

Vilniaus universitetas
Filosofijos fakultetas

Informacijos visuomenės studijų centras
SAŽININGOS INFORMACIJOS PRAKTIKA IR JOS PROBLEMOS

Eglės Nemanytės
Informacijos visuomenės studijų
magistro darbas

Mokslinis vadovas: doc. Lomanienė Nijolė

VILNIUS, 2006

Turinys

| | |
|---|----|
| Santrauka..... | 3 |
| Įvadas..... | 5 |
| 1. Privatumo problema | 7 |
| 1. 1. Asmens privatumo reikšmė etiniu aspektu | 11 |
| 1. 2. Privatumo problema sociologiniu požiūriu | 14 |
| 1. 3. Asmens duomenų rinkimas ir saugumo problemos | 19 |
| 1. 4. Skundai dėl asmens duomenų tvarkymo Lietuvoje | 21 |
| 2. Sąžiningos informacijos principai kaip etinis informacijos lauko dalyvių kodeksas | 24 |
| 2. 1. Siūlymų spektras | 25 |
| 2. 2. Atvirumo principas | 28 |
| 2. 3. Kaupimo tikslumas | 31 |
| 2. 4. Duomenų prieinamumas | 35 |
| 2. 5. Duomenų saugumas | 37 |
| 2. 6. Sąžiningos informacijos principai taikomi informacijai, surinktai iš vaikų | 39 |
| 3. Asmens privatumas ir reikalavimai informacijos lauko dalyviams | 40 |
| 3. 1. Privatumo politikos klausimas | 41 |
| 3. 2. Vartotojų budrumo reikalavimas | 45 |
| Išvados | 48 |
| Literatūra ir šaltiniai | 50 |
| Priedai | 54 |

Sąžiningos informacijos praktika ir jos problemos

Santrauka

Darbas yra skirtas asmens privatumui ir sąžiningos informacijos praktikos principams aptarti bei problemai spręsti. Darbe yra teigiama, kad paskutiniajame XX-ojo amžiaus dešimtmetyje ėmė ryškėti *įtinklinto* ir vis labiau *įsitinklinančio* informacijos žmogaus charakteristikos. Pažeidžiamumas privatumo požiūriu – viena svarbiausių įtinklinto asmens charakteristikų. Valstybės kovoja su privatumo pažeidimais juridinėmis priemonėmis, tačiau jos kaip visada – nepakankamos, todėl būtina siekti, kad informacijos lauko dalyviai patys būtų budrūs, teikdami savo privačius duomenis, ir nuteiktų informacijos kūrėjus ir valdytojus kitokiam apsiėjimui su informacija. Skelbiami sąžiningos informacijos principai yra kaip etinis informacijos lauko dalyvių kodeksas. Pagrindiniai sąžiningos informacijos praktikos principai yra: atvirumas / supratimas; rinkimas, kaupimas / sutikimas; prieinamumas / dalyvavimas; vientisumas/ saugumas ; reikalavimas, spaudimas / atlyginimas, kompensavimas. Elektroninės terpės asmens privatumui keliami grėsmė turi būti mažinama laikantis sąžiningos informacijos praktikos principų ir žvelgiant į jų saugojimą kaip į praktinę problemą: ieškant nuoseklaus jų įgyvendinimo priemonių tiek iš informacinio tinklo kūrėjų, tiek iš jo vartotojų pusės.

Fair information practice: criteria and problems

Summary

This study aims to discuss an individual's privacy and fair information practice principles as well as try to solve this problem. The paper states that during the last decade of the XX century characteristics of the *web-minded* and more and more *web-involved* information individual started to develop. Vulnerability in terms of privacy is one of the most important characteristics of the web-minded individual. States fight privacy violations through legal means, but they are usually insufficient; therefore, it is necessary to seek that the participants of the information field were themselves alert while submitting their personal data and would orient information creators and administrators to other ways of dealing with information. Fair information principles could be compared to the ethics code of participants of the information field. The main fair information practice principles are as follows: notice/awareness, choice/consent, access/participation, integrity/security, and enforcement/redress. Threat to an individual's privacy by electronic medium has to be reduced following fair information practice principles and viewing their protection as a practical problem, that is searching for consistent implementation means both from the part of creators of the information field and from the part of its users.

Išvadas

Paskutinis XX-ojo ir pirmasis XXI-ojo amžiaus dešimtmečiai esmingai pakeitė Vakarų civilizacijos būklę. Prasidėjęs visuotinės kompiuterizacijos vėjus, sparčiai tobulėjančios informacinės technologijos keičia mokymosi, darbo, kūrybos, poilsio ir komercijos sąlygas. Būdami bet kurioje pasaulio dalyje, interneto tinkle visi žmonės tampa pasaulio bendrapiliečiais. Interneto plėtra yra sudedamoji naujosios ekonomikos dalis. Daugelis paslaugų perkeliama į elektroninę terpę. Gausėja informacijos ištekliai, valstybinėse ir privačiose organizacijose diegiamos pažangios informacinės sistemos, kurios leidžia valdyti informaciją. Informacija tampa strateginiu ištekliumi. Valstybės yra suinteresuotos kurti stambias ir kuo atviresnes informacijos sistemas, kurios padėtų valstybės valdymo įstaigoms tinkamai funkcionuoti, kuo efektyviau atlikti joms skirtus uždavinius. Informacinių technologijų taikymas ir informacinių paslaugų plėtimas yra labai svarbus valstybės valdymo, ekonomikos, socialinio ir kultūrinio gyvenimo sritims. Moderni informacinė infrastruktūra keičia valstybinių, verslo, finansinių ir kitų institucijų darbo technologijas, didina šalių gebėjimą konkuruoti pasaulinėje rinkoje, suteikia naujų galimybių šalių socialinei pažangai. Dabartinė geopolitinė situacija, ir ypač kova su terorizmu, internetas, biometrija, įsibrovimo technologijos, bio duomenų bankų atsiradimas vis labiau skatina poreikį spręsti pagrindinių žmogaus teisių ir laisvių klausimus, ypač teisės į privatumą klausimą. Anot M. P. Šaulausko, paskutinis XX-ojo amžiaus dešimtmetis yra raiški pirmoji naujosios informacijos visuomenės eros dekada. Šiame laikotarpyje ėmė ryškėti kartinės *įtinklinto* ir vis labiau *įsitinklinančio* informacijos bendrabūvio gyventojų – informacijos žmogaus, *homo informaticus* – charakteristikos (Šaulauskas: 1999). Pažeidžiamumas privatumo požiūriu – viena svarbiausių įtinklinto asmens charakteristikų.

Šiuolaikinės technologijos ženkliai keičia žmonių gyvenimą visame pasaulyje. Vis labiau nyksta ribos tarp asmeninio gyvenimo privatumo ir viešumo. Privatumo klausimai įvairiose valstybėse nuolat svarstomi. Valstybinės duomenų apsaugos inspekcijos duomenimis, 2005 m. rugsėjo 14 -16 d. Montreux (Šveicarija) 27-ojoje Tarptautinėje konferencijoje Duomenų Apsaugos ir Privatumo įgalotiniai priėmė Montreux deklaraciją *Asmens duomenų apsauga ir privatumas globalizuotame pasaulyje: visuotinė teisė gerbti įvairovę*, kurioje be kitų klausimų pripažįstama, kad informacinės visuomenės plėtrai didžiąją įtaką turi informacijos apsikeitimo globalizavimas, spartus technologijų brovimasis į

duomenų tvarkymo procesus bei saugos priemonių gausėjimas, kad teisė į duomenų apsaugą ir privatumą yra svarbiausia demokratinės visuomenės sąlyga, siekiant užtikrinti žmonių teisių gerbimą, laisvą informacijos srautą ir atvirą rinkos ekonomiką, kad teisė į duomenų apsaugą ir privatumą yra pagrindinė žmogaus teisė.

Pagrindinė šio darbo tezė – asmens privatumui elektroninėje terpėje kylanti grėsmė gali būti mažinama laikantis sąžiningos informacijos praktikos principų ir žvelgiant į jų saugojimą kaip į praktinę problemą: ieškant nuoseklaus jų įgyvendinimo priemonių tiek iš informacinio tinklo kūrėjų, tiek iš jo vartotojų pusės.

Pagrindinis šio darbo tikslas – aptarti asmens privatumo problemą etiniu aspektu, išanalizuoti sąžiningos informacijos praktikos principus ir problemas, kurias sukelia neatsakingas asmens duomenų naudojimas, bei reikalavimus informacijos lauko dalyviams.

Problemos ištyrimo lygis. Ši tema gana nauja, asmens privatumu imta labiau rūpintis tik XX a. paskutiniaisiais dešimtmečiais. Lietuvių kalba apie tai galima rasti tik bendro pobūdžio literatūros, kuri labiau akcentuoja teisinę asmens duomenų apsaugą ir elektroninius privatumo pažeidimus. Asmens duomenų apsauga kurį laiką buvo viena iš primirštų temų. Žurnalistai gina žodžio laisvę, tikintieji – tikėjimo laisvę, pacifistai – teisę į alternatyvią karinę tarnybą, pensininkai – teisę į socialines garantijas. Yra organizacijų, ginančių suimtųjų teises. Tik asmeninio gyvenimo neliečiamybė mūsų ilgus metus nebuvo niekaip ginama. Tuo metu asmens duomenų pardavimo verslas išaugo ir sutvirtėjo. Informaciją apie asmens duomenis galima pigiai nusipirkti, duomenų bazės, aplenkdamos visas kliūtis, patenka į juodąją rinką, ir niekas už tai neatsako. Vis garsiau svarstoma, kur yra privatumo ribos.

Anksčiausiai asmens teisės į privatumą ir asmens duomenų saugumo temomis pradėta kalbėti JAV, todėl darbe daug remtasi JAV nekomercinės organizacijos, kurios tikslas yra vartotojų švietimas ir privatumo gynimas, *The Privacy Rights Clearinghouse* (PRC), vartotojams teikiama informacija, šios organizacijos direktorės Beth Givens publikacijomis, *Federal Trade Commission* publikacijomis, žymaus sociologo Gary T. Marxo straipsniais ir kt. žinomų mokslininkų darbais ir įvairių tarptautinių tiklalapių skelbiama informacija. Šio darbo pagrindą sudaro daugiausiai straipsnių, konferencijų taip pat ir knygų, pateiktų

internetinėse svetainėse, medžiaga. Darbe bus naudojamos naujausia medžiaga, pagrindiniai – šaltiniai ne senesniais kaip penkeri metai. Pastaraisiais dešimtmečiais tema aktuali tapo ir Europos Sąjungos bei kitose šalyse.

Magistrinio darbo uždaviniai yra:

- išanalizuoti privatumo problemą, aptarti jos etinį ir sociologinį aspektą;
- aptarti sąžiningos informacijos praktikos principus, jų svarbą ir praktines jų taikymo problemas;
- aptarti informacijos lauko dalyvių privatumo politiką ir priemones, siūlomas vartotojams, – aktyviems informacijos terpės dalyviams, taip pat privalantiems rūpintis privačios informacijos saugumu.

Šio darbo autorė pasirinko privatumo ir sąžiningos informacijos principų temą neatsitiktinai. Studijuojant magistrantūroje beveik dvejus metus, kai kurie autorės rašto darbai daugiau ar mažiau buvo susiję su asmens duomenimis, privačia informacija, todėl šis darbas – ir tąsa ankstesnių darbų, ir naujas temos aspektas. Be to, tema yra aktuali ir nepakankamai išnagrinėta.

Tyrimo objektas. Darbe analizuojama asmens teisės į privatumą problema, sąžiningos informacijos praktika (principai) ir problemos Vakarų pasaulyje paskutinįjį XX-ojo ir pirmąjį XXI-ojo amžiaus dešimtmečiais (t.y., nuo 1995 metų – WWW duomenų srautas tampa pirmaujančiu tinklo protokolu – iki šių dienų).

Rašant šį darbą naudotasi statistinės analizės, sisteminės analizės, dokumentų analizės metodais. Darbe naudoti LR Valstybinės duomenų inspekcijos statistiniai duomenys, *Privacy Rights Clearinghouse organizacijos*, *Wall Street Journal*, *Washington Post* ir telekompanijos ABC apklausų duomenys.

1. Privatumo problema

Kiekvienas individas nori išsaugoti savo individualumą, todėl atsiranda poreikis saugoti su juo susijusią informaciją. Asmens privataus gyvenimo paslapties turėjimas reiškia galimybę išlikti ar išgyventi vienoje ar kitoje aplinkoje, esant vienoms ar kitoms gyvenimo sąlygoms. Paslapties turėjimas – individo biologinių, socialinių aplinkybių nulemta reakcija į supančią aplinką. Norint

apsaugoti individą nuo pavojaus susiliesti su kitais, reikia, kad individas turėtų kokią nors paslaptį, kurią jis turėtų ar norėtų saugoti (Frayssinet: 2001).

Jau visuomenės formavimosi pradžioje išryškėja paslapčių saugojimo poreikis. Pirmosios slaptos organizacijos pradėjo formotis dar pirmykštėje bendruomeninėje santvarkoje. Pirmykštės bendruomeninės santvarkos irimas (viena iš irimo priežasčių – perteklinio gamybos produkto atsiradimas) turėjo įtakos visuomeninių santykių pasikeitimui, kuris sudarė palankias sąlygas visuomeninių santykių dalyvių elgesio bei išraiškos laisvei, nes tuo metu atskiras individas jau nebebuvo taip glaudžiai susijęs su savo gentimi ar bendruomene. Atsiranda palankios prielaidos paslapčių plėtojimuisi, o ten, kur nėra pakankamai priežasčių saugoti paslaptį, tos paslaptys tiesiog *išrandamos* ir jas *žino* tik privilegijuotieji. Primityvioje visuomenės formavimosi pakopoje paslaptingumo poreikis svarbus, nes bendra paslaptis sutvirtina visuomenę ir daro ją solidaresnę. Aukštesniame visuomenės išsivystymo lygyje paslaptis kompensuoja individualios asmenybės vientisumo stoką. Per visą savo vystymosi laikotarpį pati visuomenė ir asmuo turi ir saugo paslaptį (Louveaux: 1999).

Kas yra privatumas? Kaip jį suprasti? Būta labai daug pastangų apibrėžti *privatumą*. Pačia plačiausia, etine, prasme privatumas suprantamas kaip draudimas kištis į kitų asmeninius reikalus, išskyrus ypatingus atvejus, pvz., kai yra pavojus žmogaus gyvybei arba sveikatai. Šiuo atveju privatumas susijęs su moraliniu diskretiškumu – mokėjimu saugoti savo ir kitų žmonių paslaptis, ir gina žmogaus orumą, garbę. Terminas *privatumas* vartojamas ir kalbant apie bendravimą, ir apie žmonių tarpusavio sąveiką. Sąveika būna privati, liečianti tik sąveikaujančius žmones, būna vieša, liečianti visus. Tai svarbu, nes filosofija ir sociologija nagrinėja privatumą būtent kaip dalį dichotomijos šalia viešumo ir reiškia šiuo žodžiu ne ką kitą kaip „šeimos gyvenimo veiklos sferą, izoliuotą nuo apmokamo darbo ir politinio aktyvumo“ (Aleksejenko: 2004). Dar vienas privatumo aspektas yra susijęs su gyvenančio šiuolaikinėje visuomenėje žmogaus teisėmis ir laisvėmis. Kai kalbama apie laisvę, visų pirma prisimenama politinė ar žodžio laisvė, laisvė rengti mitingus, laisvė dalyvauti valstybės valdyme. Bet politinė laisvė yra tik vienas žmogaus laisvės komponentas. Dar vienas komponentas, kuris yra ne mažiau svarbus kiekvienam žmogui – būti laisvam nuo nuolatinio stebėjimo, laisvė turėti savo pažiūras, mintis, laisvė būti nepriklausomam, kai tu to nori (Petrosian: 2003).

Privatumą apibrėžti labai sunku. Nuo pat tų laikų, kai privatumas pateko į teisinės regos lauką, autoriai nesutaria nei dėl jo koncepcijos, nei apimties. Amerikiečių teisininkai L. Brandeis ir S. Warren vieni iš pirmųjų pabandė apibrėžti asmens teisę į privatumą (*privacy*). Jie dar 1890 m. straipsnyje *The Right to Privacy* asmens teisę į privatumą įvardino, kaip „teisę likti vienam“ (Glenn: 2004).

A. Westin veikale *Privacy and Freedom* asmens teisę į privatumą apibrėžė, kaip individų, jų grupių ar juridinių asmenų apsisprendimo teisę spręsti kada, kokiais atvejais ir kokia apimtimi informacija apie juos gali būti patikėta kitiems asmenims (Westin: 1967).

Anot R. Gavison, asmens teisę į privatumą galima apibūdinti kaip būseną, kurią žmogus gali prarasti savo paties sprendimu ar dėl kitų žmonių veiksmų. Asmens teisę į privatumą sudaro trys elementai: „anonimiškumas“ (asmens teisė išlikti neatpažintam), „vienatvė“ (asmens teisė nebūti stebimam) ir „intymumas“ (asmens teisė bendrauti su paties pasirinktais asmenimis, nepatiriant išorinio kišimosi) (Gavison: 1980).

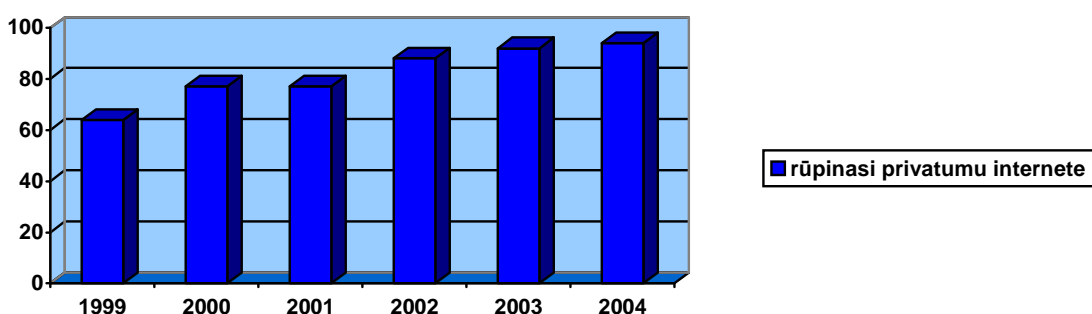
1990 metais Europos Tarybos Generalinės asamblėjos paskelbtoje rezoliucijoje *Dėl masinės informacijos priemonių* (428/1990) asmens privatus gyvenimas apibūdinamas kaip žmogaus teisė gyventi asmeninį gyvenimą, į kurį būtinai prireikus kišamasi kuo mažiausiai. Ši teisė apima privatų, šeimos ir namų gyvenimą, asmens fizinę ir psichinę neliečiamybę, garbę ir reputaciją, asmeninių faktų slaptumą, draudimą be leidimo publikuoti asmeninę nuotrauką, draudimą skelbti gautą ar surinktą konfidencialią informaciją. Individas turi teisę būti apsaugotas nuo kišimosi (fizinėmis ar informacijos priemonėmis) į jo asmeninį ir šeimos gyvenimą ar reikalus. Privatumas - „autonominė individo sritis, į kurią negali kištis nei valstybė, nei joks kitas asmuo“ (Petrosian: 2003).

1995 m. WWW duomenų srautas tapo pirmaujančiu tinklo protokolu. Internetu teikiamų paslaugų, interneto vartotojų skaičius augo, didėjo ir galimybių pažeisti asmens privatumą.

Laikraštis *Washington Post* ir telekompanija ABC 2005 metų kovo mėn. vykdė apklausą, kurios metu klausė amerikiečių, informacinių technologijų vartotojų, kokias grėsmes jiems kelia informacinių technologijų naudojimas. Atsakymai buvo tokie:

- **57%** – kad bus pažeista jų teisė į privatumą naudojant informacines technologijas;
- **72%** – kad jiems kelia nerimą, jog informacija apie juos (paso duomenys, kreditinių kortelių numeriai, informacija apie sveikatos būklę ir pan.) saugoma elektroninėse duomenų bazėse, prie kurių priėjimą galima gauti internetu;
- **84%** – kad kompanijos, kurios valdo bet kokias duomenų bazines, nepakankamai užtikrina tų duomenų bazių saugumą (CNews: 2005).

2004 metų pabaigoje *Wall Street Journal* apklausos metu buvo nustatyta, kad ženkliai didėja skaičius amerikiečių, kurie mano, kad asmeninė informacija yra pažeidžiama, jei yra netinkamai naudojama. Vis daugiau jų rūpinasi privatumo problemomis ir saugumu internete (*Wall Street Journal*: 2004). 1 diagramoje parodyta, kaip keitėsi amerikiečių, susirūpinusių privatumu internete, skaičius procentais nuo 1999 m. iki 2004 m.:



1 diagrama: Amerikiečių, besirūpinančių privatumu internete, skaičiaus dinamika 1999 – 2004 metais

1 diagramoje pastebime beveik tolydų skaičiaus didėjimą. Ženkliusias padidėjimas pastebimas 2000 metais. Palyginus su 1999 metais skaičius išaugo **13 %**, kitas ženklesnis padidėjimas - 2002 metais (palyginus su 2001 skaičius išaugo **9 %**). Per aptariamą laikotarpį (išskyrus jau paminėtus 2000 ir 2002 metus) besirūpinančiųjų privatumu internete skaičius augo vidutiniškai po **3 %** kiekvienais metais. 2004 metais besirūpinančiųjų privatumu internete buvo net **147 %** daugiau nei 1999 metais. Nepavyko aptikti atitinkamų duomenų apie pirmuosius interneto plėtros metus, tikėtina, kad tuo metu tokie tyrimai net nebuvo vykdomi. Spėtume,

kad interneto plėtros pradžioje toks rūpestis nebuvo pagrindinis – jį slopino optimizmas, susijęs su neabejotinai išaugusiomis komunikacijos ir dalinimosi informacija galimybėmis, be to, pirmieji interneto vartotojai – karinė ir akademinė bendruomenė, manytume, galėjo labiau pasikliauti moraliniu savos terpės diskretiškumu ir pagarba žmogaus teisėms. Problemos mastas ir, atitinkamai, besirūpinančių ja skaičiaus augimas neabejotinai numato platesnę, sociologiniu požiūriu – vis labiau įvairialypę interneto vartotojų terpę bei duomenų bazių skaičiaus nebesustabdomą, kartais – ir nebesukontroliuojamą augimą.

Apibendrinant būtų galima teigti, kad asmens teisė į privatumą padeda konkrečiam asmeniui išsaugoti savo individualumą. Vis labiau įsigalinčios informacinės technologijos verčia susirūpinti žmones privatumo problemomis ir saugumu internete.

1. 1. Asmens privatumo reikšmė etiniu aspektu

Etiniu požiūriu asmens privatumo klausimą bene aštriausiai kelia deontologinė etika, moralinį žmonių saitą grindžianti asmens autonomijos ir iš jos kylančio orumo kategorijomis. Pasak I. Kanto, ryškiausio šio požiūrio atstovo, „autonomija yra kiekvieno žmogaus ir kiekvienos protingos prigimties orumo pagrindas“ (Kantas: 1980, 72), tik laisvė, sprendimų autonomija, išskirianti žmogų iš kitų gamtinių būtybių tarpo, leidžia mąstyti žmoniją kaip „tikslų viešpatiją“. Pastarojoje „viskas turi arba *kainą*, arba *orumą*. Tai, kas turi kainą, gali būti pakeista kažkuo kitu, kas jam ekvivalentiška; o tai, kas aukščiau bet kurios kainos ir nieko ekvivalentiško jam nėra, turi orumą. [...] Moralė ir yra ta sąlyga, kuri tik ir leidžia protingai būtybei būti savaiminiu tikslu [...]. Taigi, tik moralė ir žmogus, kiek jis pajėgus būti moraliu, gali turėti orumą“ (Kantas: 1980, 70). Deontologinės teorijos neskaičiuoja pasekmių, yra racionalistinės – tiki, kad pareiga sudaro praktinio proto branduolį. Privalėjimai (pareigos) yra savaime vertinga, kaip išskirtinės žmogaus savybės – proto, darančio žmogų laisvės subjektu, balsas. Deontologo požiūriu, žmogiška laisvė yra vertybės šaltinis; ji reiškiasi kaip žmonių tarpusavio santykiuose regimas laisvas sutarimas; visų paklusimas universaliam dėsniui užtikrina, kad ši vertybė bus ginama ir puoselėjama; tai įgalina *tikslų viešpatiją*, kaip laisvės sistemą, kurioje kiekvienas veikėjas siekia laisvai pasirinktų

tikslų - tokiu mastu, kuris suderinamas su analogiška visų kitų laisve. Todėl etiniu aspektu asmens privatumo gynimas tampa esminiu žmogiškumo gynimu.

Viena iš deontologinės etikos atšakų – teisių teoretikai (nuo J. Locke iki R. Dworkino) apie žmogaus orumą linkę kalbėti teisių žodyno terminais, tačiau esmė ta pati: esama dalykų, į kuriuos kėsintis amoralu, kokia didelė nauda už tai bebūtų žadama. Jų požiūriu, tai prigimtinės, arba – XX a. – žmogaus teisės, kurių apsauga ir reiškia žmogiškojo orumo gynimą. Deontologiniu, taigi ir teisių požiūriu, intuityvus bet kurios moralės pagrindas – auksinė taisyklė – galėtų būti suformuluota taip: žiūrėk į kitą kaip į tikslą, o ne kaip į priemonę (plg. antiškąją *žmogiškumo formulę*: „Elkis taip, kad nei savo asmenyje, nei kieno nors kito asmenyje niekada žmogaus nepanaudotum vien kaip priemonės, o visada kaip tikslą“ (Kantas: 1980, 62), taigi nepaversk to, kas priklauso jo autonomijos, jo orumo sričiai, slapto disponavimo arba mainų objektu.

Deontologinė etika, kaip ir kitos fundamentalistinės etikos teorijos, bandžiusios pagrįsti moralinį žmonių saitą universaliu moralės dėsniu, susilaukė nemažai kritikos, tačiau kaip tik J. Locke, J.J. Rousseau ir kitų švietėjų idėjos įkvėpė Visuotinės žmogaus teisių deklaracijos kūrėjus (Lomanienė: 1996, 19).

Asmens privatumas buvo įtrauktas į *Visuotinę žmogaus teisių deklaraciją* – kaip visuotinas idealas, „kurio turi siekti visos tautos ir valstybės dėl to, kad kiekvienas žmogus ir kiekvienas visuomenės organas pasitelkę švietimą ir mokslą stengtųsi prisidėti prie to, kad šios teisės ir laisvės būtų gerbiamos ir kad būtų garantuota, kad jos bus visuotinai ir tikrai pripažįstamos ir taikomos. Visiems žmonių giminės nariams lygių bei neatimamų teisių pripažinimas yra laisvės, teisingumo ir taikos pasaulyje pagrindas“ (Visuotinė žmogaus teisių deklaracija: 2000). Anot N. Lomanienės, 1948 metais Jungtinių Tautų priimtos Visuotinės žmogaus teisių deklaracijos preambulę galima apibendrinti tokiu teiginiu: „mes priimame šį žmogaus teisių sąrašą, nes tai yra svarbu, šis sąrašas tebus riba, kurios neturi peržengti tautos, siekiančios laisvės, teisingumo ir taikos.“ (Lomanienė: 1996, 19).

Visuotinės žmogaus teisių deklaracijos dvyliktas straipsnis skelbia: „Niekas neturi patirti savavališko kišimosi į jo asmeninį ir šeiminių gyvenimą, jo buto neliečiamybę, susirašinėjimo slaptumą, kėsinimosi į jo garbę ir orumą. Kiekvienas žmogus turi teisę į įstatymo apsaugą nuo tokio kišimosi arba tokių pasikėsinimų.“

Jau minėtas John Locke, žymus XVII anglų filosofas, teigė, kad nuosavybės teisė yra prigimtinė teisė, ir visuomenė turi be išlygų gerbti šią teisę. Privatumas yra taip pat žmogaus nuosavybė, todėl jis traktuotinas kaip absoliuti, prigimtinė, neatimama teisė. Asmens garbė ir orumas yra didelė socialinė vertybė, tad įstatymai turėtų saugoti asmens garbę ir orumą bei gerą reputaciją. Tačiau pripažįstama, kad kiekvienu atveju privataus gyvenimo neliečiamumas nėra absoliuti teisė, o asmens subjektyvus suvokimas ir suteikimas tam tikriems su juo susijusiems faktams privatumo elementų objektyviai nesuformuoja tokio socialinio reiškimo, kaip privatus asmens gyvenimas. Daug dėmesio moraliniam žmogaus teisių aspektui skyrė R. Dworkinas, vienas iš garsiausių šiuolaikinių JAV teisės teoretikų. Išsakydamas savo požiūrį į žmogaus teises, R. Dworkinas teigė, kad reikia atkreipti dėmesį, ar vyriausybė gerbia moralines ir politines piliečių teises. Jis pažymėjo, kad JAV konstitucija sulieja teisinius ir moralinius dalykus, tačiau neaišku, ar konstitucija pripažįsta visas moralinės teises, kurias turi piliečiai, ar nesikėsina į jų moralines teises. R. Dworkinas atkreipia dėmesį, kad žodis *teisė* (*right*) skirtinguose kontekstuose turi skirtingą reikšmę: „Daugeliu atvejų sakydami, kad kas nors turi „teisę“ ką nors daryti, teigiame, kad būtų neteisinga jam trukdyti tai daryti ar bent jau reikia kokio nors specialaus pagrindo bet kokiam trukdymui pateisinti“ (Dworkin: 2004, 268). Jokia visuomenė, pretenduojanti pripažinti įvairias teises tuo pagrindu, kad žmogaus orumas arba lygybė gali būti pažeista įvairiais būdais, negali akceptuoti tokio principo. Žmogaus teisė į laisvę nėra absoliuti. Ji yra teisė tiek, kiek nedaro žalos visuomenei (žr. Dworkin: 2004, 262-263, 288). R. Dworkinas, kalbėdamas apie požiūrį į teises, sako, kad „valdžia savo piliečius turi traktuoti su tokia pagarba ir atodaira į orumą, kokios vieni iš kitų reikalauja suaugę bendruomenės nariai. Valdžia gali suvaržyti žmogų jo paties arba gėrio labui, tačiau šie suvaržymai privalo būti pagrįsti paties žmogaus elgesiu“ (Dworkin: 2004, 33).

Anot N. Lomanienės, šiuolaikiniai žmogaus teisių teoretikai jau nesistengia iš teorinių principų išvesti tikrąją žmogaus esmę. Vadovaujantis daugiau empirine žmogaus teisių pažeidimų generalizacija (kiekvienas priešinasi kėšinimams į jo nuosavybę, kiekvienas piktinasi, jei bus atplėšiama ir tikrinama jo korespondencija ir t.t., ir pan.), teisė būti apsaugotam nuo tų pažeidimų „tapo konvencijos būdu įtraukta į žmogaus apibrėžimą. [...] Šiuolaikinėje politinėje filosofijoje žmogaus teisės kildinamos ne iš gamtos [...] ar kokios nors metafizinės substancijos, o iš to,

kaip mes, savųjų normų autoriai, suprantame, kas yra *žmogus*” (Lomanienė: 1996, 20).

Apibendrinant tai, kas pasakyta, galima daryti išvadą, kad etiniu aspektu privatumui svarbi asmens autonomija, t.y., jo savarankiškumas priimant sprendimus. Tai būtina jo orumo (kaip tik jis žmogų išskiria iš daiktų pasaulio) sąlyga. Asmens privatumo pažeidimas įgalina manipuliacijas su asmeniu, t.y., paverčia jį daiktu.

1. 2. Privatumo problema sociologiniu požiūriu

Sociologiniam požiūriui privatumo problema labiausiai rūpi kaip socialinės kontrolės įgalinimo priemonė. Sociologiniai tyrimai kelia klausimą, kokius duomenis asmuo laiko „asmens duomenimis“, kaip atskiros socialinės grupės toleruoja intervenciją į asmens privatumą, kokios socialinės grupės yra pažeidžiamiausios privatumo požiūriu, kokios socialinės grupės daugiausia išlošia – įgyja kontrolės galią – manipuliudamos šiuolaikinių technologijų leidžiamomis informacijos kaupimo ir apdorojimo galimybėmis ir pan. Taigi, kalbant apie sociologinę privatumo problemos pusę, reikia smulkiau panagrinėti, ar informacijos panaudojimas nepažeidžia asmens privatumo, t.y., ar informacija yra sąžininga.

Kuo socialinis gyvenimas tampa sudėtingesnis, tuo įdėmesnė ir labiau išstobulinta tampa kontrolė. Ji naudoja didelį mokslo technikos pasiekimų arsenalą. Telefoniniai ir elektroniniai pasiklausymai, vizualus stebėjimas, didžiulio kiekio asmens duomenų rinkimas, kaupimas ir lyginimas kompiuterinių informacinių sistemų pagalba – visos šios šiuolaikinės socialinės kontrolės priemonės, vaizdžiai kalbant, sukuria didžiulę „rakto skylutę“, per kurią žmogų stebi valstybė, politinės ir visuomeninės organizacijos. Priverstinė būtinybė detaliai vykdyti visas (dažnai prieštaraujančias viena kitai) socialines normas padarytų gyvenimą nepakeliamą; sudėtingoje visuomenėje šizofreniškas elgesys taptų greičiau taisykle, o ne išimtimi. Per daug įdėmus, totalus stebėjimas sukelia neigiamus socialinius padarinius. Atskirų asmenų ir asmenų grupių kontrolės (valstybinių, regioninių arba ekonominių institutų) ribų nustatymas visada buvo vienu iš centrinių kovoje už individualią laisvę.

Iš esmės tradicinės teisės, įtvirtintos demokratinių šalių konstitucijose – religijos laisvė, t.y., sąžinės laisvė, gyvenamosios vietos neliečiamumas,

garantijos, kad nebūtų nesankcionuotų kratų – skirtos apriboti per daug didelį valdžios socialinės asmens kontrolės siekimą (Petrosian: 2003).

Harvardo universiteto sociologijos profesorius Gary T. Marxas savo darbuose plačiai analizavo, kokį poveikį teisėtam ir neteisėtam asmeninės informacijos ribų peržengimui turi technologijos. Jo domėjimasis susijęs su numatytais ir atsitiktinėmis socialinės kontrolės pasekmėmis. Šias temas G. Marxas tyrinėjo gilindamasis į naujų stebėjimo technologijų (šiuolaikinė slapta apsauga, vaizdo ir elektroninė padėties kontrolė ir asmens tapatybė ID) specifiką.

Visų pirma G. Marxui svarbu išsiaiškinti, kas yra vieša, o kas privatu – tai esminiai šiuolaikinių asmeninės informacijos konfliktų elementai. Elektroninių stebėjimų ginčų centre atsiduria asmeninės informacijos kontrolė. Viešumo ir privatumo ribos, tų ribų nustatymo problema yra tik viena informacijos ir visuomenės temos dalis. G. Marxas teigė, kad kiekvienas stebėjimas turi būti vertinamas apibūdinant etinę ir socialinę duomenų rinkimo tikslų ir konteksto analizės taktiką. Jis siūlo kiek plačiau pažvelgti į asmens privatumą ir formuoja esminius klausimus, kurių pagrindas – vertybių grupė. Visiems rūpima ir svarbi yra kantiškoji idėja: pagarba žmogaus orumui. Kai kažkas be žmogaus sutikimo ir žinios technologiškai gali įsibrauti į žmogaus gyvenimą, orumas ir pagarba sumažėja. Pagarbą žmogui sudaro manipuliacijos ir prievartos išvengimas. Tai daug svarbiau ir už žalos sukėlimą, ir už žmonių stebėjimą. Didelę reikšmę turi ir tai, ar stebimas asmuo atitinkamai informuojamas. Kai pasitikėjimas būna sugriautas, apgaudinėjant arba renkant duomenis atsisakoma laikytis susitarimų ir numatytų kontraktų, visuomenės vertybės būna pažeistos. Svarbiausia stebėjime (nepriklausomai nuo to kaip stebima) yra asmeninių ribų peržengimas. G. Marxas (Marx: 2001) išskiria bent keturias asmeninę informaciją saugančias ribas, kurių bent vienos peržengimas reiškia asmeninės erdvės pažeidimą:

1. „Natūrali“ riba.

Ją užbrėžia mūsų jautimai. „Normaliai“ arba „natūraliai“ žmonės mato, girdi, užuodžia, suvokia vienas kitą ir tai nelaikoma brovimusi į kito žmogaus erdvę tol, kol stebėtojo buvimas nėra slaptas. Natūralios ribos klausimas iškyla tada, kai stebėtojas naudojasi įrankiais, kurie išplečia žmogiškų jautimų ribas ir natūraliai nesuvokiamus, neprieinamus dalykus paverčia suvokiamais ir pasiekiamais. Kaip tik todėl tokių įrankių naudojimas reikalauja informuoti stebimą asmenį ir gauti jo specialų leidimą. „Natūralią“ ribą kuria ir palaiko keletas kategorijų:

- a) drabužiai, pridengiantys nuogumą ir apsaugantys kūno dalis nuo stebėjimo iš šalies;
- b) kitiems demonstruojama veido išraiška, elgesys, sakiniai, kuriuos ištariame, – dalykai, kuriais kaip kaukėmis pridengiame savo vidų – mintis ir jausmus, kurių nesame linkę atskleisti;
- c) natūralios priedangos (barjerai) – žmonės linkę tikėti, kad jų privatumą saugo sienos, uždarytos durys, tamsa, erdvinis nuotolis, tradicinis slapto stebėjimo privačiose vietose nepriimtinumai;
- d) siunčiamos informacijos adresavimas, pvz., siunčiamą laišką užklijuojame ir užrašome adresatą, pranešimas, siunčiamas elektroniniu paštu tam tikram žmogui, taip pat turi fizinę apsaugą, kad niekas, išskyrus adresatą, negalėtų jo perskaityti.

2) *Socialinė riba.*

Ją sukuria ir palaiko mūsų lūkesčiai, siejami su tam tikrais socialiniais vaidmenimis. Pvz., tokie socialiniai vaidmenys kaip gydytojas, advokatas, dvasininkas, paprastai siejami su lūkesčiu apie jiems suteiktos informacijos konfidencialumą, taip pat tikima, kad šeimos narys arba draugas neatskleis mūsų paslapčių, biurokrato socialinis vaidmuo neatsiejamas nuo lūkesčio, kad sugebės užtikrinti mūsų konfidencialių duomenų saugumą. Socialinę ribą palaiko socialinės normos, draudžiančios skaityti kitiems adresuotus fakso pranešimus, žiūrėti svetimas nuotraukas be leidimo arba, tarkime, peržiūrėti kopijavimo aparate ar spausdintuve netyčia paliktą medžiagą.

3) *Erdvinė arba laiko riba.*

Ši riba reiškia asmens biografijos pertrūkius, t.y., tikėjimą, kad be mūsų sutikimo, niekas negali raustis informacijoje apie ankstesnius mūsų biografijos periodus ar mūsų gyvenimą kitoje vietoje.

4) *Sąveikos kontekstiškumas.*

Asmuo remiasi prielaida, kad tarpusavio santykiai, komunikacija ir informacijos likučiai, pvz., šiukšlės, yra praeinantys, neatplėšiami nuo konteksto, todėl be mūsų sutikimo negali būti slapta fiksuojami vaizdo ar garso įrašymo priemonėmis arba kitaip išsaugomi ir jiems suteikiamos naujos reikšmės.

Bet kurios šių ribų pažeidimas reiškia invaziją į asmens privatumą. Technologijos gali sukurti naujų galimybių šių ribų peržengimui.

G. Marxas teigia, kad į viešumą ir privatumą nereikia žiūrėti kaip į vieną dimensiją, griežtai dichotominę ir absoliučią, turinčią nustatytas ir universalias sampratas, kurių reikšmės apibūdintos objektyviu elgesio turiniu. Privatumas ir viešumas yra greičiau multi-dimensinė samprata. Ji nenutrūkstama ir santykinė, nestabili ir situacinė ar kontekstinė, kurios reikšmė priklauso nuo interpretacijos ir sukūrimo. Kur baigiasi žmogaus privatumas ir kur prasideda viešumas? Šie klausimai anksčiau buvo labiau suderinti nei dabar, atsiradus ir išpopuliarėjus naujoms technologijoms, kurios iš pradžių buvusios ne tokios svarbios, dabar jau nepakankamai gina asmeninę informaciją (Marx: 2001).

Anonimiškumas – tai viena iš privatumo sąlygų. Kiek asmuo gali likti anonimiškas, tiek jis gali išsaugoti savo privatumą. G. Marxas skiria keletą anonimiškumo lygių. Svarbiausia privati informacija yra asmens vardas ir pavardė, toliau taip pat ne mažiau svarbi ir asmens gyvenamoji vieta. Kai kuriose situacijose asmuo lengviau pasako savo vardą, pavardę, bet ne adresą (Marx: 1999).

Slaptumas yra esminis asmens anonimiškumo ir orumo komponentas. Laisvės prasmę asmuo dažnai nustato pagal tai, kiek jis gali valdyti (kiek yra laisvas valdyti) savo gyvenimą ir nesvarbu, ar tai būtų darbas, ar žmonės, su kuriais nori bendrauti, ar gyvenamoji vieta, ar politiniai ir religiniai įsitikinimai, ar informacija, kurią nori nusišlepti ar paskelbti. Asmeniui yra labai svarbu kontroliuoti asmeninę informaciją. G. Marxas teigia, kad slaptumas ir privatumas yra svarbu visose asmens gyvenimo sferose. Pvz., darbdavys, pasitelkęs naujausias technologijas, darbe gali stebėti darbuotoją, bet toks stebėjimas pažeistų asmens teises į privatumą, sukeltų psichologinę įtampą ir net sumažintų darbo efektyvumą. Geriausia išeitis būtų *Etikos kodekso* sudarymas. Tai būtų taisyklės, kurių laikantis nebūtų pažeidžiamas asmens privatumas (Marx: 1986).

Etikos kodeksai gali būti sukuriami ir taikomi darbovietėse, kai kuriose įmonėse, įstaigose, tačiau tai padėtų išspręsti tik dalį privatumo pažeidimo problemų. Svarbu ir sąžiningos informacijos principai. G. Marxas kiek plačiau žiūri į sąžiningos informacijos principus, jo požiūris konkretnis ir informacijos lauko dalyviui ar jo tyrinėtojai (sociologui) gali būti aiškesnis. Visų pirma jis išvardija, į ką reikėtų atkreipti dėmesį renkant informaciją. Pasak G. Marxo, renkant informaciją techninėmis priemonėmis svarbu yra išsiaiškinti:

- ar nėra daroma žala (fizinė ar psichologinė);
- kokios informacijos rinkimo ribos (kad be sutikimo nebūtų peržengtos asmeninės ribos).

Svarbūs informacijos rinkimo faktoriai, kuriuos turi žinoti asmuo:

- pasitikėjimas (ar nėra pažeidžiamos prielaidos, kaip surinkta informacija bus panaudojama);
- supratimas (asmenys žino, kaip ir kodėl jų asmeninė informacija renkama ir kaupiama);
- susitarimas (asmuo sutinka, kad informacija apie jį būtų renkama);
- minimizavimo principas, taikomas renkamai informacijai (t.y., rinkti tik tiek informacijos, kiek būtina);
- teisės peržiūrėti surinktą informaciją užtikrinimas;
- teisė nuginčyti ir išreikšti nepasitenkinimą (sudaryti galimybę nuginčyti rezultatus arba pateikti alternatyvius duomenis ar jų interpretaciją);
- numatyta kompensavimo tvarka ir veiksmingos priemonės, jei asmuo buvo neteisėtai stebimas ir pažeistos procedūros, turi būti tinkamas duomenų valdymas ir apsauga (Marx: 2001).

Reikia atsižvelgti į tai, ar gali būti sukurti nepageidaujami precedentai, ar yra negatyvių efektų (ypač duomenis perduodant tretiems asmenims) ir kaip jie gali būti nustatomi. Ir dar vienas, bet taip pat labai svarbus faktorius - ar priemonės plačiai prieinamos visiems, ar apribojimai negalioja tik turtingiausiems arba galingai technikai; ar reguliavimo taktika gali naudotis visi žmonės ar reguliuoti gali tik techniškai galingesni; jei yra asmeninės informacijos reguliavimo priemonės, tai ar jos vienodai prieinamos, ar apribojamos tik patiems neprivilegijuotiems (Marx: 2001).

Apibendrinant tai, kas pasakyta, galime daryti išvadą, kad šiuolaikinių technologijų įgalintas brovimasis į privačią žmogaus erdvę ir galimybė manipuliuoti asmeniui skatina žvelgti į privatumo pažeidimus kaip į žalingas pasekmes nešantį faktą, o savotiškas etikos kodeksas - sąžiningos informacijos principų laikymasis padeda užtikrinti asmens privatumą, kuris toks svarbus šiuolaikinėje visuomenėje.

1. 3. Asmens duomenų rinkimas ir saugumo problemos

Europos Sąjungos Direktyva 95/46/EC asmens duomenis apibrėžia taip: bet kuri informacija, susijusi su asmeniu, kurio tapatybė yra nustatyta ar gali būti nustatyta; asmuo, kurio tapatybė gali būti nustatyta, yra tas asmuo, kurio tapatybė gali būti tiesiogiai ir netiesiogiai nustatyta, ypač pasinaudojus nurodytu asmens identifikavimo kodu arba vienu ar keliais to asmens fizinei, fiziologinei, protinei, ekonominei, kultūrinei ar socialinei tapatybei būdingais veiksniais.

Kiti tarptautiniai teisės aktai asmens duomenis apibrėžia panašiai, pvz., 1981 m. ET Konvencija Nr. 108 asmens duomenis apibrėžia kaip bet kokią informaciją, susijusią su asmeniu, kurio tapatybė yra nustatyta ar gali būti nustatyta (Civilka: 2005, 293).

Asmens duomens sąvoka panašiai apibrėžiama ir *Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatyme*: „asmens duomenys – bet kuri informacija, susijusi su fiziniu asmeniu – duomenų subjektu, kurio tapatybė yra žinoma arba gali būti tiesiogiai ar netiesiogiai nustatyta pasinaudojant tokiais duomenimis kaip asmens kodas, vienas arba keli asmeniui būdingi fizinio, fiziologinio, psichologinio, ekonominio, kultūrinio ar socialinio pobūdžio požymiai”.

Taigi, visuose apibrėžimuose yra panaši pozicija: tam tikros informacijos pagalba, nepasitelkiant kokių nors ypatingų metodų ar priemonių, asmuo turi būti lengvai ir nesudėtingai nustatomas.

Skaitmeninis amžius – amžius kompiuterių, informacijos, pasaulinių tinklų suteikia naujų galimybių ir naujų rūpesčių. Viena iš problemų – asmens gyvenimo neliečiamumo ir asmens duomenų apsauga ir saugumas. Vis daugiau žmonių yra susirūpinę tuo, kad informacija apie juos lengvai prieinama ir platinama be jų žinios ir sutikimo. Kalifornijos universiteto ekonomistas Hal R. Varian teigia, kad jau dabar yra informacijos apie mus rinka. Problema ta, kad mes patys toje rinkoje nedalyvaujame (Smirnov: 2003).

Nepaisant vis griežtėjančių įstatymų, reglamentuojančių asmens duomenų rinkimą, saugojimą ir platinimą, aišku, kad taikant draudimus problemos neįmanoma išspręsti. Pirma, sunku kontroliuoti tokio įstatymo vykdymą. Antra, šiuolaikinės techninės priemonės paverčia operacijas su asmens duomenimis pelningu verslu, kuriuo užsiimti pelninga beveik kiekvienam. Dauguma piliečių, kompanijų ir nekomercinių organizacijų renka informaciją kiekvieną dieną, net

negalvodamos apie tokią savo veiklą pranešti asmens duomenų tvarkymą reguliuojančioms tarnyboms. Dar praėjusio šimtmečio pabaigoje daugelis šalių vyriausybinių agentūrų JAV, Kanadoje ir Europoje išnagrinėjo metodus, kaip renkama ir naudojama asmeninė informacija – jų informacinius metodus – ir garantijas, kurios reikalingos patvirtinti, kad tie metodai sąžiningi ir užtikrina adekvatų slaptumo gynimą. Ekonominio bendradarbiavimo ir plėtros organizacija (*Organisation for Economic Cooperation and Development*) asmens duomenis skirsto į tokias grupes:

- Pirminiai duomenys: vardas, pavardė, gimimo metai, vieta, pilietybė.
- Ypatingi duomenys: ūgis, svoris, išvaizda.
- Šeimyninė padėtis: santuoka, giminės, vaikai, išlaikytiniai.
- Išsilavinimas ir įgūdžiai: informacija apie profesinį išsilavinimą.
- Gyvenimo būdas: kam teikia pirmenybę: maistas, poilsis, sportas, butas, rūkymas, alkoholis ir pan.
- Finansiniai ištekliai: pajamos, nuosavybė.
- Finansiniai identifikatoriai: banko sąskaitos detalės.
- Interneto identifikatoriai: slaptažodžiai, vartotojo vardai, tinklo sertifikatai
- Identifikatoriai, duoti valstybinių organų: paso serija ir numeris.
- Biometriniai identifikatoriai: DNR, pirštų atspaudai, akies rainelės atvaizdas.
- Kiti duomenys: rasė, tautybė, religija, politinės ir filosofinės pažiūros, narystė profesinėse sąjungose, duomenys apie sveikatą, seksualinį gyvenimą, informacija apie teistumą.

Nei viena valstybė negali apsaugoti tokio pobūdžio asmens duomenų, kuriuos žmogus pats kasdien skelbia. Informacijos surinkimo ir apdorojimo techninių priemonių vystymasis, žiniasklaida veda link to, kad asmens informacijos gynimas virsta tik deklaravimu. Valstybė negali užtikrinti asmens duomenų saugumo. Ji tai gali padaryti tik tose srityse, kuriose įmanomas techninis reguliavimas (Smirnov: 2003).

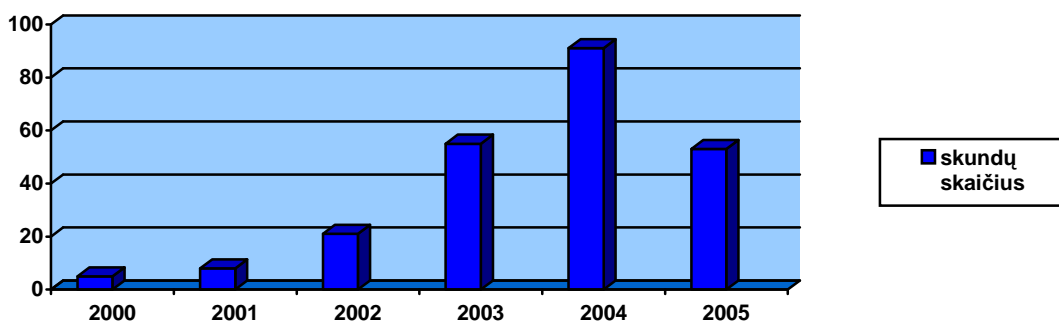
Informacija ir duomenys yra renkami pačiais įvairiausiais būdais: anketavimo, apklausų, socialinių tyrimų procedūrų realizavimo metu, pirkimo elektroninėse parduotuvėse, viešbučių, bilietų rezervavimo, elektroninių atsikaitymų, internetinės bankininkystės paslaugų metu ir t.t., ir pan. Taigi, kartais asmens duomenys renkami per tarpininkus, kartais duomenų rinkimas vyksta betarpiškai tarp asmens subjekto ir duomenų rinkėjo. Būtina žinoti asmens subjekto ir duomenų rinkėjo teises ir pareigas bei sąžiningos informacijos principus ir jų griežtai laikytis.

Taigi, būtina tinkamai informuoti asmenis apie jų duomenų rinkimą, kaupimą, saugojimą ir naudojimą. Kadangi valstybė ne visada gali užtikrinti asmens duomenų saugumą, kyla įvairiausių su saugumu susijusių problemų.

1. 4. Skundai dėl asmens duomenų tvarkymo Lietuvoje

Duomenų apsauga yra žmogaus teisių raidos istorijos dalis. Duomenų apsaugos teisinė sistema išsivystė plėtojant informacijos technologijas, darančias įtaką duomenų tvarkymo efektyvumui ir sudarančias pavojų žmogaus teisėms.

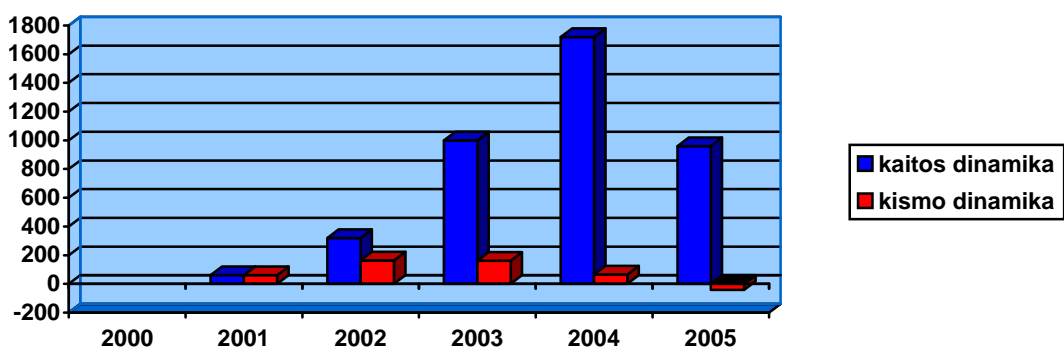
Lietuvoje Asmens duomenų teisinės apsaugos įstatymo priežiūrą vykdomi Valstybinė duomenų apsaugos inspekcija yra nepriklausoma institucija. (*Lietuvos Respublikos asmens duomenų apsaugos įstatymas* buvo priimtas 1996 metais. Paskutinė aktuali redakcija nuo 2004-04-13). Svarbiausieji Inspekcijos veiklos tikslai yra: plėtoti duomenų apsaugą, prižiūrėti asmens duomenų valdytojų veiklą tvarkant asmens duomenis, kontroliuoti asmens duomenų tvarkymo teisėtumą, kovoti su duomenų tvarkymo pažeidimais ir užtikrinti duomenų subjekto teisių apsaugą. Valstybinė duomenų apsaugos inspekcija, veiklą pradėjusi 1997 metais, nuo 2001 metų spalio mėnesio įgijo nepriklausomos institucijos statusą ir teisę savarankiškai veikti. Ši institucija iš piliečių gauna skundų ir pranešimų apie asmens duomenų tvarkymo pažeidimus. Nuo 2000 metų gaunamų skundų skaičius ženkliai kito. 2 diagramoje parodyta, kaip keitėsi duomenų subjektų skundų skaičius per paskutiniuosius šešerius metus (duomenys iš Valstybinės duomenų apsaugos inspekcijos *Metinių ataskaitų*):



2 diagrama: Duomenų subjektų skundų skaičiaus dinamika 2000 – 2005 metais

2 diagramoje matyti, kad skundų skaičius didėjo. Ženklus padidėjimas prasidėjo nuo 2002 metų ir tęsėsi iki 2005 m. (per šių trejų metų laikotarpį buvo gauta vidutiniškai po 17 skundų daugiau per metus), 2005 metais skundų gauta mažiau negu 2004 m.

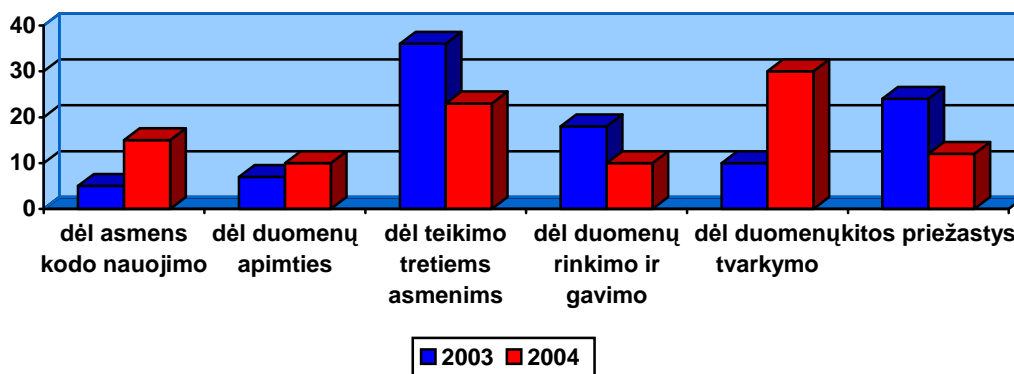
3 diagramoje parodyta asmens duomenų subjektų skundų skaičiaus kaitos ir kismo dinamika 2000-2005 metais:



3 diagrama: Skundų skaičiaus kaitos ir kismo dinamika 2000 – 2005 metais

Asmens duomenų subjektų skundų skaičius ženkliai kito. Nuo 2001 metų pastebimas ženklus didėjimas, o 2005 metais skundų skaičius sumažėjo. Stebėdami skundų skaičiaus kaitos dinamiką, matome, kad ji yra teigiama, t.y., per visą aptariamąjį laikotarpį skundų buvo daugiau palyginus su 2000 metais. Kismo dinamika šiek tiek kitokia: 2005 metais neigiama, t.y., 2005 metais skundų mažėjo - 41,8 % palyginus su 2004 metais.

Kokios pagrindinės skundų priežastys? Detaliau bus aptariama 2003 ir 2004 metų duomenys, nes tais metais skundų gauta daugiausiai (2005 metų tikslų duomenų dar nėra). 4 diagramoje pavaizduota, kaip pasiskirstė 2003 – 2004 metais gauti skundai pagal pobūdį (skaičiai pateikti procentais nuo visų gautų tais metais skundų):



4 diagrama: 2003 – 2004 metais pateiktų skundų pobūdis

Didžiausią skundų dalį sudaro skundai dėl asmens duomenų teikimo tretiems asmenims: 2003 m. – 36 %, 2004 m. – 23 %. Duomenų tvarkytojai be asmens duomenų subjekto žinios ir sutikimo teikdavo duomenis tretiems asmenims. 2003 metais nemažą dalį skundų sudarė skundai dėl asmens duomenų rinkimo ir gavimo – 18 % (pvz., buvo gautas skundas, kuriame pareiškėjas nurodė, kad savo pašto dėžutėje centriniam pašte rado UAB *IMP Baltic* laišką ir užsakymo kuponą leidiniui *Gyvūnijos pasaulyje*. Laiške buvo nurodytas ne tik pašto dėžutės numeris, bet ir pareiškėjo adresas, vardas ir pavardė. Pareiškėjui paklausus telefonu apie jo asmens duomenis, bendrovė nepaaiškino jam, iš kur gauti duomenys. Pareiškėjas prašė ištirti, iš kur ir ar teisėtai UAB *IMP Baltic* gavo jo duomenis. Inspekcija tikrinimo metu nustatė, kad UAB *IMP Baltic* tvarkė asmens duomenis tiesioginės rinkodaros tikslais negavusi duomenų subjekto sutikimo, be teisėto tvarkymo kriterijaus, asmens duomenis gavo ne iš pareiškėjo ir, prieš pradėdama juos tvarkyti, neinformavo duomenų subjekto, iš kokių šaltinių ir kokie asmens duomenys renkami, asmens duomenis tvarkė nesąžiningai ir neteisėtai bei nepranešusi Inspekcijai apie duomenų tvarkytojus.

Net 30 % 2004 metais gautų skundų sudaro skundai dėl asmens duomenų tvarkymo, 15 % dėl asmens kodo netinkamo naudojimo. Kitos skundų priežastys: dėl asmens duomenų tvarkymo tiesioginės rinkodaros tikslais, dėl ypatingų

asmens duomenų tvarkymo, dėl asmens duomenų tvarkymo kitais tikslais, t.y., tvarkant asmens duomenis lizingo, komunalinių paslaugų teikimo srityse, tvarkant asmens duomenis rinkiminės kampanijos metu ir kt., dėl teisės susipažinti su savo asmens duomenimis, dėl duomenų saugumo.

Apibendrinant šiuos duomenis, galima teigti, kad asmens duomenų subjektų skundų skaičius didėja, asmens duomenų teisėtas tvarkymas tampa vis svarbesnis žmonėms. Pagrindinės duomenų valdytojų problemos: per menkai informuojami duomenų subjektai apie jų duomenų rinkimą, tvarkymą, naudojimą, renkami pertekliniai duomenys, duomenys perduodami tretiesiems asmenims ir t.t., ir pan.

Vienas iš problemos sprendimo kelių galėtų būti geresnis sąžiningos informacijos praktikos principų taikymas.

2. Sąžiningos informacijos principai kaip etinis informacijos lauko dalyvių kodeksas

Internetas yra viena iš labiausiai plintančių ir efektyviausių komunikavimo priemonių, suteikiančių galimybę bendrauti nepriklausomai nuo atstumo, laiko ar vietos. Gyvenimas elektroninėje erdvėje tampa vis intensyvesnis ir didėja realus pavojus, jog asmeninius duomenis tretieji (pašaliniai) asmenys galės ne tik surasti, skaityti, stebėti, bet ir pakeisti, redaguoti ar sunaikinti. Internetas apibrėžiamas kaip daugybė kompiuterių, sujungtų elektroninio ryšio pagalba ir galinčių tarpusavyje keistis duomenimis. Kadangi kiekvienas prie šio tinklo prisijungęs kompiuteris tampa interneto dalimi, tokioje sistemoje sukuriamos sąlygos ne tik keistis informacija, bet ir įvairiausiais būdais ją rinkti, skelbti ir panaudoti. Informacija tampa preke, turinčia didelę komercinę vertę, todėl kai kurie subjektai nelinkę paisyti reikalavimo gerbti žmogaus teisę į privatumą. Todėl iškyla privačios informacijos ir asmens duomenų nesankcionuoto vartojimo problema. Natūraliai kyla klausimai, ar spartus informacinių technologijų vystymasis nekelia grėsmės žmogaus laisvėms ir teisėms į asmeninio gyvenimo privatumą, ar saugu perduoti privataus pobūdžio informaciją, pateikti asmens duomenis internete. Kadangi valstybės vien teisinėmis priemonėmis nepajėgios kovoti su elektroninėje terpėje privatumui ir asmens duomenų saugumui iškylančiomis grėsmėmis, reikalingi sąžiningos informacijos praktikos principai, kurie padėtų sumažinti šias grėsmes.

2. 1. Siūlymų spektras

Paskutiniaisiais XX amžiaus dešimtmečiais rimčiau susirūpinta sąžiningos informacijos praktika. Keletas organizacijų (*Organisation for Economic Cooperation and Development, Federal Trade Commission, Privacy Rights Clearinghouse* ir kt.) pradėjo skelbti sąžiningos informacijos principus ir kvietė visus – organizacijas ir asmenis – jų laikytis.

1989 metais Britų Kolumbijos (*British Columbia*) žmogaus teisių specialusis įgaliotinis David X. Flexerti suformulavo ir vėliau dar papildė rinkinį 12 principų ir informacijos apsaugos taisyklių, skirtų vyriausybinėms asmens duomenų apdorojimo sistemoms (*Data Protection Principles and Practices for Government Personal Information Systems*). Šie principai tokie (kursyvu išskirti principai, kurie buvo papildyti 1997 metais):

1. *Viešumo ir skaidrumo* (atvirumo) principas: neturi būti slaptų duomenų bazių.
2. *Būtinumo* ir relevantiško (prasmės atitikimo) informacijos rinkimo ir saugojimo procesų valdymo principas.
3. Renkamo, naudojamo ir saugomo asmens informacijos kiekio minimizavimo principas.
4. *Užbaigtumo* principas: rinkimo tikslai ir tolesnis asmens duomenų naudojimas turi būti nustatyti iš anksto).
5. *Atsakingų* už asmens duomenų apdorojimo sistemų eksploatacijos kontrolę paskyrimo principas.
6. Asmens duomenų masyvų *sujungimo*, persiuntimo kontrolės principas.
7. Būtinu duomenų subjekto sutikimo rinkti asmens duomenis gavimo principas.
8. Asmens duomenų apdorojimo sistemų tikslumo ir užbaigtumo principo laikymasis.
9. *Atsakomybės* (civilinės ir baudžiamosios) už darbo su asmens duomenimis *taisyklių pažeidimus* principas.

10. Specialių asmens duomenų saugumo taisyklių buvimo būtinumas yra konfidencialus.
11. Teisė į prieigą prie savo duomenų ir jų koregavimą/
12. *Teisė tapti užmirštam* įskaitant pilną anonimiškumą arba beveik visų asmens duomenų sunaikinimą (Garfinkel: 2003).

1981 metais Fen Labalme inicijavo projektą *Broadcatch Technologies*. Fen Lablame tyrinėjo, kaip galima būtų saugoti privatumą internete. *Broadcatch* kompanijos misija – sukurti paslaugų, labiau užtikrinančių saugumą internete, paketą. Tos paslaugos turėtų būti prieinamos kiekvienam interneto vartotojui, t. y., jos turėtų būti techniškai nesudėtingos, nebrangios. Vienas iš kompanijos tikslų – *OpenPrivacy* politikos vykdymas (ši politika suteikia galimybę egzistuoti anoniminei skaitmeninei rinkai). *Broadcatch* tikslas – tobulinti kokybišką priėjimą prie informacijos, stiprinti pasitikėjimą ir užtikrinti bendradarbiavimą, tarp visų informacijos lauko dalyvių (vartotojų, kaupėjų, rinkėjų).

Fen Labalme teigė, kad bet kuri technologinė sistema turi turėti keturis elementus, kurie užtikrintų informacijos visuomenės saugumą. Technologinei sistemai būtina:

1. visur esantis, daugiakanalis tinklas, kuris negali būti uždaras, kontroliuojamas be leidimo ar kitaip pažeidžiamas;
2. mechanizmai, garantuojantys saugumą, slaptumą, kad vartotojai be baimės galėtų naršyti internete;
3. mechanizmai, kad informacija būtų renkama ir filtruojama;
4. lanksti, asmeninė, nustatoma ir paprasta vartotojo sąsaja su tinklu (Labalme: 1998).

Kompanijos veikla nukreipta į tai, kad kiekvienam būtų užtikrintas personifikuotas, nepaperkamas priėjimas prie informacijos. Priėjimo prie informacijos būdai turi būti patogūs ne tik tiekėjui, bet ir vartotojui, kuris turėtų galimybę naudotis informacija be baimės.

Fen Lablame pritarė Federalinės Prekybos Komisijos (*Federal Trade Commission*) pranešime Kongresui skelbiamiems penkiems sąžiningos informacijos principams (*Fair Information Practice Principles*). Šie principai:

1. atvirumas / informavimas (*notice / awareness*);

2. pasirinkimas / sutikimas (*choice / consent*);
3. prieinamumas/dalyvavimas (*access / participation*);
4. sąžiningumas / saugumas (*integrity / security*);
5. reikalavimas, spaudimas / atlyginimas, kompensavimas (*enforcement / redress*).

Ekonominio bendradarbiavimo ir plėtros organizacija (*Organization for Economic Cooperation and Development*) išskyrė aštuonis sąžiningos informacijos principus (Givens: 2000):

1. atvirumas (*openness*);
2. panaudojimo apribojimas (*use limitation*);
3. individo dalyvavimas (*individual participation*);
4. saugumas (*security*);
5. rinkimo apribojimas (*collection limitation*);
6. duomenų kokybė (*data quality*);
7. tikslo apibrėžtumas (*purpose specification*);
8. atskaitomybė (*accountability*).

Anot B. Givens, ir Federalinė Prekybos Komisija (*Federal Trade Commission*), ir Ekonominio bendradarbiavimo ir plėtros organizacija (*Organisation for Economic Cooperation and Development*) skelbia panašius sąžiningos informacijos praktikos principus. Pastaroji šiek tiek išsamiau juos skirsto (įvardija dar naudojimo apribojimą, duomenų kokybę, rinkimo tikslą). Principų esmė ta pati. Tačiau svarbiausia, kad šitų principų (nesvarbu, ar jie 5, ar daugiau) būtų laikomasi (Givens: 2000).

Jason Catlett, kompanijos *Junkbusters* prezidentas, taip pat daug kalba apie sąžiningos informacijos principus. *Junkbusters* kompanijos misija – teikti žmonėms ir organizacijoms informaciją, kuri padėtų atsikratyti „internetinių“ šiukšlių, aiškinti, kaip teisiškai turi būti naudojama iš asmenų surinkta informacija. Šios kompanijos internetiniame tinklalapyje skelbiama daug vertingos informacijos apie asmens privatumo ir asmens duomenų pažeidimus. Jason Catlett pastebi, kad firmų kompiuterizacija vykdyta neskiriant reikiamo dėmesio svarbioms detalėms, todėl iškilo grėsmė saugumui, atsirado būtinybė priimti bendrus sąžiningos informacijos

praktikos principus ir jų laikytis (Catlett: 1980). 1980 metais 2000 kompanijų, siekiančių, kad būtų gerbiamas vartotojo slaptumas ir užtikrinta anketinių duomenų apsauga, priėmė *Svarbiausių principų tarptautinėms įmonėms (Guidelines for Multinational Enterprises)* rinkinį, kuriame taip pat skelbiami sąžiningos informacijos metodai (principai):

1. rinkimo apribojimo principas (*Collection Limitation Principle*);
2. duomenų kokybės principas (*Data Quality Principle*);
3. specifinių tikslų principas (*Purpose Specification Principle*);
4. naudojimo ribojimo principas (*Use Limitation Principle*);
5. saugumo garantijos principas (*Security Safeguards Principle*);
6. atvirumo principas (*Openness Principle*);
7. individualaus dalyvavimo principas (*Individual Participation Principle*);
8. atsakomybės principas (*Accountability Principle*).

Rinkinyje skelbiami principai iš esmės nesiskiria nuo jau aptartųjų, tačiau reikia pastebėti, kad atvirumo principas, kuris anksčiau aptartuose šaltiniuose yra pirmoje vietoje, čia yra minimas tik šeštoje. Tačiau visuose šaltiniuose atkreipiamas dėmesys į tai, kad asmens duomenys būtų renkami informuojant asmens duomenų subjektą apie tai, kaip, koku tikslu, kam jie renkami, kaip galima pačiam subjektui juos koreguoti, kokia atsakomybė tenka duomenų tvarkytojui, kai jis neteisėtai tvarko duomenis.

Kadangi įvairūs šaltiniai sąžiningos informacijos principus įvardija panašiai, bet ne identiškai, apbendrinant galima išskirti sąžiningos informacijos principus: atvirumą, kaupimo tikslingumą, prieinamumą asmeniui, saugumą ir atsakomybę.

2. 2. Atvirumo principas

Pats svarbiausias principas – atvirumas, vartotojo informuotumas. Vartotojams turi būti pranešama apie informacijos rinkimo faktą bei paaiškinamos rinkimo taisyklės, tikslas ir pan., prieš tai, kol bet kokia informacija bus iš jų renkama. Be pranešimo vartotojas negali argumentuotai apsispręsti, ar atskleisti ir kiek atskleisti asmeninę informaciją. Be to, trys iš kitų principų – pasirinkimas / sutikimas; prieinamumas / dalyvavimas; sąžiningumas / saugumas – yra

reikšmingi tik tada, kai asmuo žino apie asmens duomenų rinkimą ir jo teisių gerbimą.

Pranešimo galimybės ir turinys priklauso nuo nepriklausomų informacijos metodų. Štai keletas punktų, kurie buvo pripažinti kaip svarbūs ir būtini tinkamai pranešti vartotojams prieš skelbiant jų asmeninę informaciją:

- juridinio asmens, renkančio duomenis, identifikacija;
- nustatymas, kur bus duomenys laikomi;
- bet kokių potencialių duomenų gavėjų identifikacija;
- duomenų rinkimo būdai ir priemonės, kaip jie bus renkami, jei tai nėra akivaizdu (pasyvus rinkimas naudojantis elektroniniu stebėjimu ar aktyvus rinkimas, prašant vartotoją suteikti informaciją);
- ar prašomų duomenų tiekimas yra savanoriškas, ar būtinas ir kokios atsisakymo teikti reikalaujamą informaciją pasekmės;
- priemonės, taikomos duomenų rinkėjams, kad šie garantuotų duomenų konfidencialumą, sąžiningumą ir kokybę.

Kai kurie sąžiningos informacijos praktikos kodeksai teigia, kad pranešimas taip pat turi identifikuoti bet kokias prieinamas vartotojo teises, įskaitant ir šias: bet koks pasirinkimas dėl duomenų vartojimo; ar vartotojas gavo priėjimo prie duomenų teisę; vartotojo galimybė užprotestuoti klaidas; praktikos kodekso pažeidimų atlyginimo galimybė; ir kaip šios teisės gali būti įgyvendintos.

Internetu pranešimas gali būti atliktas lengvai registruojant informacijos atskleidimo praktiką, apibūdinančią juridinio asmens informacinius metodus, kompanijos internetiniame puslapyje. Kad būtų pasiektas didesnis efektas, tokia informacija turi būti aiški ir pastebima, paskelbta matomoje vietoje, lengvai pasiekama ir iš titulinio puslapio, ir iš bet kurio kito internetinio puslapio, kur informacija renkama iš vartotojo. Tai turėtų būti būtina ir suprantama taip, kad vartotojas gautų reikšmingą ir efektyvų pranešimą apie tai, kas atsitiks su jo asmenine informacija, kurią jis prašo paskelbti. Anot *Junkbusters Svarbiausių principų tarptautinėms įmonėms (Guidelines for Multinational Enterprises)* rinkinyje skelbiamos informacijos, kad asmens duomenys būtų atvirai renkami, būtina įgyvendinti individualaus dalyvavimo principą, t.y.: asmuo būti informuotas apie tai, kaip:

- gauti iš duomenų rinkėjo patvirtinimą, ar tikrai rinkėjas turi duomenis, liečiančius jį;
- bendrauti su duomenų rinkėju dėl duomenų, liečiančių jį, asmeniui patogiu ir priimtinu laiku, būdu ir forma;
- sužinoti priežastis, jei užklausa yra neigiama ir turėti galimybę keisti tokį neigimą / atmetimą;
- keisti jį liečiančius duomenis ir, jei keitimas sėkmingas, ištrinti neteisingus duomenis duomenų bazėje arba juos iš viso panaikinti.

Anot Beth Givens, 2000 metų gegužės mėn. Federalinė Prekybos Komisija (*Federal Trade Commission*) tikrino internetinius puslapius. 90 % tinklalapių, kurie dažniausiai lankomi, turi slaptumo politiką, bet tik 42 % tinklalapių laikosi atvirumo principo. Galima daryti išvadą, kad ties atvirumo principu ir sukumpo daugelis tinklalapių. Pagrindinė problema – tinklalapiai nepasirūpina, kad žmonės gautų duomenų, kuriuos renka kompanijos, kopijas (Givens: 2000).

Atvirumas ir informavimas labai svarbus, nes daugelis žmonių nesusimąsto, kokios gali būti jų nežinojimo pasekmės. Pats įprasčiausias duomenų rinkimas iš vartotojų – produktų registracijos formų, lojalumo kortelių pildymas ir pan. Užpildę vienokią ar kitokią formą, vartotojai po to gauna dar ir kitokios informacijos ar įvairios reklamos paštu, telefonu, elektroniniu paštu, jei jie parašė savo elektroninio pašto adresą pildydami bet kokią anketą. Kodėl taip atsitinka? Kai kurie vartotojai susies priežastį su efektu. Kitaip pasakius, jie žinos, kad anketų pildymas – priežastis, kodėl jie gauna įvairiausių katalogų ir „išmeta“ tiek šiukšlių iš elektroninio pašto. Daugelis to nesusies. Bet priežastis yra būtent ši. Vartotojai negauna tinkamos informacijos apie tolesnį jų duomenų panaudojimą. Anketose ar produkto registracijos formose apie tokių anketų pildymą informacija yra arba ne esminė, arba beveik nepastebima. Pvz., informacija kurią jūs teikiate, gali būti skleidžiama kitoms organizacijoms, kurios produktai arba paslaugos sudomins jus. Žodžiai *gali būti* ir *skleidžiama* netinkamai informuoja apklausos dalyvius apie tai, kaip bus tvarkomi jo asmens duomenys (Givens: 2001).

Vartotojas turi būti laiku informuojamas apie visus pasikeitimus, susijusius su jo duomenų tvarkymu. Kai kurie teigia, kad būtina klausti vartotojo sutikimo kiekvieną kartą, kada jie nori pasidalyti klientų duomenimis ir kad tai labai brangiai kainuoja. Bet, anot Beth Givens, to daryti nebūtina. Verslo pasaulis turi pateikti

klientams raštišką pranešimą, kada klientas pirmą kartą pasirašo dėl paslaugos arba prideda naują paslaugą prie jau esančių. Tokie pranešimai nulemtų vartotojo apsisprendimą sutikti, ar nesutikti su sąlygomis. Taigi, tik vienas nuoširdus pranešimas, kuris būtų reguliariai atnaujinamas – viskas, ko reikia (Givens: 2000).

Reikia atkreipti dėmesį ir į privačios informacijos registrus. Turi būti reguliuojama informacijos brokerių veikla. Šiais laikais informacijos brokeriai perka visuomenines ataskaitas iš vietinių, valstybinių, vyriausybės agentūrų, pakartotinai jas paruošia, kad būtų prieinamos užsakovams. Jie papildoma duomenų kartotekas iš komercinių duomenų šaltinių, pvz., ataskaitos apie kreditines operacijas ir vartotojo duomenų apžvalgos. Faktiškai bet kas gali gauti priėjimą prie šių aplankų, nors daugelis informacijos brokerių tvirtina, kad jie riboja priėjimą prie tokių profesijų kaip privatūs tyrėjai, skolų išieškojimo patikėtiniai, žiniasklaida ir pan. Brokerių informacija turi būti labai reguliuojama, panašiai kaip reguliuojama kredito informacija. Žmonės turėtų turėti galimybę žinoti, kada ir kas turi priėjimą prie jų asmeninės informacijos ir kokių tikslu. Jie turi turėti priėjimą prie duomenų rinkimo, kad nustatytų, ar jie tikslūs. Ir jie turi turėti galimybę paduoti į teismą, jei anketiniai duomenys gauti ir atskleisti neteisėtai (Givens: 2002).

Taigi, galime daryti išvadas, kad laikantis atvirumo principo:

- a) negali būti niekur neregistruotų privačios informacijos registrų;
- b) asmuo turi būti supažindinamas su informacijos kaupimo tikslais, būdais, panaudojimu (privatumo politika);
- c) asmuo turi būti informuojamas – supažindinamas su galimybėmis ginti savo privatumą.

2. 3. Kaupimo tikslingumas

Antrasis plačiai priimtas pagrindinis sąžiningos informacijos principas – yra asmens duomenų kaupimo tikslingumas. Anketiniai duomenys turi būti tiesiogiai susiję su tikslais, kuriais jie bus panaudojami ir būtini tiems tikslams įgyvendinti. Jie turi būti tikslūs, išsamūs ir šiuolaikiškai išsaugoti. Tikslai, kuriais anketiniai duomenys surinkti, turi būti nustatyti ne vėliau, iki jie pradėti rinkti, ir naudojami tik tais tikslais arba ir kitais tikslais (bet iš anksto suderintais), kurie būtų numatyti kiekvienu konkrečiu atveju, kai pasikeičia tikslai. Svarbios ir anketinių duomenų

rinkimo ribos. Bet kokie duomenys turi būti gaunami teisėtomis ir sąžiningomis priemonėmis bei žinant duomenų turėtojų arba turint jo sutikimą (Catlett: 1980).

Beth Givens, kalbėdama apie įvairiais būdais renkamus asmens duomenis, pabrėžia, kad surenkama daug nereikalingos informacijos. Pvz., kai vartotojas nusiperka prekę, (pvz. mikrobangų krosnelę, kompiuterį, filmavimo kamerą ir pan.) tarp kitos dokumentacijos jis randa produkto registracijos formą, kurios vienoje pusėje yra apklausos anketa, kitoje – adresas, kuriuo ją siųsti. Pirmi 6 klausimai tokiose registracijos formose skirti pirkėjo, kuris nusipirko gaminį, vardui, pavardei, adresui ir bendrai informacijai apie gaminį, kad kompanija būtų informuota, jog šis žmogus, vieno iš jos produktų savininkas, bei kompanijai naudingai informacijai, jei pirkėjas atsisakytų jos produkto. Likusioji apklausos dalis skirta asmeninei informacijai gauti:

- klausimai apie tai, kaip klientas sužinojo apie produktą, kaip tuo produktu naudosis;
- šeimos narių skaičius, respondento gimimo diena, šeimyninė padėtis ir užsiėmimas;
- nuomoja ar turi nuosavą gyvenamąją vietą;
- turimų kreditinių kortelių rūšys;
- laisvalaikio veikla, kur keliauja, ar mėgsta gaminti, siūti, medžioti, žaisti golfą, dalyvauti loterijose, ką kolekcionuoja ir pan.

Aišku, kad ši informacija nėra svarbi produkto registracijai. Bet niekur nėra nurodyta, kad ši informacija yra papildoma. Atvirkščiai, visur parašyta, kad tai svarbu. Pirkėjui sudaromas įspūdis, kad tik anketos užpildymas ir gražinimas yra viena iš produkto garantijos sąlygų, nors iš tikrųjų pirkimo čekis – tai viskas, ko reikia, kad pirkėjui būtų atlyginti nuostoliai, jei gaminyje pasirodo nekokybiškas. Greičiausiai, daugelis anketų, siunčiamų paštu, patenka į kompanijas, kurios renka asmens duomenis (Givens: 2001).

Kalbėdama apie elektroninių viešųjų ataskaitų duomenis, Beth Givens pažymi, kad jie gali būti naudojami antriniam tikslams pasiekti. Šie antriniai tikslai yra nutolę nuo pirminių duomenų rinkimo tikslų, dėl kurių iš pradžių jie ir buvo sukurti. Sudarant viešuosius įrašus iš keleto informacijos šaltinių ir sujungiant juos su komercinio sektoriaus duomenimis, atsiranda galimybė duomenis peržiūrėti ir

rūšiuoti įvairiais būdais. Yra sukuriami visai nauji įrašai. Vartotojai, kurie gali sudaryti šių naujų ataskaitų įrašus, naudojami įvairiomis priemonėmis, kad gautų duomenis. Pvz., Jutos teismas sužinojo, kad vienas viešbutis turėjo prieigą prie aplankų su informacija apie išsiskyrusius žmones ir siuntė išsiskyrusiems vienišiams žmonėms reklamą apie atostogas jų viešbutyje, kvietimus atostogauti be jų sutikimo ar prašymo. Tuo būdu viešbutis tikėjosi gauti daugiau užsakymų.

Bet yra nemažai rimtesnių pasekmių, kai išsamūs asmeninės informacijos duomenų aplankai sujungiami į dideles duomenų bazines. Palaipsniui žmonija tampa *Dosjė visuomene*. Platūs šaltiniai – tikslūs ar netikslūs – spragtelėjus pelyte tampa vis labiau prieinami praktiškai kiekvienam (Givens: 2002).

Galbūt dar nemalonesne dabartinio interneto ypatybe tapo *internetinis profiliavimas (онлайнное профилирование)*. Kompanijos vykdo interneto vartotojų stebėseną, kai jie naršo internete. Renkama informacija apie tai, kokius puslapius lanko žmogus, kiek laiko leidžia internete, kokius raktinius žodžius jis įveda paieškoje, ką perka interneto parduotuvėse, kokia reklama jiems padaro didžiausią įspūdį. Jei tai vyktų ne internete, tai būtų tokia situacija, kada į kiekvieną parduotuvę pirkėją lydėtų „žmogus, apsirengęs pilkai“ ir užsirašinėtu, ką perka, žiūrėtų per pečius, ką užsisako valgyti ir pan. Informacija, kuri renkama tokiu būdu, po to gali būti palyginama su kitais duomenimis (pvz., demografinė padėtimi regione). Galutinis rezultatas – labai smulki analizė, kuri turi tam tikrą vertę interneto rinkoje. Marketingo firmos jos pagrindu sudaro žmogaus dosjė – jo pomėgius, poreikius ir galimus pirkinius ateityje. Daugelis tokių profilių dabar nuasmeninti. Bet reikia tik juos sugretinti su informacija iš kitų duomenų bazių – su vardais, adresais ir pan. – ir profilis pasidaro susietas su konkrečiu žmogumi (Rotenberg: 2003).

Taip renkami duomenys pažeidžia visų pirma tikslingumo principą. Jie kaupiami skirtingais tikslais ir po to jungiami į išsamesnes duomenų bazines.

Žinomiausia technologija šia prasme yra slapukai (*cookies*), maži aplankai, kuriuose yra identifikaciniai numeriai. Slapukai taikomi, kai internetinio puslapio savininkas automatiškai suseka vartotojo veiksmus. Slapukų aplankai saugomi kietajame diske, kada vartotojas apsilanko puslapyje, puslapis „pažįsta“ vartotoją, kada šis atsidaro puslapį ir kitą kartą. Kai buvo išmokta naudotis slapukais iš karto keliuose tinklalapiuose, šios technologijos populiarumas ženkliai išaugo. Naują impulsą savo veiklos vystymui gavo firmos, užsiimančios reklama internete.

DoubleClick, stambiausia marketingo reklamos kompanija, turi susitarimus su daugiau nei 11 tūkstančių tinklalapių dėl slapukų naudojimo. Tai apima beveik 100 milijonų vartotojų.

Dar mažiau pastebima interneto vartotojų sekimo forma yra naudojimas taip vadinamų tinklo blakių (*web bugs*). Blakės – tai miniatiūriniai skaidrūs grafiniai piešiniai, kurie įtaisomi tinklalapyje. Uždavinys toks pat – sekti vartotoją. Blakės pagalba galima susekti vartotojo IP adresą, laiką, kada jis lankėsi ir pan. Blakę nesunku įtaisyti į elektroninius laiškus, kad būtų išsiaiškintas IP adresas, taip pat kada laiškas perskaitytas, kiek kartų persiųstas (Smirnov: 2003).

Anot M. Rotenbrego, ne interneto pasaulyje profiliavimas egzistuoja jau dešimtis metų. Kompanijos sudaro ištisas asmens duomenų bazes, naudodami daugybę šaltinių: pirkinių sąrašai supermarkete, kvitų pildymas garantiniam aptarnavimui, valstybinės informacinės sistemos, gyventojų surašymo duomenys, laikraščių ar žurnalų prenumerata, specialių tyrimų rezultatai ir pan. Teisėsaugos, draudžiančios informacijos rinkimą dėl dosjė, nėra. Kompanijos papildo šią informaciją iš kitų bazių. Dosjė gali būti susietas su kita informacija, pvz., medicinos kortelių (Rotenberg: 2003).

Teisės profesorius Jeffery Rosen savo knygoje *Nepageidaujamas spoksojimas: slaptumo griovimas Amerikoje (The Unwanted Gaze: The Destruction of Privacy in America)* svarsto neigiamas dosjė visuomenės pasekmes. Svarbiausias jo susirūpinimas – asmens duomenų po mažą „gabaliuką“ rinkimas iš įvairių šaltinių, paimtų iš konteksto, po to naudojamų priimant sprendimus apie mus. Jis rašo, kad kada skelbiama informacija, nutolusi nuo originalaus jos konteksto, ir parodoma nepažįstamiems, mes pažeidžiami, nes apie mus gali susidaryti klaidingą nuomonę (Givens: 2002).

Apibendrinant duomenų kaupimo tikslingumo principą, galima daryti išvadas, kad:

- a) kaupiamų duomenų apimtis turi būti pagrįsta – kaupiama ne daugiau, negu reikia konkrečiam tikslui;
- b) pasiekus tikslą, informacija turi būti sunaikinama;
- c) turi būti užtikrinta, kad asmeninio pobūdžio informacija, registruota vienam tikslui, nebūtų naudojama kitiems tikslams, išskyrus

įstatymais numatytus atvejus (pvz., kriminalinio nusikaltimo tyrimui) arba gavus asmens sutikimą.

2. 4. Duomenų prieinamumas

Asmens duomenų prieinamumas – taip pat labai svarbus sąžiningos informacijos principas. Anot Federalinės Prekybos Komisijos (*Federal Trade Commission*) skelbiamos informacijos, šis principas užtikrina žmogaus galimybę gauti priėjimą prie duomenų apie jį, t.y., peržiūrėti duomenis, sukauptus juridinio asmens aplankuose, ir, esant būtinybei, užginčyti tų duomenų tikslumą ir užbaigtumą. Abi (galimybės) užtikrina, kad duomenys yra tikslūs ir išsamūs. Kad būtų reikšmingesnis, priėjimas turi apimti šiuolaikinį ir nebrangų priėjimą prie duomenų, paprastas priemones tam, kad būtų galima užginčyti netikslius arba neišsamius duomenis, mechanizmą, kurio pagalba duomenų rinkėjas gali patikrinti informaciją ir priemones, kuriomis ištaisymai ir / arba vartotojų prieštaravimai būtų pridėti prie kartotekoje esančių duomenų ir nusiųsti visiems duomenų gavėjams.

Dažniausiai vartotojai skundžiasi, kad negali valdyti, reguliuoti, kontroliuoti, kaip jų asmens duomenys naudojami. Kai kurie bando susisiekti su siuntėjais, prašydami, kad jų asmens duomenys būtų sunaikinti, tačiau veltui. Asmens tapatybės vagystės – taip pat kontrolės problema. Šio nusikaltimo aukos neturi jokios priėjimo prie duomenų kontrolės. Vartotojai turi žinoti, kokios rūšies vartotojo duomenis firmos perka, parduoda arba keičia, kad sukurtų profilius, ir kokie yra jų informacijos šaltiniai, kokios rūšies pranešimus firmos teikė vartotojams dėl duomenų teikimo ir keitimosi duomenimis susijungiant firmoms (Givens: 2001).

Vartotojams turi būti sudaryta pasirinkimo galimybė, t.y., vartotojas galėtų pasirinkti, kaip gali būti naudojama bet kokia surinkta iš jo asmeninė informacija. Ypatingai pasirinkimas susijęs su antriniu duomenų naudojimu, t.y., kai naudojimas nebūtinai, kad būtų užbaigtas apsvarstytas sandoris. Tokie antriniai duomenų naudojimai gali būti vidiniai (pvz., vartotojo įrašymas į kompanijos adresatų sąrašą, kad parduotų papildomų produktų arba paslaugų) arba išoriniai (pvz., informacijos perdavimas tretiesiems asmenims).

Tradiciškai yra du pasirinkimo tipai: sutikimas arba nesutikimas. Sutikimo režimas reikalauja, kad patvirtinamieji žingsniai leistų vartotojams informacijos surinkimą ir / arba naudojimą. Nesutikimo režimas reikalauja, kad patvirtinamieji

žingsniai sustabdytų tokios informacijos surinkimą ir / arba naudojimą. Skirtumas yra tas, kad nėra taisyklių, kai jokie patvirtinantys būdai vartotojui nepriimti. Pasirinkimą gali sudaryti daugiau nei du – TAIP / NE – pasirinkimo variantai. Vartotojams gali būti sudaryta galimybė pasirinkti, ar jie nori būti viename bendrame vidiniame kompanijos ar marketingo adresatų sąrašė, parduotame tretiesiems asmenims. Kad būtų efektyviau, bet koks atrinkimo režimas turi užtikrinti paprastą ir lengvai pasiekiamą kelią vartotojui, kad šis įgyvendintų savo pasirinkimą.

Interneto aplinkoje pasirinkimas gali būti lengvai įgyvendinamas, paprasčiausiai spaudant kompiuterio ekrane mygtukus, kurie savo ruožtu parodo vartotojo apsisprendimą dėl jo informacijos naudojimo ir / arba platinimo. Interneto aplinka taip pat suteikia galimybę peržengti sutikimo / nesutikimo paradigmas. Pvz., vartotojai galėtų būti įpareigoti nustatyti informacijos naudojimo prieš įeinant į internetinį puslapį pirmenybę (Federal Trade Commission: 1998).

Asmens privatumui mažiausiai žalos padaro ta informacija, kuri yra gaunama tiesiogiai iš paties asmens. Tačiau pasitaiko atvejų, kai informacija iš vartotojo renkama nepastebimai ir be jo sutikimo. Yra du tokie mechanizmai: *atvirkštinis papildymas (reverse appending)* ir *automatinė skaičiaus identifikacija*.

Atvirkštinio papildymo praktika tokia: asmuo perka ir atsiskaito kreditine kortele. Tuo laiku jam nežinomas prekybininkas išsaugo jo ir kitų pirkėjų kreditinių kortelių numerius. Po to informacija perduodama kredito agentūrai, kuri prideda pašto adresą prie sąskaitos numerio – procesas vadinamas atvirkštiniu papildymu. Papildyti duomenys vėl nusiunčiami į prekybos štabą ir po to pagal tuos adresus išsiuntinėjami katalogai.

Rinkoje naudojama vis daugiau ir sudėtingesnių asmens duomenų rinkimo būdų. Kompiuterių, telekomunikacijų pagalba tie duomenys gali būti nepastebimai renkami.

Kitas nepastebimo duomenų rinkimo pavyzdys *automatinė numerio identifikacija*. Kada asmuo skambina nemokamu telefonu, jo numeris perduodamas užklauso gavėjui. Jei vartotojas pasirašė *automatinio numerio identifikacijos* aptarnavimo sutartį, tai gali apimti įeinančius skambučius. Tada prie telefono numerių gali būti pridedami papildomi duomenys (vardas, pavardė, gyvenamoji vieta ir pan.) Tokiu būdu kompanijos ir gauna asmens duomenis. Taip kuriama kompanijos duomenų bazė. Tik toks būdas yra neetiškas (Givens: 2001).

Tokiais atvejais asmuo negali sužinoti, koku tikslu jo informacija renkama, kur ji kaupiama ir negali koreguoti savo informacijos.

Duomenų prieinamumo principo išvada būtų tokia:

- a) individualiam asmeniui turi būti užtikrinta galimybė sužinoti, kokia informacija apie jį registruojama ir kam ji naudojama. Privatumui mažiausiai kenkia, kai informacija gaunama tiesiai iš asmens paties;
- b) asmeniui turi būti užtikrinta galimybė koreguoti informaciją apie save registruose.

2. 5. Duomenų saugumas

Ketvirtas plačiai priimtas principas – tai, kad duomenys turi būti tikslūs ir saugūs. Kad būtų užtikrintas duomenų vientisumas, rinkėjai turi imtis protingų priemonių, naudoti tik tikslus duomenų šaltinius ir nuorodas į duomenis prieš daugkartinius šaltinius, vartotojo priėjimo prie duomenų aprūpinimą ir pasenusių duomenų sunaikinimą arba jų pavertimą anoniminiais.

Kad duomenys būtų apsaugoti nuo praradimo ir neleistino priėjimo, naudojimo arba atskleidimo, būtinas saugumas, kuris apimtų ir organizacines, ir technines priemones. Organizacinės priemonės apima vidines organizacines priemones, kurios riboja priėjimą prie duomenų ir garantuoja, kad tie žmonės, kurie turi priėjimą, nepanaudos tų duomenų neteisėtai. Techninės saugumo priemonės reikalingos tam, kad būtų sustabdytas neteisėtas priėjimas prie duomenų. Jos apima šifravimą, perduodant duomenis ir duomenų saugojimą. Priėjimą riboja slaptažodžių naudojimas. Duomenys turi būti saugomi tik saugiuose serveriuose arba kompiuteriuose, kurių negalima taip lengvai visiems pasiekti modemu pagalba (Federal Trade Commission: 1998).

Anot *Junkbusters Svarbiausių principų tarptautinėms įmonėms (Guidelines for Multinational Enterprises)* rinkinyje skelbiamos informacijos, duomenų rinkėjas turi būti atsakingas už tai, kad imtųsi priemonių, užtikrinančių efektyvų principų įgyvendinimą. Anketiniai duomenys turi būti apsaugoti protingomis saugumo garantijomis prieš tokius pavojus kaip pametimas arba neteisėtas priėjimas, keitimas, naudojimas, sunaikinimas ar atskleidimas.

Pasitaiko atvejų, kai duomenų bazių saugumas nepakankamai užtikrintas. Tai sudaro palankias sąlygas duomenų nutekėjimui. Buvo atvejis, kai dėl Mičigano universiteto darbuotojų neatsakingumo medicininių duomenų bazė buvo visiems pasiekiamoje vietoje daugiau nei du mėnesius, kol ją atsitiktinai aptiko medicinos studentas, kuris ir paskelbė pavojų. Laimei, šis atvejis neatnešė pacientams žalos. Bet 2000 metais gruodį kažkoks Nyderlandų „kompiuterių genijus“ tyčia įsilaužė į Vašingtono medicinos centro kompiuterius ir pavogė 5 tūkstančius ligos istorijų. Kaltininkas teigė, jog norėjo įrodyti saugumo sistemos, saugančios duomenis, netobulumą (Smirnov: 2003).

Didelę žalą vartotojo privatumui ir asmens duomenų saugumui gali padaryti *skylės* (klaidos) saugumą užtikrinančiose sistemose. Daugelis tinklalapių neturi pakankamos apsaugos nuo atakų. M. Rotenbergas mini atvejį, kai 2000 m. kovą deimantų korporacija *De Beers* pametė 35 tūkstančius įrašų (vardai, adresai, telefono numeriai, elektroninio pašto adresai) žmonių, kurie kreipėsi su klausimais dėl deimantų įsigijimo. To priežastis - „skylė“ saugumo sistemoje. 2000 balandį visuomenė sužinojo, kad nežinomas Microsoft inžinierius įjungė į serverio programas slaptos prieigos galimybę. Užteko surinkti frazę „*Netscape engineers are weenies!*“ iš kito galo ir buvo galima gauti prieigą prie tinklalapio medžiagos. 2000 rugpjūtį kompanija *Kaiser Permanente*, kuri užsiima sveikatos draudimu JAV teritorijoje, prisipažino, kad pažeidė savo klientų konfidencialumą ir privatumą, kada išsiuntė elektroniniu paštu daugiau nei 800 laiškų. Šiuose laiškuose buvo asmens duomenys, o išsiųsti per klaidą jie buvo ne tiems, kuriems buvo skirti. Panašiai 2001 m. liepą vaisto antidepresanto kūrėjai „*Prozac*“ atskleidė daugiau kaip 700 savo pacientų, kurie buvo užsisakę naują vaistų siuntą, vardus ir elektroninio pašto adresus (Rotenberg: 2003). Šie pavyzdžiai vaizdžiai iliustruoja, kokios gali būti pasekmės, kai duomenų rinkėjai neužtikrina duomenų bazių saugumo ir prieigos prie jų.

Aptariant duomenų saugumo principą, reikėtų kalbėti ir apie duomenų rinkėjų atsakomybę. Pagrindiniai saugumo principai gali būti efektyvūs tik tada, jei yra mechanizmas, priverčiantis vykdyti juos. Kai nėra saugumo įgyvendinimo ir patirtos žalos kompensavimo mechanizmo, sąžiningos informacijos principų kodeksas praktiškai yra tik priverčiantis susimąstyti, o ne įsakantis ir negarantuoja suderinamumo su sąžiningos informacijos praktikos principais. Tarp alternatyvaus duomenų saugumo įgyvendinimo formų – savireguliacija, įstatymai, kurie sukurtų

savas priemones vartotojams, ir / arba reguliuojančios schemas, įgyvendinamos civilinėmis ir baudžiamosiomis sankcijomis (Federal Trade Commission: 1998).

Būtinai mechanizmai, garantuojantys vartotojams paprastą ir efektyvų būdą kreiptis, kai yra asmens duomenų kaupimo ar vartojimo pažeidimų. Tokiu būdu savireguliacijos sistema turi užtikrinti individualių vartotojų skundų tyrimo priemones ir garantuoti, kad vartotojai žino, kaip gauti priėjimą prie tokios sistemos.

Jei savireguliacijos kodeksas buvo pažeistas, vartotojai turi turėti priemonių, apsaugančių nuo to pažeidimo. Tokia priemonė gali apimti neteisingos informacijos taisymus (pvz., bet kokios dezinformacijos taisymas, nesąžiningų metodų nutraukimas) ir kompensacijas už bet kokią žalą, padarytą vartotojui. Sankcijos garantuotų, kad nesąžiningos informacijos aukoms būtų kompensuojama padaryta žala. Pramonės kodeksai gali numatyti patikimus alternatyvius ginčų sprendimo mechanizmus (Federal Trade Commission: 1998).

Iš to, kas pasakyta apie šį principą, galime daryti išvadą, kad duomenų rinkėjai (organizacijos ar asmenys), kaupiantys duomenis apie privačius asmenis, turi užtikrinti duomenų bazių saugumą – nuo neautorizuoto priėjimo, atskleidimo tretiesiems asmenims, duomenų iškraipymo.

2. 6. Sąžiningos informacijos principai taikomi informacijai, surinktai iš vaikų

Aukščiau išvardinti sąžiningos informacijos praktikos kodeksai neadresuoti informacijai, surinktai iš vaikų. Vaikai – lengvai pažeidžiama grupė, turint omenyje, kad jie neturi tokio analitinio mąstymo kaip suaugusieji. Tai liudija daugelis valstybinių įstatymų, kurie gina vaikus (pvz., draudimas parduoti alkoholį ir tabaką nepilnamečiams, vaikų pornografijos platinimas, tėvų sutikimo reikalavimas dėl medicininių procedūrų atlikimo ir pan.). Vis dažniau pripažįstama, kad būtina stiprinti vaikų gynimą ir tėvų vaidmenį, įgyvendinant vaikų gynimą. Pagrindinis iš vaikų surinktos informacijos principas - tėvų informavimas ir tėvų sutikimas, kad informacija iš jų vaikų būtų renkama. Būtent tėvai turi gauti informaciją ir turėti priemones, kad galėtų valdyti vaikų asmeninių duomenų rinkimą ir naudojimą. Tėvai turi būti informuojami, kaip ir kokiais tikslais iš vaiko renkama asmeninė informacija, kada surinkta informacija bus naudojama kitais tikslais. Vis dar pasitaiko nesąžiningos praktikos: yra renkama iš vaikų asmeninė informacija (pvz.,

vardas, pavardė, elektroninio pašto adresai, namų adresas, telefono numeris) ir parduodama ar kitaip atskleidžiama tretiesiems asmenims arba paskelbiama viešai internete, tinkamai neinformuojant tėvų ir nesuteikiant galimybės valdyti surinktą ir naudojamą informaciją.

Anot Federalinės Prekybos Komisijos (*Federal Trade Commission*), pranešime tėvams turi būti atkreiptas dėmesys į faktą, kad veiksmai internete gali būti unikalūs ir nežinomi tėvams. Tuo būdu pranešimas turi būti pakankamai detalizuotas, kad aiškiai tėvams pasakytų informacijos, kurią renka internetinis puslapis iš vaikų, tipą ir ką daryti tėvams, kad jie galėtų valdyti iš vaikų surinktą asmeninę informaciją. Kur tinklalapis numato dialogo veiksmus (pvz., pokalbių svetainės, skelbimo lentos, elektroninio pašto paslaugos, asmeninių internetinių puslapių registracija) tėvams turi būti paaiškinama, kad vaikų dalyvavimas suteikia galimybę kitiems tiesiogiai naudotis jų vaikų duomenimis. Toks pranešimas tėvams primena, kad tėvai gali kontroliuoti savo vaikų dalyvavimą ir padėti apginti vaikus nuo neteisėto jų duomenų naudojimo.

Tėvai dažniausiai nežino apie tai, kokia asmeninė informacija yra surinkta iš vaiko, todėl dalyvavimo principas ypač svarbus informacijos, surinktos iš vaikų, atžvilgiu. Kad būtų gautas tėvų sutikimas naudoti informaciją, surinktą iš vaikų, tėvai turi turėti prieigą prie tos informacijos. Tai svarbu ypač tada, jei tokia informacija surinkta neinformavus tėvų apie renkamos informacijos pobūdį. Tėvai suinteresuoti sužinoti viską apie informaciją, kurią internetiniai puslapiai renka iš jų vaikų. Tai labai svarbu, kai reikia priimti sprendimą, galintį kaip nors paveikti vaiką arba šeimą. Be to, vaikų informacija yra jautresnis informacijos tipas ir turi būti užtikrinama, kad vaiko asmens duomenys yra saugūs ir nebus neteisėtai panaudoti arba atskleisti (Givens: 2002).

Galima daryti išvadą, kad informacija, surinkta iš vaikų, yra *jautri informacija*, nes vaikai dažnai nesuvokia visų informacijos atskleidimo pasekmių. Tėvams turi būti sudaryta galimybė gauti informaciją, kaip renkama informacija, koks rinkimo tikslas, kaip ji bus naudojama, kokia informacija renkama ir kaip tėvai galėtų kontroliuoti, koreguoti ar kitaip tvarkyti iš vaikų renkama informaciją.

3. Asmens privatumas ir reikalavimai informacijos lauko dalyviams

Internetu apie interneto vartotojus yra surenkami milžiniški duomenų kiekiai, patiems vartotojams dažnai apie tai nieko nežinant. Ši skaidrumo trūkumo

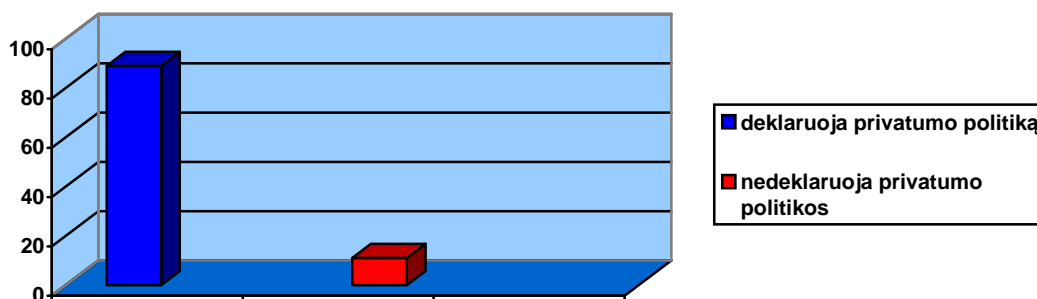
problema turi būti sprendžiama, norint pasiekti gerą asmeninių duomenų ir vartotojų apsaugos lygį.

Daugelis interneto lankytojų nori tiksliai žinoti, kas vyksta, kai jie naršo internete, naudojami internetu teikiamomis paslaugomis, rašo elektroninius laiškus ir pan. Žinojimas padėtų jiems apsaugoti privatumą, asmens duomenis. Kiekvienas internetinis puslapis turi gerbti savo vartotojų privatumą, įsipareigoti jį saugoti ir tinkamai informuoti vartotojus apie savo privatumo politiką ir praktiką, apie lankytojo galimybę pasirinkti būdus, kaip jų informacija bus renkama internete ir kaip ji bus naudojama. Taip pat kiekvienas tinklalapis turi teisę saugoti skelbiamą informaciją nuo neteisėto naudojimo. Todėl būtina privatumo politika, kuri naudinga ir reikalinga visiems informacijos lauko dalyviams.

3. 1. Privatumo politikos klausimas

Kiekvienam internetiniam puslapiui yra keliamas reikalavimas turėti privatumo politiką. Kai kurie internetiniai puslapiai nepakankamai aiškiai deklaruoja savo privatumo politiką, o kai kurie – vis dar jos neturi.

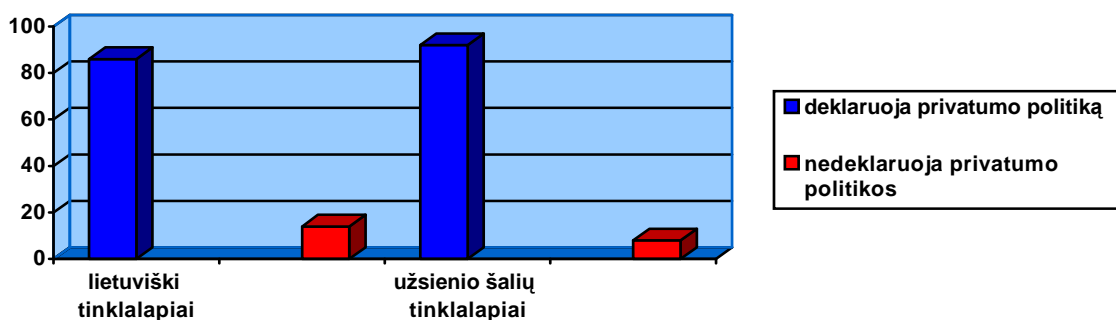
Atsitiktinės atrankos būdu (buvo peržiūrėti tinklalapiai davus užklausas paieškos sistemose *Google, Yandex, Rambler*) buvo peržiūrėta 340 tinklalapių įvairaus pobūdžio (po 170 lietuviškų ir užsienio šalių internetinių puslapių). 5 diagramoje parodyta, koks procentas peržiūrėtų internetinių puslapių deklaruoja privatumo politiką:



5 diagrama: Privatumo politikos deklaravimas internetiniuose puslapiuose

Taigi, beveik 9 kartus daugiau peržiūrėtų tinklalapių turi ir deklaruoja privatumo politiką: 303 (**89 %**) peržiūrėtuose tinklalapiuose privatumo politika yra, 37 (**11 %**) - nėra.

6 diagramoje parodytas lietuviškų ir užsienio šalių tinklalapių privatumo politikos deklaravimas (procentais nuo peržiūrėtų lietuviškų ir užsienio šalių tinklalapių):



6 diagrama: Privatumo politikos deklaravimas lietuviškuose ir užsienio šalių tinklalapiuose

Iš peržiūrėtų tinklalapių matyti, kad privatumo politiką deklaruoja daugiau užsienio šalių internetinių puslapių nei lietuviškų: **92 %** (156 tinklalapiai) užsienio šalių ir **86 %** (147 tinklalapiai) lietuviškų. Atitinkamai privatumo politika nedeklaruojama **8 %** užsienio šalių ir **14 %** lietuviškų tinklalapių (atitinkamai 14 ir 23 tinklalapiai). Visuose peržiūretuose - lietuviškuose ir užsienio šalių - tinklalapiuose, apie saugumo politiką informuojama pagrindinio puslapio apačioje nuorodomis *Privatumo politika / Privacy Policy*. Visi peržiūrėti lietuviški internetiniai puslapiai, kurie nedeklaruoja privatumo politikos, yra asmeniniai (ne įmonių ar organizacijų) tinklalapiai. Apibendrinant užsienio šalių internetinius puslapius reikia pasakyti, kad visi peržiūrėti internetiniai puslapiai, kuriuose nedeklaruojama privatumo politika, yra Rusijos (žr. priedą).

Tinklalapiai pagrindiniame puslapyje aiškiai matomoje vietoje turi įdėti pranešimą apie privatumo politiką, apie tai, ar ir kaip lankytojas turi save identifikuoti. JAV Komercijos departamento (*U.S. Department of Commerce*) privatumo praktika – *Saugaus uosto* programa. Šios programos privatumo praktikos principai: pranešimas, pasirinkimas, nukreiptas į priekį perdavimas, prieiga ir tikslumas, saugumas bei priežiūra/ vykdymas. Privatumo politika reikalinga ir internetinio puslapio savininkui, ir lankytojams. Ji yra savotiškas taisyklių, kuriomis vadovaujasi tinklalapio savininkas ir kurias turėtų žinoti bei jų laikytis lankytojas, rinkinys. Dažniausiai internetiniai puslapiai savo privatumo politikoje lankytojus informuoja apie:

a) *autorines teises:*

- informuojama, kad be nuorodų į tinklalapį negalima kitose svetainėse, žiniasklaidos priemonėse naudoti ar platinti esamos tekstinės ir grafinės informacijos;
- lankytojų teisės skelbti tinklalapyje savo turimą informaciją ir tinklalapio atsakomybė/neatsakomybė už paskelbtos informacijos turinį, tikslumą.

b) *asmeninę informaciją:*

- kaip, koku tikslu, koku būdu bus renkama asmeninė informacija;
- kaip / ar ji bus perduodama trečiosioms šalims
- lankytojo identifikavimas: kokios technologijos ir kokiai techninei informacijai (pvz., interneto protokolo adresui, naršyklės tipui sužinoti ir pan.) rinkti naudojamos.
- asmeninės informacijos saugumas;
- asmeninės informacijos tikslumas (pvz., klientui suteikiama galimybė prieiti prie savo informacijos, ją peržiūrėti ir keisti).

c) *draudžiamą informaciją:*

- kokią informaciją draudžiama skelbti (pvz., informacija, kurioje kurstoma tautinė, rasinė, religinė, socialinė bei lyčių neapykanta; platinama, propaguojama ar reklamuojama pornografija ir pan.);
- kaip bus elgiama su paskelbta draudžiama informacija, atsakomybė už jos paskelbimą.

d) *esamos privatumo apsaugos politikos pakeitimus:*

- ar bus pranešama apie privatumo politikos pasikeitimus.
- kaip bus pranešama apie pasikeitimus (pvz., jei internetinio privatumo pareiškime atnaujinamos nuostatos, bus pranešama apie pasikeitimus ir atnaujinama dokumento peržiūros data - tada lankytojas/klientas visada galės žinoti, apie atnaujinimus.

e) *kontaktinę informaciją (kur lankytojas/klientas gali kreiptis, jei iškiltų klausimų).*

Taip pat tinklalapiai savo privatumo politikoje turėtų numatyti saugoti vaikų privatumą ir skatinti tėvus ir globėjus aktyviai domėtis tuo, ką vaikai veikia ir kuo domisi internete.

Dar vienas reikalavimas internetiniams puslapiams – saugumo sertifikatai. Kad tinklalapio privatumo praktika atitinka privatumo programos reikalavimus, įrodo privatumo spaudas, kuris taip pat turi būti pagrindinio puslapio matomoje vietoje, kad lankytojas iš karto pastebėtų. Pasaulinio voratinklio konsorciumas (W3C) sukūrė naują privatumo technologiją P3P (ji yra Microsoft Internet Explorer 6 naršyklėje), kuri leidžia vartotojui papildomai kontroliuoti savo asmeninę informaciją ir priimti daugiau informuotus pasirinkimus apie tai, kaip internete naudojami jo asmeniniai duomenys. Naudojant P3P technologiją, galima taip sukonfigūruoti savo naršyklę, kad ji automatiškai nustatytų, ar svetainė renka asmenį identifikuojančią informaciją, ar naudoja tokią informaciją vartotojo profiliams kurti ir ar leidžia lankytojams šio duomenų rinkimo atsisakyti (Jarukaitis: 2005, 323).

Kai kurios svetainės skelbia nuorodas, kuriomis pasinaudojus, galima išeiti į trečiųjų šalių internetinius puslapius. Šios svetainės nekontroliuoja tokių internetinių puslapių privatumo politikos, todėl apie tai taip pat turėtų pranešti savo privatumo politikoje. Jei internetiniame puslapyje renkami slapti (pažeidžiami) duomenys, tinklalapyje, kai veikia saugumo priemonė (pvz., šifravimas) turėtų būti naršyklės lango matomoje vietoje pavaizduotas simbolis (pvz., rakto ar užrakintos spynos). Kai kurie internetinių puslapių savininkai nori, kad jo tinklalapio nekopijuotų visai, ar dalimis. Tokiu atveju savininkai privalo visur uždėti © - *copyright* ženklą. Kai kalbama apie tinklalapį, kurio savininkas nenori visiems parodyti pvz., mokami puslapiai, tai jis paprasčiausiai juos apsaugo identifikavimo slaptažodžiu, kurį klientas gauna sumokėjęs pinigų. Kad geriau apsaugotų lankytojų privatumą, tinklalapis turi pateikti pranešimą, kuris paaiškina, kaip naudotis informacija ir kokias alternatyvas, susijusias su informacijos kaupimu ir naudojimu šiame puslapyje, lankytojas turi. Jei lankytojas nesutinka su tinklalapio privatumo politika, jis neturėtų naudotis tuo internetiniu puslapiu.

Apibendrinant galima daryti išvadą, kad kiekvienas tinklalapis turi tinkamai informuoti lankytojus apie tai, kas vyksta, kai lankytojas apsilanko tinklalapyje, kokia informacija renkama, kaip ji naudojama, kaip lankytojas gali naudoti rastą

informaciją ir pan. Kad informavimas būtų išsamus ir aiškus būtina deklaruoti internetinio puslapio privatumo politiką.

3. 2. Vartotojų budrumo reikalavimas

Kuomet interneto vartotojas jungiasi prie interneto, jis naudojami tam tikrų organizacijų paslaugomis. Šios organizacijos turi galimybę atlikti įvairias duomenų registravimo ir apdorojimo operacijas (pvz., telekomunikacijų operatoriai registruoja sujungimus, interneto paslaugų teikėjas registruoja aplankytas interneto svetaines ir t.t.), ir tai gali būti susiję su asmens privatumu.

Yra daug patarimų interneto vartotojams, kaip elgtis, kad jie būtų sunkiau atpažįstami. Anot B. Givens, kiekvienas vartotojas, kai pradeda naršyti internete, iš pradžių turi ieškoti internetinio tinklalapio, kuriame jis lankosi, slaptumo politikos. Daugelis komercinių tinklalapių rašo apie tai. Pvz., TRUST`e – galima matyti emblemą, kuri parodo, kad jie laikosi tam tikrų informacijos atskleidimo metodų. JAV Federalinė Prekybos Komisija (*Federal Trade Commission*) kontroliuoja komercinius puslapius, kurie renka informaciją apie žmones, besilankančius tuose puslapiuose, kad matytų, ar renka informaciją, kokie informacijos rinkimo metodai taikomi, ar informacijos slaptumas pakankamas. Jie 2000 metų gegužę atliko tyrimus, paskelbė 1400 tinklalapių apžvalgos rezultatus ir nustatė, kad **92 %** iš jų renka informaciją. Bet tik **14 %** atskleidė, kokie informacijos rinkimo metodai. Blogiau, kad net 89 % vaikams skirtų tinklalapių renka informaciją ir tik 10 % iš jų numato tėvų leidimą (Givens: 2001).

Taigi, vis dažniau asmens duomenų rinkimas ir tvarkymas vyksta naudojant internetą, todėl privačiam asmeniui sunkiau pasinaudoti savo susipažinimo su duomenimis, ištaisymo, ištrynimo, kompensacijos teisėmis. Techninės ir organizacinės priemonės padedančios užkirsti kelią neteisėtam asmens duomenų rinkimui, pakeitimui, atskleidimui ar neteisėtam susipažinimui su jais yra ypač svarbios. Asmuo pats turėtų būti budrus ir žinoti, kokias technines priemones naudoti, kokių nuorodų ieškoti lankomuose tinklalapiuose, kokius filtrus ar apsaugas diegti savo kompiuteriuose, kad nebūtų taip lengvai aptinkamas virtualioje erdvėje ir nepatirtų moralinės ar materialinės žalos.

Daugelis žmonių naudojami elektroniniu paštu. Nemažą elektroninių laiškų dalį sudaro nepageidaujamas paštas. Kad būtų gaunama mažiau nepageidaujamo

pašto, gali padėti nepageidaujamo pašto filtrai, kurie padėtų nukreipti nepageidaujamus laiškus (deja, jie negali visiškai apsaugoti pašto dėžutės).

Kiekvienas interneto vartotojas turi būti budrus. Kaip pastebi Ryšių reguliavimo tarnyba, vis dažniau pasitaiko informacijos išgavimo apgaule /duomenų žvejojimo (*fishing*) atvejų: kai kuriais elektroniniais laiškais siekiama apgaule išgauti naudingą informaciją. Siuntėjas prašo nurodyti kredito kortelių duomenis, tinklo slaptažodžius ar sąskaitų numerius. Tokiuose laiškuose nurodyti tinklalapiai atrodo teisėti, tačiau priklauso internetiniams vagims. Įvedęs duomenis asmuo suteikia internetiniams vagims informaciją, reikalingą patekti į jo kompiuterį ir gauti prieigą prie duomenų. Vartotojai turi žinoti keletą paprastų taisyklių, kaip jiems elgtis:

- neįvedinėti svarbios informacijos į iššokstančius (*pop-up*) langus;
- įsitikinti, kad puslapis, kuriame naudojama konfidenciali informacija, veikia šifruoto protokolo – https - pagrindu. Tokio puslapio adresas turi prasidėti ne http:// , o https://, be to, naršyklės dešiniajame apatiniame kampe atsiranda specialus ženklelis, kurį paspaudus galima patikrinti šifravimo sertifikatą;
- naudoti *antiSpyware* programinę įrangą;
- naudoti *anti-spam* programinę įrangą, nes dauguma *fishing* atakų prasideda nuo *spam* srauto;
- laiku atnaujinti antivirusines programas, nes dauguma antivirusinių programų sugeba atpažinti piktybines programas, kuriomis gali būti bandoma pažeisti operacinę sistemą ir jas blokuoti;
- nesinaudoti nuorodomis, kurios būna įdėtos neaiškios kilmės elektroniniuose laiškuose, nes tai gali būti ne nuoroda, o paslėptas kenksmingas kodas;
- nuolat domėtis, kas vyksta elektroninėje erdvėje.

Interneto vartotojus galima būtų skirstyti į dvi grupes:

- 1) kurie teikia savo duomenis, būtinus užsisakant prekę ar paslaugą, dalyvaujant kokiame nors projekte ar programoje ir pan.;
- 2) kurie tik naršo internete.

[k]ą visų pirma turėtų atkreipti dėmesį pirmos grupės internetinio puslapio vartotojas (jie yra iš anksto turėtų būti supažindinami, kokius duomenis turi pateikti):

- kaip renkama jo informacija;
- kokia prieiga prie informacijos;
- kaip panaudojama sukaupta informacija;
- kiek laiko saugomi jo duomenys;
- koks tinklalapio saugumas;
- kaip jis bus informuojamas apie privatumo politikos pasikeitimus;
- kaip gali susisiekti su internetinio puslapio savininkais.

Antros grupės vartotojai, kurie patys neteikia duomenų, bet yra savotiški duomenų teikėjai, turėtų atkreipti dėmesį į tai:

- ar tinklalapis renka ir ar turi teisę rinkti vartotojų informaciją (pvz., fiksuoti prisijungusių prie tinklalapio asmenų IP adresus, laiką, trukmę, aplankytus puslapius ir pan.);
- kam tinklalapis naudos tokią informaciją (pvz., naudos šią informaciją savo vidinei statistikai, taip pat teiks apibendrintą statistiką apie tinklalapio lankytojus tretiesiems asmenims ir pan.);
- kokias technologijas naudoja renkant informaciją (pvz., slapukus (*cookies*));
- Ar turi ir kokias saugumo priemones tinklalapis turi (lankytojas turi ieškoti saugumo priemones nurodančių simbolių).

Visa ši informacija turėtų būti aiškiai matomoje vietoje, kad lankytojai lengvai ją pastebėtų.

Apibendrinant, galima daryti išvadą, kad asmuo daugiau dėmesio pats turi skirti savo saugumui internete stiprinti. Jis turi domėtis naujausiomis techninėmis priemonėmis, jų diegimu, nuolatiniu atnaujinimu, domėtis tinklalapyje esančia saugumo politika. Taip pat asmuo turi pats geriau saugoti savo asmeninę informaciją ir jos taip lengvai neatskleisti.

Išvados

1. Etiniu požiūriu, pirmoji žmogaus orumo sąlyga – jo autonomija, t.y., asmens galimybė laisvai ir savarankiškai daryti sprendimus, liečiančius jį patį. Galimybė laisvai spręsti numato asmens teisę į privatumą. Pastarosios nepaisymas atveria kelią manipuliacijoms su jo asmeniu, taigi – naikina asmens laisvę.
2. Paskutiniame XX-ojo ir pirmajame XXI-ojo amžiaus dešimtmečiais, sparčiai vystantis informacinėms komunikacijos technologijoms, atsirado visaapimančios kontrolės galimybė ir iškilo reali grėsmė žmogaus teisei į privatumą ir nesankcionuotam asmens duomenų naudojimui. Augant ekonominei informacijos svarbai, manipuliavimas asmens duomenimis darosi vis labiau pasiekiamas daugeliui.
3. Sociologiniai duomenys, liudijantys žmonių, besirūpinančių savo asmens duomenų saugumu, skaičiaus didėjimą, interpretuoti dviem požiūriais: viena vertus, skaičiaus augimas gali būti paaiškintas sparčia interneto ir asmens duomenų rinkimo bei sisteminimo technologijų (taigi, ir pažeidimo galimybių) plėtra, antra vertus, ši dinamika skatina manyti, kad auga informacinės terpės dalyvių jautrumas neteisėtoms manipuliacijoms jų asmens duomenimis.
4. Sociologiniu požiūriu, galimybė neteisėtai manipuluoti asmens duomenimis (be jo žinios ir sutikimo) yra galinga socialinės kontrolės, prieštaraujančios demokratinėms visuomenės vertybėms, priemonė.
5. Asmens duomenų rinkimo, tvarkymo, taigi, ir saugumo reikalavimus reglamentuoja įstatymai bei poįstatyminės normos, tačiau šiuolaikinėje įtinklintoje ir vis labiau įsitinklinančioje visuomenėje, sparčiai tobulėjant arba randantis naujoms asmens stebėsenos bei kontrolės technologijoms, vis labiau aktualėja atitinkamo etinio sauto – sąžiningos informacijos praktikos – kūrimo ir palaikymo procesas, prasidėjęs 9-tajame XX a. dešimtmetyje.
6. Sąžiningos informacijos praktikos principų įvairovėje svarbiausiais laikytini: atvirumas asmeniui (informavimas), informacijos kaupimo tikslingumas, duomenų prieinamumas asmeniui, duomenų saugumas trečiųjų šalių atžvilgiu. Sąžiningos informacijos principų, kaip etikos kodekso, tikslas –

stiprinti pasitikėjimą ir užtikrinti bendradarbiavimą tarp visų informacijos lauko dalyvių (vartotojų, kaupėjų, rinkėjų).

7. Tyrimas parodė, kad vis dažniau asmens duomenų rinkimas ir tvarkymas vyksta naudojant internetą, tačiau nepaisant visiems internetiniams puslapiams keliamo reikalavimo apibrėžti savąją privatumo politiką, kai kurie internetiniai puslapiai ją deklaruoja nepakankamai aiškiai, o kai kurie – vis dar jos neturi. Be to, daugelyje svetainių skelbiamos nuorodos į trečiųjų šalių internetinius puslapius, nepranešant, kad šios svetainės nekontroliuoja tų privatumo politikos.
8. Sąžiningos informacijos praktikos palaikymas dėl virtualios erdvės interaktyvaus pobūdžio kelia ir vartotojo / lankytojo budrumo reikalavimą. Pats asmuo turėtų domėtis naujausiomis techninėmis savaugos priemonėmis, neformaliai ieškoti lankomuose tinklapiuose privatumo politikos nuorodų, žinoti, kokius filtrus ar apsaugas diegti savo kompiuteriuose, kad nebūtų taip lengvai aptinkamas virtualioje erdvėje ir nepatirtų moralinės ar materialinės žalos.
9. Siekiant, kad sąžiningos informacijos principai taptų informacijos visuomenės etine norma, valstybės turėtų nuolat tobulinti teisinį informacijos praktikos reglamentavimą ir siekti, kad asmens privatumo pažeidėjai neliktų nenubausti, IKT profesionalai turi rūpintis techninėmis ir organizacinėmis priemonėmis, padedančios užkirsti kelią neteisėtam asmens duomenų rinkimui, pakeitimui, atskleidimui ar neteisėtam susipažinimui su jais (pvz., tokiomis kaip P3P technologija), o vartotojų budrumas turėtų būti skatinamas ir įgalinamas ne tik tinkamu švietimu, bet ir aktyvia paties vartotojo pozicija bei savišvieta.

Literatūra ir šaltiniai

1. Алексеенко, Т. *Договоримся о терминах* . - Privacy International и Electronic Privacy Information Center, 2004;
<http://privacy.hro.org/about/common/term.php>, 2005-10- 05.
2. Catlett, J. *Fair Information Practices* . - Guidelines for Multinational Enterprises, 1980; www.junkbusters.com, 2005-12-01.
3. Civilka M. *Asmens duomenų apsauga taptautinėje ir EB teisėje // Elektroninių ryšių teisė/ Jarukaitis I., Lamanauskas T., Civilka M., Makauskaitė A..-Vilnius: Eugrimas, 2005.-382.*
4. CNews, *Большинство американцев боятся интернета*. - Опрос газеты Washington Post и телекомпании ABC, 2005;
<http://privacy.hro.org/docs/sociology/>, 2006-01-10.
5. Dworkin R. Rimtas požiūris į teises: teisės sociologija.- Vilnius: Lietuvos rašytojų sąjungos leidykla, 2004.- 516.
6. Europos Tarybos informacijos biuras. *Visuotinė Žmogaus teisių deklaracija*.- Vilnius: Lietuvos žmogaus teisių centras, 2000.-109;
<http://www.etib.lt/>, 2005-12-06.
7. Federal Trade Commission. *Fair Information Practice Principles* . - Privacy Online: A Report to Congress.1998;
<http://www.ftc.gov/reports/privacy3/fairinfo.htm>, 2005-10-25.
8. Frayssinet J. *Is Protection of Personal Data Guaranteed on the Internet* . - Ethics and Information Technology, 2001. Vol. 4, no. 3; pp. 157-169;
http://droit-internet-2001.univ.paris1.fr/pdf/ve/Frayssinet_EN.pdf, 2005-12-02.
9. Гарфинкель С. Все под контролем: частная жизнь под угрозой, - Журнал "Неприкосновенный запас" 2003, №. 42, pp.56;
<http://bugtraq.ru/library/books/dbnation/>, 2005-12-03.
10. Gavison R. *Privacy and the Limits of the Law*. - Yale Law Journal, Vol. 89, No. 3, 1980; pp. 139-152
11. Givens B. *Public Records on the Internet: The Privacy Dilemma*.- Privacy Rights Clearnighouse, 2002;
www.cfp2002.org/proceedings/proceedings/givens.pdf 2005-11-10.

12. Givens B. *True or False? You Can Find Out Anything about Anybody on the Net* . - Presentation to Western Regional Home Management and Family Economics Educators, 1998; <http://www.privacyrights.org/ar/cybercon.htm> 2005-11-25.
13. Givens B. *The Information Marketplace: Merging and Exchanging Consumer Data* . - Comments to the Federal Trade Commission Workshop, 2001-04-31; <http://www.ftc.gov/bcp/workshops/infomktplace/comments/givens.htm>, 2005-11-05.
14. Givens B. *What's Missing from This Picture? Privacy Protection in the New Millennium* . - National Association of Attorneys General Annual Conference 2000-06-22; <http://www.privacyrights.org/ar/nagg-mill.htm>, 2005-11-10.
15. Glenn A. R. *The Right To Privacy: Rights And Liberties Under The Law*.- Yale Law Journal, Vol. 14, No. 4, 2004; pp.275-279; <http://www.bsos.umd.edu/gvpt/lpbr/subpages/reviews/Glenn404.htm>, 2005-11-12.
16. Jarukaitis I. *Asmens privatumo ir informacijos apsauga elektroninių ryšių sektoriuje* // Elektroninių ryšių teisė/ Jarukaitis I., Lamanauskas T., Civilka M., Makauskaitė A.-Vilnius: Eugrimas, 2005.-382.
17. Kantas I. *Dorovės metafizikos pagrindai*.- Vilnius: Mintis, 1980. - 114 p.
18. Labalme F., Dawaik J., *An Infomediary Approach to Privacy problem (Lumeria Whitepaper), Fair Information Principles* . - Privacy Online: A Report to Congress, 1998; <http://www.broadcatch.com/lumeria/paper1/fairinfo4.shtml>, 2005-12-10.
19. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas // Valstybės žinios.-2003, Nr.15-597.
20. Lietuvos Respublikos ryšių reguliavimo tarnyba. *RRT įspėja elektroninių paslaugų vartotojus saugoti savo duomenis* . - Aktualijos, 2005; <http://www.rrt.lt/index.php?136129431>, 2006-01-01.
21. Lomanienė N. *Žmogaus teisės: idėjos istorija* // Žmogaus teisės Lietuvoje: teoriniai ir praktiniai aspektai/sudarė ir redagavo N. Lomanienė, - Vilnius: VPU leidykla, 1996.-167.
22. Louveaux S. *Privacy Issues* . - ECLIP Research Paper, deliverable 2.1.3., 1999; http://www.jura.uni-muenster.de/eclip/eclip_1.htm, 2005-11-25.

23. Marx G. *Identity and Anonymity: some Conceptual Distinctions and Issues for Research* . - Documenting Individual Identity. Princeton University Press, 2001; <http://web.mit.edu/gtmarx/www/garyhome.html>, 2005-10-10.
24. Marx G. *Monitoring On The Job: How to Protect Privacy as Well as Property* . - Technology Review, Nov.-Dec., 1986; <http://web.mit.edu/gtmarx/www/garyhome.html>, 2005-10-03.
25. Marx G. *Murky Conceptual Waters: the Public and the Private* . - Ethics and Information Technology, 2001. Vol. 3, no. 3; pp. 157-169; <http://web.mit.edu/gtmarx/www/murkypublicandprivate.html>, 2005-12-05.
26. Marx G. *What's in a Name? Some Reflections on the Sociology of Anonymity* . - The Information Society, special issue on anonymous communication forthcoming, 1999; <http://web.mit.edu/gtmarx/www/garyhome.html>, 2005-12-15.
27. Пазюк А. *Право на приватность* . - Privacy International и Electronic Privacy Information Center, 2004; <http://privacy.hro.org/about/common/pazuk.php>, 2005-10-25.
28. Петросян М. *О праве на неприкосновенность частной жизни* . - Доклад на конференции „Неприкосновенность частной жизни в сети”, 2003; <http://www.hro.org/editions/karta/nr3435/petr.php>, 2005-11-23.
29. Privacy Rights Clearinghouse. *Consumers*. - Nonprofit Consumer information and Advocacy Organization, 2002. www.privacyrights.org, 2005-11-15.
30. Ротенберг М. *Право на неприкосновенность частной жизни* . - Privacy International и Electronic Privacy Information Center, 2003; http://www.hro.org/docs/rep/privacy/phr2002/phr2002_19.php, 2005-12-03.
31. Смирнов, С. *Информационная приватность (приватность персональных данных)* // Смирнов С. Приватность.- Москва: Права человека, 2003,-232; http://privacy.hro.org/docs/books/smirnov/index_4.php, 2005-11-05.
32. Смирнов С. *Концепция персональной информации* .- Доклад Consumers International, 2003; <http://privacy.hro.org/docs/laws/projects/conception.php>, 2005-10-05.

33. Šaulauskas M. P. *Homo informaticus apžavas: du prietarai, trys svajos* . - Informacijos Mokslai, Vilnius, 1999;
<http://www.fsf.vu.lt/filk/mps/homoinfo.htm> 2005-11-08.
34. The OpenPrivacy. *OpenPrivacy platform* . - www.openprivacy.org/, 2006-01-04.
35. The Wall Street Journal Online. *Internet Privacy* . - Wall Street Journal, 2004. December 6; <http://online.wsj.com/public/us>, 2005-12-30.
36. U.S. Department of Commerce. Export Portal. *Safe Harbor* . - US Department of Commerce, Office of Telecommunications, WashingtonDC, 2000; <http://www.export.gov/safeharbor/>, 2006-01-04.
37. Valstybinė duomenų apsaugos inspekcija. *Montreux deklaracija*.- Konferencijų dokumentai, 2005;
<http://www.ada.lt/index.php?lng=lt&action=page&id=126> 2005-11-18.
38. Valstybinė duomenų apsaugos inspekcija. *2002 metų veiklos ataskaita*.- Metinės ataskaitos, 2002; 41; www.ada.lt, 2006-12-04.
39. Valstybinė duomenų apsaugos inspekcija. *2003 metų veiklos ataskaita*.- Metinės ataskaitos; www.ada.lt, 2006-12-04.
40. Valstybinė duomenų apsaugos inspekcija. *2004 metų veiklos ataskaita*.- Metinės ataskaitos; www.ada.lt, 2006-12-04.
41. Westin A. *Privacy and Freedom*.- New York: Atheneum, 1967, 487;
<http://www.privacilla.org/fundamentals/privacyandfreedom.html>, 2005-12-01.
42. Žmogaus teisės. Europos Tarybos ir Europos Sąjungos dokumentai. – Vilnius: Lietuvos žmogaus teisių centras, 2000.-109.

Priedai

1 lentelė: JAV interneto vartotojų, besirūpinančių saugumu internete, skaičiaus dinamika 1999-2004 metais

| Metai | Skaičius procentais |
|-------|---------------------|
| 1999 | 64 |
| 2000 | 77 |
| 2001 | 79 |
| 2002 | 88 |
| 2003 | 92 |
| 2004 | 94 |

Šaltinis: The Wall Street Journal, <http://online.wsj.com/public/us>

2 lentelė: Duomenų subjektų skundų skaičiaus dinamika 2000-2005 metais Lietuvoje

| Metai | Skundų skaičius |
|-------|-----------------|
| 2000 | 5 |
| 2001 | 8 |
| 2002 | 21 |
| 2003 | 55 |
| 2004 | 91 |
| 2005 | 53 |

Šaltinis: Valstybinė duomenų apsaugos inspekcija, www.ada.lt

3 lentelė: Duomenų subjektų skundų skaičiaus kaita ir kismas 2000-2005 metais

| Metai | 2000 | 2001 | 2002 | 2003 | 2004 | 2005 |
|-----------------------------------|------|------|---------|---------|--------|---------|
| Skundų skaičius | 5 | 8 | 21 | 55 | 91 | 53 |
| Skundų skaičius - kaitos dinamika | 0 % | 60 % | 320 % | 1000 % | 1720 % | 960 % |
| Skundų skaičius - kismo dinamika | 0 % | 60 % | 162,5 % | 161,9 % | 65,5 % | -41,8 % |

Šaltinis: Valstybinė duomenų apsaugos inspekcija, www.ada.lt

4 lentelė: Pateiktų skundų pobūdis 2003-2004 metais (procentais nuo pateiktų skundų skaičiaus)

| Skundų pobūdis / metai | 2003 | 2004 |
|----------------------------------|------|------|
| Dėl asmens kodo naudojimo | 5 | 15 |
| Dėl duomenų apimtys | 7 | 10 |
| Dėl teikimo tretiesiems asmenims | 36 | 23 |
| Dėl duomenų rinkimo ir gavimo | 18 | 10 |
| Dėl duomenų tvarkymo | 10 | 30 |
| Kitos priežastys | 24 | 12 |

Šaltinis: Valstybinė duomenų apsaugos inspekcija, www.ada.lt

5 lentelė: Privatumo politikos deklaravimas internetiniuose puslapiuose

| | Tinklapių skaičius (vnt.) | Tinklapių skaičius (%) |
|----------------------------------|------------------------------|---------------------------|
| Deklaruoja privatumo politiką | 303 | 89 |
| Nedeklaruoja privatumo politikos | 37 | 11 |

6 lentelė: Privatumo politikos deklaravimas lietuviškuose ir užsienio šalių tinklalapiuose

| | Deklaruoja privatumo politiką | | Nedeklaruoja privatumo politikos | |
|-----------------------------|-------------------------------|-----------|----------------------------------|-----------|
| | skaičius | procentai | skaičius | procentai |
| Lietuviški tinklalapiai | 147 | 86 | 23 | 14 |
| Užsienio šalių tinklalapiai | 156 | 92 | 14 | 8 |

Užsienio šalių internetiniai puslapiai, kurie nedeklaruoja privatumo politikos:

1. <http://irkpost.ru/>
2. <http://www.soc.pu.ru/>
3. <http://www.dialog-21.ru/>
4. <http://www.medialaw.ru/>
5. <http://www.sreda-mag.ru>
6. <http://5ballov.com.ru/>
7. <http://eduworld.ru>
8. <http://www.tsure.ru>
9. <http://www.peronline.ru>
10. <http://www.bdva.ru>
11. <http://www.best-info2005.narod.ru>
12. <http://law.ilca.ru>
13. <http://www.informator.com.ru>
14. <http://rotten.splane.ru>