakomybės tokius veiksmus atliekantiems subjektams. Tačiau likusi demokratinio pasaulio dalis dažniausiai laikosi kitokios nuostatos ir baudžia už netinkamą disponavimą asmenine informacija. Kitas klausimas yra susijęs su draudimų efektyvumo įgyvendinimu, kuris toli gražu ne visada būna toks, kokio tikėjosi teisės aktų rengėjai. Nepaisant kai kurių reguliavimo spragų kontrolės buvimas duomenų valdytojus bei tvarkytojus priverčia atsakingiau žiūrėti į savo darbą asmens duomenų apsaugos srityje, o duomenų subjektai gali jaustis saugiau, kadangi žino, jog jiems užtikrinamas minimalus privatumo apsaugos lygis. Išnykus šiam saugumo minimumui grėsmė kyla ne tik privatumui. Netinkamos operacijos su asmens duomenimis, jų praradimas, pakeitimas ar sugadinimas gali iššaukti gerokai sunkesnių padarinių nei tik moralinis diskomfortas. Iš esmės yra dvi visiškai skirtingos privatumo pažeidimo rūšys. Tai tikslinės atakos (angl. *targeted attacks*) bei duomenų rinkinėjimas (angl. *data harvesting* arba *data mining*). Tikslinių atakų metu vienas subjektas nori sužinoti kito subjekto privačią informaciją. Jei duomenų subjektas yra fizinis asmuo, ši veika vadinama tykojimu arba persekiojimu (angl. *stalking*), jei juridinis – minėtieji veiksmai bus traktuojami kaip pramoninis šnipinėjimas (špionažas), o jei duomenys renkami iš valstybės, veika vadinama tiesiog šnipinėjimu. Visos šios alternatyvos yra neteisėtos ir kompiuterinės apsaugos sistemos gali padėti apsaugoti tokius duomenis, tačiau jei tikslinės atakos vykdytojas turi pakankamai resursų, jis gali apeiti saugumo priemones. Duomenų rinkinėjimas paprastai pasitelkiamas nusitaikant į tam tikras tikslines grupes, pavyzdžiui konkretaus teritorinio vieneto interneto vartotojus. Naudojant kryžminės koreliacijos metodą galima surasti asmenis ar asmenų grupes pagal skirtingas charakteristikas, o skaitmeninė informacija bei jos apdorojimo sparta, pigumas bei kokybiškumas

neabejotinai leidžia geriau atsirinkti aukas brukalų siuntinėjimo ar sukčiavimo tikslais. Siekiant apsaugoti asmens duomenų subjektus nuo duomenų rinkinėjimo reikia apsunkinti priėjimą prie asmeninės informacijos naudojant teisines, technines bei programines priemones. Tačiau programinė bei techninė apsauga veikia tik tol, kol duomenys laikomi kompiuteriuose. Perduodant ar gabenant informaciją iš vienos į saugyklos į kitą taip pat galimas informacijos nutekėjimas ir šiuo atveju apsauga yra neveiksminga. Duomenų saugumą galima užtikrinti tik kompleksinėmis priemonėmis, kurios be kita ko apjungtų ir atitinkamą personalo paruošimą, modernių administravimo metodų taikymą ir pan. Deja, absoliuti duomenų apsauga yra neįmanoma, kadangi tobulėjant apsaugos mechanizmams tobulėja ir jų nulaužimo priemonės, todėl idealus kompiuterinių asmens duomenų apsaugos variantas iš tiesų yra utopinis.

Anksčiau minėti pažeidimai privatumo bei asmens duomenų apsaugos srityje yra tiesiogiai susiję su kitomis kur kas sunkesnėmis ir sudėtingesnėmis nusikalstamomis veikomis bei grėsmėmis. Pačios ryškiausios ir didžiausią įtaką šiuolaikinėje visuomenėje darančios veikos bei grėsmės, susijusios su privatumo bei asmens duomenų apsaugos pažeidimais elektroninėje erdvėje, yra:

- Tapatybės vagystės bei tapatybės klastotės (pirmuoju atveju, tai veika, kai pasinaudojus asmens duomenimis neteisėtai pasisavinama kito asmens tapatybė be tikrojo asmens duomenų subjekto žinios ir siekiama naudotis paslaugomis, užsisakyti prekių ar atlikti pinigines operacijas kito asmens vardu, antruoju atveju – veika, kai apgaulės būdu naudojamasi pasisavinta tapatybe kriminaliniams nusikaltimams vykdyti);
- Elektroninis tykojimas (veika, kurios metu pasinaudojus tinklinėmis technologijomis yra persekiojamas kitas asmuo siekiant bauginti, sukelti įtampą bei dvasinį ar fizinį diskomfortą);
- Marketinginis sukčiavimas (veikos, kurių metu sukčiai siūlo investuoti į „pelningą“ verslą, vėliau ilgą laiką moka procentus, kol galiausiai pateikia „išskirtinį pasiūlymą“ investuoti didelę pinigų sumą su didžiulėmis palūkanomis. Kai pervedimai įvyksta sukčiai dingsta su pinigais.);
- Nepageidaujami elektroniniai pranešimai (veikos, kai be asmens sutikimo į jam priklausančią elektroninio pašto dėžutę siuntinėjami elektroninio pašto pranešimai, dažniausiai reklaminio – komercinio pobūdžio);

Čia pateikiamos tik dažniausiai pasitaikančios nusikalstamos veikos susijusios su privatumo bei asmens duomenų apsaugos pažeidimais. Šių veikų rūšių bei porūšių yra kur kas daugiau. Jos buvo tarsi technologinio progreso išdava, todėl net neabejojama, jog tokio pobūdžio nusikaltimų daugės, o žala atsirandanti dėl šių veiksmų ar neveikimo didės. Aišku ir tai, jog sparčiai diegiant inovatyvias technologijas informacinių technologijų (toliau – IT) sektoriuje gali atsirasti naujų nusikalstamų veikų

rūšių bei formų. Visi aukščiau paminėti nusikaltimų modeliai „nepaiso“ teritorinių ribojimų. Tinklinės technologijos įgalina nusikaltėlius naudoti pasaulio gyventojus lyg „melžiamą karvę“. Jie naudojasi teisinio reguliavimo spragomis nacionalinėje bei tarptautinėje teisėje, keičia buvimo vietą priklausomai nuo veikos padarymo sudėtingumo, galimų bausmių ar apskritai tokių veiksmų kriminalizavimo buvimo ar nebuvimo atskirose valstybėse. Kovoti prieš tokias veikas sunku ir todėl, kad kai kurios šalys nėra suinteresuotos užkardyti šių nusikaltimų organizavimo dėl gaunamos finansinės naudos. Pavyzdžiui, Nigerijoje marketinginis klastojimas neoficialiai laikomas trečiu didžiausiu šalies verslu, todėl niekas nėra suinteresuotas imtis ryžtingų veiksmų šiems nusikaltimams sustabdyti.

3.3. Skyriaus apibendrinimas

Privatumo bei asmens duomenų apsaugos poreikis šiandieniniame pasaulyje yra akivaizdus taip kaip yra akivaizdžios grėsmės minėtoms vertybėms. Šiuo klausimu vėl išsiskiria atskirų regionų politika dėl taikomų apsaugos bei prevencinių priemonių. Į privatumo apsaugą svarbu žiūrėti plačiai bei kompleksiškai neapsiribojant vien verslo subjektų kontrole. Valstybių vykdoma privatumo ribojimo politika ilgainiui gali palikti kur kas gilesnius randus visuomenės sąmonėje nei tūkstantis tapatybės vagysčių. Taip pat nedera pamiršti ir klasikinės privatumo bei asmens duomenų apsaugos pažeidimo sampratos ir su tuo susijusių nusikaltimų, kurie, nors ir daromi virtualioje erdvėje, turi labai ryškų atgarsį realiame pasaulyje. Šiuo atveju globalios technologijos kertasi su nacionalinio bei tarptautinio reguliavimo skirtingumu ar trūkumu. Valstybių principingas savos pozicijos laikymasis atstovaujant skirtingoms interesų grupėms atveda prie šio klausimo sprendimo akligatvio ir ieškoti geriausios išeities tokiomis sąlygomis sudėtinga. Taigi apibendrinant šį skyrių galima teigti jog:

- Privatumo apsauga yra ypač svarbi šiandieninių technologijų kontekste;
- Į privatumo bei asmens duomenų apsaugą reikia žvelgti kompleksiškai, įtraukiant ne tik verslo subjektus, bet ir valstybės institucijas;
- Privatumo bei asmens duomenų apsaugos pažeidimai gali lengvai peraugti į gerokai sunkesnius nusikaltimus;
- Valstybių negalėjimas ar nenorėjimas laikytis vieningos pozicijos privatumo bei asmens duomenų apsaugos srityje sąlygoja elektroninių nusikaltimų klestėjimą bei veikų skaičiaus augimą;

4. NAUJOS KARTOS TARPTAUTINIS PRIVATUMO BEI ASMENS DUOMENŲ APSAUGOS REGULIAVIMAS. BŪTINA, BEPRASMIŠKA AR NEIŠVENGIAMA?

Grėsmes privatumui sukelia daugybė tarpusavyje susijusių veiksnių. Trečiame skyriuje nagrinėti pavojai, atsirandantys dėl netinkamos privatumo bei asmens duomenų apsaugos ir su tuo susiję šalutiniai reiškiniai. Pastebima tendencija, jog nusikaltimų, susijusių su privatumo bei asmens duomenų apsaugos pažeidimais, skaičius nuolat auga. Šis augimas yra tiesiogiai susietas su informacinių technologijų naudojimu bei globalios ekonomikos įsigalėjimu. Asmens duomenų rinkimo būdai tampa tobulesni ir vis labiau prieinami plačiai visuomenės daliai. 2008 metais interneto saugumo sprendimų kompanija Symantec atliko [58]tyrimą, kuriuo aiškinosi virtualaus nusikalstamo pasaulio tendencijas ir aktualijas. Nuo 2007 m. iki 2008 m. liepos interneto forumus, pokalbių kanalus ir kitas vietas stebėję Symantec aprašė dažniausiai pasitaikančius virtualius nusikaltimus bei tokiu elementus kaip: specifinės programinės įrangos kainas, kenkėjiškų įrankių pirkėjų ir kūrėjų bendravimo būdus bei priemones, naudojamas priemones nusikalstamoms veikoms atlikti, pavogtos informacijos kelius ir keletą kitų niuansų. Populiariausia nelegali prekė internete - kreditinių kortelių duomenys, kurie sudaro 30% visų šios juodosios rinkos pardavimų. Taip pat paklausi informacija apie banko sąskaitas su prisijungimo prie jų duomenimis. Iš viso Symantec suskaičiavo, kad jų stebimose virtualiuose erdvėse bendravę nusikaltėliai per metus uždirbo apie 275 milijonus JAV dolerių. Prie to pridėjus pajamas, gautas iš kenkėjiškų priemonių panaudojimo, apskaičiuota, jog juodosios interneto rinkos dydis vien JAV siekia 7 milijardus dolerių. Tarp bendrovės identifikuotų tendencijų - augantis kibernetinių nusikaltėlių grupių aktyvumas Rusijoje ir Rytų Europoje. Pastebima, kad agresyvumu jos jau lenkia programišius iš vakarų. Tyrimo rezultatai rodo, jog vagystės, susijusios su asmens duomenimis, tampa puikiu pasipelnymo šaltiniu nusikaltėliams, o patys nusikaltimai nepaiso valstybių sienų bei nacionalinių įstatymų. Akivaizdu, kad senasis privatumo ir asmens duomenų apsaugos reguliavimas turi rimtų trūkumų, todėl ketvirtame skyriuje bus aptariami galimi šių problemų sprendimo būdai bei galimo naujo tarptautinio reguliavimo teigiami nei neigiami aspektai.

4.1. Dabartinis privatumo bei asmens duomenų apsaugos reguliavimo efektyvumas

Nemažai autorių, tokių kaip Daniel‘is Solove‘as, Paul‘as M. Schwartz‘as ar Marc‘as Rotenberg‘as pastebi, jog privatumo apsaugos reguliavimas turi daugybę spragų ir kad vien teisinėmis

[58] Symantec report of underground economy
http://www.symantec.com/business/theme.jsp?themeid=threatreport [2008-12-03, 18:20]

priemonėmis neįmanoma užtikrinti tinkamos šios vertybės apsaugos. Pasaulio veidas nuo 1980 m., kai buvo priimtos EBPO gairės dėl privatumo apsaugos ir asmens duomenų judėjimo tarp valstybių narių, stipriai pasikeitė žvelgiant tiek ekonominiu, tiek socialiniu, tiek technologiniu požiūriu. Deja, pasaulis netapo mažiau susiskaldęs ar silpniau veikiamas pavienių interesų nei anksčiau. Žinoma, galima teigti, jog sovietų bloko subyrėjimas, stipresnės Europos sukūrimas bei demokratinių vertybių iškilimas pakeitė žmoniją ir ji tapo atsakingesnė, taikesnė bei altruistiškesnė. Autoriaus nuomone šios prielaidos yra klaidingos. Taikos ir ekonominės gerovės sąlygomis jos gal ir turi tam tikrą loginį pamatą, tačiau vos prasidėjus konkurencijai dėl „vietos po saule“, tampa akivaizdu, jog nueitas kelias yra ganėtinai trumpas, o pati pasaulinio stabilumo bei vienybės idėja tėra utopija.

Utopija tėra ir efektyvus tarptautinis privatumo bei asmens duomenų apsaugos reguliavimas. Autorius mano, jog pasaulio valstybės bei regionai yra labai skirtingi įvairiais aspektais. Nekalbant apie politinę ideologiją dar egzistuoja kultūra, religija bei papročiai, kurie smarkiai įtakoja vienos ar kitos valstybės gyventojų elgseną. Vieša paslaptis yra ir tai, jog pasaulio politinės bei ekonominės dinamikos tendencijas diktuoja keletas ekonominiu bei kariniu požiūriu stipriausių valstybių ir panašu, jog ši tendencija tikrai nepasikeis artimiausiu metu. Įvairios tarptautinės organizacijos, įskaitant ir JT, bando prižiūrėti tarptautinių procesų virsmus, bet ši priežiūra, poveikis bei rekomendacijos veikia tik tol, kol nepaliečiami strateginiai stiprių valstybių interesai. Tarptautinės teisės normos galios tik tuo atveju, jei šalys savanoriškai sutiks laikytis bendrųjų principų bei sugebės paaukoti mažą dalį savo interesų pasaulinio stabilumo vardan. Kol svarstomi klausimai, susiję su priemonėmis, reikalingomis ekonominių procesų optimizavimui, tarptautinė viešoji teisė veikia puikiai. [59]Sugebama priimti tarptautinius teisės aktus reguliuojančius vieną ar kitą ekonominio gyvenimo sritį, kadangi tai naudinga visoms susitariančioms valstybėms. Problemų kyla tada, kai tarptautinių susitarimų reikalavimai neigiamai veikia valstybių interesus. Tokie susitarimai paprastai turi sąsajų su žmogaus teisių klausimų sprendimu, karinių priemonių naudojimu, ekonominių apribojimų taikymu ir panašiai. Pavyzdžių, kai vienos įtakingos valstybės atsisakymas prisijungti prie tarptautinio dokumento pakerta pačią jo dvasią, yra apsčiai. Kioto protokolą, kuris veikia kaip pasaulio valstybių elgesio kodeksas, reguliuojantis šiltnamio efektą sukeliančių dujų išmetimą, yra pasirašę bei ratifikavę absoliuti dauguma pasaulio valstybių, tačiau šiame sąraše nėra Jungtinių Valstijų, kurios atsisako prisijungti prie dokumento. JAV yra viena iš pirmaujančių valstybių pagal šiltnamio efektą

[59] Pavyzdžiui, 1956 m. Ženevos tarptautinio krovinių vežimo keliais sutarties konvencija nustato vienodas krovinių vežimo tarptautiniu automobilių transportu taisykles. Remiantis šia konvencija krovinių pervežimai vyksta sklandžiau, greičiau, patikimiau, o svarbiausia tai, jog suvienodintas reguliavimas išlaisvina verslą bei neša naudą visoms valstybėms prisijungusioms prie dokumento. Kitaip tariant, aplinkybės, reikalingos tarptautinių teisės normų priėmimui ir įgyvendinimui, palankiausios būna tada, kai tokio teisės akto priėmimas pagerina šalies, kuri prisijungia prie konvencijos, ekonominę ar socialinę būklę.

sukeliančių dujų išmentimą į aplinką. Šios šalies nebuvimas tarp protokolą ratifikavusiųjų iš esmės padaro jo poveikį aplinkai niekiniu arba bent jau abejotinu. Kitas pavyzdys, [60]Konvencija dėl elektroninių nusikaltimų. Rusija yra pasirašiusi šį dokumentą, tačiau atsisako jį ratifikuoti dėl nesuderinamumo su jos nacionaline teise. Šios šalies piliečiai yra gerai žinomi elektroninių nusikaltimų organizavimo bei vykdymo srityje. Kibernetinių atakų vykdymas prieš suverenias valstybes, plataus mąsto nelegalios finansinės operacijos bei aukšto lygio piratavimas jau yra tapę Rusijos „vizitine kortele“. Nepaisant to, Rusija yra įtakinga pasaulinės politikos žaidėja ir šios šalies vadovai puikiai žino, jog kitos valstybės oponentės geriausiu atveju „išreikš susirūpinimą“ dėl tokios padėties. Ši taisyklė taikytina ir kitoms didžiosioms valstybėms. Tuo tarpu jei panašiai elgtųsi smulkios tarptautinės arenos veikėjos, joms būtų daromas politinis arba ekonominis spaudimas ir reikalai (neturint stiprių užtarėjų) greitai pajudėtų iš mirties taško pagal didžiųjų valstybių scenarijų.

Kita kliūtis visuotinio bei veiksmingo tarptautinio teisės akto sukūrimui slypi pačioje teisės į privatumą koncepcijoje. Anksčiau jau buvo minėta, jog šios teisės apsauga įmanoma tik demokratinėje valstybėje, kurioje vyrauja natūralistinės krypties požiūris į teisę. Remiantis juo, [61]pripažįstama, kad žmogaus teisės ir jų įgyvendinimas priklauso asmeniui iš prigimties (gimimo), kad jos nuo valstybės nepriklausomos ir neatimamos. Valstybė ir visuomenė privalančios jas tik saugoti, lemti jų įgyvendinimą. Demokratinio modelio valstybės prigimtines teises naudoja kaip visuomenės sutarties pagrindu sukurtos sistemos vieną iš sudedamųjų elementų. Pats šių teisių pobūdis preziumuoja, jog pagrindinės žmogaus teisės nėra valstybės malonė asmeniui. Valstybė turi tik saugoti asmens teises, kurias jis pats įgijo atitinkamų pareigų vykdymu. Bet yra teisių, kurios atsiranda kaip valstybės teisėkūros rezultatas: pavyzdžiui, teisė į susirašinėjimo slaptumą ar būsto neliečiamybę. Tačiau tai taip pat nereiškia, kad valstybė gali pripažinti šias teises ar jų nepripažinti. Žmogus objektyviai turi teisių į šias socialines vertybes, nes jos yra išvestinės iš žmogaus orumo ir laisvės. Bet kad šios teisės iš teisnumo statuso pereitų į subjektinę teisę, reikia, kad valstybė pripažintų tai įstatymais. Problema, jog šioje srityje privatumo teisių apsauga vertinama nevienareikšmiškai ir nacionalinė ar regioninė apsaugos įgyvendinimo forma gali skirtis viena nuo kitos. Nesant vieningos nuomonės nacionaliniu lygmeniu dar sunkiau surasti sprendimą tarptautiniame kontekste.

[60] Konvencija dėl elektroninių nusikaltimų, http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=228195&p_query=&p_tr2= [2008-12-04],
[61] Alfonsas Vaišvila. Teisės teorija. Vilnius: Justitia, 2000. P. 139

Kita teorinio pobūdžio problema – valstybės, kurios savo modelį konstruoja pagal pozityvistinį požiūrį į teisę. Šis požiūris teigia, kad žmogaus teisės kyla iš valstybės, o ši savo nuožiūra jas žmogui suteikia, nustato jų apimtį ir panorėjusi gali jas taip pat savo nuožiūra siaurinti, o kai kurias ir visiškai likviduoti . Tuo norima pasakyti, kad žmogus iš prigimties neturi jokių teisių, kad jos ateina tik iš tos organizuotos bendrijos, kurioje asmuo gyvena, veikia ir kuri gali laisvai manipuliuoti jo teisėmis. Šis požiūris paprastai būdingas autoritarinėms arba totalitarinėms valstybėms, ekonomiškai atsilikusioms visuomenėms, kur asmuo nepajėgia be valstybės ar visuomenės paramos garantuoti bent minimalios savo teisių saugos. Kinijos Konstitucijos 37 straipsnyje kalbama apie šios šalies piliečių teisę į susirašinėjimo slaptumą, tačiau tuo pačiu pažymima, jog ši teisė gali būti ribojama nacionalinio saugumo interesų vardan. Totalitarinėse valstybėse labai daug sričių patenka po „nacionalinių saugumo interesų gynybos“ skėčiu. O privatumą minimaliai užtikrinančios teisės galioja tik tiek, kiek tai netrukdo valdžios vykdomai politikai bei kitiems interesams.

Tenka pripažinti, jog privatumo bei asmens duomenų apsaugos klausimai turi tiesioginių sąsajų ne tik su ekonominiais, bet ir su politiniais interesais, neužmirštant ir kertinių teorinio pobūdžio problemų. Nemažai autorių išskiria 1980 m. EBPO gairių „atsparumą“ laiko bei technologijų iššūkiams. Džiaugiamasi, jog šio dokumento pagrindu formuojama pasaulinė keitimosi asmens duomenimis bei privatumo apsaugos praktika. Pabrėžiamas didžiulis tuo metu suformuotų principų vaidmuo privatumo teisės gynimo kontekste. Žinoma, gairių įtaka yra nenuginčijama ir buvo pakankamai efektyvi savo sukūrimo laikmečiu, tačiau pasikeitus pasaulinei situacijai viskas atrodo kiek kitaip. Šis dokumentas yra naudingas vien tuo, jog jam paprasčiausiai nėra rimtos alternatyvos, atitinkančios šiandienos realijas. Ne išimtis ir 1981 m. Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu. Savu laiku ji nustatė imperatyvaus pobūdžio taisykles, skirtas apsaugoti asmenų privatumą, tačiau laikui bėgant šios nuostatos tapo nepakankamos visapusiškai apsaugai pasiekti ir galiausiai virto deklaracijomis, kurios gražiai atrodo popieriuje, bet mažai teįgyvendinamos praktikoje. Autorius nemano, jog minėtų dokumentų siūlomas reguliavimo modelis yra netinkamas. Jis paprasčiausiai nėra pakankamas ir šiuolaikinių technologijų kontekste neužtikrina asmens teisių į privatumą apsaugos. Kaip pastebi Paul‘as M. Schwartz‘as bei kiti autoriai privatumo ir asmens duomenų apsaugos srityje, minėtąją teisę šiuo metu įmanoma apsaugoti tik naudojant kompleksines priemones ir vien naujo pobūdžio teisinis reguliavimas problemos neišspęs.

4.2. Problemų, kylančių dėl naujos kartos teisinio reguliavimo nebuvimo privatumo bei asmens duomenų apsaugos srityje, analizė

Skirtingas teisinių santykių reglamentavimas globalumo ženklu pažymėtose srityse visada sukelia papildomų rūpesčių tiek valstybėms, tiek verslininkams, tiek paprastiems asmenims. Skirtingas teisės į privatumą reguliavimas – ne išimtis. Jau anksčiau minėta regioninė konkurencija dėl privatumo gynybos modelio abiem pusėms kainavo nemažai emocinių bei finansinių resursų. Nesunku įsivaizduoti, kokia buvo JAV verslo atstovų reakcija, kai buvo pranešta, jog remiantis ES Privatumo direktyva jie negalės keistis asmens duomenimis su Sąjungos valstybėmis narėmis, nes JAV neatitinka adekvataus apsaugos lygio reikalavimų. Nuotaikos priešingoje, ES, stovykloje taip pat turėjo būti ne pačios maloniausios, kai žmogaus teisių aktyvistai, inicijavę Privatumo direktyvos priėmimą, sužinojo, jog ES nuo šiol aktyviau kovos prieš terorizmą ranka rankon su Jungtinėmis Valstijomis ir priims Direktyvą, kurios pagrindinis tikslas – kaupti bei saugoti plataus spektro srauto bei vietos nustatymo duomenis. Tiek vienas, tiek kitas scenarijus suveikė todėl, kad šios dvi milžiniškos ekonomikos nesusitarė tarpusavyje ir atskirais veiksmais išbalansavo teisių į privatumą gynybą pasauliniu mastu. Griežtas bei detalus asmens duomenų apsaugos reglamentavimas pagal 95/46/EB bei kitas direktyvas davė tam tikrų rezultatų, bet pasaulis nuo to nepasikeitė, nes sudėtingas ir kartais brangiai kainuojantis teisės normų reikalavimų vykdymas pagimdo kitus neigiamus reiškinius, tokius kaip vengimas vykdyti prievoles ar spragų teisės aktuose išnaudojimas. Konkurencija grįsti santykiai tarp atskirų blokų srityje, kurioje būtinas susitarimas bei pagarba vienas kitam, privedė prie to, ką teisės mokslininkai vadina privatumo krize.

Iššūkiai, atsirandantys dėl vieningo reguliavimo trūkumo, gali būti skirstomi į tris grupes. Visų pirma, tai teisinis nesuderinamumas, susietas su vieningu teisės taikymu identiškų problemų atveju. Teisę į privatumą pripažįstama demokratinėse valstybėse, tačiau jos tolimesnis plėtojimas susiduria su problemomis, kadangi privatumo sampratos aiškinimui didžiulę įtaką daro tokie veiksniai kaip šalies politinis klimatas, papročiai bei kultūra. Teisės mokslininkai tvirtina, jog „privatumo“ sąvoka yra tokia paini, kad yra be galo sunku ją konkretizuoti bei aiškiai nubrėžti liniją tarp to, kas privatu ir to, kas vieša. Kai kurie autoriai piktinasi tokiu sąvokos neapibrėžiamumu ir atvirai jį kritikuoja kaip [62]„nepakenčiamai neaiškų bei miglotą“, [63]„užterštą žalingu dviprasmiškumu“, kiti tiesiog pažymi, jog [64]„bandymai konceptualizuoti privatumą nėra sėkmingi“. Bene taikliausią bei aštriausią įžvalgą teisės į

[62] Arthur R. Miller, The assault on privacy: computers, data banks, and dossiers, 1971, P.: 25
[63] Hyman Gross, The Concept of Privacy, 1967, 43 N.Y.U. L. Rev., P.: 34 – 35
[64] Colin J. Bennet, Regulating privacy: data protection and public policy in Europe and the United States, 1992, P.: 25

privatumą atžvilgiu yra padariusi filosofė Judith'a Jarvis Thomson, kuri sako, jog [65]„niekas iš tiesų aiškiai nesuvokia kas tai yra". Ši sąvoka yra išties labai plati ir persipynusi su kitomis vertybinėmis kategorijomis. Logiškiausia ją būtų vertinti ne kaip informaciją, intymumą ar neprieinamumą, o kaip visų šių elementų visumą, kadangi teisė į privatumą apima ne tik informaciją apie asmenį, bet ir jo teisę į intymią erdvę bei neliečiamumą. Žiūrint plačiau, šios teisės veikimo apimtis suvokiama skirtingai. Europos šalyse ji – socialiai orientuota ir nukreipta individo apsaugai iškeliant ją virš verslo interesų, tuo tarpu JAV svarbesne laikoma žodžio laisvė, o teisės į privatumą gynimu stengiamasi nekliudyti verslo subjektams. Vieningos teisinės privatumo sampratos nebuvimas apsunkina bendro problemos vardiklio ieškojimo procesą.

Antroji problema – ekonominiai veiksniai. Duomenų tvarkytojams bei valdytojams nekyla problemų, kai jie veikia vieningą reguliavimą privatumo atžvilgiu turinčiose teritorijose. Tačiau subjektams, kuriems gyvybiškai svarbus keitimasis asmens duomeninis su trečiosiomis šalimis, reguliavimo skirtumų klausimas tampa rimtu galvos skausmu. Teisiniai varžtai spaudžia verslo subjektus ir šie verčiami ieškoti kitų problemos sprendimo priemonių, kartais – nelegalių. Šiuo atveju nekalbama apie asmens duomenų apsaugos panaikinimą ar ribojimų atsisakymą, nes verslo interesų kontrolės mechanizmai turi būti, tiesiog dėl skirtingų reguliavimo nuostatų stipriai išauga išlaidos operacijoms su duomenimis. Dvigubų standartų taikymas neigiamai įtakoja ne tik techninę – materialinę reiškinio pusę, bet ir sukuria žmogiškųjų išteklių problemą, nes kiekvienos šalies partnerės teisinės bazės išmanymas yra būtinas norint sklandžiai vykdyti veiklą. Per dideli draudimai ir ribojimai niekada neskatino verslo aktyviau imtis teisėtos individualios veiklos, jie greičiau veikia kaip slopinantis veiksnys, o tai galiausiai įtakoja ir viso pasaulio ekonominius rodiklius, kadangi tie sektoriai, kurie dažniausiai disponuoja asmeninio pobūdžio informacija, veiklą vykdo globaliniu mastu, taip kurdami pridėtinę vertę keliose valstybėse iš karto.

Trečiasis neigiamą įtaką darantis veiksnys – technologinis. Teisinis reguliavimas dažniausiai gerokai atsilieka nuo technologinio vystymosi. Tai stabdo progresą bei sudaro papildomas kliūtis inovacijų diegimui. Teisiškai labai sunku prognozuoti visuomenės raidos kryptis bei kokias pasekmes ar kokiu pavojus sukels viena ar kita techninė naujovė, todėl, paprastai, reguliavimo imamasi tada, kai išryškėja nauji neigiami technologijų naudojimo aspektai. Prieš dvidešimt metų elektroniniai nusikaltimai buvo pavienis reiškinys, neįtakojęs bendros kriminogeninės padėties pasauliniu lygmeniu. Šiandien nuostoliai, patiriami dėl veikų, susijusių su virtualia erdve, skaičiuojami šimtais milijonų dolerių. Bandydamos apsisaugoti nuo galimų grėsmių šalys stengiasi nacionalinių teisinių instrumentų

[65] Judith Jarvis Thomson. The Right to Privacy, in philosophical dimensions of privacy: An anthology. 1984., P.: 272

pagalba riboti nusikalstamas veikas, tačiau elektroninėje erdvėje, kuri yra beribė ir nepripažįstanti teritorijos, ši kontrolė tampa sudėtinga. Skirtingas teisinis reguliavimas iš vienos pusės slopina technologijų pažangą, kadangi išaugus kaštams reikia daugiau investuoti į automatizuotas sistemas, o tai ne visada apsimoka finansiškai. Kita vertus, panašūs reguliavimo skirtumai gali ir padėti technologiniam progresui įgauti pagreitį, tik šiuo atveju, inovacijos bus kuriamos ne vieningam bei saugiam duomenų perdavimo užtikrinimui, o pavienių saugos sistemų nulaužimui bei apėjimui, siekiant neteisėtų tikslų.

Taigi, jei reguliavimo skirtumai iš tiesų yra didžiąja dalimi žalingi tiek teisiškai, tiek ekonomiškai, tiek technologiškai, kodėl nesiimama ryžtingų veiksmų teisinio reguliavimo suvienodinimui? Viena vertus, teisė paprasčiausiai nespėja sulig technologijomis ir sureguliavus vieną probleminę sritį viskas gali apsiversti aukštyn kojom papūtus naujiems pažangių sumanymų vėjams. Pats teisinių priemonių apsvarstymo bei priėmimo procesas nėra pigus, kadangi reikalauja tiek laiko, tiek kapitalo sąnaudų. Pavėluotas bei brangiai kainuojantis tokio reguliavimo įgyvendinimas gali nepasiekti savo tikslų, dėl kurių ir buvo kuriamas. Kita vertus ideologinės priešpriešos įneša savo dalį į panašių problemų sprendimą. Skirtingas tų pačių kategorijų suvokimas neabejotinai apsunkina kompromisinių variantų paieškas. Trečias aspektas – ekonominė nauda. Griežti privatumo bei asmens duomenų apsaugos reikalavimai gal ir padeda asmens duomenų subjektams jaustis saugesniais, bet ekonominiu požiūriu toks reguliavimo pobūdis yra nuostolingas, todėl kai kurios šalys pasirenka vieną blogybę iš dviejų ir vysto verslo sektorių privatumo sąskaita, juolab kad ir pats šios vertybės užtikrinimas ne visada atneša lauktus rezultatus, turint omenyje kaip greitai šiuolaikinių technologijų pagalba galima keistis informacija, ir kaip sunku tokius srautus kontroliuoti. Šią kovą su „vėjo malūnais“ galima iliustruoti Didžiosios Britanijos pavyzdžiu. [66]Šalies oficialios institucijos bandė riboti informacijos platinimą bei komentavimą apie ponios Rosemary West, tuo metu kaltintos dėl dalyvavimo visuomenę sukrėtusiose serijinėse žmogžudystėse, bylos eigą, kadangi buvo norima sumažinti kišimąsi į nešališką teismo procesą. Informacijos ribojimas gal ir būtų suveikęs tradicinėse žiniasklaidos priemonėse, tačiau minėtos pastangos nuėjo perniek interneto erdvėje, kadangi straipsniai bei komentarai plūdo iš už Britanijos sienų. Šis ir panašūs atvejai įrodo, kad probleminių klausimų šioje srityje yra daug ir nepanašu, jog jų skaičius mažėtų. Veikdamos pavieniui šalys nesugeba ir ateityje vargu ar sugebės susidoroti su iššūkiais privatumui elektroninėje erdvėje, todėl būtina derinti įvairias priemones siekiant geriau apginti šią teisę, jei išvis įmanoma tai padaryti.

[66] T. Miller. Law, Privacy and Cyberspace // Communications Law, 1996, P. 143-145.;

4.3. Naujų privatumo bei asmens duomenų apsaugos reguliavimo modelių privalumai bei trūkumai

Nors situacija privatumo bei asmens duomenų apsaugos srityje sudėtinga, visgi ji nėra be išeities. Vienokio ar kitokio pobūdžio korekcijos įmanomos šalims susitarus tarpusavyje bei pradėjus taikyti priemonių paketą, skirtą teisių užtikrinimui įgyvendinti. Šiuo atveju kalbama ne tik apie teisinę reikalo pusę. Nederėtų užmirši ir techninių galimybių, kurias suteikia tie patys veiksniai, kurie ir sukūrė problemą. Anksčiau ar vėliau reikės iš esmės persvarstyti privatumo bei asmens duomenų apsaugos problematiką, nes pasaulis šuoliuoja į priekį septynmyliais žingsniais, o teisės normos sukuria stagnaciją, kadangi nespėjama paskui technologijų traukinį. Norom nenorom kyla ir kitas klausimas: ar ne per vėlu rūpintis privatumo bei asmens duomenų apsauga, kai keitimosi duomenimis procesai jau seniai įgavę pagreitį nepriklausomai nuo esamo reguliavimo? Faktas, jog šimtu procentų minėtųjų teisių apginti nepavyks, galbūt nepavyks to padaryti net penkiasdešimčia atvejų iš šimto, tačiau tai toli gražu nereiškia, jog apskritai reikia atmesti privatumo apsaugos svarbą, kadangi už kiekvienos apgintos teisės slypi kažkieno teisėti interesai, o apsaugojus konfidencialią informaciją gali būti išvengta nusikalstamų veikų duomenų subjektų atžvilgiu, todėl šioje dalyje ir bus nagrinėjamos galimos alternatyvos bei papildomos priemonės, reikalingos veiksmingesnei privatumo bei asmens duomenų apsaugai užtikrinti.

4.3.1. Naujo tarptautinio teisės akto, reglamentuojančio privatumą bei asmens duomenų apsaugą, privalumai bei trūkumai teisės į privatumą aspektu

Dar visai neseniai vos ne mados dalyku buvo tapęs teiginys, jog [67]internetui bei su juo susijusioms technologijoms negalioja tradiciniai įstatymų rėmai. Tokie ir panašūs pasvarstymai yra gerokai išpūsti ir priskirtini mitų apie IT kategorijai. Nors tinklinės technologijos ir yra teritoriškai beribės, santykinai naujos bei nestokojančios iššūkių tradicinėms normoms bei vertybėms, jos visgi nėra nepasiekiamos įstatymui. Žinoma, dalis teisės aktų yra parengti taip, kad jų pritaikymas naujiems procesams yra komplikuotas, tačiau didžioji jų dalis visgi yra technologiškai neutralūs ir šiek tiek pakeitus normų interpretavimą galima įstatymuose esančias nuostatas pritaikyti ir virtualiam pasauliui. Todėl klausimą: „ar galima dabartinį reguliavimą taikyti tinklinių technologijų atžvilgiu“ reikėtų keisti

[67] Viena iš labiausiai retoriškai išplėstų šio tvirtinimo versijų yra išsakyta John‘o perry Barlow‘o „Kibernetinės erdvės nepriklausomybės deklaracijoje“ paskelbtoje internete 1996 metų vasarį.
http://homes.eff.org/~barlow/Declaration-Final.html [2008-12-10];

kitu: „kaip minėtąsias reguliavimo nuostatas reikėtų taikyti naujųjų technologijų kontekste?“ Antrasis klausimas suskyla į keletą mažesnių, tokių kaip:

- Ar teisinis reguliavimas duoda norimų rezultatų?
- Ar tinkamai suderinami skirtingų grupių interesai?
- Ar rezultatai, kuriuos sąlygoja reguliavimo buvimas nėra netikėti ar neprognozuoti blogąja prasme?
- Ar teisės normos aiškiai apibrėžia leistinus ir neleistinus veiksmus elektroninėje erdvėje?

Kalbant apie poveikį pasauliniams procesams galima teigti, jog dažniausiai (bet ne visada) teisinio reguliavimo normos duoda teigiamus bei lauktus rezultatus. Atvejai, kai toks reguliavimas neveikia yra specifiniai, nes tiek tarptautinio, tiek regioninio pobūdžio dokumentuose apie tinklines technologijas kalbama gana aptakiai, išimtis galėtų būti nebent direktyva 2002/58/EB, tačiau ji taikoma tik telekomunikacijų sektoriui ir neapima visos elektroninės erdvės. Kitais specifiniais atvejais reguliavimo efektyvumas gali kelti abejonių. Pavyzdžiui, Europos Sąjunga labai plačiai užsimojo taikydama Privatumo direktyvą. Ji numato, jog tam tikrais išimtiniais atvejais Direktyvos nuostatos gali būti taikomos už ES sienų (jei duomenų valdytojas veikiantis trečiojoje šalyje naudoja techninę įrangą, kuri yra skirta kitiems tikslams nei tik mechaniniam duomenų perdavimui ir ši įranga yra šalyje narėje). Toks platus Direktyvos taikymas yra praktiškai neįmanomas, kadangi kitos šalys bematant užginčytų šią ES prisiimtą teisę.

Kaip jau minėta, tarptautinio pobūdžio teisės aktai aptakiai kalba apie naujųjų technologijų sukurtus iššūkius bei sunkiai sugeba prisitaikyti prie nūdienos realijų. Šiuo metu pasigirsta nuomonių, jog reikia pereiti prie trečios kartos privatumo bei asmens duomenų apsaugos teisinio reguliavimo. Šios kartos teisės aktai pasižymėtų didesniu dėmesiu privatumo apsaugai elektroninių technologijų kontekste. Tačiau efektyvus tokio teisės akto priėmimas būtų sunkiai įmanomas. Teisėje, priešingai nei technologinėje sferoje, naujos reguliavimo formos bei būdai sunkiai skinasi kelią į šviesą. Konservatyvus požiūris bei baimė pabloginti esamą situaciją dažnai sulaiko vieną ar kitą šalį nuo ryžtingų sprendimų priėmimo bei įgyvendinimo. Žinoma, jei JAV ir ES pavyktų rasti kompromisą dėl privatumo bei asmens duomenų apsaugos lygio, galbūt būtų įmanoma bendrą poziciją „eksportuoti“ į kitus demokratinius regionus. Demokratinė teisių į privatumą prigimtis šiuo atveju yra ir stiprybė, ir silpnybė tuo pačiu metu. Stiprioji pusė yra ta, jog minėtoji vertybė turi tvirtą bei nenuginčijamą pagrindą, grįstą prigimtinėmis žmogaus teisėmis bei laisvėmis. Silpnoji grandis – demokratijos poreikis siekiant šią teisę tinkamai realizuoti. Kinijoje interneto vartotojų skaičius auga ne procentais, o kartais,

tuo tarpu pati valstybė yra griežtai autoritarinė ir teisės į privatumą ribos yra labai miglotos, jei išvis įmanomos. Prognozuojama, jog XXI a. antrojoje pusėje pasaulio ekonominės galios ašis nukryps į Azijos valstybes. Klausimas: ko vertas naujo pobūdžio tarptautinis dokumentas, jei prie jo neprisijungia didžiausią gyventojų skaičių bei potencialių tinklinių technologijų naudotojų skaičių turinti šalis? Ir Kinija toli gražu nėra vienintelė valstybė, kurioje demokratijos procesai nuslopinti, o teisė į privatumą nuolat pažeidinėjama prisidengiant „nacionalinio saugumo interesais“. Autoriaus nuomone reikėtų ne stengtis sukurti naują tarptautinį teisės aktą, o tobulinti senąjį reguliavimą, nes:

- Neprisijungus prie naujojo dokumento įtakingoms, ekonomiškai stiprioms, bet totalitarizmo pagrindais valdomoms valstybėms, pati tokio teisės akto veiksmingo veikimo idėja būtų pakirsta;
- Sukurti universalų dokumentą, kuris išsamiai reglamentuotų elektroninėje erdvėje vykstančius procesus yra be galo sudėtinga, dėl minėtųjų procesų kitimo dinamikos bei sunkiai nuspėjamų virsmų, galinčių iš esmės pakeisti technologijų kryptį;

Naujos kartos tarptautinio teisės akto efektyvus veikimas yra abejotinas, bet tai toli gražu nereiškia, jog nieko neįmanoma padaryti siekiant apsaugoti privatumą bei asmens duomenis. Visų pirma reikėtų iš naujo peržiūrėti tarptautinį, regioninį bei nacionalinį reguliavimą. Kiekviena šalis turėtų surengti plataus masto diskusiją, kurios pagrindinė tema būtų „naujųjų technologijų iššūkiai teisės į privatumą užtikrinime“. Ši diskusija turėtų apimti įvairias sritis, pradedant nuo įstatyminės bazės peržiūros, mokslininkų pastebėjimų bei pasiūlymų, iki technikų pastabų technologijų raidos kontekste. Išsiaiškinus esminius klausimo aspektus bei sutarus dėl naujų bendrųjų principų derėtų inicijuoti diskusijas tarptautiniu mastu, kadangi ir pačios technologijos, iššaukusios naujų formų reguliavimo poreikį, yra globalios. Nepradėjus privatumo klausimo reguliavimo kelti tarptautiniu lygmeniu, atskirų valstybių pastangos bent kiek sutvarkyti šią sritį tebus teisinių spragų lopymas, kurio nauda abejotina dėl reguliuojamų santykių specifikos. [68]Valstybės, atsinešę savo patirtį, įžvalgas bei gerąją praktiką į tarptautinius forumus turėtų iš naujo suformuluoti leistino elgesio elektroninėje erdvėje standartus, kuriuose didelis dėmesys būtų skiriamas privatumui bei asmens duomenų apsaugai. Taip pat reikėtų peržiūrėti EBPO gairių dėl privatumo apsaugos ir asmens duomenų judėjimo tarp valstybių narių principus. Jiems jau beveik 30 metų ir šiuolaikinių technologijų kontekste minėtosios principinės nuostatos turi didelių spragų. Gairės turėtų būti papildomos tokiomis nuostatomis kaip [69]teise būti neindeksuotam; teise koduoti asmeninę informaciją; teise reikalauti, kad asmeninė

[68] G Greenleaf. Privacy Principles: Irrelevant to Cyberspace? // Privacy Law and Policy Reporter, 1996, volume 114, P. 118-119;
[69] Mindaugas Civilka. Asmens duomenų apsaugos reguliavimas interneto kontekste. Vilnius, 2001

informacija būtų teisingai ir sąžiningai tvarkoma viešosiose infrastruktūrose užtikrinant, kad asmuo nebūtų neteisėtai nušalintas nuo galimybės dalyvauti ginant savo teises; teise tikrinti bei suprasti automatinius sprendimus; teise reikalauti, kad būtų atskleistas asmeninės informacijos, kurios pagrindu gali būti kuriamas asmens profilis, rinkimas. Atlikus šiuos bei kitus papildymus būtų galima sukurti skaidresnę, atviresnę bei saugesnę erdvę asmens duomenų subjektams, kur jie patys turėtų daugiau įtakos kontroliuojant veiksmus, atliekamus su asmens duomenimis.

Nacionalinės valdžios, kaip pagrindinės privatumo bei asmens duomenų apsaugos gynėjos statusas taip pat turėtų būti persvarstytas, kadangi nemaža dalis su privačia informacija susijusių pažeidimų ir kyla būtent iš valstybinių institucijų. JAV 1993 m. buvo pateikta iniciatyva dėl leidimo „nulaužti“ asmeninės informacijos duomenų kodus taip siekiant apsaugoti visuomenę nuo [70]„gangsterių, teroristų bei narkotikų platintojų“. Šie veiksmai turėjo būti atliekami be teismo leidimo ir galėjo apimti informacijos rinkinėjimą lankomose interneto svetainėse, forumuose bei virtualiuose pokalbių kambariuose. Be abejo, visuomenės saugumas ir sveikata yra didelės vertybės, tačiau potencialus skaičius žmonių, kuriuos tokia nuostata apsaugotų ir skaičius tų, kuriems galėtų būti pakenkta yra toli gražu ne proporcingas. Galiausiai reikėtų šviesti bei mokyti visuomenę gerbti asmenų privatumą, nustatant aukštus šios teisės apsaugos standartus ne tik valstybei, atskiriems piliečiams bei verslo subjektams, bet ir žiniasklaidai, kuri dėl moderniųjų technologijų skvarbos patiria didžiulę konkurenciją bei spaudimą „pateikti karščiausias žinias“, o tai neretai pastūmėja žurnalistus peržengti kitų asmenų privatumo ribas.

Privatumo bei asmens duomenų apsaugos principai nėra netinkami šiandieninei situacijai, jie tiesiog yra per daug abstraktūs bei deklaratyvūs. Atsižvelgiant į interneto bei kitų tinklinių technologijų plėtrą reikia ne tik peržiūrėti bei papildyti senąsias reguliavimo nuostatas, bet ir pradėti didžiulę švietimo kampaniją, kurios pagrindinis tikslas – atskleisti žmogaus teisių instituto svarbą bei gynybos būtinybę plačiajai visuomenei. Visiškai naujo bei „revoliucingo“ tarptautinio dokumento priėmimas vargu ar padėtų rasti išeitį iš susidariusios situacijos, kadangi technologijų kursas gali bet kurią akimirką pakeisti kryptį. Be to, neturint vieningo privatumo bei asmens duomenų apsaugos supratimo nebūtų įmanoma ir efektyvi šių teisių gynyba.

[70] R. Wacks. Privacy in Cyberspace: Personal Information, Free Speech and the Internet in P Birks // Oxford: Privacy and Loyalty, 1997 P.: 107

4.3.2. Probleminiai privatumo bei asmens duomenų apsaugos savireguliacijos aspektai

Savireguliacija nėra kažkuo išskirtinis reiškinys procesuose, susijusiuose su privatumu bei asmens duomenų apsauga. Kai tam tikros interesų sritys susikerta tarpusavyje ir tam nėra tinkamo valstybinio reguliavimo, suinteresuotų grupių savarankiškas problemų sprendimas paprastai būna pirmoji priemonė, kurios imamasi. Savireguliacija kartais būna veiksmingesnė už „priverstinį" reguliavimą, kadangi geriausiai išreiškia skirtingų grupių požiūrius bei padeda suderinti interesus tokiu lygmeniu, kokio pageidauja visos suinteresuotos šalys. Tačiau tokio reguliavimo efektyvumas įmanomas tik tada, kai visos pusės yra daugmaž „vienodų svorio kategorijų". Privatumo bei asmens duomenų apsaugos atveju, ši taisyklė nelabai tinka, kadangi valstybiniai bei verslo subjektai yra gerokai „galingesni" už eilinius piliečius, todėl yra pavojus, jog normos nereprezentuos visų grupių interesų tinkamai, o tai privestų prie piktnaudžiavimo galia bei rimtų privatumo bei asmens duomenų apsaugos pažeidimų.

Savireguliacija vertinama nevienareikšmiškai. Vieni [71]autoriai mano, jog šios priemonės pagrindinė funkcija ne reguliacinė, o strateginė, kadangi verslas, prisidengdamas asmenine iniciatyva savarankiškai sureguliuoti problemines sritis, bando atitolinti (arba sustabdyti) teisinio reglamentavimo procesus valstybiniu lygmeniu. Kita vertus, savireguliacija gali pasitarnauti kaip eksperimentinė priemonė prieš įvedant teisinį reguliavimą. Ši interesų derinimo forma yra lankstesnė, todėl geriau galima numatyti reguliavimo normų padarinių teigiamus ar neigiamus aspektus. Trečia, savireguliacija puikiai tinka specifinio pobūdžio sferose, kur teisinis reguliavimas būtų itin siauros apimties. Ir, galiausiai, gali pasitarnauti kaip esamo reguliavimo papildymas, pritaikytas naujiems reiškiniams, kuriems dar nėra parengti tinkami teisės aktai.

Jungtinės Valstijos derina sektorinį, valstybinį bei savireguliacijos modelius. Stipresnio verslo grupių protegavimo atveju, tokia reglamentavimo forma pasiteisina, nes juridiniai asmenys gali sau susikurti palankesnes sąlygas veiklai pernelyg nenutoldami nuo valstybinės politikos. Direktyvos 95/46/EB 27 straipsnyje skatinamos pastangos parengti etikos kodeksus, kurie padėtų tinkamai įgyvendinti nacionalines nuostatas, valstybių narių priimtas pagal Direktyvą, atsižvelgiant į specifinius įvairių sektorių bruožus. Tokiu būdu siekiama derinti nacionalinį reguliavimą su verslo subjektų savireguliacija taip gerinant asmens duomenų apsaugą specifinėse srityse. Autoriaus nuomone, pasauliniu lygmeniu taip pat būtų naudinga derinti privatumo bei asmens duomenų apsaugos normas (šiuo atveju pežiūrėtus bei papildytus EBPO gairių principus) su savireguliacijos principais, nes kartais

[71] Peter J. Hustinx. Co-regulation or self-regulation by public and private bodies – the case of data protection // 2002;

problemos geriau matomos „iš vidaus“, be to, tokioje srityje kaip informacinės technologijos itin svarbu remtis moderniausiais, progresyviausiais sprendimais bei operatyviai raguoti į iškylančias grėsmes, o įstatymų leidybos srityje greitas efektyvių teisės aktų priėmimas yra mažai tikėtinas dėl būtinų atlikti procedūrų, kurios imlios laikui bei finansiniams resursams.

4.3.3. Techninė asmens duomenų apsauga

Teisinio reguliavimo trūkumai bei atsilikimas nuo technologinio progreso verčia ieškoti išeičių pasitelkiant alternatyvias duomenų apsaugos priemones. Techninė duomenų apsauga yra viena tų alternatyvų, kurių pagalba galima pakankamai efektyviai kontroliuoti asmeninės informacijos srautus, tokių duomenų rinkimą bei naudojimą. Tačiau klausimas, ar techninės priemonės gali pasiūlyti visapusišką asmens duomenų apsaugą, išlieka atviras. Šiuo atveju viskas priklauso nuo investicijų į sektorių bei laiką. Programuojant kodavimo bei kitas apsaugos sistemas nesistengiama sukurti tobulo, visais aspektais neįveikiamo „monstro“, kadangi tokie bandymai dar neprasidėjus būtų pasmerkti žlugimui. Nėra nenulaužiamų apsaugos priemonių. Visoms joms įveikti reikalingi trys elementai: laikas, kapitalas ir intelektas. Kuo brangesnis ir kuo ilgiau trunka sistemos nulaužimas, tuo ji laikoma saugesne, todėl stengiamasi, jog apsaugos mechanizmų nulaužimo kaštai būtų didesni už galimą naudą. [72]Techninė apsauga greičiausiai netaps panacėja ir nepadės užtikrinti idealios privatumo bei asmens duomenų apsaugos. Tačiau [73]privatumą didinančių technologijų naudojimas gali būti adekvačiu atsaku į analogiškų metodų pritaikymą duomenims rinkti. Privatumo bei asmens duomenų apsaugai naudojama programinė bei techninė įranga paprastai būna nukreipta prieš neteisėtą privačios informacijos rinkimą bei disponavimą ja. Tokių technologijų pavyzdžiai galėtų būti programos, saugančios vartotojų anonimiškumą internetinių mokėjimų ar prisijungimo prie tinklo metu. Kodavimas – taip pat vienas iš galimų variantų privačiai informacijai apsaugoti. Naudojant kodavimo bei šifravimo įrangą, duomenų subjektas galėtų pats spręsti kokią informaciją ir kam atskleisti. Žinoma, norint, kad kodavimo sistemos veiktų globaliai, reikėtų didžiulių investicijų tiek į infrastruktūrą, tiek į mokymą.

Techninė informacijos apsauga turėtų būti nuosekliai derinama su teisiniu reguliavimu bei savireguliacijos normomis tarptautiniu mastu. Šis metodas yra ganėtinai patikimas, pritaikomas plačiai vartotojų grupei bei atitinkantis laikmečio dvasią. Tobulėjant duomenų apsaugos įrangai neabejotinai vystysis ir jų rinkimo priemonės, nepaisant to, nuolat investuojant bei plėtojant technologinę duomenų

[72] Šiuo atveju kalbama ne tik apie technologinę, bet ir programinę pusę.
[73] Privacy Enhancing Technologies (PET)

apsaugą kai kuriais atvejais įmanoma sulaukti kur kas geresnių rezultatų nei vien remiantis įstatymo raide. Nusikaltimų išaiškinimo procentas elektroninėje erdvėje yra menkas, todėl tikimybė atgrasyti potencialų nusikaltėlį nuo jį dominančios informacijos yra labai maža, todėl šiuo atveju, svarbiau turėti „gerą spyną“ nei „garsiai lojantį šunį“.

4.4. Skyriaus apibendrinimas

Per pastaruosius 30 metų įvyko daugybė pokyčių įvairiose gyvenimo srityse. Technologija pasiekė iki tol neregėtas aukštumas, tačiau teisiniu požiūriu šis staigus šuolis į priekį sukėlė daug klausimų dėl technologinių procesų reguliavimo būtinumo. Šiuo metu tenka konstatuoti, jog teisinės priemonės pasiteisino tik iš dalies, todėl būtina iš naujo peržiūrėti senąsias nuostatas bei pritaikyti jas prie nūdienos realijų. Privatumo samprata yra labai skirtinga pasauliniu lygmeniu. Demokratinės valstybės šią teisę pripažįsta, tuo tarpu totalitaristinėse šalyse ji yra labiau „kosmetinė“ ir deklaratyvi. Todėl naujos kartos teisės akto, veikiančio visuotinai ir efektyviai, priėmimas yra komplikuotas ir, autoriaus nuomone, mažai tikėtinas. Vietoje to, reikėtų iš pagrindų peržiūrėti tiek pasaulinį, tiek regioninį, tiek nacionalinį privatumo bei asmens duomenų apsaugos reguliavimą, išsiaiškinti jo stipriąsias bei silpnąsias puses, atskirti gerąją praktiką nuo nenusisekusių reglamentavimo pavyzdžių bei papildyti esamus tarptautinio pobūdžio teisės aktus naujomis nuostatomis, labiau atitinkančiomis technologinę realybę, nepamirštant teisinio reguliavimo derinti su savireguliacija bei techninėmis apsaugos priemonėmis. Apibendrinant šį skyrių galima teigti jog:

- Tarptautinis privatumo bei asmens duomenų pasaugos reguliavimas nėra efektyvus, nes dabartiniai teisės aktai nevisiškai atitinka šiandienos technologinę situaciją;
- Skirtingas tų pačių procesų aiškinimas, socialiniai, kultūriniai, politiniai bei ekonominiai skirtumai stipriai apsunkina naujos kartos efektyvaus teisės akto priėmimo galimybę;
- Jau esančių tarptautinių dokumentų peržiūrėjimas be papildymas šiandienos realijas atitinkančiomis nuostatomis, visuotinis švietimas, sutarimas identiškų klausimų sprendime, savireguliacijos bei techninių priemonių derinimas gali tapti raktu į geresnę privatumo bei asmens duomenų apsaugą elektroninėje erdvėje;

IŠVADOS

Nagrinėdamas darbo temą įvade suformuluoto tikslo bei iš jo sekančių uždavinių rėmuose autorius pastebi, jog privatumo bei asmens duomenų apsaugos tarptautinis reguliavimas nėra efektyvus. Šią situaciją lemia keletas tarpusavyje susietų veiksnių: globalizacijos procesų spartėjimas; informacinių technologijų progresas; pasaulio regionų skirtingas požiūris į privatumo gynybą; šalių politinis, kultūrinis, ekonominis bei socialinis klimatas. Teisės mokslininkai kalba apie senojo privatumo bei asmens duomenų apsaugos reguliavimo neefektyvumą, tačiau kol kas nesiima giliau nagrinėti minėtos problemos. Autorius pritaria nuomonei, jog privatumo apsauga šiuo metu yra stagnacijos būsenoje, o vienareikšmiškų atsakymų kaip visa tai pakeisti – nėra. Darbe buvo ne tik apžvelgtos stipriosios bei silpnosios tokio reguliavimo pusės, bet ir išskirtos alternatyvios reglamentavimo formos bei jų įtaka pasauliniams privatumo apsaugos procesams. Aptariami pavojai bei grėsmės, galinčios atsirasti dėl netinkamos šių vertybių gynybos, keliami probleminiai klausimai, susieti su naujos kartos tarptautinio teisės akto priėmimu. Taip pat nagrinėjami trukdžiai efektyviam pasaulinio masto reguliavimui bei pateikiami tokio reguliavimo tobulinimo variantai, kuriuos derinant tarpusavyje įmanoma bent dalinai pagerinti situaciją šioje srityje. Atsižvelgiant į tai kas nagrinėta magistriniame darbe būtina išskirti ir sistemiškai išdėstyti pagrindines išvadas:

1. Nagrinėjama tema yra plati ir apjungianti daug probleminių aspektų. Nepaisant to, kol kas nėra daug mokslininkų nuomonių tarptautinio privatumo reguliavimo efektyvumo klausimu.
2. Oficialiai pripažinta teisė į privatumą atsirado kaip atsakas į priespaudą, asmens laisvių suvaržymus bei terorą, vyravusį Europoje iki XX a. antrosios pusės. Rytų Europoje ši situacija pasikeitė tik paskutinį XX a. dešimtmetį. Jos pripažinimas tarptautiniu mastu užtikrino asmenims papildomas teises į privataus gyvenimo neliečiamumą plačiąja prasme.
3. Dėl tarptautinių teisinių instrumentų trūkumo, privatumas bei asmens duomenų apsauga pradėta reguliuoti regioniniu lygmeniu. ES ir JAV naudoja skirtingus šios srities reguliavimo modelius. Elektroninė erdvė nepripažįsta valstybių sienų, tad skirtingi reguliavimo modeliai neigiamai veikia minėtų vertybių apsaugą pasauliniu mastu. Dėl reguliavimo skirtumų sunkiau kovoti su naujos kartos nusikalstamomis veikomis, skiriasi reikalavimai verslo subjektams, o asmenys gali jaustis diskriminuojami dėl

skirtingų nuostatų taikymo nacionaliniu lygmeniu, nors realiai jie veikia globalioje erdvėje.

4. Tiek ES, tiek JAV stengiasi apginti savo pozicijas privatumo bei asmens duomenų apsaugos srityje. Griežtesnis ES reguliavimo modelis bei jo nuostatos privertė trečiąsias šalis prisitaikyti prie šio apsaugos lygio, tačiau terorizmo grėsmė pačią ES pastūmėjo apriboti teises į privatumą. Dėl to susidarė kritinė situacija ir nei viena pusė negali teigti, jog jos modelis yra pranašesnis.
5. Nors baigtinę privatumo koncepciją pateikti sudėtinga, grėsmės šiai vertybei yra realios ir rimtos. Grėsmių šaltiniai gali būti įvairūs – pavieniai fiziniai asmenys, verslo subjektai, valstybinės institucijos.
6. Tarptautinio reguliavimo analizė privatumo bei asmens duomenų apsaugos srityje parodė, jog dabartiniai dokumentai tik iš dalies gina minėtą vertybę, nes pagrindinis reguliavimas yra abstraktus, didžiaja dalimi – rekomendacinis bei nepritaikytas prie šiandienos technologinių realijų.
7. Kultūriniai, ekonominiai, socialiniai bei politiniai šalių skirtumai trukdo vieningai ir efektyviai spręsti tarptautinio reguliavimo problemas. Vertybinis privatumo interpretavimas JAV ir ES skiriasi, tuo tarpu esama valstybių, turinčių didelį politinį bei ekonominį svorį pasauliniu mastu, tačiau iš esmės neginančių teisės į privatumą.
8. Dėl pasaulio daugialypiškumo, globalizacijos, technologijų susiliejimo bei informacinių technologijų vystymosi greičio naujos kartos privatumo reguliavimas tarptautiniu mastu yra sunkiai tikėtinas.
9. Norint pagerinti privatumo bei asmens duomenų apsaugos padėtį tarptautiniu mastu reikia peržiūrėti bei papildyti senąjį reguliavimą, derinti jį su atskirų sektorių savireguliacija ir techninėmis asmeninės informacijos apsaugos priemonėmis. Taip pat reikia mokyti bei šviesti visuomenę, siekiant geresnio minėtų teisių supratimo.

Magistrinio darbo hipotezė pasitvirtino. Ryšiai tarp globalizacijos, specifinių elektroninės erdvės savybių bei teisinio reguliavimo neefektyvumo iš tiesų egzistuoja. Ekonominės bei politinės aplinkybės daro įtaką teisės į privatumą užtikrinimo galimybėms tarptautiniu lygmeniu, todėl reikia ieškoti alternatyvų dabartiniam reguliavimui.

Abejotina ar kada nors bus įmanoma garantuoti absoliučią teisių į privatumą apsaugą. Tiek pati vertybės sąvoka, tiek jos užtikrinimo mechanizmai yra sudėtingi ir sunkiai realizuojami praktiškai. Stebėjimo kamerų, interneto bei telekomunikacinių tinklų klestėjimo laikais asmeninio pobūdžio

informacija vis dažniau patenka į viešąją erdvę. Informacinių technologijų vartotojai skatinami rūpintis privačios informacijos apsauga, nes teisinis reguliavimas gelbsti ne visada. Privatumo apsauga pasauliniu lygmeniu susirūpinta per vėlai, o apsaugos lygio klausimas vertinamas prieštaringai ir kelia diskusijas tarp teisės mokslininkų. Gal visuomenei ir negresia išvysti realų absoliutaus stebėjimo scenarijus modelį, tačiau akivaizdu, jog riba tarp privatumo ir viešumo plonėja ir pasauliui teks su tuo susitaikyti.

LITERATŪROS SĄRAŠAS

Norminė literatūra

1. Lietuvos Respublikos Konstitucija // Valstybės žinios, 1992, Nr. 33-1014;
2. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas // Valstybės žinios, 2003; Nr. 15-597;
3. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo 23 ir 26 straipsnių pakeitimo įstatymas // Valstybės žinios, 2004; Nr. 60-2120;
4. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo pakeitimo įstatymas // Valstybės žinios, 2008; Nr. 22-804;
5. Lietuvos Respublikos elektroninių ryšių įstatymas // Valstybės žinios, 2004, Nr. 69-2382;
6. Lietuvos Respublikos teismų įstatymo pakeitimo įstatymas // Valstybės žinios. 2002-02-20, Nr. 17-649;
7. Lietuvos Respublikos visuomenės informavimo įstatymo pakeitimo įstatymas // Valstybės žinios. 2006-07-27, Nr. 82-3254;
8. Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija // Valstybės žinios, 2000, Nr. 96-3016;
9. 1980 m. EBPO gairės dėl privatumo apsaugos ir asmens duomenų judėjimo tarp valstybių narių, http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html, [2008-09-12, 15:20];
10. Konvencija dėl elektroninių nusikaltimų // Valstybės žinios, 2001, Nr. 36-1188;
11. 1981 m. Strasbūro konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu. Pagrindinės Europos Tarybos sutartys. - Vilnius: Europos Tarybos informacijos ir dokumentacijos centras, 2000;
12. Visuotinė žmogaus teisių deklaracija // Valstybės žinios, 2006-06-17, Nr. 68-2497;
13. Tarptautinis pilietinių ir politinių teisių paktas // Valstybės Žinios, 2002, Nr. 77-3288;
14. Europos Sąjungos steigimo sutartis, http://eur-lex.europa.eu/lt/treaties/dat/11992M/word/11992M.doc [2008-11-10, 15:59]
15. Europos Parlamento ir Tarybos direktyva dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (95/46/EB) // 2004 Specialusis leidimas, Nr. 1;
16. Europos Parlamento ir Tarybos direktyva dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (2002/58/EB) // 2004 Specialusis leidimas, Nr. 1;

17. Europos Parlamento ir Tarybos direktyva dėl duomenų, generuojamų arba tvarkomų teikiant viešai prieinamas elektroninių ryšių paslaugas arba viešuosius ryšių tinklus, saugojimo (2006/24/EB) // Oficialusis leidinys L, Nr. 105-5
18. Ministrų komiteto rekomendacija Nr. R (99) 5, http://www.ada.lt/images/cms/File/Rekomendacijos%20ministru%20tarybos/R_99_%205%20priv_aps_intern_rekom.pdf [2008-11-26, 00:35];
19. Ministrų komiteto rekomendacija Nr. R (95) 4, http://www.ada.lt/images/cms/File/Rekomendacija%20Nr.%20R%20(95)%204.pdf [2008-11-26, 00:40];
20. Jungtinių Amerikos Valstijų Konstitucija su pataisomis, http://www.archives.gov/exhibits/charters/constitution.html, [2008-11-12, 16:00];
21. Personal Information Protection and Electronic Documents Act of 2000, http://www2.parl.gc.ca/HousePublications/Publication.aspx?pub=bill&doc=C-6&parl=36&ses=2&language=E, [2008-10-10, 14:00];
22. The privacy act of 1974, http://www.usdoj.gov/oip/privstat.htm, [2008-10-10, 14:10];
23. The freedom of information act, http://www.usdoj.gov/oip/foiastat.htm, [2008-10-10, 14:30];
24. Sex Offenders Act 1997, http://www.opsi.gov.uk/acts/acts1997/ukpga_19970051_en_1, [2008-11-03, 05:20];
25. Sexual Offences Act 2003, www.opsi.gov.uk/ACTS/acts2003/en/ukpgaen_20030042_en_1, [2008-11-03, 05:40];
26. Code of Fair Information Practices, http://www.ftc.gov/reports/privacy3/fairinfo.shtm, [2008-12-01, 20:20];
27. Федеральный закон Российской Федерации Об информации, информационных технологиях и о защите информации // Росийская газета (oficialus valstybinis leidinys). 2006 liepos 27 d.,. Nr. 149-ФЗ;

Specialioji literatūra

28. Mindaugas Kiškis, Rimantas Petrauskas, Irmantas Rotomskis, Darius Štitilis. Teisės informatika ir informatikos teisė. Vilnius: Mykolo Romerio universitetas, 2006. P. 115.;
29. Vilenas Vadapalas. Tarptautinė Teisė. Vilnius: Eugrimas, 1998. P. 30-55.;
30. Alfonsas Vaišvila. Teisės teorija. Vilnius: Justitia, 2000. P. 139.;

31. Toma Birmontienė, Egidijus Jarašiūnas, Egidijus Kūris ir k.t. Lietuvos konstitucinė teisė. Vilnius: : Lietuvos teisės universiteto Leidybos centras, 2002. P. 486.;
32. Daniel J. Solove. The Digital person: technology and privacy in the information age. New York: NYU Press, 2004. P. 56-75.;
33. Daniel J. Solove, Marc Rotenberg, Paul M. Schwartz. Privacy, Information, and Technology. New York: Aspen Publishers, 2005. P. 33-47.;
34. Daniel J. Solove. The future of reputation: gossip, rumor and privacy on the internet, New Haven & London: Yale University Press, 2007. P. 1-50.;
35. Mindaugas Civilka. Asmens duomenų apsauga tarptautinėje ir EB teisėje. Vilnius, 2001;
36. Mindaugas Civilka. Asmens duomenų apsaugos reguliavimas interneto kontekste. Vilnius, 2001;
37. Daniel J. Solove. The virtues of knowing less: justifying privacy protections against disclosure // Duke Law Journal, 2003, volume 53, P. 967-1064.;
38. Daniel J. Solove. Privacy and Power: Computer Databases and Metaphors for Information Privacy // Stanford Law Review, 2001, volume 53, P. 1393-1461.;
39. Daniel J. Solove. Digital dossiers and the dissipation of fourth amendment privacy // Southern California Law Review, 1997, volume 75, P. 1083-1167.;
40. Daniel J. Solove. „I‘ve got nothing to hide“ and other misunderstandings of privacy // The George Washington Law School, 2006.;
41. Philip E. Agre, Mark Rotenberg. Technology and privacy: the new landscape. Mit Press, 1998. P. 219 – 236.;
42. Samuel D. Warren, Louis D. Brandeis. The right to be left alone // Boston, 1890;
43. http://www-swiss.ai.mit.edu/6805/articles/privacy/Privacy_brand_warr2.html [2008-05-20, 20:10];
44. Roger Clarke, Gillian Dempsey. Technological aspects of internet crime prevention // Paper presented at the conference: Internet Crime held in Melbourne, 16-17 February 1998, by the Australian Institute of Criminology;
45. Ulco van de Pol. Aiming for effective co-regulation of data protection: policies and practices of the Dutch DPA;
46. Kallol Bagchi , Godwin Udo. An analysis of the growth of computer and Internet security breaches // Communications of the Association for Information Systems, 2003,Volume 12, P. 684-700;

47. Robert A. Dahl. A Democratic Dilemma: System Effectiveness versus Citizen Participation // Political Science Quarterly, 1994, Volume 109, Issue 1, P. 23-34;
48. R. Wacks. Privacy in Cyberspace: Personal Information, Free Speech and the Internet in P Birks // Oxford: Privacy and Loyalty, 1997 P.: 107
49. Winnie Chung and John Paynter. Privacy Issues on the Internet // Proceedings of the 35th Hawaii International Conference on System Sciences, 2002;
50. Klaus Brunnstein & Jacques Berleur. Human Choice and Computers, Issues of Choice and Quality of Life in he Information Society // Montréal: Kluwer Academic Publ., 2002, P. 89-108.;
51. Ljiljana Brankovic and Vladimir Estivill-Castro. Privacy issues in knowledge discovery and data mining.;
52. Maria Vicien-Milburn. The united nations and personal data protection // Jusletter 3, 2005.;
53. Dr. Ian Lloyd. An outline of the European Data Protection Directive // Journal Information Law & Technology, 1996.;
54. Joel R. Reidenberg, Paul M. Schwartz. Data protection law and on-line services: regulatory responses // Study;
55. Paul M. Schwartz. Property, privacy and personal data // Harvard law review, 2004, volume 117, Nr. 7.;
56. Paul M. Schwartz and William M. Treanor. The new privacy // Chicago, 2003.;
57. Henry Farrell. Constructing the International Foundations of E-Commerce—The EU-U.S. Safe Harbor Arrangement // International Organization, 2003, Nr. 57, P. 277–306.;
58. Winnie Chung and John Paynter. Privacy Issues on the Internet // Department of Management Science and Information Systems, 2002;
59. Peter J. Hustinx. Co-regulation or self-regulation by public and private bodies – the case of data protection // 2002;
60. Privacy Policy Compliance for Web Services // published in Proceedings of the IEEE International Conference on Web Services (ICWS 2004). San Diego, California, USA. July 6-9, 2004. NRC 46566;

Internetiniai šaltiniai

61. Amnesty International svetainė // http://www.amnesty.org/, [2008-10-20, 14:00];

62. Azijos šalių asmens privatumo raidos apžvalga // http://www.caslon.com.au/privacyguide6.htm [2008-06-23; 14:20];
63. Dataprotection.eu svetainė // http://www.dataprotection.eu/, [2008-12-01, 15:50];
64. Federalinės Šveicarijos duomenų apsaugos bei informacijos komisijos puslapis // http://www.edoeb.admin.ch/org/00828/index.html?lang=en [2008-01-15; 20:40];
65. Internetinė enciklopedija "Wikipedia" // http://en.wikipedia.org/wiki/Privacy [2008-05-12; 20:20]; http://en.wikipedia.org/wiki/Internet_privacy [2006-05-12; 20:30];
66. Kanados Asmens privatumo komisijos puslapis // http://www.privcom.gc.ca/legislation/02_07_01_01_e.asp [2008-06-23; 20:30];
67. Media Awareness Network // http://www.media-awareness.ca/english/issues/privacy/intl_guidelines_privacy.cfm [2008-05-12; 20:30];
68. Oficialaus Rusijos valstybinio leidinio (Росийская газета) svetainė // http://www.rg.ru/ [2008-01-15; 20:30];
69. Privataus gyvenimo ribojimas elektroninių ryšių srityje nusikaltimų tyrimo tikslais: problemos ir galimi sprendimai // http://www.hrmi.lt;
70. Privacy international svetainė // http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-559535 [2008-06-22; 21:00]; http://www.privacyinternational.org/survey/phr2003/countries/japan.htm [2008-06-22; 21:30];
71. Privacy.org svetinė // http://privacy.org/, [2008-10-10, 20:00];
72. Symantec svetainė // http://www.symantec.com/index.jsp, [2008-11-30] ;

Kalinauskas M. Privatumo ir asmens duomenų apsaugos reguliavimas tarptautiniu mastu / Informatikos teisės magistro baigiamasis darbas. Vadovas Doc. Dr. D Štitilis. – Vilnius: Mykolo Romerio universitetas, Ekonomikos ir finansų valdymo fakultetas, 2008

SANTRAUKA

Šiame darbe nagrinėjami privatumo bei asmens duomenų apsaugos probleminiai aspektai tarptautiniu mastu. Apibūdinti šia vertybę yra išties nelengva, kadangi joje persipynę daugybė skirtingų, bet tarpusavyje susietų kategorijų. Nepaisant to, privatumas priskirtinas prie svarbiausių žmogaus teisių bei laisvių ir yra gerbtinas bei saugotinas. Šio darbo tikslas – pažvelgti į dabar esantį tarptautinį teisinį reguliavimą privatumo bei asmens duomenų apsaugos srityje, atskleisti bei aptarti grėsmes privatumui XXI a. pradžioje bei atsakyti į klausimą: ar dabartinis privatumo bei asmens duomenų apsaugos reguliavimas atitinka šiandienos technologines, socialines bei ekonomines realijas. Magistriniame darbe keliama hipotezė, jog privatumo bei asmens duomenų apsaugos reguliavimas nėra pakankamas, todėl jį būtina iš naujo peržiūrėti bei papildyti. Autorius išsako nuomonę, jog pasaulis yra per daug skirtingas ir kad vieningo bei efektyvaus teisės akto priėmimas šiomis aplinkybėmis tampa sunkiai įmanomu. Darbe aptariamas tarptautinis bei regioninis privatumo bei asmens duomenų apsaugos reglamentavimas, supažindinama su galimais pažeidimais šioje srityje, keliami probleminiai klausimai dėl atskirų šios teisės apsaugos reguliavimo aspektų bei pateikiami pasiūlymai dėl efektyvesnio iškilusių problemų sprendimo. Iškeltam tikslui bei iš jo sekantiems uždaviniams įgyvendinti naudojami lingvistinis, loginis, lyginamasis, sisteminės analizės bei kiti tyrimo metodai. Darbą sudaro keturi skyriai, kuriuose nagrinėjamos atskiri, tačiau tarpusavyje susieti privatumo bei asmens duomenų apsaugos reguliavimo aspektai tarptautiniu lygmeniu. Pabaigoje pateikiamos išvados bei pasiūlymai kaip būtų galima gerinti privatumo apsaugą pasauliu lygiu naujųjų technologijų progreso bei globalizacijos laikmečiu.

Pagrindinės sąvokos: Privatumas, asmens duomenų apsauga, tarptautinis privatumo reguliavimas, elektroninė erdvė, globalizacija, privatumo bei asmens duomenų apsaugos probleminiai aspektai, privatumo krizė, duomenų rinkinėjimas, tikslinės atakos, valstybės vykdomas stebėjimas, trečiosios kartos privatumo bei asmens duomenų apsaugos reguliavimas, privatumo bei asmens duomenų apsaugos savireguliacija, techninė privatumo apsauga.

Kalinauskas M. Regulation of privacy and data protection in International level. / Master's thesis in Informatics law. Supervisor Doc. Dr. D. Štitilis. – Vilnius: Mykolas Romeris university, Faculty of Economics and Finance Management, 2008.

SUMMARY

The main research issue of this master thesis is problem-oriented approach of privacy and data protection regulation in international level. It's hard to conceptualize privacy as a value, because it's very complex ant closely intertwined with other categories of similar topic. Nevertheless, privacy is numbered as one of the fundamental human rights and should be treated with respect and under great protection. The main objective of the final paper is to overlook today's legal basis of international law norms concerning privacy and data protection. Also, to reveal and discuss main threats to mentioned value at the beginning of XXI century and answer the question: is nowadays regulation of privacy and data protection in international level deals with challenges of technological, social and economical reality. In this final paper author comes with the hypothesis that privacy and data protection regulation is ineffective in international level. Legal acts must be revised and supplemented with new norms which should be up to date considering nowadays reality. It is also noted that differences of various countries are huge and effective new generation privacy and data protection regulation is more like a utopia. Some problematic aspects are discussed in master's thesis concerning privacy violations, legal norm regulation effectiveness and possible ways of solving these problems. In order to achieve goals of objective, author uses scientific methods for his research. These methods are linguistic, comparative, systematic analysis and others. Final paper consists of four chapters in which author researches main problem-oriented aspects of privacy and data protection regulation in international level. At the end of the paper there are personal conclusions and proposals for better protection of this value in the context of technologic development and globalization.

Key words: Privacy, data protection, international privacy regulation, cyber-space, globalization, problem-oriented aspects of privacy and data protection, privacy crisis, data harvesting, data mining, targeted attacks, state surveillance, third generation privacy and data protection regulation, privacy self-regulation, co-regulation, technical privacy protection.