



**KAUNO TECHNOLOGIJOS UNIVERSITETAS**  
**SOCIALINIŲ, HUMANITARINIŲ MOKSLŲ IR MENŲ FAKULTETAS**

**Rita Plauškienė**

**ASMENS DUOMENŲ APSAUGOS SISTEMA EUROPOS  
SĄJUNGOJE: LIETUVOS ATVEJO ANALIZĖ**

Baigiamasis magistro projektas

**Vadovas**  
Dr. Vaidas Morkevičius

**KAUNAS, 2017**

**KAUNO TECHNOLOGIJOS UNIVERSITETAS**  
**SOCIALINIŲ, HUMANITARINIŲ MOKSLŲ IR MENŲ FAKULTETAS**

**ASMENS DUOMENŲ APSAUGOS SISTEMA EUROPOS  
SAJUNGOJE: LIETUVOS ATVEJO ANALIZĖ**

Baigiamasis magistro projektas

Viešasis administravimas (kodas 621N70001)

**Vadovas**

(parašas)

Dr. Vaidas Morkevičius

(data)

**Recenzentas**

(parašas)

Prof. Algis Junevičius

(data)

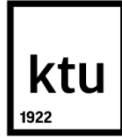
**Projektą atliko**

(parašas)

Rita Plauškienė

(data)

**KAUNAS, 2017**



**KAUNO TECHNOLOGIJOS UNIVERSITETAS**

Socialinių, humanitarinių mokslų ir menų

(Fakultetas)

Rita Plauškienė

(Studento vardas, pavardė)

Viešasis administravimas, SMVN-4/5

(Studijų programa, kursas)

Baigiamojo projekto „Asmens duomenų apsaugos sistema Europos Sąjungoje: Lietuvos atvejo analizė“

**AKADEMINIO SAŽINGUMO DEKLARACIJA**

20 17 m. sausio 9 d.  
Kaunas

Patvirtinu, kad mano, **Ritos Plauškienės**, baigiamasis projektas tema „Asmens duomenų apsaugos sistema Europos Sąjungoje: Lietuvos atvejo analizė“ yra parašytas visiškai savarankiškai ir visi pateikti duomenys ar tyrimų rezultatai yra teisingi ir gauti sąžiningai. Šiame darbe nei viena dalis nėra plagijuota nuo jokių spausdintinių ar internetinių šaltinių, visos kitų šaltinių tiesioginės ir netiesioginės citatos nurodytos literatūros nuorodose. Įstatymų nenumatytų piniginių sumų už šį darbą niekam nesu mokėjęs.

Aš suprantu, kad išaiškėjus nesąžiningumo faktui, man bus taikomos nuobaudos, remiantis Kauno technologijos universitete galiojančia tvarka.

\_\_\_\_\_  
(vardą ir pavardę įrašyti ranka)

\_\_\_\_\_  
(parašas)

Plauskiene Rita. *The System of Personal Data Protection in the European Union: Analysis of Lithuania Case*: Master's thesis in Public Administration / supervisor dr. Vaidas Morkevicius. The Faculty of Social Sciences, Arts and Humanities, Kaunas University of Technology.

Research area and field: 03 S

Key words: personal data, privacy, data protection, data controller, data subject.

Kaunas, 2017. 64 p.

## SUMMARY

The right to private life is a novelty in Lithuania. In rapid development of technologies it is significantly relevant to provide favourable conditions for the development of information technologies and create safe legal environment, which would protect human rights towards privacy. However, it seems that the development of technologies poses danger to the integrity of personal data and illegal use of information. The protection of human rights and lack of protection for personal data endangers personal privacy. It therefore becomes relevant to examine Lithuanian system of data protection as it is currently in the stage of infancy. The object of this project is the system of personal data protection and related problematic phenomena. The aim of the project is to examine current Lithuanian data protection system and to compare it to the one that functions in Norway. The first objective was to identify the elements of data protection system. Therefore, the first part of the thesis describes the main principles of personal data management. Main conceptions of personal data system are as follows: *personal data*, *data subject* and *data controller*. In order to give effect to the second objective of this project, the paper provides analysis of the system used for the regulation of data protection both in Lithuania and the European Union. The second part of the project analyses main legal acts regulating the protection of personal data, identifies general institutions as well as its functions at the level of the entire European Union.

The paper provides the examination of the provisions of the main legal document the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Other legal acts that regulate the protection of personal data in the European Union are also analysed. The provisions and amendments of the new directive, which came into effect in 2016, are also discussed. Key areas with possible future changes are highlighted.

The third part of this thesis includes the case of Lithuania. Lithuanian personal data system and legal regulation are being assessed. Case analysis is carried out in comparison to the Norwegian data protection system. General similarities and differences of the implementation of data protection applicable in both these countries are highlighted. According to the results of the project, personal data protection system functions insufficiently in Lithuania. The comparison of Lithuanian and Norwegian systems shows that the society of Lithuania lacks knowledge on personal data protection. When processing personal data, Lithuanian data processors not always follow the general aim set. As per the results of the thesis, Lithuania should follow the Norwegian personal data management practice – after data are deleted, anonymized or the goal of the process is reached. In addition, data processing should be bound with more strict rules, whereas data controllers should be obliged to provide data subjects with the information related to their personal data. A number of analyses show that the representatives of Lithuanian business and public institutions lack knowledge on the protection of personal data. In order to improve the implementation of Lithuania's personal data policy, technologies should be used to provide more information about problems in the system of personal data, about protections tools. Besides, it could also be useful to organise conferences, to publish research data in various means of media. Project data should be used as guidance. The identified problems should form basis for the action plan needed to improve the system of data protection in Lithuania.

## Turinio struktūra

<b>LENTELĖS .....</b>	<b>2</b>
<b>PAVEIKSLAI .....</b>	<b>2</b>
<b>PRIEDAI .....</b>	<b>3</b>
<b>ĮVADAS .....</b>	<b>5</b>
<b>1. ASMENS DUOMENŲ KONCEPCIJOS ANALIZĖ.....</b>	<b>8</b>
1.1. Asmens duomenų samprata bei jos raida.....	8
1.2. Teisės į privatumą samprata bei ryšys su asmens duomenų apsauga.....	12
1.3. Asmens duomenų apsaugos principai.....	14
1.4. Duomenų valdytojo ir duomenų subjekto samprata.....	15
1.5. Bendrieji duomenų tvarkymo principai.....	18
1.6. Netinkamas asmens duomenų naudojimas ir grėsmių privatumui šaltiniai.....	22
<b>2. ASMENS DUOMENŲ APSAUGOS SISTEMA EUROPOS SĄJUNGOJE.....</b>	<b>24</b>
2.1. Pagrindiniai teisinių normų aktai reglamentuojantys asmens duomenų apsaugą Europos Sąjungoje.....	24
2.2. Europos Sąjungos institucijų, atsakingų už asmens duomenų apsaugą, funkcijos ir vaidmuo tarptautiniu lygmeniu.....	28
2.3. Europos Sąjungos asmens duomenų apsaugos reguliavimo priemonės.....	30
<b>3. PROJEKTO TIRIAMOJI IR ANALITINĖ DALIS.....</b>	<b>33</b>
3.1. Pagrindiniai Lietuvos teisės aktai reglamentuojantys duomenų apsaugą nacionaliniu lygmeniu.....	33
3.2. Institucijos, atsakingos už asmens duomenų priežiūrą ir vykdymą.....	36
3.3. Asmens duomenų sistemoje esančių problemų identifikavimas.....	40
3.4. Asmens duomenų apsaugos priemonių paplitimas ir panaudojimas Lietuvoje.....	42
3.5. Norvegijos asmens duomenų apsaugos sistema.....	48
3.5.1. Teisės aktai reglamentuojantys duomenų apsaugą Norvegijoje.....	50
3.5.2. Už asmens duomenų apsaugą atsakinga institucija.....	52
3.6. Asmens duomenų panaudojimas ir įgyvendinimas Norvegijoje.....	53
<b>IŠVADOS .....</b>	<b>56</b>
<b>REKOMENDACIJOS.....</b>	<b>58</b>
<b>LITERATŪRA .....</b>	<b>59</b>
<b>ŠALTINIAI.....</b>	<b>63</b>

## **LENTELIŲ IR PAVEIKSLŲ SĄRAŠAS**

1. lentelė . Europos Sąjungos institucijos atsakingos už asmens duomenų apsaugą.....	28
2. lentelė. Inspekcijos vykdomos veiklos.....	36
3. lentelė. VDAI Elektroninių paslaugų sistemos teikiamos paslaugos.....	38
4. lentelė.Principai, sudarantys Norvegijos asmens duomenų teisę.....	49
1.pav. Pagrindiniai informaciniai šaltiniai.....	9
2.pav. Asmens duomenų sąvokos elementai.....	11
3.pav. Privatumo sąvokos koncepcijos.....	14
4.pav. Reikalavimai asmens duomenims.....	18
5.pav. Asmens duomenų kokybės principai.....	19
6.pav. Valstybinės duomenų inspekcijos administracijos struktūra.....	38

## SĄVOKŲ SĄRAŠAS

***Asmens duomenys*** – reiškia bet kurią informaciją, susijusią su asmeniu (duomenų subjektu), kurio tapatybė yra nustatyta arba gali būti nustatyta; asmuo, kurio tapatybė gali būti nustatyta, yra tas asmuo, kurio tapatybė gali būti nustatyta tiesiogiai ar netiesiogiai, ypač pasinaudojus nurodytu asmens identifikavimo kodu arba vienu ar keliais to asmens fizinėi, fiziologinei, protinei, ekonominei, kultūrinei ar socialinei tapatybei būdingais veiksniais (Europos Parlamento ir Tarybos direktyva (95/46/EB)).

***Duomenų valdytojas*** – reiškia tokį fizinį ar juridinį asmenį, valstybės valdžios instituciją, agentūrą ar bet kurį kitą organą, kuris vienas ar drauge su kitais nustato asmens duomenų tvarkymo tikslus ir būdus; jeigu tvarkymo tikslus ir būdus nusako nacionaliniai arba Bendrijos įstatymai bei norminiai aktai, tai duomenų valdytoją arba specifinius kriterijus, pagal kuriuos skiriamas duomenų valdytojas, gali apibrėžti nacionaliniai arba Bendrijos įstatymai (Europos Parlamento ir Tarybos direktyva (95/46/EB)).

***Duomenų subjektas*** – reiškia fizinį ar juridinį asmenį, valstybės valdžios instituciją, agentūrą ar bet kurį kitą organą, kuris tvarko asmens duomenis duomenų valdytojo vardu (Europos Parlamento ir Tarybos direktyva (95/46/EB)).

***Asmens duomenų tvarkymas (tvarkymas)*** – reiškia bet kurią operaciją ar operacijų rinkinį, automatiniiais arba neautomatiniais būdais atliekamus su asmens duomenimis, kaip antai: rinkimas, užrašymas, rūšiavimas, saugojimas, adaptavimas ar keitimas, atgaminimas, paieška, naudojimas, atskleidimas perduodant, platinant ar kitu būdu padarant juos prieinamus, išdėstymas reikiama tvarka ar sujungimas derinant, blokavimas, trynimas ar naikinimas (Europos Parlamento ir Tarybos direktyva (95/46/EB)).



## IVADAS

*Temos aktualumas.* Teisė į asmens duomenų apsaugą atsirado iš teisės į privataus gyvenimo gerbimą. Sudedamoji teisės į privatą gyvenimą dalis yra informacija apie asmenį bei šios informacijos sauga. Garantuojant asmens teisę į privatą gyvenimą, kartu garantuojama ir jo asmens duomenų apsauga, o kita vertus – užtikrinant asmens duomenų apsaugą yra saugomas ir asmens privatus gyvenimas (Petraitytė, 2011, p.165). Taigi, galima pastebėti privatumo ir asmens duomenų saugos sąsajas. Asmens privačios erdvės apsauga nuo kitų subjektų, visų pirma valstybės, įsikišimo pirmą kartą tarptautinėje teisinėje priemonėje buvo nustatyta 1948 m. Jungtinių Tautų (JT) visuotinės žmogaus teisių deklaracijos 12 straipsnyje dėl teisės į privataus ir šeimos gyvenimo gerbimą. Remiantis šia deklaracija galima teigti, kad kartais gali būti sudėtinga visiškai atskirti privataus ir profesinio gyvenimo sritis. Dažniausiai atliekant tam tikras operacijas susijusias su asmeniu būtina identifikuoti žmogaus tapatybę, tad yra dirbama su konfidencialia informacija. Taigi, asmens duomenimis yra laikoma bet kuri informacija, susijusi su fiziniu asmeniu – duomenų subjektu, kurio tapatybė yra žinoma arba gali būti tiesiogiai ar netiesiogiai nustatyta pasinaudojant tokiais duomenimis – asmens kodas, vienas arba keli asmeniui būdingi fizinio, fiziologinio, psichologinio, ekonominio, kultūrinio ar socialinio pobūdžio požymiai (Asmens duomenų teisinės apsaugos įstatymas 1996, 2 str. 1 d.). Akivaizdu, kad tapatybei nustatyti reikalingi tam tikri asmens duomenų elementai, kuriuose asmuo aprašomas taip, kad jį galima atskirti nuo visų kitų asmenų ir atpažinti kaip konkretų asmenį. Teisinėse apibrėžtyse, susijusiose su asmens duomenimis, išsamiau nepaaiškinama, kada asmens tapatybė laikoma nustatyta.

Teisė į privatą gyvenimą yra viena iš naujausių žmogaus teisių Lietuvoje. Asmens duomenų apsaugos tradicijos mūsų šalyje plėtojamos nuo pat Nepriklausomybės atkūrimo. Nuo 1997 m. veikianti Valstybinė duomenų apsaugos inspekcija įgyvendina plėtoja duomenų apsaugą, prižiūri asmens duomenų valdytojų veiklą tvarkant asmens duomenis, kontroliuoja asmens duomenų

tvarkymo teisėtumą, nagrinėja duomenų tvarkymo pažeidimus, bendradarbiauja su Valstybine vartotojų teisių apsaugos tarnyba.

Reikia paminėti, kad asmens privataus gyvenimo apsauga ir neliečiamumas yra ginamas ir pagrindinio šalies įstatymo – Lietuvos Konstitucijos. Taip pat ši teisė yra reglamentuojama ir tarptautiniu lygmeniu: Visuotinėje žmogaus teisių deklaracijoje, Europos žmogaus teisių ir pagrindinių laisvių konvencijoje, asmens duomenų apsaugos direktyvoje, Europos Sąjungos pagrindinių teisių chartijoje.

**Tyrimo problema:** Nors atrodytų, kad asmens duomenų apsaugai skiriama pakankamai dėmesio, tačiau šių nuostatų įgyvendinimas yra nepakankamas. Sparčiai vystantis naujoms technologijoms, pasauliniu mastu susiduriama su problema – kaip sudaryti palankias sąlygas informacijos technologijų plėtrai ir sukurti saugią teisinę aplinką, kurioje būtų ginama žmogaus teisė į privataus gyvenimo neliečiamumą. Iškilę naujų pavojų asmens duomenų neliečiamumui, neteisėtam informacijos panaudojimui. Technologijų naudojimas padėjo institucijoms naudotis asmens duomenimis, tačiau taip pat įgalino valdžią ir teisėsaugos institucijas kaupti informaciją apie asmenis, sukūrė sąlygas naujiems privatumo pažeidimams. Kompiuteriniai tinklai išskėlė dar didesnę grėsmę. Susirūpinimą žmogaus teisių apsaugos požiūriu kelia ir vis dažnesnis nepagrįstas asmens kodo panaudojimas kuris sukuria galimybes prieiti prie daugelio asmens duomenų ir taip pažeisti jų privatų gyvenimą. Išryškėja visuomenės noras naudotis technologinės revoliucijos atneštomis galimybėmis, kurios kartu kelia ir daug neaptartų problemų, kurias visuomenė turėtų neatidėliodama spręsti, o viena didžiausių problemų – žmogaus teisių apsauga ir nepakankamai apsaugoti asmens duomenys kelia grėsmę asmens privatumui. Pastebima, kad nėra pakankamai atliktų mokslinių tyrimų šioje srityje, todėl ši problema yra aktuali ir nagrinėtina.

**Magistro baigiamojo projekto objektas:** Asmens duomenų apsaugos sistema ir su ja susiję probleminiai reiškiniai

**Tikslas:** Išanalizuoti Lietuvos asmens duomenų apsaugos sistemą ir palyginti su Norvegijos sistema

**Uždaviniai:**

1. Identifikuoti asmens duomenų apsaugos sistemos elementus.
2. Išnagrinėti asmens duomenų apsaugos reguliavimo sistemą Lietuvoje ir Europos Sąjungoje.

3. Išanalizuoti Lietuvoje funkcionuojančią asmens duomenų apsaugos sistemą ir palyginti su Norvegija
4. Suformuluoti išvadas.

**Projekte taikyti tyrimo metodai.** Siekiant visapusiškai atskleisti ir išanalizuoti nagrinėjamą temą projekte buvo taikomi įvairūs tyrimo metodai. Įgyvendinant iškeltus uždavinius yra taikoma literatūros šaltinių ir teisės norminių aktų analizė, lyginamosios analizės metodai. Literatūros ir teisės norminių aktų analizės metodas naudojamas siekiant išanalizuoti ir nuosekliai ištirti esamą asmens duomenų apsaugos sistemą nacionaliniu ir Europos Sąjungos lygmeniu, pateikiant praktinį taikymą, jos efektyvumą bei problematiškumą asmens duomenų apsaugos kontekste. Lyginamosios analizės metodu buvo pažvelgta į tam tikrus Lietuvos ir Norvegijos teisinio reguliavimo ir asmens duomenų apsaugos politikos įgyvendinimo aspektus. Pasitelkus įvairius visuomenės, valstybės institucijų, verslo atstovų požiūrio tyrimus identifikuotos esamos problemos asmens duomenų apsaugos sistemoje.

**Projekto struktūra.** Pirmame projekto skyriuje buvo identifikuojami pagrindiniai asmens duomenų sistemos elementai. Aptariami duomenų tvarkymo principai, dalyviai. Antrame skyriuje pateikiama susisteminta Europos Sąjungos teisės aktų, atsakingų institucijų jų atliekamų funkcijų ir reguliavimo priemonių įgyvendinimo analizė, asmens duomenų apsaugos srityje. Trečiame skyriuje analizuojama asmens duomenų sistema Lietuvoje, išskiriant pagrindines atsakingas institucijas. Siekiant identifikuoti esamas problemas sistemoje, analizuojami tyrimai atlikti tiriant visuomenės, valstybės institucijų ir verslo atstovų požiūrį į asmens duomenų apsaugą. Taip pat lyginama Lietuvos ir Norvegijos asmens duomenų sistemą reglamentuojantys teisės aktai, tyrimai siekiant išsiaiškinti skirtumus įsisavinant Europos Sąjungos nurodomas reguliavimo priemones ir patiriamas, esamas problemas.

Projektą sudaro 64 puslapiai, 4 lentelės, 6 paveikslai, 3 priedai. Panaudota 45 mokslinės literatūros šaltinių ir 16 teisės aktų ir duomenų šaltinių.

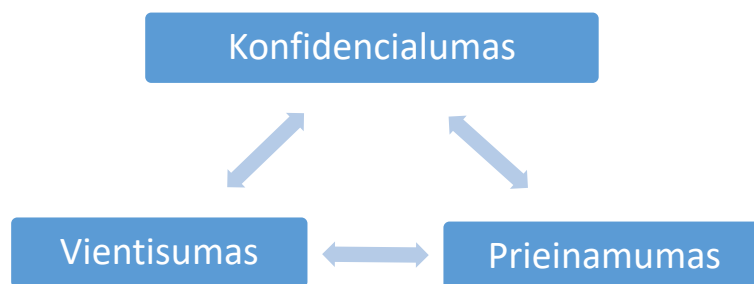
# 1. ASMENS DUOMENŲ KONCEPCIJOS ANALIZĖ

*Šiame skyriuje bus aptariama asmens duomenų sąvoka bei jos sąsajos su privatumu. Analizuojama žmogaus teisė į privatumą, ieškant sąsajų su asmens duomenų apsauga. Taip pat analizuojami bei nurodomi pagrindiniai asmens duomenų apsaugos principai bei reikalavimai duomenų valdytojams, dirbantiems ar susijusiems su asmens duomenimis*

## 1.1. Asmens duomenų samprata ir jos raida.

Asmens duomenų apsaugos terminas turi pakankamai daug įvairių aiškinimų. Paprastai kalbant asmens duomenys – tai informacija apie tam tikrą asmenį. Asmens duomenų termino aiškinimo galima rasti tiek nacionaliniu, tiek tarptautiniu mastu. Tačiau vienas pagrindinių dokumentų, kuriame buvo imta kalbėti apie asmens privatumo laisvę buvo – *Europos žmogaus teisių ir pagrindinių laisvių konvencija* (1948), kurios 8 straipsnio pirmoje dalyje yra nurodoma, kad: „Kiekvienas turi teisę į tai, kad būtų gerbiamas jo asmeninis ir jo šeimos gyvenimas, buto neliečiamybė ir susirašinėjimo slaptumas”. Taigi, žmogaus asmeninio ir privataus gyvenimo detalės gali identifikuoti tam tikrą asmenį, galima atpažinti konkretaus asmens savybes. *Europos žmogaus teisių ir pagrindinių laisvių konvencija ir Europos Sąjungos duomenų direktyva* – pagrindiniai tarptautinių taisyklių rinkiniai, kuriais yra grindžiami Lietuvos nacionaliniai privatumo teisės aktai. *Asmens duomenų teisinės apsaugos įstatymas* (1996), –tai pagrindinis teisės aktas koordinuojantis asmens duomenų apsaugą, – Jo tikslas – ginti žmogaus privataus gyvenimo neliečiamumo teisę tvarkant asmens duomenis. Galima pabrėžti, kad ir kitos Europos šalys turi panašias įstatyminius aktus, pvz., Norvegijos karalystės asmens duomenų įstatymas (2000) taip pat turi panašų tikslą kaip ir Lietuvos asmens duomenų apsaugos įstatymas. Šios šalies asmens duomenų įstatymo (2000) pirmajame straipsnyje taip pat yra pabrėžiama, kad šis įstatymas padeda užtikrinti, kad asmens duomenys būtų tvarkomi laikantis pagrindinių politikos interesų, įskaitant būtinybę saugoti asmens vientisumą, konfidencialumą ir tinkamą asmens duomenų kokybės užtikrinimą. Taigi, galima teigti, kad Norvegijos šalies atveju įstatymų tikslai yra identiški, tačiau šios šalies turimo įstatymo tikslu taip pat nurodomas siekis išsaugoti asmens vientisumą ir konfidencialumą.

Parker (1981) išskyrė tris pagrindinius informacinius tikslus, kurie žinomi kaip triada CIA (angl. Confidentiality, Integrity, Availability) ir reiškia konfidencialumą, vientisumą ir prieinamumą. (žr. 1 pav.)



**1 pav. Pagrindiniai informaciniai tikslai (sudaryta autorės)**

Taigi, šios trys kategorijos yra skirtos užtikrinti infrastruktūrą ir saugius informacinius išteklius. Kalbant apie konfidencialumą galima paminėti, kad tai tam tikrų duomenų ar informacijos įslaptinimas, – taikant tam tikrus prieigos kontrolės metodus, – bei šių išteklių slėpimas.

Asmens vientisumą galima apibūdinti kaip asmens ir jo duomenų patikimumą, autentiškumą siekiant apsaugoti nuo klaidingo ar neleistino jų pakeitimo. Vientisumas yra ypač svarbi savybė saugumo ir finansiniams duomenims. Tačiau, – tai ne vienintelė vientisumo kategorija. Bygravis ir Schartumas (2004, p.24) išskiria geografinio vientisumo, kūno neliečiamybę, psichologinę neliečiamybę, komunikacijos ir informacijos vientisumą. Šios kategorijos apibūdina įvairius moralinius reikalavimus, pavyzdžiui, – geografinis vientisumas apima pagarbą asmens privatumui ne tik fiziniam, bet ir teritoriniam. Asmuo, būdamas savo namuose, gali laisvai elgtis ir gali būti apsaugotas nuo kitų neteisėto poveikio.

Šios naujos kategorijos svarba yra apibrėžiama ir Norvegijos Konstitucijos (1814) 102 straipsnio pataisoje (2014), kuris teigia *"Kiekvienas žmogus turi teisę, kad būtų gerbiamas jo privatus ir šeimos gyvenimas, būsto neliečiamybė ir jo ryšiai. Kratos neturi vykti, išskyrus baudžiamąsias bylas. Vyriausybės institucijos turi užtikrinti asmens vientisumo apsaugą."*

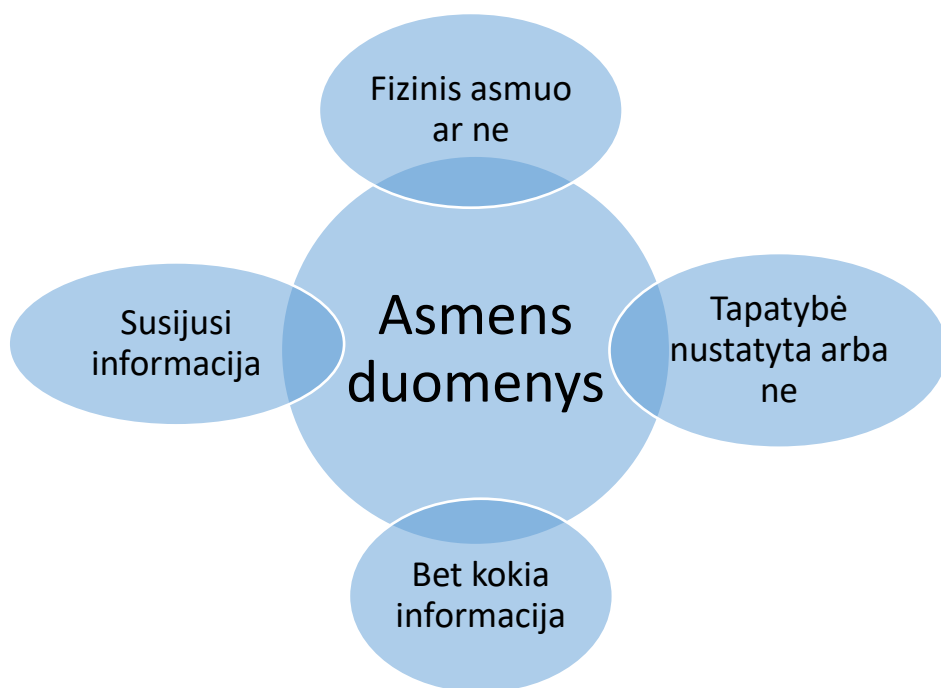
Prieinamumas, kaip trečiasis informacijos tikslas, suteikiama galimybę naudotis informacija ar ištekliumi, tačiau ši informacija yra prieinama ne visiems vartotojams.

Minint, informacinius tikslus, – svarbu apibrėžti būtent **asmens duomenų sąvoką**. Šios sąvokos apibrėžimų galima rasti ne viename Europos Sąjungos teisiniame dokumente, taip pat nacionaliniuose teisės aktuose. Europos Sąjungos teisiniuose dokumentuose galima rasti pirmuosius „asmens duomenų“ sąvokos apibūdinimus. 1995 m. *Europos Parlamento ir Tarybos Direktyvoje ( 95/46/EB) „Dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo”*( toliau direktyvoje (1995)) – asmens duomenys suprantami kaip bet kuri informacija, susijusi su asmeniu (duomenų subjektu);

- kurio tapatybė yra nustatyta arba gali būti nustatyta; asmuo,
- kurio tapatybė gali būti nustatyta tiesiogiai ar netiesiogiai, ypač pasinaudojus nurodytu asmens identifikavimo kodu arba vienu ar keliais to asmens fizinei, fiziologinei, protinei, ekonominei, kultūrinei ar socialinei tapatybei būdingais veiksniais.

Reikia paminėti, kad nacionaliniu lygmeniu nagrinėjant šios sąvokos pavartojimo būdus pastebima, kad Lietuvai priėmus šią direktyvą, buvo tobulinamas ir asmens duomenų teisinės apsaugos įstatymas (1996) prieš tai atsižvelgiant į šios direktyvos rekomendacijas. O asmens duomenų sąvoka liko nepakitusi ir jos apibrėžimas buvo tiesiogiai panaudotas kuriant nacionalinius įstatyminius aktus. *Lietuvos Respublikos Asmens duomenų teisinės apsaugos įstatymas (2002)* (toliau asmens duomenų teisinės apsaugos įstatymas) identifikuoja konkretų asmens duomenų terminą, kuriuo ne tik apibrėžiama žmogaus teisė į privatumą, bet taip pat yra apibrėžiami požymiai kaip gali būti asmuo nustatomas.

Žvegiant į kitų šalių praktiką galima rasti ir daugiau šios sąvokos skirstymų. Pavyzdžiui, pateikiamoje Norvegijos oficialioje ataskaitoje (2009, p.46) asmens duomenų sąvoka yra pateikiama iš keturių elementų (žr. pav.2):



**2.pav. Asmens duomenų sąvokos elementai (sudaryta autorės)**

Šie elementai yra glaudžiai susiję vienas su kitu. Vienas iš jų negali atitikti asmens duomenų sąvokos, visi jie turi sudaryti šio termino visumą. Galima daryti prielaidą, kad duomenų samprata yra ganėtinai plati ir turi teigiamą praktinę reikšmę.

Asmens tapatybė gali būti identifikuota tiesioginiu arba netiesioginiu būdu, vadinasi atsiranda galimybė nustatyti asmenį ne tik turint tiesioginius duomenis (tokius kaip pavyzdžiui asmens kodas ar vardas bei pavardė), bet ir valdant kitokią informaciją, kurios turinys netiesiogiai gali nurodyti asmenį. Platesnis požiūris į asmens duomenis, įtraukiant netiesioginio asmens nustatymo galimybę užtikrina geresnę asmens teisę į privatumą, – tvarkant asmens duomenis. Identifikavimo reikalavimai, kad informacija būtų laikoma asmens duomenimis pagal įstatymus turi būti susijusi su konkrečiu asmenimi. Apskritai galima teigti, kad asmuo identifikuojamas, kai yra atskiriamas nuo didesnės ar mažesnės grupės kitų asmenų. Kaip yra teigiama oficialioje Norvegijos ataskaitoje (2009, p.48) asmuo gali būti identifikuojamas pagal išorės požymius: išvaizdą, ūgį, svorį, plaukų ar drabužių spalvą. Asmenį tiesiogiai galima nustatyti ir pagal jo užimamas pareigas, profesiją, vardą ar pavardę. Reikia paminėti, kad vien pavardės žinojimas nepadedą identifikuoti tam tikro asmens, nes tam tikroje žmonių grupėje – pavardė nesuteikia pakankamai informacijos. Tačiau netiesioginės informacijos, tokios kaip telefono numerio žinojimas ar kitas susijęs duomenų rinkinys, gali padėti rasti daugiau susijusios informacijos.

Norvegijoje žinant telefono numerį galima rasti ne tik asmens adresą, bet ir vardą, pavardę, – taip pat asmens, registracijos vietą pagal savininko telefono numerio registraciją. Kitas netiesioginis asmens nustatymo pavyzdys: kreipimasis į tam tikrą asmenį nurodant pareigų laipsnį „vyresnysis policijos pareigūnas” suteikia netiesioginės informacijos, kuria pasinaudojant galima tiksliai identifikuoti asmenį.

*Apibendrinant galima teigti, kad asmens duomenys tai – tam tikra informacija apie konkretų asmenį, kuri gali būti tiesiogiai ar netiesiogiai nustatyta iš tam tikrų asmens požymių bei savybių. Asmens duomenų sąvoka vertinant tarptautiniu ir nacionaliniu lygmeniu turi tą pačią teisinę reikšmę, nes nacionaliniai įstatymai reglamentuoja Europos Sąjungos galiojančias direktyvas bei kitus teisinius aktus.*

## **1.2. Teisės į privatumą samprata ir ryšys su asmens duomenų apsauga**

Asmens duomenų apsauga ir nuo jos neatsiejama privatumo sąvoka jau buvo žinomos nuo XIX amžiaus pabaigos Jungtinėse Amerikos Valstijose. Ypatingą dėmesį privatumo teisei skyrė Warrenas ir Brandeisas (1890) parašydami straipsnį „The right to privacy”. Šio straipsnio pasirodymas padarė didelę įtaką Jungtinių Amerikos Valstijų teisiniai doktrinai. Autorių iškelta teisė į privatumą buvo įvardijama kaip socialinė vertybė, o privatumas buvo suprantamas kaip teisė būti palinktam ramybėje. Intensyvus perėjimas iš industrinės visuomenės į informacinę stipriai paveikė socialinių santykių vystymąsi, technologijų revoliucija palietė ir žmogaus asmeninį gyvenimą, jam suteikdama galimybę realizuotis socialinės egzistencijos ir užimtumo procesuose.

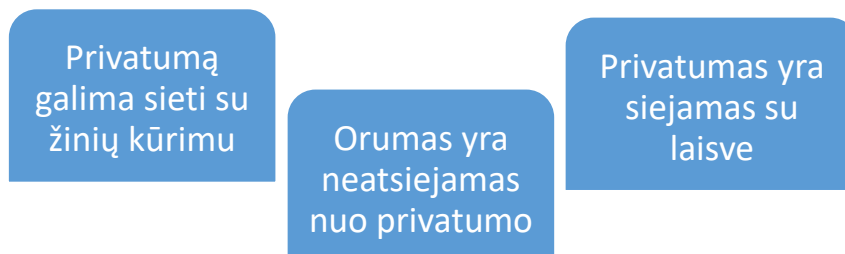
To rezultatas, asmens duomenys tapo svarbūs, o jų saugumas tapo itin aktualia tema. Valstybės tiek nacionaliniu, tiek tarptautiniu mastu ėmėsi teisiškai reguliuoti bei garantuoti pagrindines žmogaus teises ir laisves, taip pat ir privatumo teisę. Asmens privatumo teisė yra ginama daugelyje tarptautinių teisinių dokumentų. Pasak Meškauskaitės (2004, p. 215) socialinės, ekonominės ir politinės teisės buvo įtvirtintos anksčiau nei privatumo teisė. Tačiau ypatingas dėmesys imtas skirti šios teisės įtvirtinimui siekiant teisiškai sudaryti vienodas sąlygas visiems žmonėms. *Visuotinėje žmogaus teisių deklaracijoje* (1948) buvo siekiama įtvirtinti žmonių žodžio bei įsitikinimų laisvę bei išlaisvinti paprastus žmones iš baimės ir skurdo.



Tad privatumas bei asmens duomenų sauga buvo vienos pagrindinių teisių: „*niekas neturi patirti savavališko kišimosi į jo privatumą, šeimos gyvenimą, buitį ar susirašinėjimą arba kėsintis į garbę ir reputaciją*”. Galima išvelgti, – šios deklaracijos panašumų su *Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos* (1995) 8 straipsniu, kuris taip pat įtvirtina privatumo teisę. Nacionaliniu mastu, žmogaus privatumas yra ginamas *Lietuvos Konstitucijos*. Informacija apie privatų asmens gyvenimą gali būti renkama tik motyvuotu teismo sprendimu ir tik remiantis įstatymu, kad niekas nepatirtų savavališko ar neteisėto kišimosi į asmeninį ir šeimos gyvenimą, garbę ir orumą (Lietuvos Respublikos Konstitucija 1992, 22 str.). Reikia paminėti, kad tai – ne vienintelis teisinis šaltinis ginantis žmogaus privatumo teisę. *Lietuvos Respublikos Civilinis Kodeksas* (2000) saugo ne tik privatumo teisę, bet ir kitas asmenines neturtines teises ir vertybes. Kalbant apie asmens duomenų apsaugą galima išskirti „*Asmens duomenų teisinės apsaugos įstatymą*” (1996), kurio vienas pagrindinių tikslų yra: „*ginti žmogaus privataus gyvenimo neliečiamumo teisę ryšium su asmens duomenų tvarkymu*”. Šis įstatymas reglamentuoja santykius, atsirandančius tvarkant asmeninius duomenis. Galima daryti prielaidą, kad asmenys dirbantys su asmens duomenimis, laikydamiesi šio įstatymo turi užtikrinti asmens privatumą; – asmens duomenys negali būti apdorojami nesilaikant įstatymo. Taigi, privatumas kaip sąvoka yra neatsiejama nuo asmens duomenų apsaugos. Pasak Soloves (2002, p. 1101–1102) teisė būti palikti ramybėje yra privatumo forma, kuria sukuriamas imunitetas ar atskirimas nuo visuomenės, autoriaus nuomone, šis apibrėžimas yra per platus. To rezultatas, kad šis apibrėžimas yra nepakankamai identifikuojantis, kad būtų galima lyginti su kitais interesais kaip saviraiškos laisvės ar efektyvaus valdymo. Analizuojant kitų autorių darbus galima pasakyti, kad dauguma jų išskiria privatumą kaip ribotą teisę į savarankiškumą. Yra pabrėžiamas asmens poreikis slėpti tam tikrą informaciją. Kaip teigia, filosofas Sissela Bokas (1983, p. 10-11, cit. Norvegijos oficiali ataskaita, 2009, p.37) „*privatumas – tai asmens galimybė būti apsaugotam nuo nepageidaujamo kitų asmenų dėmesio*”. Privatumo apsauga yra svarbi ne tik kiekvienam asmeniui ir žmonių gerovei, bet ir naudinga visuomenei. Terminas privatus yra kilęs iš lotyniško žodžio „privo”, kuris reiškia kažką atimti ir būti laisvam arba būti atskirtam nuo kažko. Būdvardis „privatus” būdinga individui nepriklausančiam nuo valstybės. Eglehardtas (2000, p.121, cit. Norvegijos oficiali ataskaita, 2009, p. 37) teigia, kad būti privačiu asmeniu, reiškia nepriklausyti politikai ir nebūti visuomenės gyvenimo dalimi. Galima rasti daugybę

privatumo sąvokos aiškinimų, bet galima daryti prielaidą, kad privatumas apima daugybę sričių ir jo aiškinimas kinta nagrinėjant skirtingus objektus.

Anot Posto (2001, p.2087) galima išskirti tris skirtingas šios sąvokos koncepcijas, tai (žr. pav.3):



### 3pav. Privatumo sąvokos koncepcijos

*Apibendrinant galima teigti, kad privatumas nėra vien tik susijęs su informacijos slėpimu. Privatus gyvenimas apima tiek fizinį, tiek psichologinį asmens identitetą. Akivaizdu, kad teisė į asmens duomenis yra laikoma viena iš įstatymo ginamų privataus gyvenimo vertybių, todėl negalima vertinti kaip dviejų atskirų tarpusavyje nesusietų, ar nutolusių viena nuo kitos, teisių. To rezultatas, kad asmens duomenų apsauga ir teisė į privatumą yra neatsiejama ir dažniausiai nagrinėjama kartu.*

### 1.3. Asmens duomenų apsaugos principai

Kiekviena valstybė priklausanti Europos Sąjungai turi laikytis ne tik savo šalies įstatymų, bet ir paklusti įvairiems Europos Sąjungos nustatytiems įstatymams, Direktyvoms, turi vadovautis Europos šalims skirtomis rekomendacijomis. Asmenų apsaugos sritis yra viena iš nišų, kuri yra itin svarbi ne nacionaliniu, bet ir valstybiu – Europos Sąjungos mastu. Šiais informacinių technologijų laikais privati asmens duomenų informacija tampa preke, kuri itin aktuali ne tik informacijos savininkams, bet ir asmenims norintiems užsiimti neteisėta veikla, todėl duomenų saugumas yra itin svarbus. Europos Sąjungos šalys įsipareigoja tvarkyti asmens duomenis teisingai ir teisėtai, laikantis reglamentuojančių įstatymų.

Remiantis Direktyvos (1995) 6 straipsniu galima išskirti pagrindinius reikalavimus, asmens duomenų tvarkymui. *Asmens duomenų teisinės apsaugos įstatyme* (1996) yra nurodomi „bendrieji duomenų tvarkymo principai” arba kaip nurodoma Direktyvoje „*duomenų kokybės principai*”. To rezultatas, visi asmens duomenų valdytojai turi laikytis šių principų dirbdami su asmens duomenimis.

Reikalinga juos rinkti ir toliau tvarkyti. Šio principas turi panašumų su trečiuoju principu, kuriame nurodoma, kad duomenys turi būti atnaujinti – kitaip tariant – tinkami. To rezultatas – visi principai glaudžiai susiję su numatytu tikslu, o duomenų tvarkymas – privalo atitikti visus šiuos principus. Duomenų apimtis negali kisti, tad duomenų valdytojo veiklos sritis, tvarkant duomenis, negali plėstis ir pažeisti įstatymuose nustatytus reikalavimus. *Asmens duomenų teisinės apsaugos įstatymo* (1996) 5 straipsnyje nurodoma, kad jau surinkti asmens duomenys, kurie nėra tapatūs ir tinkami atsižvelgiant į tikslus, turi būti ištrinami.

*Penktuoju principu* yra nurodoma duomenų saugojimo forma, kuria remiantis asmens duomenys turėtų būti tvarkomi. Duomenų valdytojo pareiga užtikrinti principų įgyvendinimą. Šiuo principu duomenų valdytojas įsipareigoja naudotis asmens duomenimis tam tikrą laikotarpį, susietą su tikslu, kol duomenys yra naudojami. Tačiau, kai duomenys yra nebereikalingi identifikuotiems tikslams, duomenų valdytojas turi pasirūpinti, kad duomenys būtų ištrinti arba anonimizuojami. Tokiu būdu, duomenų valdytojas gali disponuoti asmens duomenimis. Asmens duomenų teisinės apsaugos įstatymo paskirtyje nurodoma, kad asmuo turi būti identifikuojamas, bet jei jo duomenys anoniminiai, informacija nėra pasiekama kiekvienam vartotojui ir asmuo nėra duomenų valdytojas, turintis tam reikalingą tikslą.

*Apibendrinant galima paminėti, kad asmens duomenų tvarkymo tvarka yra nurodoma teisiniuose dokumentuose. Asmens duomenis tvarkantis asmuo yra vadinamas duomenų valdytoju. Duomenų valdytojo pareiga laikytis įstatymuose apibrėžtų penkių principų, siekiant tinkamo duomenų apdorojimo. Bet kokios asmens informacijos apdorojimas, visų pirma, turi turėti nustatytą tikslą, kodėl ši informacija yra renkama, siekiant išvengti netinkamo jos apdorojimo. Duomenų valdytojas įsipareigoja, kad duomenys bus tikslūs, sąžiningi ir teisėti, esant būtinybei atnaujinti ir tik tokios apimties kiek reikalinga siekiant užsibrėžto tikslo. Nebenaudojami duomenys turi būti ištrinti ar anonimizuoti, siekiant tinkamos duomenų apsaugos.*

#### **1.4. Duomenų valdytojo ir duomenų subjekto samprata**

Nors ir netiesiogiai, tačiau galima įvardinti asmens duomenų valdytoją kaip instituciją atsakingą už asmens duomenų apsaugą. Hierarchiškai žvelgiant, ši

institucija yra pavaldi asmens duomenų inspekcijai ir turi laikytis keliamų reikalavimų, siekiant išsaugoti duomenų saugumą.

Galima įvardinti daugybę institucijų atsakingų už duomenų apsaugą, tačiau visos šios institucijos įgyja duomenų valdytojo statusą, kai ima tvarkyti asmens ne asmeniniais tikslais. **Duomenų valdytojas**- tai juridinis ar fizinis asmuo, kuris vienas arba drauge su kitais nustato asmens duomenų tvarkymo tikslus ir priemones (Asmens duomenų teisinės apsaugos įstatymo pakeitimo įstatymas, 2008). Duomenų valdytojas įsipareigoja, kad asmens duomenys bus renkami užsibrėžtais ir teisėtais tikslais, duomenys turi būti nuolat tvarkomi, taisomi jei reikia sunaikinami. Pagrindinis Direktyvos (1995) 21 straipsnio 1 dalies tikslas yra užtikrinti duomenų subjektų ar bet kokių kitų asmenų asmens duomenų tvarkymo skaidrumą, taip pat sustiprinti visuomenės galimybę imtis veiksmų prieš svarbių asmens duomenų tvarkymą, kurie taip pat vaidinama prevencinį vaidmenį, nes registras yra savotiška skelbimų lenta. Reikia paminėti, kad ne kiekvienas asmuo gali tapti duomenų valdytoju. Kaip teigiama Europos duomenų vadove (2014, p.48) pagal Europos Sąjungos teisę privatiems asmenims, kurie kitų asmenų duomenis tvarko tik asmeninems ar šeimos reikmėms, duomenų apsaugos Direktyvos taisyklės netaikomos. Visgi, galima teigti, kad yra galimas duomenų nuasmenimas, kai duomenų valdytojas gali būti neįpareigotas laikytis nustatytų įstatymų. Tačiau tokiu atveju, asmens duomenys tampa neidentifikuoti su tam tikru asmeniu. Kaip yra teigiama nuasmenimo rekomendacijoje (2015, p. 1) duomenų valdytojams nuasmeninimas – gali būti vertingas kaip strategija, ypač atvirųjų duomenų panaudojimo reikmėms, kartu mažinant susijusiems asmenims gresiančius pavojus. Tačiau, pagrindinė duomenų valdytojo ar tvarkytojo statuso pasekmė yra susijusi su teisine atsakomybe laikytis atitinkamų duomenų apsaugos teisėje nustatytų pareigų. Galima daryti prielaidą, kad šį statusą gali įgyti tik tie subjektai, kuriuos pagal taikytiną teisę galima laikyti atsakingais.

Tačiau, taisyklėse nėra aiškiai nurodoma, ar bendro duomenų valdymo atveju būtina, kad bendras tikslas atitiktų kiekvieno duomenų valdytojo tikslą, ar tiesiog užtenka, kad jų tikslai sutaptų iš dalies. Kaip teigiama Europos duomenų vadove (2014, p.50) – svarbu tinkamai ir lanksčiai išaiškinti bendrą duomenų valdymo sąvoką, siekiant spręsti sudėtingus duomenų tvarkymo klausimus. Kaip pavyzdį projekto autorė pateikia bylą, kurioje dalyvavo Pasaulinė tarpbankinių finansinių telekomunikacijų organizacija (SWIFT) (Bylos pavyzdys- prieduose). Šioje byloje paaikškėjo, kad SWIFT neteisėtai prisiėmė duomenų valdytojo vaidmenį, to

rezultatas, buvo netinkamai atskleisti duomenys ir bankai turėjo prisiimti atsakomybę, nes neprižiūrėjo duomenų tvarkytojų.

Žinoma, kyla klausimas: kas gi yra duomenų tvarkytojas ir kuo jis skiriasi nuo duomenų valdytojo? Duomenų apsaugos Direktyvos (1995) 2 straipsnyje pateikiama, kad **duomenų tvarkytojas**- tai asmuo, kuris asmens duomenis tvarko duomenų valdytojo vardu. Duomenų tvarkytojai –vykdo tam tikrą veiklą, kuri yra susijusi su konkrečia užduotimi ar tam tikromis sąlygomis ir yra gana bendro ir plataus pobūdžio. Svarbu paminėti, kad ši veikla gali įgyti kitą tikslą jei duomenų valdytojas ketina atlikti savus tikslus nesusijusius su duomenų valdytojo tikslais. Tokiais atvejais, duomenų tvarkytojai įgyja savarankiškų duomenų valdytojo statusą. Tačiau, reikia nepamiršti, kad sudarant sutartį su duomenų tvarkytoju , duomenų valdytojas vis tik turi teisę daryti įtaką duomenų tvarkytojo sprendimams dėl tvarkymo būdų. Kaip teigiama, Europos duomenų vadove (2014, p.52) – duomenų valdytojas yra atsakingas už duomenų tvarkytojo veiksmus, jis turi prižiūrėti, kad duomenų tvarkytojo veiklą ir užtikrinti, kad jų sprendimai atitiktų duomenų apsaugos teisę. Taigi, siekiant aiškumo ir skaidrumo, duomenų valdytojo ir duomenų tvarkytojo ryšys turi būti išsamiai nustatytas rašytinėje sutartyje.

**Duomenų gavėjai ir trečiosios šalys.** Asmenys, kurie nėra duomenų valdytojais ar duomenų subjektais yra vadinami – trečiaja šalimi. Taip pat kaip ir duomenų valdytojas yra susaistytas teisiniais ryšiais su duomenų tvarkytoju. Asmens duomenų atskleidimas tretiesiems asmenims – turi turėti teisinį pagrindą. Direktyvos (1995) 29 straipsniui, sudaryta nepriklausoma darbo grupė, nustatė „*asmenys, dirbantys kitai organizacijai, net jei ji priklauso tai pačiai grupei arba kontroliuojančiajai bendrovei, paprastai yra trečiosios šalys*” (2010, p. 30). Duomenų apsaugos kontekste, šią sąvoką reikėtų aiškinti kaip bet kurį subjektą, kuris neturi jokios konkrečios teisės ar leidimo tvarkyti asmens duomenis, pagrįsto, pavyzdžiui, jo vaidmeniu (duomenų valdytojas, duomenų tvarkytojas ar kurio nors iš jų darbuotojas).

Svarbu pabrėžti, kad ši trečios šalies apibūdinimas yra naudojimas siekiant nustatyti draudimus, apribojimus ir įsipareigojimus tais atvejais, kai asmens duomenis gali tvarkyti trečiosios šalys, iš esmės neturinčios teisės tvarkyti tam tikrų asmens duomenų.

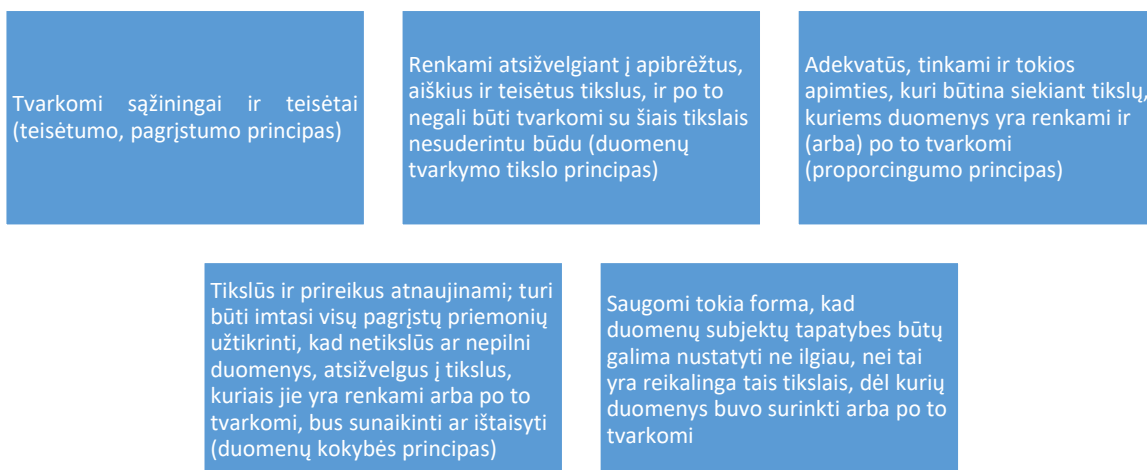
*Apibendrinant galima teigti, kad duomenų valdytojas yra paskiriamas nustatčius duomenų tvarkymo tikslą. Duomenų valdytojas gali pavesti nustatyti duomenų tvarkymo būdus, tačiau esminius klausimus nuo kurių priklauso duomenų*

*tvarkymo teisėtumas sprendžia duomenų valdytojas. Tuo tarpu, duomenų tvarkytojas yra tiesiogiai pavaldus duomenų valdytojui.*

*Jis turi tenkinti dvi pagrindines sąlygas: viena, jis turi būti nuo duomenų valdytojo atskiras juridinis asmuo, antra, jis turi tvarkyti asmens duomenis duomenų valdytojo vardu. Trečioji šalis apibrėžiama kaip bet kuris subjektas, kuris neturi jokios konkrečios teisės ar leidimo tvarkyti asmens duomenis, pagrįsto, pavyzdžiui, jo vaidmeniu (duomenų valdytojas, duomenų tvarkytojas ar kurio nors iš jų darbuotojas). Asmens duomenis teisėtai ar neteisėtai gavusi trečioji šalis iš esmės būtų naujas duomenų valdytojas, jei ši šalis tenkina kitas duomenų valdytojo sąlygas ir duomenų apsaugos teisės aktų taikymo sąlygas.*

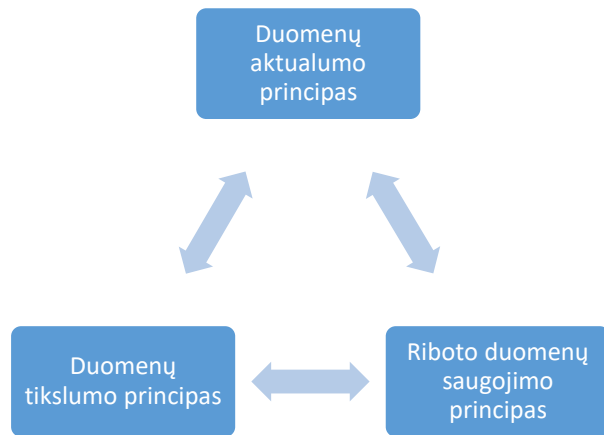
### **1.5. Bendrieji duomenų tvarkymo principai**

Asmens duomenys gali būti tvarkoma automatiniu arba neautomatiniu būdu. Tačiau, šie būdai neturi didelės reikšmės. Duomenų tvarkymas yra viena pagrindinių sąvokų naudojamų įvairiuose įstatymuose bei direktyvose. Žinoma, viena svarbiausių taisyklių reglamentuojančių tvarkymo teisėtumą, yra tvarkymas automatiniu būdu. Kaip teigiama, Asmens duomenų teisinės apsaugos įstatymo komentare (2005) duomenų tvarkymo automatiniu būdu apibrėžimas apima duomenų tvarkymo veiksmus, visiškai ar iš dalies atliekamus automatinėmis priemonėmis. Asmens duomenys gali būti nustatyti tiesioginiu ar netiesioginiu būdu, pasinaudojant tokiais duomenimis kaip asmens kodas, vienu ar keliais tam tikram asmeniui būdingais požymiais. Reikia pabrėžti, kad asmens duomenys turi atitikti tam tikrus reikalavimus. Kaip nurodoma Europos Parlamento ir Tarybos reglamento (2001) ketvirtajame straipsnyje asmens duomenys turi būti (žr. 4 pav.):



**4 pav. Reikalavimai asmens duomenims (sudaryta autorės)**

Analizuojant įvairius straipsnius galima rasti ir kitokius reikalavimus susijusius su asmens duomenimis. Asmens duomenims gali būti taikomi – duomenų kokybės principai. Šių principų turi laikytis duomenų valdytojai norėdami tvarkyti su asmens duomenimis susijusias operacijas. Nurodomas riboto duomenų saugojimo principas, kai duomenys turi būti iškart ištrinami, kai jų nebereikia tikslams dėl kurių jie buvo surinkti. Europos asmens duomenų apsaugos teisės vadove (2014, p.70) nurodoma, kad asmens duomenų kokybės principai yra (žr. pav.5):



5.pav. Asmens duomenų kokybės principai (sudaryta autorės)

*Aktualumo ir proporcingumo principo panašumai.* Žvelgiant į šiuos principus galima pastebėti sąsajas su anksčiau išleistais Europos Parlamento ir Tarybos reglamento reikalavimais. Pastebimas šių reikalavimų ir principų panašumas. Pateikiamas aktualumo principas yra vienodo pobūdžio kaip ir proporcingumo principas. Abu šaltiniai byloja, kad asmens duomenys turi būti renkami siekiant bendro operacijų tikslo ir duomenų valdytojas turi užtikrinti, kad būtų renkama tik tokia su duomenimis susijusi informacija, kuri tiesiogiai atitinka konkretų duomenų valdymo tikslą. Visgi, šiuolaikinėje visuomenėje aktualumo principas yra aplinkybė, į kurią reikia papildomai atsižvelgti naudojant specialias didesnę privatumo apsaugą padedančias užtikrinti technologijas. Tačiau, kartais yra įmanoma visiškai išvengti asmens duomenų naudojimo arba naudoti pseudoniminius duomenis, tad tokiais atvejais tai nebūtų privatumą pažeidžianti priemonė. Pasitaiko atvejų, kad duomenų valdytojo ir duomenų subjekto interesai

dažnai susikerta, siekiant išaiškinti ar duomenų rinkimas ir tvarkymas buvo teisėtas ir proporcingas.

Šiuo atžvilgiu, yra svarbu nustatyti ar nebuvo peržengta riba, kuomet pažeidžiamas asmens duomenų konfidencialumas. Kaip pabrėžia Petraitytė (2011, p.159) asmens duomenų tvarkymo tikslai turi atitikti realius duomenų valdytojo poreikius. Taigi, turi būti išlaikomas proporcingumas bei balansas, siekiant išvengti interesų konflikto. Turi būti gerbiama asmens teisė į privatumą, o asmens duomenys neturi būti kaupiami jei jiems nebuvo nustatyto tikslo.

*Duomenų kokybės reikalavimai ir duomenų tikslumo principas.* Galima teigti, kad duomenų tikslumas yra pareiga, kurią turi atlikti duomenų valdytojas, kuri vertinama atsižvelgiant į duomenų tvarkymo tikslą. Reikia paminėti, kad duomenų tikslumas yra svarbus dėl žalos, kurią gali patirti duomenų subjektas dėl netikslių duomenų. Susiję teisiniai reglamentai byloja, kad duomenų valdytojais negali rinkti papildomos informacijos apie asmenį jei tai nėra apibrėžta jo teisiniu pagrindu priimtuose tiksluose. Taigi, nagrinėjant duomenų tvarkymo principus, nusistatyti tikslai užima svarbią vietą duomenų tvarkymo principų sistemoje. Duomenų tvarkymo tikslas – taip glaudžiai susijęs su ir su kitais reikalavimais duomenų saugumui. Žinoma, teisiniu požiūriu būtų galima teigti, kad įvairios valstybinės institucijos neoficialiai pažeidžia šį principą, nes kaupia informaciją apie įvairius asmenis. Ir kaip teigia, Meškauskaitė (2015, p. 163) valstybinių institucijų sukaupta informacija, nors ir atitinka realius faktus pažeidžia žmogaus privatumą, kai šios informacija kaupiama kelius metus ir tampa nebeaktuali. Galima daryti prielaidą, kad ši informacija gali tapti diskriminuojanti, kai sakykim, asmuo prieš kelerius metus buvo teistas, bet šiuo metu yra išnykęs jo teistumas. Tokio tipo problemos ne kartą buvo nagrinėtos ir Europos Strasbūro teisme siekiant, kad asmens požymius atitinkanti informacija būtų užmiršta, jei šiuo metu ji yra nebeaktuali. Taigi, duomenų kokybės principas itin svarbus kalbant apie asmens duomenis. Ypatingai, kai Lietuva būdama Europos Sąjungos šalimi yra priėmusi ne vieną teisinį reglamentą bei direktyvą, kurios turinys yra perkeltas į šalies įstatyminę bazę. O bendradarbiavimas su kitomis valstybėmis bei teisinėmis institucijomis turi būti paremtas perduodamos asmens informacijos tikslumu, siekiant išvengti nesusipratimų bei žmogaus pagrindinių teisių tame tarpe ir asmens privatumo išsaugojimu. Kaip yra teigiama Tarybos pamatinio sprendime (2008) kompetetingos institucijos turi imtis visų priemonių siekian užtikrinti duomenų



tikslumą, išsamumą. Neteisingi ir pasenę duomenys turi būti atnaujinami ar panaikinami tam, kad šie duomenys toliau nebūtų naudojami, nes būtų pažeidžiamas įstatymuose numatytas duomenų kokybės principas.

*Riboto duomenų saugojimo principas.* Šis principas konstatuoja, kad asmens duomenys, kai galima nustatyti duomenų subjekto tapatybę gali būti naudojami nei ilgiau nei, nei tai yra reikalinga nustatytais tikslais, dėl kurių duomenys buvo surinkti ir tvarkomi. Todėl pasiekus šiuos tikslus duomenys turi būti sunaikinti. Asmens duomenys gali tapti įvairių asmenų bei institucijų nusikalstamų veikų objektu, tad svarbu sudaryti tinkamas sąlygas darbui su konfidencialia informacija. Kiekvienas duomenų valdytojas prisiima atsakomybę, kad asmens duomenis tvarkys sąžiningai, nesaugos duomenų ilgiau nei numatytais tikslais ir remsis galiojančiais įstatymais. Kaip teigiama Europos asmens duomenų apsaugos teisės vadove (2014, p. 73) teisėtas nebereikalingų duomenų saugojimas galėtų būti atliekamas tokius duomenis anonimizuojant arba pseudonimizuojant. Anot Točickienės (2003, p. 118) Direktyvoje įtvirtinti pagrindiniai asmens duomenų apsaugos principai atitinka Europos Tarybos Konvencijoje dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu įtvirtintus principus. Žinoma, galima išskirti ir daugiau įvairių principų, kurie yra aktualūs kalbant apie asmens duomenų apsaugą. Projekto metu buvo išskirtas pagrindinis, autorės nuomone, aktualus principų skirstymas. Žvelgiant į įvairius šaltinius galima taip pat paminėti ir keletą kitų principų, kurie yra neatsiejami nuo jau paminėtų. Kaip principai, kuriais duomenų valdytojas įsipareigoja, kad skaidriai, sąžiningai rinkti duomenis apie subjektus bei įgyti visuomenės narių pasitikėjimą. Todėl svarbu, kad duomenų tvarkymo operacijos neturi būti atliekamos slapta ir neturėtų sukelti nenumatytų neigiamų pasekmių. Duomenų subjektas taip pat turi teisę, kad jo prašymu duomenų valdytojas jį informuotų, ar jo duomenys tvarkomi ir, jei taip, kokie duomenys tvarkomi. Ekonominio bendradarbiavimo ir plėtros organizacija (EBPO) 2013 m. priėmė privatumo gaires, kuriose atkreipė dėmesį į tai, kad duomenų valdytojai atlieka svarbų vaidmenį užtikrindami praktinę duomenų apsaugą. Gairėse apibūdinant *atskaitomybės principą* nurodoma, kad „*duomenų valdytojas turėtų būti atsakingas už tai, kad būtų laikomasi priemonių, kuriomis įgyvendinami pirmiau nurodyti (esminiai) principai*”.

*Apibendrinus šiuos duomenų apsaugos principus galima teigti, kad duomenų valdytojas dirbdamas su asmens duomenimis įsipareigoja atsižvelgti į tam*

*tikras nuostatas- principus. O tai atitinka tam tikras aplinkybes pagal kurias leidžiamas asmens duomenų tvarkymas. Duomenų aktualumo, tikslumo ir riboto duomenų saugojimo principas identifikuoja pagrindinius reikalavimus būdingus tinkamai ir saugiai duomenų apsaugai.*

### **1.6. Netinkamas asmens duomenų naudojimas ir grėsmių privatumui šaltiniai**

Nors ne kartą šiame projekte buvo minima asmens duomenų sąvoka, tačiau atlikti įvairūs visuomenės nuomonės tyrimai rodo, kad ne kiekvienas asmuo turi pakankamai žinių, kokios grėsmės tyko, jei asmens konfidenciali informacija patenka nesąžiningiems asmenims ar institucijoms. Splinter research (2014) atlikti visuomenės nuomonės tyrimai atskleidė, kad net 49 procentai apklaustųjų nežino ar nesugeba apibūdinti kas yra asmens tapatybės vagystė. Galima išskirti du pagrindinius šaltinius, kurie gali turėti įtakos įvairiems duomenų panaudojimo nusikaltimams bei kelia didžiausią pavojų asmens privatumui bei duomenų apsaugai.

- Pirmajam šaltiniui galima priskirti- fizinius bei juridinius asmenis, kurie užsiima netiesėtomis veikomis tokiomis, kai neteisėtai disponuoja, pardavinėja ar kitaip naudojami kito asmens duomenimis.
- Kitą šaltinį galėtumėme išskirti kaip gana abstraktų - valstybės ir jos institucijų veiklą naudojant, kaupiant bei kitaip apdorojant asmens duomenimis, vykdamas viešąsias paslaugas bei ginant nacionalinius interesus.

Žinoma galima teigti, kad didžiausia grėsmė visgi yra fiziniai ir juridiniai asmenys bandantys pasinaudoti svetima asmens informacija siekdami sau naudos. Tačiau dažnai privatumas ir konfidencialumas yra vartojami sinoniskai, nors šios dvi sąvokos yra skirtingos. Kaip teigia prof. Allen (cit. Goldman ir Choy, 2006) *privatumą* galima apibrėžti: „*kaip fizinį privatumą, informacinį privatumą, nuosavybės privatumą ir sprendimų priėmimo privatumą*“. Fizinį privatumą galima suprasti kaip erdvinį vientisumą ir kaip jau buvo minėta projekte vienatvę (teisė būti pamirštam). Visgi, asmens duomenų panaudojimo atžvilgiu yra aktualus- **informacinis privatumas**. Informacinį privatumą apima konfidencialumas, slaptumas, duomenų apsauga ir asmeninės informacijos kontrolė. Visos šios sritys yra itin aktualios kalbant apie grėsmes asmens duomenims, nes atskirų fizinių bei juridinių asmenų disponavimas privačia asmens informacija gali sukelti rimtą

pavojų asmens privatumui. Tokios aktualios informacijos kaip – mokėjimo ar kreditinės kortelės ar paso duomenys patekę į sukčių rankas gali asmeniui pridaryti ne tik moralinės, bet ir materialinės žalos.

Pasinaudoję vartotojo duomenimis sukčiai gali išsimti pinigus iš banko sąskaitos, paimti greituosius kreditus, parduoti nekilnojamą turtą ar atlikti kitą neteisėtą veiklą. Pasitelkę technologijų galimybes asmenys gali atlikti įvairius informacijos pardavimus kitose šalyse gyvenantiems asmenims, o grėsmės privatumui kyla ne tik nacionaliniu, bet ir tarptautiniu lygmeniu.

Svarbu pabrėžti, kad šios grėsmės paliečia ne tik privačius asmenis, bet verslo atstovus bei žinoma valstybę. Siekiant išvengti šių grėsmių, yra kuriama valstybinė bei tarptautinė duomenų apsauga siekiant išvengti žalos vis tobulėjančioje technologijų visuomenėje. Valstybė ir jos atsakingos institucijos – tai pagrindiniai objektai disponuojantys konfidencialia asmenų ir visuomenės informacija. Nors atrodytų pakankamai saugu pasitikėti valstybės institucijomis, bet reiktų nepamiršti, kad valstybė - tai tam tikras administracinis aparatas, kuriame dirba visuomenės išrinkti atstovai, kurie gali turėti ir savavališkų tikslų. Bet kokia žmogiška klaida valstybės sistemoje gali sudaryti sąlygas asmens duomenų grėsmei, ypač, kai valstybė turi pakankamai daug įvairių priemonių kaupti informaciją apie kiekvieną asmenį, visuomenę. Valstybei patogiu turėti pakankamai informacijos apie savo piliečius, nes taip gali vykdyti teisingumą jei pilietis nesilaiko tam tikrų taisyklių siekiant nubausti piliečius už šalies įstatymų nesilaikymą.

Tačiau yra svarbu išlaikyti balansą tarp asmens teisių bei pareigų tam, kad būtų užtikrinta asmens duomenų apsauga ir privatumo teisė. O valstybės stebėjimas bei kontrolė nepažeistų asmens teisės į privatumą.

*Apibendrinant galima teigti, kad visuomenei trūksta žinių identifikuojant grėsmes jų privatumo saugumui ir asmens duomenų apsaugai. Dažniausiai grėsmės kyla iš juridinių ar privačių asmenų neteisėto pasinaudojimo tam tikrais duomenimis. Taip pat galima išskirti valstybės ir institucijų veiklą, kurių sistemose kaupiama informacija apie asmenis kartais būna panaudojama ne pagal paskirtį ir nesusijusi su darbo specifiška ir tikslais. Informacinis privatumas- tai sritis, kurioje kyla grėsmės žmogaus privatumui.*

## 2. ASMENS DUOMENŲ APSAUGOS SISTEMA EUROPOS SAJUNGOJE

*Šiame skyriuje aptariami pagrindiniai Europos Sąjungos lygmeniu asmens duomenų apsaugą reglamentuojantys teisės aktai. Analizuojamos už asmens duomenų apsaugą atsakingos institucijos jų veiklos sritys. Taip pat išskiriamos asmens duomenų apsaugos priemonės.*

### 2.1. Pagrindiniai teisės normų aktai reglamentuojantys asmens duomenų apsaugą Europos Sąjungoje

Per pastaruosius dešimtmečius yra priimama vis daugiau teisės aktų dėl privatumo ir asmens duomenų apsaugos. Europos Sąjungos šalys – narės turi vis mažiau laisvės nustatyti nacionalinę asmens duomenų apsaugą, nes privalo laikytis Europos Sąjungos nurodytų rekomendacijų, kurios privalo garantuoti privatumo teisę ne tik šalyje, bet ir Europos Sąjungoje. Tarptautiniai teisės aktai nustato įvairius minimalius reikalavimus, kurių atskiros tautos yra priverstos laikytis tarptautiniuose teisės aktuose nurodytų reikalavimų. Dalis reglamentuojančių dokumentų vienaip ar kitais įtvirtina pagrindines žmogaus teises. Šios sutartys sudaro normatyvinį pagrindą daugumai kitų teisės aktų šioje srityje tiek nacionaliniu, tiek tarptautiniu mastu.

*Visuotinė žmogaus teisių deklaracija* (1948) - tai vienas pirmųjų teisės reglamentų, kuris ėmė ginti žmogaus teises. Jungtinės Tautos priėmė šią deklaraciją kaip tarptautinę teisinę priemonę, siekiant nustatyti teisinę apsaugą ne tik nuo privačių asmenų, bet ypač nuo valstybės. *Deklaracijos* (1948) 12 straipsnis byloja, kad asmuo neturi patirti savališko kišimosi į asmens privatų gyvenimą. Asmenims garantuojama įstatymo nustatyta apsauga. Šios Deklaracijos priėmimas ėmė įtakoti kitų žmogaus teisės priemonių plėtrą Europoje. Galima teigti, kad žmogaus teisių apsauga yra reikalinga, nes žmogaus teisės ir laisvės gali būti pažeistos ir vadinamojoje privačioje srityje. Nors šis teisinis dokumentas buvo labiau

rekomendacinio pobūdžio, tačiau padarė didžiulę įtaką žmogaus teisių vystymuisi bei apsaugai visame pasaulyje. To rezultatas – ši deklaracija tapo pagrindu daugeliui kitų teisės dokumentų, sutarčių rengiant tarptautinius ir nacionalinius teisinius reglamentus.

Remiantis Vidrickaite (2006, p. 6) galima paminėti, kad paskelbus Visuotinės žmogaus teisių deklaraciją, vėliau, 1966 m., buvo priimti Tarptautiniai ekonominių, socialinių ir kultūrinių teisių paktai, Tarptautinis pilietinių ir politinių teisių paktas bei Tarptautinio pilietinių ir politinių teisių pakto 1966 m. ir 1989 m. fakultatyviniai protokolai, kurie sudarė *Tarptautinę žmogaus teisių chartiją*.

Žmogaus teisių chartija yra sudėtinė Europos Konstitucijos dalis. Europos Konstitucija yra taikoma ES institucijoms ir valstybėms narėms, įgyvendinančioms ES teisę. Joje yra ne tik įtvirtintos Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos numatytos pilietinės ir politinės teisės, bet ir papildomos teisės: socialinės ir darbuotojų teisės, aplinkos apsauga, teisė į gerą administravimą ir kt. Po šios Visuotinės žmogaus teisių deklaracijos 1950 metais buvo priimta ***Europos žmogaus teisių ir pagrindinių laisvių konvencija***, kuria buvo siekiama apsaugoti žmogaus teises bei pagrindines laisves. Kaip teigia Kjølås (2010, p. 205) ši konvencija nustato pagrindines žmogaus teises tokias kaip teisė į gyvybę, apsaugą nuo kankinimo, privatumo apsaugą ir žodžio laisvę. Reikia paminėti, kad viešosios valdžios institucijos išimties tvarka gali koreguoti konvencijos įgyvendinimą savo šalies įstatymuose. Svarbu pabrėžti, kad įsikišimas yra galimas, tuo atveju jei yra teisinis pagrindas, procedūros yra būtinos arba kai intervencijos yra reikalingos, įgyvendinant paminėtus atvejus. Konvencijos pagrindu yra pabrėžiama teisinės valstybės svarba bei poreikis išvengti savavališkų intervencijų, įgyvendinant konvencijoje įtvirtintas teises. Ši konvencija skirta palaikyti ir skatinti idealus ir vertybes demokratinėje visuomenėje. *Europos žmogaus teisių konvencijos* (1950) 8 straipsnyje teigiama, kad turi būti pasiekta pusiausvyra tarp individo teisių ir viešojo intereso, pasiektas *proportingumo principas*. Pasak, Kilkelly (2001, p. 31) pagal proporcingumo principą pripažįstama, kad žmogaus teisės nėra absoliučios ir individo teisės turi būti tikrinamos atsižvelgiant į platesnės visuomenės interesus.

Galima teigti, kad šio principo įgyvendinimas turi būti subalansuotas, randama pusiausvyra tarp visuomenės viešojo intereso ir atskirų pagrindinių teisių. Taip pat, konvencijos 12 straipsniu yra apibrėžta privatumo teisė ir nurodomi privatumo suvaržymo pagrindai. Kilkelly (2001) nurodo, kad proporcingumo principas, kuriuo remiantis asmens privatumas, gali būti ribojimas siekiant užtikrinti viešąjį

interesą. Svarbu paminėti, kad Europos žmogaus teisių ir pagrindinių laisvių konvencija nereglementavo asmens duomenų apsaugos.

Pirmieji asmens duomenų apsaugą reglamentuojantys teisės aktai buvo priimti Heneso srityje Vokietijoje (1970 m.), vėliau sekė nacionalinis Švedijos asmens duomenų apsaugos įstatymas (1973 m.), visos Vokietijos mastu įstatymas priimtas 1974, o Prancūzijoje 1978 metais (privatumo ir žmogaus teisių ataskaita, 2006). Tačiau, šie teisiniai aktai buvo tik nacionalinio lygmens. 1980 metais Ekonominio bendradarbiavimo ir plėtros organizacija (EBPO), atsižvelgdama į spartėjantį pasaulio ekonominį ir demokratijos vystymąsi, nustatė pagrindines asmens duomenų apsaugos gaires. Pasitelkiant šias gaires buvo nustatyti ir susisteminti – pagrindiniai asmens duomenų tvarkymo principai. Kaip teigia, Civilka (2001, p. 5) privatumo apsaugos principų rinkinys yra taikomas bet kokiai informacijai susijusiai su identifikuotu ar identifikuotinu asmeniu (duomenų subjektu), privačiam ir viešam sektoriui, visoms kompiuterizuoto asmens duomenų tvarkymo sistemoms ir priemonėms. Svarbu paminėti, kad šios gairės nėra privalomos Europos Sąjungos valstybėms narėms, jos yra labiau rekomendacinio pobūdžio.

Vėliau 1981 metais buvo priimta *Europos Tarybos konvencija dėl asmens duomenų apsaugos*. Ši konvencija yra vienintelė, kuri tiesiogiai susijusi su asmens duomenų apsauga. Europos šalys ratifikavusios šią konvenciją prisiima atsakomybę įtvirtinti šios konvencijos principus savo nacionalinėse teisinėse sistemose. Šios konvencijos tikslas – įtvirtinti minimalius standartus reikalingus dirbant su asmens duomenimis. Kaip teigia, Kjølås (2010, p. 206) įgyvendinant šią konvenciją siekiama sudaryti sąlygas palengvinti asmens duomenų perdavimą kitoms Europos šalims. To rezultatas, užtikrinta galimybė laisvai gauti ir perduoti informaciją ir padėti skatinti tarptautinę prekybą ir ekonominį augimą.

Svarbiausias šių taisyklių rinkinys yra *Europos Sąjungos direktyva (1995) „dėl asmens duomenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo“*. Šioje direktyvoje yra nustatyta reglamentavimo sistema, kurioje griežtai nustatyti asmens duomenų rinkimo ir naudojimo apribojimai. Kiekvienoje valstybėje narėje įsteigiama nepriklausoma nacionalinė institucija, kontroliuojanti visus veiksmus, susijusius su asmens duomenų tvarkymu (Europos Parlamento ir Tarybos Direktyva (95/46/EB)). Šios Direktyvos tikslas – apsaugoti asmens duomenų teises ir laisves, susijusias su asmens duomenų tvarkymu,

nustatant pagrindinius kriterijus, įgyvendinant duomenų tvarkymo teisėtumą ir duomenų kokybės principus.

Direktyvos veikimo sritis turi tam tikrą dinamiškumą, nes yra taikoma Bendrijos šalyse. O tai reiškia, kad direktyva gali būti koreguojama, atsižvelgiant į kylančias problemas bendrijoje, praplečiant sutarties sritis. Tačiau, tai neturėtų būti taikoma visuomenės saugumo, gynybos ir nacionalinio saugumo valstybės veiklos baudžiamosios teisės srityje. Kaip teigia, Schartumas ir Bygraves (2016, p.128) Direktyva yra bandoma įvairiais būdais sukurti minimalius standartus, kurių turi laikytis valstybės narės, leisdamos įstatymus įgyvendinant direktyvą, bei garantuoti asmens duomenų apsaugą savo šalyje, kad ši nebūtų prastesnė nei nurodoma šiame teisiniame reglamente. Ši direktyva taip pat nustato ir ryšius tarp institucijų, kurios dirba su asmens duomenų apsauga Europos Sąjungoje, tarp bendrijos organų ir nacionalinių valdžios institucijų. Reikia paminėti, kad Direktyvos įgyvendinimas turėjo ir tam tikrų trūkumų, tačiau Duomenų apsaugos direktyvos (95/46/EB) įgyvendinimo ataskaitoje (2003) teigiama, kad buvo pasiektas tikslas užtikrinti aukštą apsaugos lygį. Buvo nustatyti – vieni aukščiausių pasaulyje, duomenų apsaugos standartai. Svarbu paminėti, kad susiduriama su sunkumais kuriant įstatymus valstybėse narėse, nes įstatymai skiriasi nuo Direktyvos pateikiamų reikalavimų. Galima teigti, kad yra sudėtinga kurti duomenų apsaugos politiką Europoje. Tačiau atsakingos institucijos dirba ieškodamos šios problemos sprendimų ir svarbu paminėti, kad iš pateikto Komisijos komunikato Tarybai ir Europos Parlamentui dėl tolesnių veiksmų pagal Geresnio Duomenų apsaugos direktyvos įgyvendinimo (2007) pastebimas pagerėjimas, nes visos šalys- narės yra perkėlusios direktyvą į savo nacionalinę teisę.

Galima daryti prielaidą, kad tobulėjant technologijoms bei įgyvendinant programą yra nuolatos tobulinama Direktyva bei jos įgyvendinimas Europos šalyse, siekiant nuoseklaus bendradarbiavimo su narėmis, bei išorės šalimis. 2012 metais buvo imtasi reformuoti duomenų apsaugos taisykles, o nuo 2016 metų gegužės mėnesio įsigalioja naujas reglamentas. Direktyva bus pradėta įgyvendinti nuo 2018 metų. Europos Sąjungos šalys privalės iki 2018 metų perkelti direktyvos nuostatas į nacionalinę teisę. Su šiuo nauju taisyklių rinkiniu yra siekiama suteikti piliečiams galimybę kontroliuoti savo asmeninius duomenis ir supaprastinti reglamentavimo aplinką verslui. Nauja reforma bus sukurta bendroji skaitmeninė rinka. Reforma padės Europos piliečiams ir įmonėms visapusiškai pasinaudoti skaitmenine rinka.

Kitas svarbus teisinis reglamentas - tai “ *Privatumo ir elektroninių ryšių direktyva*”, kuri buvo išleista 2002 metais.

Šio reglamento tikslas – sukurti naują teisėkūros priemonę, kuri padėtų išdėstyti prisijungimo duomenų saugojimo valstybėse narėse policijos priežiūros tikslais, nepageidaujamų elektroninių pranešimų siuntimo, vadinamųjų slapukų (angl. cookies) naudojimo ir asmens duomenų įtraukimo į viešus abonentų sąrašus nuostatus. Remiantis privatumo ir elektroninių ryšių direktyva (2013) yra įpareigota viešai prieinamų elektroninių paslaugų tiekėjus informuoti apie asmens duomenų apsaugos pažeidimus, jei jų klientų asmens duomenys yra prarandami, pavagiami ar kitaip jiems pakenkiama. 2008/2008 lapkričio mėnesį 977/TVR 27 buvo priimtas pamatinis Europos Tarybos sprendimas dėl asmens duomenų tvarkymo. Kuriam yra nustatomi bendri teisinio reglamentavimo pagrindai vykdant policijos ir teisminių bendradarbiavimą baudžiamosiose bylose.

## **2.2. Europos Sąjungos institucijų, atsakingų už asmens duomenų apsaugą, funkcijos ir vaidmuo tarptautiniu lygmeniu**

Asmens duomenų apsaugą Europos Sąjungoje reglamentuoja ne vienas teisinis aktas. Visoms Europos Sąjungos šalims yra sukurtas teisinis pagrindas reguliuoti ir valdyti asmeninę informaciją. Siekiant įgyvendinti už asmens duomenų apsaugą priimtus reglamentus ir vykdyti jų priežiūrą yra sukurtos specialios administracinės įstaigos įvairiuose sektoriuose. Europos Sąjungos lygmeniu, yra nurodomos trys pagrindinės institucijos atsakingos už asmens duomenų apsaugą. Institucijos pateikiamos lentelėje (žiūrėti 1 lentelę):

1.Lentelė.Europos Sąjungos institucijos, atsakingos už asmens duomenų apsaugą

<b>Europos Komisija pateikia šias atsakingas institucijas:</b>
- Nacionalinės duomenų apsaugos institucijos;
- Europos duomenų priežiūros pareigūnas (EDAPP);
- Europos Komisijos duomenų apsaugos pareigūnas



Europos Komisija nurodo, kad *Europos duomenų priežiūros pareigūnas* yra nepriklausoma Europos Sąjungos institucija, atsakinga už duomenų apsaugos taisyklių stebėseną Europos institucijose.

Priežiūros pareigūnas – Giovanni Buttarelli ir priežiūros pareigūno pavaduotojas Wojciechas Wiewiórowskis 2014 m. gruodžio mėn. Europos Parlamento ir ES Tarybos nutarimu paskirti šioms pozicijoms. Svarbu paminėti, kad priimant šiuos pareigūnus buvo laikomasi nešališkumo principo, siekiant išvengti interesų konflikto. Šios institucijos veikla – nuostatoma, remiantis reglamentu dėl asmenų apsaugos ryšium su asmens duomenų tvarkymu. Galima daryti prielaidą, kad šios institucijos veiklos sritis yra Europos Sąjungos lygmenyje, o veikimas yra panašus į nacionalinių duomenų apsaugos institucijų. Šis institucija gali nagrinėti ir tirti skundus, užtikrinti ir prižiūrėti. Šios institucijos veiklos sritis apima stebėjimus ir patarimus taikant reglamentą Europos Sąjungos institucijoms ir įstaigoms tvarkant asmens duomenis. Taip pat ši institucija turi pakankamai kompetencijos ne tik koordinuojant kitas institucijas, bet ir konsultuoti Europos Komisiją priimant bei rengiant pasiūlymus, teisės aktus ir strategijas, susijusias su asmens duomenų tvarkymu. Institucija teikia strategines rekomendacijas, kurios padėtų išspręsti naujus ir nenumatytus iššūkius duomenų apsaugos srityje. Reikia paminėti, kad yra siekiama užmegzti ir išlaikyti veiksmingą bendradarbiavimą su įvairiomis institucijomis Europos Sąjungoje ir jai nepriklausančiomis šalimis bei nacionalinėmis ir tarptautinėmis organizacijomis. Šioje institucijoje taip pat dirba kompetetinga teisininkų, informacinių technologijų specialistų, administracijos komanda užtikrinanti duomenų apsaugą ir privatumo politikos standartus teisinėje ir praktinėje srityje.

### ***Europos Komisijos duomenų apsaugos priežiūros pareigūnas***

Yra paskiriamas kiekvienoje Europos Sąjungos institucijoje. Šio pareigūno užduotis yra savarankiškai užtikrinti veiklą institucijų viduje, taip pat glaudžiai bendradarbiauti su Europos duomenų apsaugos priežiūros pareigūnu. Kartu su kitomis Europos institucijomis taikyti konkrečius nustatytus teisinius įsipareigojimus duomenų apsaugos reglamente (EB, Nr 45/2001). Šios institucijos pagrindinis uždavinys – nepriklausomai nuo institucijos vidaus nuostatų, užtikrinti reglamento įgyvendinimą. Taip pat ši institucija privalo saugoti bei užtikrinti asmens duomenų registrą, kurį vykdo kitos Europos Sąjungos institucijos,

dirbdamos su asmens duomenimis. Šiame registre turi būti pateikiama konkreti informacija, paaiškinanti tikslus ir aplinkybes, kaip buvo dorojama informacija ir pateikiama suinteresuotam asmeniui.

Galima išskirti ir – *Europos duomenų apsaugos valdybą*. Valdybą sudaro kiekvienos valstybės narės vienos priežiūros institucijos vadovai ir Europos duomenų apsaugos priežiūros pareigūnas arba jų atitinkami atstovai. Kaip teigiama, Europos Parlamento ir Tarybos reglamente ( 2016, 68 straipsnis, p.76) Europos duomenų apsaugos priežiūros pareigūnas balsavimo teisę turi priimant tik tuos sprendimus, kurie yra susiję su Sąjungos institucijoms, įstaigoms organams ir agentūroms taikomais principais ir taisyklėmis, kurie iš esmės atitinka šiame reglamente nustatytus principus ir taisykles. Europos duomenų apsaugos priežiūros pareigūnas balsavimo teisę turi priimant tik tuos sprendimus, kurie yra susiję su Sąjungos institucijoms, įstaigoms organams ir agentūroms taikomais principais ir taisyklėmis. Taip pat Komisija gali dalyvauti Valdybos veikloje, tačiau neturi balsavimo teisės.

Svarbu paminėti ir *Europos elektroninių ryšių reguliavimo instituciją* (angl. BEREC), kuri įgyvendina 2009 metais Europos Parlamento priimtą reglamentą Nr. 1211/2009 dėl telekomunikacijų reformos. Ši institucija pakeitė anksčiau įsteigtą Europos elektroninių ryšių ir paslaugų reguliavimo grupę ir tapo savarankiška ir funkcionalia institucija, siekiančia užtikrinti nuoseklų reguliavimo sistemos funkcionavimą telekomunikacijų sektoriuje.

### **2.3. Europos Sąjungos asmens duomenų apsaugos reguliavimo priemonės**

Europos Sąjungos vykdoma duomenų apsaugos politika yra viena iš saugiausių visame pasaulyje. Jos vykdoma politika kelia pasitikėjimą ne tik Europos Sąjungos šalims, bet šalims nepriklausančioms šiam blokui. Vykdamt bei plėtojant asmens duomenų apsaugos politiką Europoje bei pasaulyje yra remiamasi, jau anksčiau darbe paminėtais, teisiniais reglamentais. Tam, kad sėkmingai būtų dirbama šioje srityje yra svarbu apibrėžti apsaugos reguliavimo priemones, kurios apima ne tik teisinius aktus, bet įvairius kitus nuostatus, rekomendacijas, projektus.

Galima teigti, kad priimti įvairūs teisiniai reglamentai nebuvo pakankamai informatyvūs, kalbant apie taikomas priemones.

Viena pirmųjų bendro europinio lygmens priemonių – buvo priimtas *Tarybos sprendimas 2008/977/TVR dėl asmens duomenų, tvarkomų vykdant policijos ir teisminį bendradarbiavimą baudžiamosiose bylose*.

Šis nutarimas buvo vienas pamatinių sprendimų užtikrinančių fizinių asmenų pagrindinių teisių ir laisvių aukšto lygio apsaugą, kai jų asmens duomenys tvarkomi vykdant policijos ir teisminį bendradarbiavimą baudžiamosiose bylose. Ir kaip yra teigiama Direktyvos (1995, 1str., p. 31) pirmojo straipsnio penktoje dalyje: „*valstybės narės gali nustatyti griežtesnių apsaugos priemonių, skirtų nacionaliniu lygiu renkamų ar tvarkomų asmens duomenų apsaugai užtikrinti bei vykdyti*”. To rezultatas, 2008 metais priimtas sprendimas tik teikia aukštesnį visuomenės saugumą. Komisijos ataskaitoje (2012) nurodoma, kad pamatiniame sprendime išdėstomos asmens duomenų tvarkymo teisėtumo taisyklės, siekiant užtikrinti, kad bet kuri informacija, kuria gali būti keičiamasi, būtų tvarkoma teisėtai ir laikantis duomenų kokybei taikomų pagrindinių principų.

Apibendrinant galima teigti, kad ši ataskaita (2012) yra rengiama siekiant iširti šio sprendimo įgyvendinimą valstybėse narėse perkeliant šį sprendimą į nacionalinę šalių teisę. Šis pamatinis sprendimas yra teisinė priemonė, kurios įgyvendinimą tiria Komisija atsižvelgdama į valstybių narių rekomendacijas bei kylančius sunkumus. Tikslas – sukurti išsamius duomenų apsaugos reglamentavimo pagrindus ir užtikrinti aukšto lygio asmens duomenų apsaugą policijai ir teismams bendradarbiaujant baudžiamosiose bylose ir sklandesnį keitimąsi asmens duomenimis tarp valstybių narių policijos ir teisminių institucijų, laikantis subsidiarumo principo. Europos Parlamento ir Tarybos direktyva 95/46/EB (3) taikoma visai asmens duomenų tvarkymo veiklai valstybėse narėse tiek viešajame, tiek privačiajame sektoriuose. Tačiau, ji netaikoma tvarkant asmens duomenis, kai yra užsiimama tokia veikla, kuri nepatenka į Bendrijos teisės taikymo sritį, pavyzdžiui, veikla teismo bendradarbiavimo baudžiamosiose bylose ir policijos bendradarbiavimo srityse. Galima teigti, kad priimtas pamatinis sprendimas buvo viena iš priemonių, kurių dėka buvo įgyvendintas į Bendrijos teisės sritį nepatenkanti veikla. Siekiant veiksmingos asmens duomenų apsaugos visoje Sąjungoje, reikia stiprinti duomenų subjektų teises ir asmens duomenis tvarkančiųjų pareigas. Taip pat atitinkamus stebėsenos, kaip laikomasi asmens duomenų apsaugos taisyklių, bei tokių taisyklių laikymosi užtikrinimo įgaliojimus valstybėse narėse. Reikia paminėti, kad Europos Parlamento ir Tarybos direktyvoje

95/46/EB (3) buvo nepakankamai apibrėžtos ir nustatytos, fizinių asmenų apsaugos tvarkant asmens duomenis taisyklės ir laisvo asmens duomenų judėjimo, taisyklės. Sparčiai modernėjant visuomenei, tobulėja ir asmenų galimybės rasti jiems aktualią, konfidencialią asmens informaciją.

Tad, *Europos Parlamento ir Tarybos reglamente (ES) 2016/679 (2) nustatytos bendrosios taisyklės*, kuriomis siekiama užtikrinti fizinių asmenų apsaugą tvarkant asmens duomenis ir užtikrinti laisvą asmens duomenų judėjimą Sąjungoje. Remiantis šiuo naujuoju 2016 metais išleistu reglamentu bus panaikinama 1995 metais priimta Direktyva. Nors 1995 metų Direktyvos tikslai ir principai yra pagrįsti, bet svarbu pabrėžti, kad vastybėse narėse yra skirtingas duomenų apsaugos lygis, ko rezultatas – gali būti trikdomas laisvas asmens duomenų judėjimas Sąjungoje. Europos Parlamento ir Tarybos reglamente (2016, p. 2) numatoma galimybė valstybių narių teisėje konkrečiau apibrėžti reglamento taisykles ar numatyti jų apribojimus, valstybės narės, kiek tai būtina suderinamumui užtikrinti. O siekiant, kad nacionalinės nuostatos būtų suprantamos asmenims, kuriems jos taikomos, suteikiama galimybė į savo nacionalinę teisę įtraukti šio reglamento elementus.

Dar viena iš priemonių priimtų 2016 metais tai „*Privatumo skydas*“, kuria siekiama įgyvendinti Europos Sąjungos piliečių teises, kad asmuo turi turėti teisę gauti informaciją iš įstaigų, kurios dirba su jo duomenimis, taip pat pakeisti šiuos duomenimis jei jie yra pasenę ar netikslūs. Taip pat Europos Komisijos pateikiamame straipsnyje *Europos Sąjunga – JAV. „Privatumo skydas visu pajėgumu nuo šiandien“* (2016) nurodo, kad šia priemone bus siekiama nenutrūkstamo bendradarbiavimo su Jungtinių Amerikos valstijų institucijomis dirbančiomis su Europos Sąjungos piliečių duomenimis, taip pat bus nustatomi sprendimo mechanizmai, esant skundams bei žalai. Kaip teigia vartotojų ir lyčių lygybės teisės komisarė Vera Jourova (2016) pasitelkiant Privatumo skydo priemonę bus kuriamas Europos piliečių pasitikėjimas, kad jų asmens duomenys bus perduodami saugiai, užtikrinant pagrindines teises, lengvesnį žalos atlyginimą kilus skundams.

### 3. PROJEKTO TIRIAMOJI IR ANALITINĖ DALIS

*Šiame skyriuje bus analizuojama Lietuvos asmens duomenų sistema ir lyginama su Norvegija. Išskiriami pagrindiniai teisės aktai, asmens duomenų apsaugos institucijos Lietuvoje. Taip pat aptariama asmens duomenų apsaugos sistema Norvegijos Karalystėje. Pasitelkiant įvairius atliktus tyrimus duomenų apsaugos srityje analizuojama Norvegijos Karalystės ir Lietuvos atvejų analizė, išskiriant pagrindines problemas ir perspektyvas asmens duomenų apsaugos srityje.*

#### **3.1. Pagrindiniai Lietuvos teisės aktai reglamentuojantys duomenų apsaugą nacionaliniu lygmeniu**

Asmens privatumas bei jo duomenų apsauga yra įtvirtinta ne viename tarptautiniame teisės reglamente. Žinoma, asmens duomenų apsauga yra reglamentuojama ir Lietuvos teisinėje sistemoje. Asmens duomenų saugumo bei privatumo teisė – apibrėžiama ir pagrindiniame šalies įstatyme – Lietuvos Konstitucijoje (1992), 22 straipsnyje yra nurodoma:

*Žmogaus privatus gyvenimas yra neliečiamas. Asmens susirašinėjimas, pokalbiai telefonu, telegrafo pranešimai ir kitoks susižinojimas neliečiami. Informacija apie privatų asmens gyvenimą gali būti renkama tik motyvuotu teismo sprendimu ir tik pagal įstatymą. Įstatymas ir teismas saugo, kad niekas nepatirtų savavališko ar neteisėto kišimosi į jo asmeninį ar šeimyninį gyvenimą, kėsಿನimosi į jo garbę ar orumą.*

Lietuvos Konstitucijoje (1992) nurodomos nuostatos turinys apie asmens duomenų apsaugą ir privatumą yra atskleidžiamas Lietuvos Respublikos Konstitucinio Teismo aiškinimuose. Kaip teigia Petraitytė (2011, p.127) teisinio reguliavimo dalimi laikytini Lietuvos Respublikos Konstitucinio Teismo asmens į privatumą, žmogaus privataus gyvenimo sampratos aiškinimai. Konstitucinis teismas 1999 m. spalio 21 d. Nutarime Nr. 14/98 konstatavo, jog Lietuvos Konstitucijos 22 straipsnio normos gina žmogaus teisę į privatumą. Šiuo

Konstitucinio Teismo nutarimu buvo apibrėžta privatumo sąvoka, kurios turiniu tapo ne tik asmens privatus gyvenimas, bet ir privatumo sąvokai priskiriamas asmeninių faktų slaptumas, surinkta ar gauta konfidenciali informacija apie asmenį.

1996 metais buvo priimtas *Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas*. Šiame teisės akte buvo apibrėžti informacijos apie fizinius asmenius rinkimo, kaupimo, apdorojimo, saugojimo, naudojimo, teikimo reikalavimai, valstybės informacinėse sistemose. Asmens duomenų teisinės apsaugos įstatymas (1996) reglamentuoja santykius, kurie atsiranda tvarkant asmens duomenis automatiniu būdu ir neautomatiniu būdu tvarkant asmens duomenų susistemintas rinkmenas: sąrašus, kartotekas, bylas, sąvadus ir kita. Įstatymas nustato fizinių asmenų kaip duomenų subjektų teises, šių teisių apsaugos tvarką, juridinių ir fizinių asmenų teises, pareigas atsakomybę tvarkant asmens duomenis. Šis įstatyminis aktas yra vienas pagrindinių teisinių aktų, reglamentuojančių asmens duomenų apsaugą Lietuvoje.

2016 metais kovo mėnesio įsigaliojusiame 36 straipsnio 4 dalies pakeitime, pagrindinė institucija atsakinga už asmens duomenų apsaugą - *Valstybinė duomenų apsaugos inspekcija* neturi teisės kontroliuoti asmens duomenų tvarkymo, kuri atlieka teismai, vykdydami teisingumą (Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo Nr.I-1374 36 straipsnio pakeitimo įstatymas, 2015). Taigi, galima daryti prielaidą, kad asmens duomenų inspekcija teisiškai negali naudotis, vykdyti duomenų apsaugos jei yra vykdomas teisingumas baudžiamosiose bylose. Analizuojant asmens duomenų bei privatumo apsaugos sistemą yra svarbu aptarti ir kitus teisinius įstatymus, reguliuojančius griežtus ir centralizuotus tiesioginio valdymo ir kontrolės principus susijusius su asmens duomenimis. Reikia paminėti, kad informacijos technologijų saugos svarba valstybiniu mastu buvo nurodyta informacijos technologijų saugos valstybinėje strategijoje, patvirtintoje *2001 m. gruodžio 22 d. Lietuvos Respublikos Vyriausybės nutarimu Nr. 1625*. Kaip teigia, Paškauskas (2006, p.86) 2001- 2004 m. vykdant patvirtintą šios strategijos įgyvendinimo planą, nauja redakcija buvo išdėstyti Bendrieji duomenų saugos reikalavimai, patvirtinti Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimo. Privataus gyvenimo apsaugą reglamentuoja ne tik civilinį teisė, bet ir administracinė ir baudžiamosios teisės šakos. Vienas iš pavyzdžių, *Lietuvos Respublikos Civilinis Kodeksas (2000) 2.23*

straipsnis, kuriame išskiriama ne tik teisė į privatumą, bet ir draudžiamas informacijos rinkimas be asmens sutikimo. Įstatymais yra reglamentuojama, kad asmuo turi teisę susipažinti su surinkta informacija.

Šiuo įstatymu taip pat apibrėžiamos veiklos sričių apribojimai, tai neteisėtas įėjimas į privačią asmens teritoriją, jo stebėjimas, filmavimas, susijusių vaizdų panaudojimas. Taigi, galima teigti, kad šiame įstatyme nurodomi keletas informacijos rinkimų būdų, kurie identifikuoja tam tikrą konkretų asmenį. Šis duomenų rinkimas yra galimas tik įstatymo nustatyta tvarka, tačiau, kai įvairi konfidenciali informacija yra renkama savavališkais veiksmais už tai gresia administracinė ar baudžiamoji atsakomybė.

Aktualus teisinis reglamentas tiriantis neleistinai rinktos, kauptos ar kitaip apdorotos informacijos panaudojimą – *Lietuvos Respublikos Administracinių teisės pažeidimų kodekso pakeitimo ir papildymo bei kodekso papildymo įstatymas (2004)*, kurio 214 straipsnyje nagrinėjami asmens duomenų apsaugos pažeidimai. Asmenys ar institucijos nesilaikančios „Asmens duomenų teisinės apsaugos įstatymo“ nustatytos tvarkos yra baudžiami administracine tvarka. Reikia paminėti, kad šiame pakeitimo įstatyme (2004) yra panaikinamas „duomenų tvarkymo“ frazė ir įrašoma telekomunikacijų sritis. Taigi, praplečiama asmens duomenų apsaugos sritis, įstatymo pataisoje atsiranda nauja – komunikacijų sritis. Įvykdyti pažeidimai komunikacijų srityje yra baudžiami taip pat administracine tvarka. Kaip teigia, Petraitytė (2011, p.127) sparti kompiuterinių technologijų sklaida lėmė, kad informaciją apie fizinius asmenis informacinėse sistemose pradėjo tvarkyti ne tik valstybė, bet ir privatūs asmenys.

*Lietuvos Respublikos Elektroninių ryšių įstatymas (2004)* pakeitė anksčiau galiojusį Telekomunikacijų įstatymą. Šiuo reglamentas reguliuojamas ir grindžiamas veiksmingo ribotų išteklių valdymo ir naudojimo, technologinio neutralumo, funkcinio lygiavertiškumo, proporcingumo, mažiausio būtino reguliavimo, teisinio tikrumo kintančioje rinkoje, ekonominės plėtros, veiksmingos konkurencijos užtikrinimo, vartotojų teisių apsaugos, reguliavimo kriterijų, sąlygų ir procedūrų objektyvumo, skaidrumo ir nediskriminavimo principais. Šis įstatymas koreguojamas atsižvelgiant į atitinkamas Europos Bendrijos rekomendacijas. Įstatymo pagalba siekiama užtikrinti paslaugų gavėjų interesų apsaugą, plėsti vidaus rinką, atsižvelgiant į Europos Sąjungos teisės aktų reikalavimus.

Vienas naujausių įstatymų ginančių asmens duomenų apsaugą – 2011 metais priimtas – *Lietuvos Respublikos Asmens duomenų, tvarkomų vykdant*

### ***policijos ir teisminį bendradarbiavimą baudžiamosiose bylose, teisinės apsaugos įstatymas.***

Šio įstatymo paskirtis: „*siekiama užtikrinti fizinių asmenų pagrindinių teisių, ypač teisės į privataus gyvenimo neliečiamumą ir teisės į asmens duomenų apsaugą, apsaugą tvarkant asmens duomenis vykdant policijos ir teisminį bendradarbiavimą baudžiamosiose bylose, numatytą Sutarties dėl Europos Sąjungos*” (Lietuvos Respublikos Asmens duomenų, tvarkomų vykdant policijos ir teisminį bendradarbiavimą baudžiamosiose bylose, teisinės apsaugos įstatymas, 2011). Baudžiamoji atsakomybė yra ne tik apibrėžiama šiame įstatyme. Galima paminėti, kad Lietuvos Respublikos baudžiamojo kodekso redakcijoje (2003) nurodoma, kad draudžiamos veikos susijusios su neteisėtos informacijos apie privatų asmens gyvenimą atskleidimu bei panaudojimu, o tai už šią veiką numatoma baudžiamoji atsakomybė. To rezultatas, kad 2011 metais priimtas įstatymas suteikia daugiau galių tiriant įvairias nusikalstamas veikas bendradarbiaujant su kitomis šalimis bei Europos Sąjungos institucijomis bei teismais. Vienas iš tarptautinio lygmens priimtas sprendimas dėl užtikrinančių fizinių asmenų pagrindinių teisių ir laisvių apsaugą, kai jų duomenys tvarkomi vykdant policijos ir teisminį bendradarbiavimą šiose bylose. Šis įstatymas yra tiesiogiai derinamas su Europos Sąjungos aktais.

### **3.2. Institucijos atsakingos už asmens duomenų priežiūrą ir vykdymą**

Lietuvoje už asmens duomenų apsaugą yra atsakinga Valstybinė duomenų apsaugos inspekcija (toliau Inspekcija). Ši institucija privalo kontroliuoti kaip šalies teritorijoje yra taikomi pagal 1995 metais priimtos Direktyvos nuostatai, galiojantys visoms Europos Sąjungos šalims. Kaip teigiama, asmens duomenų teisinės apsaugos įstatymo komentare (2005, p.238) kiekvienai valdžios institucijai suteikiami įgaliojimai tirti, sužinoti tvarkymo operacijų turinį ar įgaliojimai surinkti visą informaciją, reikalingą priežiūros funkcijoms atlikti. *Asmens duomenų teisinės apsaugos įstatyme* (1996) taip pat nurodoma, kad asmens duomenų teisinės apsaugos inspekcija turi prižiūrėti duomenų valdytojų veiklą tvarkant asmens duomenis, kontroliuoti asmens duomenų tvarkymo teisėtumą, užkirsti kelią duomenų tvarkymo pažeidimams, užtikrinti duomenų subjekto teisių apsaugą.

Lietuvos Respublikos Vyriausybės 2004 m. birželio 28 d. nutarimu Nr. 816 (Žin., 2004 Nr. 103-3791), Inspekcija – paskirta nacionalinės priežiūros institucija.



Inspekcijos paskirtis – nepriklausomai stebėti Lietuvos Respublikos asmens duomenų perkėlimo, paieškos ir teikimo Europolui leistinumą ir nagrinėti, ar tai nepažeidžia duomenų subjekto teisių. Tačiau kaip ir kituose įstatymuose taip ir šios inspekcijos nuostatuose nurodoma, kad ši institucija neturi teisės kontroliuoti asmens duomenų tvarkymo teismuose. Inspekcija apima ne vieną instituciją, kuri dirba su asmens duomenimis, tad atsižvelgdami į Europos Sąjungos teisinius reglamentus yra priimti įvairūs nutarimai reglamentuojantys asmens duomenų apsaugą. Asmens duomenų apsaugos inspekcija yra atsakinga už nepriklausomą perkeltų į Muitinės informacinę sistemą asmens duomenų priežiūrą, užtikrinančią, kad Muitinės informacinėje sistemoje saugomų asmens duomenų tvarkymas ir naudojimas nepažeistų suinteresuotų asmenų teisių. Galima paminėti, kad dauguma teisės aktų yra derinami ir rengiami atsižvelgiant ne tik į šalies įstatyminę bazę, bet ir Europos Sąjungos teisinius nuostatus. O vykdant tarptautinius įsipareigojimus yra koreguojamos ir inspekcijos veiklos sritys.

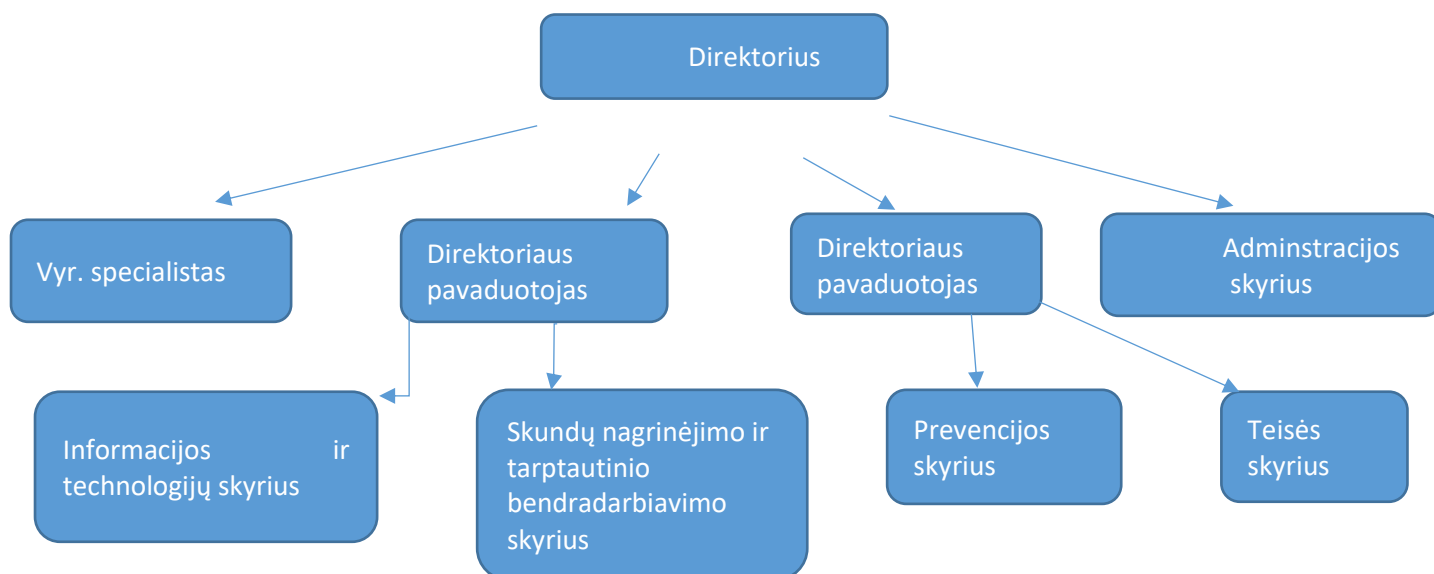
2009 m. kovo 15 d. Įsigaliojus *Elektroninių ryšių įstatymo pakeitimui* dar kartą išsiplėtė Inspekcijos kompetencija, kadangi šio įstatymo pakeitime devintojo skirsnio nuostatos jau taikomos ne tik fiziniams, bet ir juridiniams asmenims. Atsižvelgiant į tai, išsiplėtė Inspekcijos atliekamų duomenų tvarkymo ir privatumo apsaugos tikrinimų, prašymų ir skundų nagrinėjimo bei konsultacijų teikimo elektroninių ryšių srityje apimtys. Taigi, atitinkamai padidėjo ir inspekcijos veiklos apimtys. Inspekcija įgaliota taip pat kaupti informaciją apie elektroninių ryšių įstatymo 65 straipsnio 2 dalyje nurodytų duomenų, reikalingų sunkių ir labai sunkių nusikaltimų, kaip jie apibrėžti Lietuvos Respublikos baudžiamajame kodekse, tyrimo, atskleidimo ir baudžiamojo persekiojimo tikslais, teikimą kompetentingoms institucijoms. Ši institucija kasmet teikia Europos Bendrijų Komisijai statistinius duomenis. Remiantis šio įstatymo 70 straipsniu, galima pastebėti, kad Inspekcija teikia duomenis susijusius su duomenų, generuojamų arba tvarkomų teikiant viešąsias elektroninių ryšių paslaugas arba viešuosius ryšių tinklus, saugojimu ir apimančius atvejus.

Svarbu paminėti, kad Inspekcija turi kompetenciją ne tik kaupti duomenis ar juos pateikti Europos Bendrijų Komisijai. 2010 metais buvo priimtas *Administracinių teisės pažeidimų kodekso (2010)* 15 straipsnio pakeitimas, kuriuo buvo patraukti atsakomybėn statutiniai valstybės tarnautojai. Anksčiau, Inspekcijos pareigūnai

negalėjo surašyti administracinių teisės pažeidimų už neteisėtus asmens duomenų pažeidimus, o tik galėjo juos perduoti svarstyti kitai atsakingai institucijai.

Tačiau šiuo metu galioja tokia tvarka, kad Inspekcija kaip institucija gali pati patraukti baudžiamojon atsakomybėn statutinį valstybės tarnautoją. Tai, itin svarbu kalbant apie visuomenės narių privatumo išsaugojimą tvarkant asmens duomenis. Nes apsaugomos ne tik viešojo sektoriaus, bet ir privataus asmens teisės.

Taigi, svarbu aptarti ir pačios Inspekcijos struktūrą, kuri pateikiama paveiksle (žr. 6 pav.):



**6 pav. Valstybinės duomenų inspekcijos administracijos struktūra**

(Sudaryta autorės remiantis Vastybinės duomenų inspekcijos pateikta schema)

Žvelgiant į pateiktą paveikslą galima paminėti, kad Inspekcijoje dirba du direktoriaus pavaduotojai, jų veiklos sritys padalintos į keturis skyrius, kurie yra atskaitingi paskirtam pavaduotojui bei inspekcijos vadovui. Taip pat, galima išskirti

<b>Inspekcijos vykdomos veiklos</b>
Teisės aktų, užtikrinančių duomenų apsaugą, rengimas ir derinimas
Duomenų valdytojų priežiūros organizavimas
Gyventojų teisės į privatumą užtikrinimas tvarkant asmens duomenis
Tarptautinių įsipareigojimų duomenų apsaugos srityje vykdymas

ir tam tikras veiklos sritys, kurias koordinuoja šie skyriai.

### 3. Lentelė. Inspekcijos vykdomos veiklos

Analizuojant Inspekcijos pateiktus duomenis, galima pastebėti, kad ši institucija teikia įvairias paslaugas visuomenei, duomenų subjektams, duomenų valdytojams (žr. 2 lentelę).

Institucija registruoja duomenų valdytojus, rūpinasi jų patikra, išduoda įvairius

(sudaryta autorės)

leidimus, teikti duomenis kitoms institucijoms ar trečiosioms šalims. Taip pat aptarnauja duomenų subjektus, priima jų prašymus bei skundus dėl neteisėto asmens duomenų panaudojimo. Svarbu pabrėžti, kad yra teikiamos elektroninės paslaugos, suinteresuoti asmenys gali užsisakyti elektronines paslaugas. Siekiant šio tikslo sukurta elektroninių paslaugų sistema (EPS). Remiantis 2012 metais atliktos apklausos dėl asmenų aptarnavimo Valstybinėje Asmens duomenų apsaugos inspekcijoje kokybės, teigiama, kad per pastaruosius trejus metus laikotarpyje 2010-2012 metais asmenys kreipėsi į Inspekciją dėl duomenų valdytojo ar tvarkytojo veiksmų. Tuo tarpu žvelgiant į skundų apibendrinimus, 2014 metais galima pastebėti, kad pagrindinės sritys, kuriose įvyko daugiausiai pažeidimų buvo advokatų neteisėta veikla, netinkamas privačios informacijos pateikimas, jos atskleidimas tretiems nesuinteresuotiems asmenims. Galima išskirti dar vieną pažeidimų sritį – dėl asmens duomenų teikimo sutartyje apibrėžto tikslo. Inspekcijos duomenimis, asmens duomenys, remiantis nustatytais atvejais teikiami pagal duomenų valdytojo ir duomenų gavėjo sudarytą asmens teikimo sutartį. Taigi, praktiškai sutartyje yra nurodomas asmens duomenų naudojimo tikslas, teikimo ir gavimo teisinis pagrindas, sąlygos, tvarka ir teikiamų asmens duomenų apimtis. Inspekcijos darbas yra remiantis Asmens duomenų teisinės apsaugos įstatymo nuostatomis, įvertinti įvairaus pobūdžio situacijas bei priimti sprendimus dėl netinkamo asmens duomenų panaudojimo, nustatant pažeidimus nevykdant sutartyse užsibrėžto tikslo.

Žinoma, Inspekcija vykdo ne tik skundų ar duomenų valdytojų, duomenų subjektų patikrą ar registrą. Ši institucija taip pat rūpinasi ir visuomenės informavimu apie naujausias technologijas, privatumo apsaugos priemones, nes nuolat tobulėjant technologijoms vis dažniau ir patys asmenys susiduria su asmens duomenų panaudojimo pažeidimais ne tik tiesioginiais, bet ir vykstančiais virtualioje aplinkoje. Visuomenės informavimas ir bendradarbiavimas su kitomis institucijomis yra gana svarbi užduotis siekiant tinkamo visuomenės bei kitų institucijų supratimo apie duomenų apsaugą. Tik pakankamas visuomenės narių

išprusimas, šioje srityje, garantuoja saugų asmens duomenų panaudojimą. Remiantis Inspekcijos duomenimis, veikla šioje srityje organizuojama vykdant įvairias konferencijas, pranešimus spaudai, leidžiant naujienų biuletenius, organizuojant įvairius informatyvius renginius.

*Apibendrinant galima teigti, kad Valstybinė asmens duomenų inspekcija yra pagrindinė institucija Lietuvoje atsakinga už asmens duomenų apsaugą. Siekiant Inspekcijos efektyvumo įgyvendinat paslaugas buvo sukurta elektroninių paslaugų sistema (EPS), kurios pagalba teikiamos elektroninės paslaugos duomenų valdytojams bei duomenų subjektams. Šios sistemos pagalba vykdomas abipusis bendradarbiavimas su vartotojais.*

### **3.3. Asmens duomenų sistemoje esančių problemų identifikavimas**

Kaip ir minėta anksčiau galimos įvairios grėsmės privatumui dėl kitų asmenų ar institucijų netinkamos veiklos. Modernėjančios technologijos asmens duomenų apsaugos srityje tampa itin aktualios. Kaip teigia, Europos vartotojų apsaugos komisarė Kunewa (2011) : „*asmens duomenys yra nauja alyva ir valiuta internetui skaitmeniniame pasaulyje*” (Spiekermann, Novotny 2015, p. 181- 200, cit. Kunewa, 2011). Remiantis, Bostono konsultavimo grupės duomenimis yra prognozuojama, kad iki 2020 metų, asmens duomenų naudojimas Europoje ekonomikoje gali sudaryti 330 milijardų eurų metinio pelno Europos organizacijoms. Tačiau, vis daugiau europiečių nerimauja kaip įvairios įstaigos, įskaitant paieškos sistemas, socialinius tinklus, naudoja jų asmens duomenis.

Europos Komisija pateikė 2011 metais Eurobarometro atlikto naujo nuomonės apie duomenų apsaugą ir elektroninę tapatybę tyrimo išvadas, kuriose nurodoma, kad 62 proc. Europos Sąjungos gyventojų, siekdami apsaugoti savo tapatybę, teikia mažiausią būtiną informacijos kiekį, o 75 proc. – pageidauja turėti galimybę panorėję ištrinti internete esančią asmens informaciją, t. y. „*teisę būti pamirštam*”. Vėliau 2014 metais buvo nustatytas EMC privatumo indeksas. Šiame tyrime dalyvavo 15000 asmenų iš 15 šalių siekiant nustatyti asmenų suvokimą ir požiūrį apie duomenų privatumo atskleidimą dėl didesnio patogumo ir naudos internete. Paradoksalu, tačiau tyrimo rezultatai atskleidė, kad vartotojai nori naudotis technologijomis patogiai, nesiimti jokių veiksmų saugant privatumą, dalintis

informacija nevaržomai, tačiau nenori atskleisti jokių privačių asmens duomenų. Šis tyrimas taip pat atliktas Norvegijos Karalystėje ir Lietuvoje.

Žmogaus teisių stebėjimo institutas atliko analogišką tyrimą „*Privatumo paradoksas: Lietuvos gyventojų nuostatos apie duomenų apsaugą*“ (2016).

Lyginant ir analizuojant Lietuvos ir Norvegijos atvejus buvo siekiama iširti vartotojų požiūrį į privatumą ir asmens duomenų apsaugą, išskirti pagrindines problemas. Tyrimo duomenys atskleidė, kad Norvegijos vartotojai yra labiau susirūpinę asmens duomenų apsauga lyginant su pasaulio vidurkiu. Rezultatų duomenimis, 75% apklaustųjų Norvegijoje nesutinka atskleisti savo privačių duomenų dėl paprastesnio naudojimosi skaitmeninėmis paslaugomis.

***Surinktos informacijos panaudojimas.*** Lyginant Eurobarametro (2015) atliktus duomenis galima teigti, kad 50% Lietuvos gyventojų nerimauja dėl valstybės institucijų ir privačių bendrovių turimų duomenų panaudojimo ne tais tikslais. Net 47% nejaucia nerimo, kad jų duomenys bus panaudoti netinkamai. Galima daryti išvadą, kad lietuviai nėra labai susirūpinę asmens duomenų apsauga lyginant su Europos Sąjungos vidurkiu. 78% procentai Europos Sąjungos piliečių nesijaučia saugūs ir, jų nuomone, duomenys gali būti panaudoti vykdant tiesioginę rinkodarą, kryptingą interneto reklamą ar profiliavimą. Nagrinėjant Inspekcijos pateiktų skundų nutartis galima paminėti, kad netinkamas informacijos panaudojimas yra aktuali probleminė sritis. 2015 metais nagrinėta byla dėl informacijos teikimo tretiesiems asmenims tik įrodo, kad vykdant tam tikras operacijas susijusias su asmens duomenimis žmogaus privatumas nėra pažeidžiamas, tai nereiškia, jog panaudojant turimą informaciją jis nebus pažeidžiamas vėliau. Projekto autorė pateikia Inspekcijos atvejį, kai advokatas raštu atskleidė minėtos civilinės bylos duomenis vienos valstybinės institucijos vadovui, nesusijusiam su civiline byla. Advokatas išsiuntė prašymą, kuriame pateikė pareiškėjo asmens duomenis bei kitą privačią informaciją. Šioje byloje buvo nustatyta, kad asmens duomenų atskleidimas perduodant ar kitaip padarant juos prieinamus yra neteisėtas. Duomenų valdytojas privalo supažindinti duomenų subjektą su jo teise nesutikti, kad jo duomenys būtų tvarkomi. Taigi, galima daryti išvadą, kad šiuo atveju advokatas galėjo atskleisti duomenų subjekto duomenis tik turėdamas pastarojo sutikimą. Analizuojant Norvegijos praktiką tokiose bylose paaiškėjo, kad tokie atvejai nėra dažni, nes taikomos griežtos taisyklės. Taip pat įstatymuose nurodoma, kad įvykdžius numatytą tikslą, duomenys turi būti ištrinami. Tačiau Lietuvos

praktikoje nėra nustatytų griežtų taisyklių, kad duomenų valdytojas turi ištrinti duomenis pasiekus užsibrėžtą tikslą.

Tačiau įsigaliojusi 2016 metų direktyva numatyta, kad tokie duomenys turės būti ištrinti, o duomenų subjektui pareikalavus šie duomenys ne tik turės būti pateikti, bet pareikalavus – ištrinti ar koreguojami.

***Nepakankama apsaugos kontrolė.*** Nors yra pakankamai vykdomų teisinių, praktinių priemonių atsakingų už duomenų apsaugą, bet galima rasti trūkumų. Tobulėjant technologijoms, atsakingos institucijos nuolatos turi stebėti esamą situaciją ne tik Lietuvoje, bet ir Europos Sąjungoje. Teisiniai reglamentai yra atnaujinami, siekiant išvengti spragų dėl kurių gali kilti įvairūs nesusipratimai bei vykdomos netinkamos veiklos. 1995 metais priimta ir ratifikuota Direktyva dėl asmens duomenų, tačiau 2016 metų liepos 6 dieną buvo priimta – Europos Parlamento ir Tarybos Direktyva (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti. Ši direktyva bus įgyvendinama ne tik Europos Sąjungoje, bet ir Norvegijoje. Tai tik įrodo, kad tobulėjant informacinėms technologijoms daugybė paslaugų ir informacijos yra persikėlusios į internetinę erdvę. Informacijos sklaida internete pakeitė tradicines verslo formas, pavyzdžiui rinkodaros verslą. Civilkos (2015, p. 128) teigimu, interneto vartotojai dalindamiesi įvairia asmenine informacija ar lankydami tam tikrus tinklapius papildo milžinišką globalią duomenų bazę ( angl. Big data) ir suteikia tam tikrus asmeninius duomenis kitiems rinkos dalyviams. Kiškis (2014) taip pat teigia, kad : „*Istatymai saugo net ir viešą asmeninę informaciją, o kiti asmenys ją gali panaudoti tik tiek, kiek tai būtina dėl viešo intereso ar numatyta įstatymuose*“. Remiantis autorių nuomone, galima teigti, kad vieša asmeninė informacija gali pažeisti asmens teises į privatumą, tačiau svarbu, kad šios informacijos panaudojimas būtų pagrįstas įstatymų.

***Atskaitingumo ir skaidrumo stoka.*** Visuomenės narių juridinė teisė išlaikyti asmens duomenis apsaugotus ir jų teisė į informacinį apsisprendimą yra nustatyta įstatymų. Tačiau pastebima, kad atsiranda vis daugiau duomenų brokerių, kurie daugiau ar mažiau siekia teisėtai prekiauti asmens duomenimis. Spiekermann, Novotny (2015, p. 181- 200) teigimu šešėlinė duomenų prekyba egzistuoja, kai žmogaus teisė į privatumą ir duomenų apsauga neturi pusiausvyros su ekonominiu efektyvumu, to rezultatas – grėsmės privatumui. *Nepakankamas atskaitingumas* rinkoje kenkia plėtrai ir trukdo paslaugų inovacijoms rinkoje. Analizuojant autorių pateiktą straipsnį galima teigti, kad klientai ir asmens duomenų apsaugos

institucijos turi pagrindo skųstis, nes pastebimas informacinio apsisprendimo ir privatumo mažėjimas rinkoje. Pavyzdžiui, Inspekcijos nagrinėtas atvejis dėl asmens duomenų teikimo sutartyje apibrėžto tikslo. Sutartyje turi būti nurodytas asmens duomenų naudojimo tikslas, teikimo ir gavimo teisinis pagrindas, sąlygos, tvarka ir teikiamų asmens duomenų apimtis.

Nustatyta, kad sutartis neatitinka imperatyvių teisės normų reikalavimų ir todėl Druskininkų savivaldybės administracija pareiškėjo duomenis apie jo nekilnojamąjį turtą, esantį (duomenys neskelbtini), rinko ir gavo neteisėtai. Nustačius šias aplinkybes, VDAI teisėtai ir pagrįstai Druskininkų savivaldybės administracijai davė nurodymą įgyvendinti ADTAI 6 straipsnio reikalavimus, kad asmens duomenys pagal VĮ Registrų centro ir Druskininkų savivaldybės administracijos Nekilnojamojo turto registro duomenų teikimo internetu sutartį iš VĮ Registrų centro būtų renkami tik esant sutartyje įtvirtintam duomenų gavimo tikslui (administracinė byla Nr. eA-831-261-2015). Šio atvejo analizė parodo, kad grėsmė asmens duomenims gali kilti ir valstybės institucijose. Svarbu, stebėti ir domėtis ar asmens duomenys yra apdorojami tinkamai. Šio atvejo analizė įrodo, kad nėra pakankamos kontrolės tarp valstybės institucijų.

***Asmens duomenų apsaugos principų pažeidimai.*** Proporcingumo principo pažeidimai taip pat gana aktuali problema asmens duomenų apsaugos sistemoje. Šio principo veikimas susijęs su teisės į privataus ir šeimos gyvenimo gerbimą bylose prieš Lietuvą. Tačiau ribojimas negali būti laikomas proporcingu, įgyvendinant užsibrėžtą tikslą. Proporcingumas – tai pusiausvyra tarp ribojimo ir gaunamo tikslo. Analizuojant pateiktąjį atvejį galima teigti, kad pažeidimai ne tik susiję su nepakankama kontrole institucijose, bet ir su proporcingumo principo įgyvendinimu. Europos Žmogaus Teisių Teisme (toliau EŽTT) yra nagrinėjama ne viena byla, kurioje pažeidžiamas šis principas. Šis proporcingumo principas yra vienas iš būtinumo demokratinėje visuomenėje principo elementų ir išreiškia įstatyme numatyto, neatidėliotiną visuomenės poreikį atitinkančio apribojimo ir juo siekiamo teisėto tikslo pusiausvyrą. Leonaitė (2010, p.115) teigia, kad siekis nustatyti „*teisingą pusiausvyrą*“ tarp bendruomenės intereso ir individo pagrindinių teisių apsaugos lemia proporcingo pasirinktų priemonių ir siekiamo tikslo santykio poreikį. Galima teigti, kad yra svarbu laikytis ne tik teisės aktų, bet principų, kurie būdingi demokratinei valstybei. Tinkamai dirbti su privačia asmens informacija, o ją kontroliuojant svarbu žinoti, kad ribojimų mastas turi būti proporcingas rezultatams.

*Aktualumo principas.* Pasitaiko atveju, kuomet paslaugų teikėjai – bendrovės ne visada laikosi šio principo ir iš duomenų subjektų reikalauja daugiau asmens duomenų nei nurodyta sutartyje.

Duomenų subjektas, norėdamas, jog jam būtų teikiamos elektroninių ryšių paslaugos, tiek sutartyje, tiek užsakymo formoje privalėjo nurodyti asmens kodą, Inspekcija pagrįstai sprendė, kad šiuo konkrečiu atveju asmens sutikimas dėl jo asmens kodo naudojimo nelaikytinas savanorišku, vadinasi, bendrovė jo asmens kodą naudojo neturėdama duomenų subjekto sutikimo. Pažymėjo, kad įmonei, vadovaujantis ADTAI 7 straipsnio 3 dalimi, nesuteikiama teisė naudoti asmens kodą be asmens sutikimo.

Inspekcija priėjo pagrįstą išvadą, kad bendrovė asmens kodą naudojo, taip pat sutartyje bei užsakymo formoje nurodė neteisėtai. Teismo nutartyje taip pat nurodoma, kad įmonė neturėjo teisės naudoti asmens kodą be sutikimo.

Apibendrinant galima teigti, kad įmonė negali rinkti daugiau informacijos nei yra reikalinga. Šiuo atveju, jei įmonė norėjo naudoti asmens kodą, tai turėjo gauti duomenų subjekto sutikimą. Neturėdama šio sutikimo bendrovė pažeidžia žmogaus teisę į privatumą.

### ***Visuomenės ir verslo atstovų nuomonės tyrimai***

2016 metais priimta direktyva nurodo didesnę atsakomybę už netinkamą asmens duomenų panaudojimą. Kaip teigia Zaleckas (2012) įmonė norėdama tvarkyti asmens duomenis turės suteikti daugiau informacijos duomenų subjektui, o už netinkamą informacijos panaudojimą bus nustatytos didesnės baudos, susietos su tam tikru metinių pajamų procentu. Naujai priimta direktyva (2016) taip pat nustatoma teisė būti pamirštam, ypač internete asmeniui atšaukus sutikimą tvarkyti jo duomenis, pasibaigus duomenų saugojimo terminui ar duomenis tvarkant neteisėtai duomenų subjektai gali reikalauti ištrinti jų duomenis ir reikalauti užkirsti kelią tolimesniam jų naudojimui. Siekiant išsiaiškinti verslo atstovų pasirengimą įgyvendinti naująjį reglamentą, 2016 metais buvo atliktas tyrimas „*Lietuvos verslo pasirengimas įgyvendinti bendrąjį asmens duomenų apsaugos reglamentą*“. Tyrimo duomenys atskleidė keletą svarbių faktų:

- verslo atstovai (74%) yra patenkinti Lietuvoje galiojančiu asmens duomenų apsaugos reguliavimu;
- Net 72% verslo įmonių atstovų teikia yra susirūpinę ir teikia didelę reikšmę asmens duomenų apsaugai;



- Lietuvos verslas drąsiai naudoja elektroninės erdvės įrankius;
- Verslo įmonės asmens duomenų apsaugos problemas sprendžia dažniausiai pasitelkdamos vidinius resursus (personalą, administracijos darbuotojus, IT specialistus);

Kiškis M., Bitiukova N., Liutkevičius K. (2016) atlikę šį tyrimą konstatavo, kad Lietuvos verslas yra imlus naujovėms, tačiau neturi pakankamai žinių apie asmens duomenų apsaugos sistemą Lietuvoje. Verslo atstovai naudoja naujomis technologijomis, tačiau savo problemas sprendžia konsultuodamiesi su personalu. Šie duomenys kelia dar didesnę nerimą, jog įmonės ne iki galo supranta pavojus asmens duomenims elektroninėje erdvėje. Įmonės pernelyg pasitiki vidiniais resursais, nesikonsultuoja su specialistais ir neinvestuoja į mokymus. Be to, įmonės, įsiregistravusios asmens duomenų valdytojais, mano įvykdžiusios formalias asmens duomenų apsaugos pareigas, tačiau įsigaliojus naujai direktyvai turės prisiimti didesnę atsakomybę už asmens duomenų apsaugą, suteikti daugiau informacijos apie duomenis – duomenų subjektui.

Siekiant išsiaiškinti visuomenės ir verslo atstovų informuotumą buvo atlikti tyrimai „*Privatumo paradoksas*“ (2016) apie ES duomenų apsaugos reformą. Tyrimai organizuoti vykdant bendrą Lietuvos ir Norvegijos Karalystės projektą. Privatumo paradokso (2016) duomenimis net 78% gyventojų nieko nežino apie naujai priimtą direktyvą (2016). Tai gali būti sąlygota, kad dažniausiai apie reglamentą kalbama profesionalams skirtose publikacijose. Žmogaus teisių stebėjimo instituto atstovė Bitiukova atlikus šį tyrimą konstatavo, kad dauguma žmonių susidūrę su privatumo pažeidimais, niekur nesikreipia, nors teigia, kad privatumas yra svarbus. Lyginant Lietuvos duomenis su Norvegija galima paminėti, kad norvegų tauta yra labiau susirūpinusi savo asmens duomenų ir privatumo saugumu. EMC privatumo indekso (toliau EMC) atlikto tyrimo duomenimis, norvegai yra apsaugoti nuo kibernetinių grėsmių lyginant su kitomis pasaulio šalimis. Norvegų pasitikėjimas savo valdžia siekia 62%, tai įrodo, kad jie tiki valdžios suinteresuotumu apsaugoti piliečių privatumą. Projekto autorės nuomone, lietuviams trūksta pasitikėjimo valdžios institucijomis. O šį nepasitikėjimo jausmą dažnai sustiprina įvairūs valdžios pareigūnų nusižengimai ir nepakankamai funkcionuojančios sistemos. Kaip pavyzdį galima išskirti 2016 metų Seimo rinkimus, kai „rinkejopuslapis.lt“ nepakanakamai funkcionavo ir daugybės rinkėjų

duomenys buvo neapsaugoti. Anot Kiškio (2016) – tai buvo didžiausias masinis privatumo pažeidimas, kuris patvirtino masinio duomenų tvarkymo nesaugumą.

Šis atvejis įrodo, kad asmens duomenų apsaugos sistema nėra tinkamai funkcionuojanti. Projekto autorė, pritardama Kiškio (2016) pasisakymams, taip pat teigia, kad valstybės institucijoms nevykdant tinkamos duomenų apsaugos, turėtų būti taikomi vienodi standartai ir lygiavertės sankcijos.

Tokia įstatymų nustatyta tvarka, yra taikoma Norvegijos asmens duomenų apsaugoje. Spillingo nuomone, yra mažai dėmesio vartotojų požiūrio tyrimams, kai kalbama apie asmens privatumą.

### **3.4. Asmens duomenų apsaugos priemonių paplitimas ir panaudojimas Lietuvoje**

Kaip minėta anksčiau duomenų valdytojai yra pagrindinė institucija tiesiogiai apdorojanti, kaupianti su asmens duomenimis susijusią veiklą. Taigi, duomenų valdytojų bei tvarkytojų užduotis yra parinkti tinkamas organizacines ir technines duomenų saugumo priemones. Kaip teigiama Valstybinės duomenų apsaugos inspekcijos direktoriaus įsakyme (2013) duomenų valdytojai turi vadovautis bendraisiais reikalavimais organizacinėms ir techninėms duomenų saugumo priemonėms, patvirtintais Valstybinės duomenų apsaugos inspekcijos direktoriaus 2008 m. lapkričio 12 d. įsakymu Nr. 1T-71(1.12) ir Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu (1996). Šių priemonių įgyvendinimas turi užtikrinti tokį saugumo lygį, kuris atitiktų saugotinių asmens duomenų pobūdį ir jų tvarkymo keliamą riziką. Kaip jau ir minėta anksčiau duomenų valdytojas turi užtikrinti visus aktualius asmens duomenų principus. Valstybinė duomenų inspekcija būdama viena pagrindinių institucijų atsakingų asmens duomenų apsaugą pateikia tris **duomenų saugumo lygius**. Valstybinės duomenų apsaugos inspekcijos direktoriaus įsakyme (2008) šie lygiai skirstomi:

- *pirmasis saugumo lygis*, šiam lygiui priskirtas saugumo priemones turi užtikrinti visi duomenų valdytojai, tvarkantys viešai skelbiamus asmens duomenis, taip pat duomenų valdytojai, automatiniu būdu tvarkantys asmens duomenis duomenų bazėje (-se), prie kurios (-ių) nėra prieigos per išorinius duomenų perdavimo tinklus;
- *antruoju lygmeniu* priskirtas organizacines ir technines duomenų saugumo priemones turi užtikrinti duomenų valdytojai, automatiniu būdu tvarkantys asmens

duomenis duomenų bazėje (-se), prie kurios (-ių) yra prieiga per išorinius duomenų perdavimo tinklus, taip pat duomenų valdytojai, automatinio būdu tvarkantys ypatingus asmens duomenis duomenų bazėje (-se), prie kurios (-ių) nėra prieigos per išorinius duomenų perdavimo tinklus;

- *trečiasis saugumo lygis* – šiam saugumo lygiui priskirtas organizacines ir technines duomenų saugumo priemones turi užtikrinti duomenų valdytojai, automatinio būdu tvarkantys ypatingus asmens duomenis duomenų bazėje, prie kurios yra prieiga per išorinius duomenų perdavimo tinklus.

Reikia paminėti, kad šis saugumo lygio nustatymas yra viena iš priemonių siekiant tinkamai apsaugoti apdorojamus duomenis.

Taip pat raštiškai turi būti nurodomi ir kiti duomenys tokie kaip atliekamos funkcijos, teisės aktai, asmens duomenų sąrašai, konkretūs veiksmai bei procedūros. Šis išsamus raštiškas nurodymas yra vienas iš viešumo būdų, kuriuos siekiama tinkamo, įstatymais reglamentuoto darbo. Žinoma, duomenų saugumo lygio nustatymas negarantuoja visiško asmens duomenų saugumo. Tam reikalingos ir priėjimo prie įvairių duomenų bazių įslaptinimas, tai siekiant gauti tam tikrą informaciją yra būtinas *slaptažodžio naudojimas*. Kaip nurodoma duomenų apsaugos priemonių aprašuose (2013) yra reikalingos ir organizacinės, fizinės, duomenų gavimo, teikimo duomenų saugumo priemonės.

Fizinėmis priemonėmis galima įvardinti tam tikram asmeniui suteikta prieiga prie kompiuterio duomenų bazių. Siekiant identifikuoti tam tikrą asmenį, kuris dirbo su konfidencialia informacija gali būti naudojami naudotojo vardai bei specialūs slaptažodžiai, kurie identifikuoja tam tikrą darbuotoją, kuris dirbo su tam tikra informacija. Žinoma, jei tai yra kita tam tikra institucija, tai turi būti užtikrinama ir patalpų, kuriuose saugomi vaizdo duomenys, saugumas.

Vienas iš būdų apsaugoti tolesnę asmens duomenų apsaugą tai - ***asmens duomenų nuasmeninimas***. Kaip yra teigiama nuasmeninimo rekomendacijoje (2015) šiuo būdu tvarkomi asmens duomenys suteikia galimybę panaudoti duomenis, kurie anksčiau buvo susieti su asmeniu, kurio tapatybė galėjo būti nustatyta, bet dabar nebesuteikia tokios galimybės. Tokiu būdu asmens duomenys yra nebesusiejami su tam tikru asmeniu ir gali būti panaudojami pavyzdžiui atliekant tam tikrus tyrimus.

Visi asmens duomenys yra vienaip ar kitaip apdorojami, gaunami bei teikiami. Taigi, svarbu užtikrinti šių duomenų saugumą, įstatymais yra nustatyta, kad turi

būti nustatytas išorinių duomenų laikmenų registravimas, kontrolė, duomenų sunaikinimas po jų panaudojimo. Kitas iš būdų apsaugoti asmens duomenis, tai jų šifravimas. Ypatingai reikalingas šių duomenų šifravimas, kai duomenys yra gaunami elektroniniu paštu, interneto tinklu.

Augant asmenų naudojimuisi informacinėmis technologijomis ne nuostabu, kad daug informacijos yra apdorojama pasitelkiant interneto, elektronio pašto pagalbą. Lietuvai įgyvendinus Europos Parlamento ir Tarybos privatumo elektroniniuose ryšiuose direktyvą 2011 m. rugpjūčio 1 d. įsigaliojo Elektroninių ryšių įstatymo (2011) pakeitimas įtvirtinantis reikalavimą, jog paslaugų naudotojo galiniuose įrenginiuose (kompiuteriuose, išmaniuosiuose telefonuose ir kt.) *slapukai* gali būti išsaugojami tik turint išankstinį šio asmens sutikimą.

Ši technologinė priemonė siekiama užtikrinti prieigą prie paslaugos teikėjo interneto svetainės, kurios atsisakius yra apsunkinama naudojimas svetaine arba svetainės turinys yra neprieinamas. Saugoti informaciją arba suteikti galimybę naudotis jau saugoma informacija naudotojo kompiuteryje ar kitame prisijungti prie svetainės naudojamame įrenginyje leidžiama tik tuo atveju, jei naudotojas aiškiai ir išsamiai informuojamas apie slapukų naudojimo tikslą ir yra davęs sutikimą juos įrašyti. Šia saugos priemone siekiama kaupti lankomos svetainės informaciją, o lankantis toje pačioje svetainėje yra analizuojama sukaupta informacija ir prisiderinama prie vartotojų reikmių.

### **3.5. Norvegijos asmens duomenų apsaugos sistema**

Norvegijos Karalystės (toliau Norvegijos) Konstitucijos (1814) 102 straipsnyje yra nurodoma: „*Kiekvienas asmuo turi teisę, kad būtų gerbiamas jo privatus ir šeimos gyvenimas, būsto neliečiamybė ir jo bendravimas. Kratos neturi vykti išskyrus baudžiamąsias bylas. Valstybės institucijos turi užtikrinti asmens neliečiamybės apsaugą*“. Galima teigti, kad žmogaus privatumo užtikrinimas Norvegijos teisės aktuose buvo apibrėžtas pakankamai anksti lyginant su su Lietuvos atveju. Kaip teigia Bingas (1991, p.28) Komisijos pateikiamose ataskaitose 1974 ir 1975 metų pirmą kartą panaudotas sąvoka – asmens duomenų apsauga. Ko rezultatas buvo, kad Teisės Departamentas 1977 metais teikė pasiūlymą dėl asmens duomenų teisės. Tačiau tik 1980 metais ši teisė įsigaliojo ir imta taikyti privačiam ir viešajam sektoriui. Asmens duomenų apsaugos teisė –

apima dvi pagrindines koncepcijas: asmens duomenis ir asmens duomenų registrą. Pasak Bingo (1991) asmens duomenys tai tam tikra informacija, kuri yra susijusi su tam tikru konkrečiu asmeniu.

Ši informacija prieinama panaudojus asmens vardą, asmens kodą, kliento numerį, sąskaitos numerį ar kitą identifikuojančią elementą. Norvegijos įstatymuose taip pat yra nurodoma, kad specialiais asmens duomenimis yra laikomi juridinių asmenų akcijų kursai. Visi duomenys yra registruojami asmens duomenų registre. Šie duomenys apima privatų ir viešąjį sektorių. Bingas (1991, p.30) pateikia keturis pagrindinius principus, kurie sudaro asmens duomenų apsaugos teisę Norvegijoje (žr. 4 lentelę):

4.Lentelė. Principai, sudarantys Norvegijos asmens duomenų teisę

1. Duomenų apsauga
2. Tam tikri įstatymo principai
3. Įsipareigojimai
4. Specialus tam tikros veiklos reguliavimas

(sudaryta projekto autorės)

*Pirmuoju principu* yra nurodomas specialus administracinis organas – Asmens duomenų institucija, kurios tikslas yra įgyvendinti asmens duomenų apsaugos teisę. Ši institucija savo veiklą pradėjo vykdyti nuo 1980 metų.

*Antruoju principu* nurodoma, kad visos asmens duomenų teisės nurodomos nuostatos galioja visiems asmens duomenų registre esantiems objektams.

*Trečiuoju principu* yra išskiriama, kad asmens duomenų apsaugos teisę sudaro dvi grupės, tai įprasti duomenys ir neskelbtini duomenys susiję su sveikata, nuobaudomis ir kt. Tačiau šiuos duomenis gali naudoti ne visi, siekiant priėjimo prie šių duomenų: teikiamas prašymas asmens duomenų institucijai, nurodomas tikslas, kodėl reikalingi tam tikri duomenys. Taip nustatomi duomenys, kurie turi būti registruojami, saugumo priemonės, kas gaus duomenis, kokių tikslu. Įstatymuose nurodoma, kad šių duomenų atskleidimas tretiesiems asmenims yra draudžiamas.

*Ketvirtasis principas* – susijęs su licencijos reikalavimais. Remiantis asmens duomenų registro reikalavimais, turi būti nurodomos veiklos sritys, kuriose bus naudojami asmens duomenys.

Tokios sritys, kaip asmens kreditavimas, apklausa, marketingas turi būti pateikiamos, nes kiekvienai iš šių veiklos sričių yra numatomi atskiri straipsniai asmens duomenų apsaugos teisėje.

Taip pat nurodoma, kad asmens duomenų institucija turi būti informuojama jei asmens duomenys bus naudojami užsienio duomenų registruose.

### **3.5.1. Teisės aktai reglamentuojantys duomenų apsaugą Norvegijoje**

Vienas pagrindinių teisės aktų – *Asmens duomenų įstatymas*, tai bendrasis įstatymas dėl asmens duomenų tvarkymo Norvegijoje. Šis įstatymas įsigaliojo nuo 2001 metų ir pakeitė anksčiau galiojusį 1978 metų asmens duomenų registro įstatymą. Technologinė pažanga atvėrė daugiau galimybių tvarkyti asmens duomenis nenaudojant registro sukūrimo, o sukuriant įstatymą, kuris būtų koreguojamas atsižvelgiant į šiandieninę situaciją ir ES duomenų apsaugos direktyvos (1995) nurodymus (2016 m. priimta nauja direktyva, kuri iki 2018 metų pakeis galiojančią 1995 metų direktyvą). Iki 2001 metų asmens duomenų registro įstatymas numatė visišką kontrolę asmens duomenų institucijai.

Duomenų valdytojai, naudodamiesi 1978 metų įstatymu, asmens duomenis, kurie buvo renkami automatinio būdu ar pasinaudojant kitais registrais, galėjo apdoroti tik turėdami licenciją. Taip pat asmens duomenų įstatymo (2001) 11 straipsnyje nurodoma: „*asmens duomenys – gali būti apdorojami tik turint pagrįstą ir nustatytą tikslą*“. Duomenų valdytojas privalo užtikrinti registruoto duomenų subjekto teises, teisę į informaciją, skaidrumą, ištaisyti ir ištrinti netinkamus duomenis. Svarbu paminėti, kad duomenų valdytojas turi ištrinti asmens duomenis, kai numatytas tikslas bus pasiektas. Norvegijos oficialioje ataskaitoje (2009, p. 63) teigiama, kad tokia informacija yra būtina sąlyga duomenų subjektui, nes suteikia galimybę atkreipti dėmesį į klaidas ir trūkumus, reikalauti, kad duomenys būtų ištrinti ar kitaip kontroliuoti ar duomenų valdytojas atlieka savo pareigas.

Per pastaruosius keturis dešimtmečius buvo priimtas ne vienas teisės aktas dėl asmens privatumo teisės. Norvegija nors ir nėra Europos Sąjungos šalis, tačiau priklauso Europos Ekonominėi erdvei (toliau EEE). Taip yra ratifikavusi ir šalies įstatymuose įtvirtinusi tarptautinius Europos Sąjungos asmens duomenų apsaugą reglamentuojančius teisės aktus. Kaip pabrėžiama oficialioje Norvegijos ataskaitoje (2009, p. 54) valstybės narės ir Norvegija turi vis mažiau laisvės nustatyti taisykles. Remiantis Europos Sąjungos teisės aktais yra nustatomi įvairūs

minimalūs reikalavimai, kurių šalys privalo laikytis. Šie teisės aktai sudaro normatyvinį pagrindą ir tampa reguliavimo sistemos dalimi nacionaliniu ir tarptautiniu mastu. Teisės reglamentai – tai visapusiški taisyklių rinkiniai, kurie apima specifinius reikalavimus tvarkant asmens duomenis.

Svarbiausias šių taisyklių rinkinys – *ES Direktyva dėl asmens duomenų apsaugos (Direktyva 95/46/EB) ir Europos Tarybos Konvencija dėl asmens duomenų apsaugos (1981)*. Galima teigti, kad visos kitos priemonės nėra privalomos yra rekomendacinio pobūdžio (rekomendacijos, gairės ir kt.). Dauguma taisyklių rinkinių taikomi daugelyje sektorių, įvairiuose kontekstuose. Tačiau Europos Taryba aktyviai dalyvauja rengiant konkrečias tam tikrų sektorių rekomendacijas. Vienas šių rinkinių – *ES direktyva dėl elektroninių ryšių ir privatumo (2002/58/EB)*.

Tobulėjant technologijoms buvo nustatyta, kad reikalinga reforma asmens duomenų apsaugos srityje. Europos Komisija 2012 metais pateikė siūlymą modernizuoti ES privatumo taisykles. Buvo pasiūlyti du nauji reglamentai: reglamentas dėl asmens duomenų apsaugos ir direktyva dėl asmens duomenų tvarkymo policijos ir baudžiamosios teisės sektoriuje.

Žinoma, šie reglamentai buvo svarstomi Europos Parlamente. Tačiau svarbus faktas, kad Norvegija negalėjo dalyvauti svarstant ir priimant šiuos sprendimus, nes nėra Europos Sąjungos narė, todėl negalėjo dalyvauti valstybių – narių sudarytoje darbo grupėje. 2012 metais pateiktas teisės akto projektas buvo vertinamas Norvegijos teisingumo ir visuomenės saugumo ministerijos, buvo teigiama, kad šis projektas iš esmės leidžia taikyti pagrindinius principus, esančius Norvegijos privatumo įstatymuose. Tačiau, nauji teisės aktai keičia dabartinę praktiką, nes nauja direktyva bus labiau suderinta su privatumo politika visose Europos Sąjungos valstybėse. Europos teisės interneto svetainėje teigiama, kad naujasis reglamentas suteiks mažiau galimybių keisti teisės aktus nacionaliniu, tačiau vienodas taisyklių rinkinys užkirs kelią skirtingam ir sudėtingam privatumo taisyklių įgyvendinimui. Sudarys vienodas sąlygas bendradarbiaujant tarptautiniu mastu, nes piliečiai ar įmonės turės laikytis vieno bendro Europos taisyklių rinkinio. 2016 metais priimta nauja direktyva yra teigiamai vertinama Norvegijos Karalystės, nes nepažeidžia jų įstatymuose apibrėžtų privatumo principų. Nagrinėjant šios šalies pateikiamus duomenis galima paminėti, kad Norvegija remia neutralų nuo technologijų nepriklausomo principo įgyvendinimą, nes tokios taisyklės užtikrina tinkamą darbą tobulėjant technologijoms ateityje.

Nors atrodytų, kad nauja 2016 metų direktyva išspręs daugybę problemų, tačiau Norvegija nenori uždėti nereikalingos naštos verslui, ypač mažams ir vidutinėms įmonėms.

Taigi, šiuo atžvilgiu išsakoma pozicija už subalansuotą požiūrį, pagal kuri svarbiausia, užtikrinti asmens teises, atsižvelgiant ir į privataus sektoriaus poreikius. Aktualu ir tai, kad išreiškiamas ir šalies siekis išlaikyti nacionalinį lankstumą atsižvelgiant ir į kitus svarbius aspektus, tokius kaip: viešumo principą, su sveikatos, mokslo ir istoriniais tikslais susijusius duomenis. Norvegijos ES delegacijos teisininkė Solhaug teigia, kad 2016 metais priimtos direktyvos taisyklės nurodo griežtesnes taisykles negu 1995 metų direktyva, naujosios taisyklės yra labiau pritaikytos prie visuomenės gyvenimo internete. Anot autorės, griežtesni reikalavimai apima asmens teisę, kad jo duomenys būtų ištrinti arba perkelti kitam iš vieno paslaugų tiekėjo kitam (duomenų perkeliamumas), gauti informaciją apie saugumo pažeidimus, teisę ištrinti ar pakeisti duomenis. Taip pat sudaromos sąlygos piliečiams ir verslo atstovams patyrus pažeidimus kitoje šalyse kreiptis į asmens duomenų inspekciją. Bus vykdomas vieno langelio principas.

**3.5.2. Už asmens duomenų apsaugą atsakinga institucija.** Asmens duomenų institucija buvo įkurta 1980 metais. Ši institucija yra nepriklausoma administracinė įstaiga. Svarbu paminėti, kad Karalius ir atsakingos ministerijos negali nurodyti ar panaikinti institucijos sprendimų. *Duomenų institucijos veiklos sritys.* Remiantis 42 įstatymo trečiąja dalimi, institucija yra atsakinga už asmens duomenų apsaugos politikos įgyvendinimą, kontroliavimą, orientavimą įgyvendinant asmens duomenų apsaugos politiką šalyje. Šios institucijos veiklos sritys apima asmens duomenų įstatymo teisę, sveikatos registro teisę, sveikatos tyrimų teisę, Šengeno informacinės sistemos teisės aktus. Asmens duomenų institucija atlieka pagrindinį vaidmenį patariant ir teikiant rekomendacijas dėl priimamų teisės aktų šioje srityje. Šios institucijos tikslas yra užtikrinti ir privatumo teisę. Norvegijos oficialioje ataskaitoje (2009, p. 63) pateikiama, kad esant nusiskundimams dėl institucijos nutarimų ar veiklos šiuos nusiskundimus sprendžia Asmens duomenų apsaugos tribunolas. Tai – nepriklausoma privatumo valdyba, kuri yra atsakinga Karaliui ir Vyriausybei. Svarbu pabrėžti, kad duomenys apie privačius asmenis esantys nacionaliniame registre yra slapti, tačiau gali būti atskleistos tam tikros detalės, kaip pavyzdžiui asmens kodas gali būti atskleistas privatioms ar valstybinėms



institucijoms esant tam tikroms sąlygoms. Šie atvejai dažniausiai susiję su statistiniais duomenimis ar tam tikrais tyrimais.

Duomenys patekę į nacionalinį registrą turi būti tikslūs ir išsamūs, nes remiantis jais yra priimami įvairūs teisės sprendimai, paskirstomos teisės ir pareigos gyventojų atžvilgiu. Ataskaitos duomenimis konfidencialumo užtikrinimas tampa vienas svarbiausių siekių, nes vis dažniau tapatybė tampa preke ir pasitaiko nusikaltimų šioje srityje.

### **3.6. Asmens duomenų panaudojimas ir įgyvendinimas Norvegijoje**

*Aktualumo principas.* Nagrinėjant Lietuvos atvejį buvo aptarta keletas asmens duomenų pažeidimų. Vienas jų – netinkamas asmens kodo panaudojimas. Norvegijos asmens duomenų teisės dokumentuose nurodoma, kad asmens kodas yra unikalus identifikavimo numeris, kuris yra suteikiamas visiems Norvegijoje gimusiems ar nuolatos gyvenantiems asmenims. Tačiau šis numeris nėra laikomas ypatingai slapta ir konfidencialia informacija. Norvegijos asmens duomenų inspekcija (2013) nurodo, kad asmens kodas nors ir nėra ypatingai slapta informacija, tačiau turi griežtas naudojimo ribas. Asmens kodas gali būti panaudojamas tik tada, kai yra objektyvus poreikis ir yra būtinas asmens kodas yra privalomas asmens identifikavimui. Viešojo administravimo institucijos, bankai, draudimo įmonės, mokesčių institucijos ir kitos institucijos, kurios privalo rengti įvairias ataskaitas apie asmenis, gali naudoti asmens kodą siekdamos identifikuoti tam tikrą asmenį, siekdamos nustatyti asmens tapatybę. Tačiau asmens tapatybės identifikavimui nepakanka tik asmens kodo yra būtina kaip ir Lietuvoje pateikti asmens tapatybę patvirtinantį dokumentą. Kaip pavyzdžiui, asmens kreditinį patikrinimą gali atlikti įmonė, kai nori įdarbinti asmenį darbui su asmens duomenimis, siekdama išsiaiškinti ar asmuo yra mokus ir neturi finansinių problemų. Tačiau tokiu atveju asmuo yra informuojamas laišku, kad tam tikra įmonė nori patikrinti asmens mokumą, su tikslu įdarbinti asmenį. Remiantis šiais reikalavimais galima teigti, kad asmens patikrinimas informuojant asmenį apie ketinamus atlikti veiksmus ir suteikiant asmeniui galimybę prieštarauti tokių veiksmų atlikimui. Tačiau ši taisyklė negalioja atvejais, kai tam tikra įmonė

administruoja asmens duomenis siekdama kaupti informaciją apie asmenį ar asmuo tampa tam tikros įmonės nariu ar naudotoju. Tokiu atveju asmens identifikavimui gali būti naudojami asmens vardas, pavardė, adresas, gimimo data.

Asmens duomenų inspekcija ir 1995 metų direktyva taip pat nurodo, kad asmens kodas negali būti perduodamas tretiems asmenims. Įmonė perduodama ar persiūsdama duomenis su asmens kodu įsipareigoja šiuos duomenis perduoti tik tam asmeniui. O siekiant asmens duomenų apsaugos įmonės yra įpareigtos duomenis perduoti saugiais interneto tinklais ir šifruodami duomenis.

*Asmens duomenų principų įgyvendinimas.* Norvegijos asmens privatumo teisės pagrindu yra laikoma, kad visi turi teisę nuspręsti apie savo asmens duomenis. Privatumo principai taip pat grindžiami Europos Tarybos Konvencija, EBPO ir ES privatumo direktyva. Asmens duomenų inspekcija nurodo, kad asmens privatumas yra prioritetas, o asmens duomenų tvarkymas ir naudojimas galimas tik turint asmens sutikimą ar kitą teisinį pagrindą. Asmens duomenų tvarkymas yra grindžiamas laisvu, aiškiu ir sąmoningu sutikimu. Svarbu paminėti, kad valstybinės institucijos daugeliu atveju turi apdoroti asmens duomenis nepriklausomai nuo sutikimo, tačiau tokiais atvejais turi būti teisinis pagrindas. Norvegijoje, tai užtikrinama remiantis asmens duomenų teise, sveikatos ar policijos registro teisės aktais. Įstatymuose nurodoma, kad asmens duomenų tvarkymas neturi sukelti pernelyg didelės naštos asmens vientisumui ir suverenitetui. Galima paminėti, kad Norvegijos ir Lietuvos atveju yra taip pat nurodoma, kad turi būti išlaikoma pusiausvyra ir pagarba tarp duomenų valdytojo ir duomenų subjekto, o duomenų rinkimas turi būti proporcingas tikslui. Asmens duomenų inspekcija nurodo, kad asmens duomenų tvarkymas visada turi turėti dvi alternatyvas tikslą ar arba teisinį pagrindą.

*Numatyto tikslo įgyvendinimas.* Asmens duomenų teisės įstatyme nurodoma, kad asmens duomenys turi būti renkami tik įvardytais ir teisėtais tikslais. Taip pat teigiama, kad asmens duomenys negali būti naudojami kitais tikslais tikslais nei buvo nurodyta prieš juos renkant. Įstatymai draudžia rinkti daugiau informacijos nei būtina. Surinkti duomenys, kai nebėra būtini nurodytam tikslui turi būti sunaikinti ar pakeisti taip, kad taptų anoniminiais. Šis principas garantuoja, kad asmens duomenys yra sunaikinami, kai pasiektas tikslas. Pavyzdžiui, jei asmuo anksčiau nevykdė mokėjimo įsipareigojimų, asmeniui juos įvykdžius ir sąžiningai

atliekant mokėjimus, duomenų valdytojas negali kaupti tokios informacijos apie klientą.

*Asmens duomenų apsaugos priemonės.* Norvegijos asmens duomenų inspekcija taip pat nurodo, kad asmenys jaučiantys nesaugūs internete gali kreiptis į interneto svetainę [www.slettmeg.no](http://www.slettmeg.no). Ši interneto svetainė sukurta teikti įvairias programas – mokymus, išmokyti asmenis pašalinti nepageidaujamą informaciją iš interneto. Taigi, galima teigti, kad asmenims yra suteikiama teisė ištrinti asmens duomenis. Suteikiama galimybė asmenims mokytis patiemis pašalinti nepageidaujamą savo duomenis, taip pat suteikiama įvairūs mokymai ne tik atlikti tai savarankiškai, bet ir teikiama ir pagalba.

Vienas iš reikalavimų įgyvendinant asmens duomenų saugos priemones, tai – slapukai. Slapukai – tai mažas tekstinis failas, kurio pagalba kaupiam informacija apie vartotojo įpročius svetainėje. Vartotojas sutikęs instaliuoti slapukus savo kompiuteryje suteikia informaciją apie savo vartojimo pobūdį, remiantis šiais duomenis yra sudaromos sąlygos vartotojui pasiekti reikalingą. Šis reikalavimas yra įgyvendinamas remiantis Europos Sąjungos Elektroninių ryšių įstatymu. Norvegijoje šio įstatymo įgyvendinimas yra prižiūrimas nacionalinės telekomunikacijų tarnybos, kuri taip pat reguliuoja ir prižiūri pašto ir telekomunikacijų sektorių, atsakinga už radijo dažnių valdymą.

Taip pat galima paminėti ir duomenų šifravimą, šios priemonės įgyvendinamas turi griežtas taisykles, ypatingai asmenims dirbantiems su asmens duomenų apsauga. Asmens duomenų saugumui pasiekti yra taikomos įvairios priemonės. Duomenų valdytojai ir tvarkytojai turi naudotis asmenį identifikuojančiomis kortelėmis, asmeniniais kodais. Sistemose, kuriose yra apdorojami duomenys kaupiami įrašai apie duomenų tvarkytojus, registruojami pakeitimai prireikus gali identifikuoti su duomenimis dirbusį asmenį. Taip pat vykdomi įvairūs mokymai, seminarai apie asmens duomenų apsaugojimo priemones. Periodiškai atliekami patikrinimai, mokymai internetu ir konferencijose. Analizuojami atvejai, kai duomenys buvo atskleisti, ieškoma būdų sistemų pagalba apsaugoti duomenis nuo fizinės asmens klaidos.

*Apibendrinant galima teigti, kad Norvegijos asmens duomenų sistema turi griežtas apsaugos taisykles. Duomenų valdytojai pasiekę duomenų tvarkymo tikslą, asmens duomenis turi ištrinti arba anonimizuoti. Lyginant Lietuvos ir Norvegijos atvejus paaiškėjo, kad asmens duomenų apsauga ypatingai svarbi norvegams. Lietuvoje trūksta informacijos apie asmens duomenų apsaugos priemones ir būdus.*

## **IŠVADOS**

1. Asmens duomenys – tai informacija apie konkretų asmenį, kurį galima tiesiogiai arba netiesiogiai nustatyti iš tam tikrų asmens požymių. Lietuvos asmens duomenų sistema funkcionuoja remiantis asmens duomenų teisinės apsaugos įstatymu. Svarbu paminėti, kad Lietuva ir Norvegija yra įsipareigojusi reglamentuoti Europos Sąjungoje galiojančias direktyvas ir įvairius teisės aktus.
2. 1995 metų direktyva yra vienas pagrindinių teisės aktų reglamentuojančių asmens duomenų apsaugą Europos Sąjungos lygmeniu. Ši direktyva nustato pagrindines taisykles ir principus, kaip turi būti įgyvendinama asmens duomenų politika Lietuvoje ir Norvegijoje. Modernėjančios technologijos verčia keisti teisės aktus, nes asmens duomenys tampa nepakankamai apsaugoti, tad 2016 metais priimta nauja direktyva numato papildomus reikalavimus asmens duomenų apsaugai.
3. Analizuojant projekto duomenis paaiškėjo, kad Lietuvoje asmens duomenys yra tvarkomi netinkamai, nustatomi duomenų apsaugos pažeidimai privataus ir viešojo administravimo institucijose. Remiantis norvegų pavyzdžiu, reikėtų griežtinti asmens duomenų apsaugos taisykles ir reikalavimus.
4. Projekto metu paaiškėjo, kad asmens duomenų apsaugos sistema funkcionuoja nepakankamai. Išanalizavus įvairius atvejus paaiškėjo, kad duomenų valdytojai ne visada laikosi iškelto tikslo tvarkant asmens duomenis. Pažeidžiamos duomenų subjekto teisės. Lyginant su Norvegijos atveju, galima daryti išvadą, kad Lietuva

turėtų remtis šios šalies praktika ir pasiekus užsibrėžtą tikslą, asmens duomenis privalėtų ištrinti arba anonimizuoti.

5. Nagrinėjama tema yra problematiška, apima daugybę aspektų. Projekto metu paaiškėjo, kad nėra pakankamai atliktų visuomenės, verslo ir valdžios institucijų požiūrių tyrimų. Tarptautinių Europos Sąjungos teisės aktų įgyvendinimas Lietuvoje ir Norvegijoje yra nevienodas ir nepakankamas.
6. Už Lietuvos asmens duomenų apsaugos įgyvendinimą atsakingos institucijos neturi pakankamai resursų sprendžiant su privatumo nusižengimais susijusias problemas. Darbuotojams trūksta apmokymų tobulinant savo žinias asmens duomenų apsaugos srityje. Norvegų praktika rodo, kad apmokymai turi vykti nuolatos ir įvairiais būdais: konferencijos, apmokymai internetu.
7. Lyginant Lietuvos ir Norvegijos sistemų atvejus paaiškėjo, kad Lietuvos visuomenė neturi pakankamai žinių apie asmens duomenų saugumą. Taip pat nepasitiki valdžios institucijomis, retai kreipiasi dėl pažeidimų tvarkant asmens duomenis. Duomenų subjektai taip pat turėtų būti informuojami apie jų duomenų tvarkymą. Tai didintų visuomenės pasitikėjimą duomenų valdytojais ir asmens duomenų inspekcija.
8. Verslo atstovai aktyviai naudojami technologijomis tvarkant asmens duomenis, tačiau neturi pakankamai žinių apie galimas grėsmes. Taip pat nustatyta, kad privačiame sektoriuje trūksta apmokymų darbuotojams, nesikonsultuojama su specialistais, problemos sprendžiamos naudojant vidinius resursus. Lyginant su norvegų praktika turėtų vykti apmokymai ir konsultacijos darbuotojams.

## REKOMENDACIJOS

1. Remiantis projekto rezultatais Valstybinei asmens duomenų inspekcijai rekomenduojama griežtinti asmens duomenų tvarkymo taisykles. Nustatyta, kad duomenų valdytojai tvarko duomenis pažeisdami duomenų tvarkymo principus. Žiniasklaidos priemonėse turėtų būti skelbiamos asmens duomenų apsaugos būdai, rengiamos konferencijos, teikiama informacija apie naujų technologijų privalumus ir apsaugos būdus.
2. Visuomenė turi nepakankamai žinių apie asmens duomenų apsaugą. Inspekcija turėtų organizuoti įvairius projektus, konferencijas visuomenei. Remiantis norvegų praktika įgyvendinti įvairius mokymus internetu. Informuoti visuomenę apie galimas grėsmes ir duomenų apsaugos būdus. Tokiais būdais gerėtų ne tik visuomenės žinios apie duomenų apsaugą, bet ir didėtų pasitikėjimas valstybės institucijomis.
3. Inspekcija turėtų vykdyti bendradarbiavimą su Lietuvos verslo atstovais. Paaiškėjo, kad įmonės retai konsultuojasi su specialistais apie galimas grėsmes asmens duomenims. Nuolatos vykdomos konsultacijos ir mokymai verslui padėtų išvengti asmens duomenų apsaugos pažeidimų. Nenustrūkstamas bendradarbiavimas taip pat padėtų Lietuvos verslui pasiruošti priimti 2016 metais naujai priimtos direktyvos įgyvendinimui.
4. Lietuvos asmens duomenų inspekcija turėtų įgyvendinti daugiau projektų su kitomis šalimis, domėtis kitų šalių praktika asmens duomenų apsaugos srityje. Tai pagerintų inspekcijos teikiamų paslaugų kokybę, padėtų išspręsti kylančias problemas šioje srityje.

## LITERATŪRA

1. Aktualių Teismo sprendimų apibendrinimas. [žiūrėta: 2016-12-06]. Prieiga internetu: [https://www.ada.lt/get\\_file.php?file..](https://www.ada.lt/get_file.php?file..)
2. Ar Lietuvos verslui ir vartotojams rūpi asmens duomenų apsauga? [žiūrėta: 2016-10-31]. Prieiga internetu: [http://www.spinter.lt/site/lt/vidinis\\_noslide/menutop/9/home/publish/ODU1Ozk7OzA=](http://www.spinter.lt/site/lt/vidinis_noslide/menutop/9/home/publish/ODU1Ozk7OzA=)
3. Asmens duomenų teisinės apsaugos įstatymo komentaras. [žiūrėta: 2016-10-07]. Prieiga internetu: <http://www.ada.lt/images/cms/File/komentaras%20adtai.pdf>
4. Bing Jon. Personvern i faresonen. Oslo. [žiūrėta: 2016-10-12]. Prieiga internetu: <http://www.nb.no/nbsok/nb/f3548c5aad3a11dc499db72cd1635f6f.nbdigital?lang=no#29>
5. Civilka M. (2001). Asmens duomenų teisinis reguliavimas interneto kontekste. ) [žiūrėta: 2016-10-12]. Prieiga internetu: <http://media.search.lt/GetFile.php?OID=92932&FID=269994>
6. Civilka M., Šlapimaitė L. (2015). Asmens duomenų samprata elektroninėje erdvėje. ISSN 1392-1274. Teisė. [žiūrėta: 2016-12-21]. Prieiga internetu: <http://www.zurnalai.vu.lt/teise/article/view/8761/7647>
7. Data protection bodies. [žiūrėta: 2016-10-17]. Prieiga internetu: [http://ec.europa.eu/justice/data-protection/bodies/index\\_en.htm](http://ec.europa.eu/justice/data-protection/bodies/index_en.htm)
8. Duomenų apsauga. Kas yra privatumas? [žiūrėta: 2016-10-05]. Prieiga internetu: <https://www.datatilsynet.no/personvern/Hva-er-personvern/>
9. Europos duomenų apsaugos priežiūros pareigūnas. [žiūrėta: 2016-10-17]. Prieiga internetu: <https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/cache/offonce?lang=lt#>
10. Europos duomenų teisės vadovas. [žiūrėta: 2016-12-01]. Prieiga internetu: <http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-lt.pdf>
11. Europos Komisijos Eurobarometro tyrimas “Duomenų apsauga” [žiūrėta: 2016-12-20]. Prieiga internetu: [http://ec.europa.eu/public\\_opinion/archives/ebs/ebs\\_431\\_fact\\_lt\\_lt.pdf](http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_fact_lt_lt.pdf)

12. Europalov. [žiūrėta: 2016-12-20]. Prieiga internetu:  
<http://www.europol.no/rettsakt/personvernforordningen-om-behandling-av-persondata/id-5275#behandlende-organ>
13. EU-U.S.Privacy Shield fully operational from today. [žiūrėta: 2016-10-22]. Prieiga internetu: [http://ec.europa.eu/newsroom/just/item-detail.cfm?item\\_id=33704](http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=33704)
14. Individas ir vientisumas. Asmens duomenų apsauga skaitmeninėje visuomenėje. Oficiali ataskaita 2009:1. [žiūrėta: 2016-10-06] . Prieiga internetu:  
<https://www.regjeringen.no/contentassets/c6e6901fea06412fa8f78ae3eae9c33f/no/pdfs/nou200920090001000dddpdfs.pdf>
15. Jarukaitis I.,Makauskaitė A., Civilka M., Lamanuskas T. (2005). *Elektroninių ryšių teisė*. Vilnius.Eugrimas
16. Kilkelly U. (2001).The right to respect for private and family life. (p.31) [žiūrėta: 2016-10-12]. Prieiga internetu:  
<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168007ff47>.
17. Komisijos ataskaita Europos Parlamentui,Tarybai, Europos Ekonomikos ir Socialinių reikalų komitetui ir regionų komitetui. [žiūrėta: 2016-10-22]. Prieiga internetu: <http://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:52012DC0012>
18. Kjølås C. (2010). *Personvern i arbeidsforhold*.Universitetsforlaget.Oslo.
19. Leonaitė E. (2010). Proporciningumo principas ir jo taikymas EŽTT bylose prieš Lietuvą pagal EŽTK 8 straipsnį. [žiūrėta: 2016-12-06]. Prieiga internetu:  
<http://www.zurnalai.vu.lt/files/journals/5/articles/197/public/113-125.pdf>. Teisė. ISSN 1392-1274 2010 77
20. Lietuvos Respublikos Vyriausybės 2004 m. birželio 28 d. nutarimu Nr. 816 „Dėl atsakingų institucijų paskyrimo ir įgaliojimų suteikimo įgyvendinant Lietuvos Respublikos įstatymą „Dėl konvencijos, parengtos vadovaujantis Europos Sąjungos Sutarties K.3 straipsniu, dėl Europos policijos biuro įsteigimo (Europolo konvencijos) ir jos protokolų ratifikavimo“ Žin., 2004 Nr. 103-3791
21. Meškauskaitė L. (2004). Žiniasklaidos teisė. Vilnius: Teisinės informacijos centras
22. Muitinės jungtinės priežiūros institucija ir asmens duomenų apsauga. [žiūrėta: 2016-12-02]. Prieiga internetu: <https://www.ada.lt/go.php/lit/Muitines-jungtines-prieziuros-institucija-ir-asmens-duomenu-apsauga>
23. Nesitikėkite, kad Europos Sąjunga apgins Jūsų privatumą.[žiūrėta: 2016-12-27]. Prieiga internetu: <http://kiskis.eu/2016/10/>
24. Norvegai labai susirūpinę privatumo apsauga .[žiūrėta: 2016-12-19]. Prieiga internetu: <http://www.digi.no/artikler/nordmenn-svaert-opptatt-av-personvern/288369>
25. Nuasmeninimo metodai. [žiūrėta: 2016-10-27]. Prieiga internetu:  
<https://www.ada.lt/go.php/Valstybines-duomenu-apsaugos-inspekcijos-rekomendacijos122122>



26. Paškauskas Ž. (2006).Elektroninės informacijos saugos tarptautinio teisinio reguliavimo analizė: Lietuvos padėtis. [žiūrėta: 2016-10-26]. Prieiga internetu:  
<http://etalpykla.lituanistikadb.lt/fedora/objects/LT-LDB-0001:J.04~2006~1367155561076/datastreams/DS.002.0.01.ARTIC/content>.  
Jurisprudencija. Mokslo darbai 2006 5(83); 82-89
27. Personvernreform vedtatt i EU. [žiūrėta: 2016-10-26]. Prieiga internetu:  
<https://www.regjeringen.no/no/aktuelt/personvernreform-vedtatt-i-eu/id2484114/>
28. Petraitytė (2011). Asmens duomenų apsaugos teisinis reguliavimas teisės sistemoje. [žiūrėta: 2016-10-24]. Prieiga internetu:  
<http://www.zurnalai.vu.lt/teise/article/viewFile/175/137> ISSN 1392–1274. teisė 2011 79
29. Post, R.C. (2001). Three concepts of privacy. [žiūrėta: 2016-10-09]. Prieiga internetu:  
[http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1184&context=fss\\_papers](http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1184&context=fss_papers).  
The Georgetown Law Journal, 89, 2087-2098.
30. Privacy and Confidentiality in Health Research (2006). [žiūrėta: 2016-10-31]. Prieiga internetu:  
<http://www.onlineethics.org/cms/8076.aspx>
31. Privacy and Human Rights Report (2006). [žiūrėta: 2016-10-13]. Prieiga internetu:  
<http://www.worldlii.org/int/journals/EPICPrivHR/2006/PHR2006-The-2.html#fn38>
32. Privatumo paradoksas: Lietuvos gyventojų nuostatos apie duomenų apsaugą“ (2016). [žiūrėta: 2016-12-01]. Prieiga internetu: <http://hrmi.lt/wp-content/uploads/2015/10/Privatumo-paradoksas-1.pdf>
33. Privatumo ekspertas: šifravimas beprasmis, jei slaptažodis- „Lietuva1”[žiūrėta: 2016-12-27]. Prieiga internetu: <http://hrmi.lt/privatumo-ekspertas-sifravimas-beprasmis-jei-slaptazodis-lietuva1/>
34. Projektas „Valstybinės duomenų apsaugos inspekcijos ir Lietuvos bibliotekininkų draugijos bendradarbiavimo didinimas įgyvendinant asmens duomenų apsaugos politiką“. [žiūrėta: 2016-12-01]. Prieiga internetu:  
<https://www.ada.lt/go.php/lit/Bendradarbiavimas-su-lietuvos-bibliotekininku-draugija-projektasvalstybines-duom...mens-duomenu-apsaugos-politika/8>
35. Schartum, Dag Wiese og Lee A. Bygrave (2004). *Personvern i informasjonssamfunnet. En innføring i vern av personopplysninger*. Bergen: Fagbokforlaget. ISBN: 82 450 0120 1
36. Schartum D.W. ir Lee A. Bygrave L.A.(2016). *Personvern i informasjonssamfunnet*.Fagbokforlaget.Bergen.
37. Skundų nagrinėjimo veiklos apibendrinimai. [žiūrėta: 2016-11-30]. Prieiga internetu:  
<https://ada.lt/go.php/Skundu-nagrinejimo-veiklos-apibendrinimai333>
38. Štilis D., Pakutinskas P.,Laurinaitis M., Dauparaitė I. (2011). *Tapatybės vagystė elektroninėje erdvėje: socialiniai, elektroninio verslo ir teisinio reguliavimo aspektai*. Kolektyvinė mokslo monografija. Vilnius

39. Teisininko komentaras: Europos Komisija nekeičia krypties asmens duomenų apsauga turi būti griežtesnė ir mažiau formalizuota. [žiūrėta: 2016-10-31]. Prieiga internetu: <http://www.delfi.lt/news/daily/law/teisininko-komentaras-europos-komisija-nekeicia-krypties-asmens-duomenu-apsauga-turi-buti-grieztesne-ir-maziau-formalizuota.d?id=54873431>
40. The EMC privacy index. [žiūrėta: 2016-12-20]. Prieiga internetu: <https://www.emc.com/collateral/brochure/privacy-index-global-in-depth-results.pdf>
41. Točickienė N. (2003). Asmens duomenų apsaugos reglamentavimas Europos Sąjungos ir Lietuvos Respublikos teisėje. Jurisprudencija, 2003, T. 44(36); 114-123
42. Viešų asmens duomenų apsauga. [žiūrėta: 2016-12-27]. Prieiga internetu: <http://kiskis.eu/viesu-asmens-duomenu-apsauga/>
43. 2003m. Gegužės 15d. Komisijos pranešimas Pirmoji Duomenų apsaugos direktyvos (95/45EB) įgyvendinimo ataskaita. [žiūrėta: 2016-10-13]. Prieiga internetu: <http://eur-lex.europa.eu/legal-content/LT/TXT/?uri=URISERV%3A114012>
44. 29 straipsnio duomenų apsaugos darbo grupė. Nuomonė Nr. 1/2010 dėl sąvokų „duomenų valdytojas“ ir „duomenų tvarkytojas“ [žiūrėta: 2016-12-02]. Prieiga internetu: [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169\\_lt.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_lt.pdf)
45. 2013 OECD Privacy Guidelines. [žiūrėta: 2016-12-05]. Prieiga internetu: <https://www.oecd.org/internet/ieconomy/privacy-guidelines.htm>

## ŠALTINIAI

1. Asmens duomenų apsauga. [žiūrėta: 2016-10-13]. Prieiga internetu: <http://eur-lex.europa.eu/legal-content/LT/TXT/?uri=URISERV%3A114012>
2. Asmens duomenų teisinės apsaugos įstatymas. [žiūrėta: 2016-10-04]. Prieiga internetu: <https://www.e-tar.lt/portal/lt/legalAct/TAR.5368B592234C/IGOrBAvuZc>
3. Europos žmogaus teisių deklaracija 1948m. [žiūrėta: 2016-10-09]. Prieiga internetu : <https://www.e-tar.lt/portal/legalAct.html?documentId=TAR.181EDAC3A371>
4. Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija. *Žin.* 1995, Nr. 40-987
5. Lietuvos Respublikos Asmens duomenų, tvarkomų vykdančios policijos ir teisminių bendradarbiavimą baudžiamosiose bylose, teisinės apsaugos įstatymas 2011m. [žiūrėta: 2016-10-26]. Prieiga internetu: [https://www.e-tar.lt/portal/lt/legalAct/TAR.299D835159BE/TAIS\\_435407](https://www.e-tar.lt/portal/lt/legalAct/TAR.299D835159BE/TAIS_435407)
6. Lietuvos Respublikos civilinis kodeksas. Antroji knyga. Asmenys 2.23 straipsnis. [žiūrėta: 2016-10-26]. Prieiga internetu: <https://www.infolex.lt/ta/20799:str2.23>
7. LR Asmens duomenų teisinės apsaugos pakeitimo įstatymo Nr. I-1374 36 straipsnio pakeitimo įstatymas. ). [žiūrėta: 2016-10-13]. Prieiga internetu: <https://www.e-tar.lt/portal/legalAct.html?documentId=03360f109e6811e58fd1fc0b9bba68a7>
8. Lietuvos Respublikos baudžiamojo kodekso 168 straipsnis. [žiūrėta: 2016-10-26]. Prieiga internetu: <https://www.infolex.lt/ta/66150:str168>
9. Lietuvos Respublikos Konstitucija. *Žin.*, 1992, Nr. 33-1014.
10. Lietuvos Respublikos Elektroninių ryšių įstatymo 1, 3, 7, 12, 34, 77 straipsnių devintojo skirsnio ir priedo pakeitimo ir papildymo bei įstatymo papildymo nauju priedu įstatymas. *Žin.*, 2004, Nr. 69-2382; 2007, Nr. 46-1723
11. Lietuvos Respublikos Konstitucinio teismo 1999 m. spalio 21 d. Nutarimas Nr. 14/98 *Žin.* (1999-10-21, Nr.90-2662).
12. Norvegijos įstatymas dėl asmens duomenų tvarkymo.[žiūrėta: 2016-10-06]. Prieiga internetu: <https://lovdata.no/dokument/NL/lov/2000-04-14-31?q=personopplysningsloven>
13. Norvegijos karalystės Konstitucija. [žiūrėta: 2016-10-06]. Prieiga internetu: [https://lovdata.no/dokument/NL/lov/1814-05-17/KAPITTEL\\_5#§102](https://lovdata.no/dokument/NL/lov/1814-05-17/KAPITTEL_5#§102)

14. Telekomunikacijų įstatymas (1998, nebegaliojantis). [žiūrėta: 2016-10-26]. Prieiga internetu: <https://www.e-tar.lt/portal/lt/legalAct/TAR.027489452776>
15. 1995m. Spalio 24d. Europos Parlamento ir Tarybos direktyva (95/46/EB) dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo. [žiūrėta: 2016-10-13]. Prieiga internetu: <http://eur-lex.europa.eu/legalcontent/LT/TXT/?uri=CELEX:31995L0046>
16. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) [žiūrėta: 2016-10-13]. Prieiga internetu: <http://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN>