MYKOLO ROMERIO UNIVERSITETO
TEISĖS FAKULTETO
KONSTITUCINĖS IR ADMINISTRACINĖS TEISĖS INSTITUTAS

VITA MACIENĖ

ADMINISTRACINĖS TEISĖS STUDIJŲ PROGRAMA

ASMENS DUOMENŲ APSAUGA NACIONALINĖJE IR EUROPOS SĄJUNGOS TEISĖJE

Magistro baigiamasis darbas

Darbo vadovas -
Prof. dr. Algimantas Urmonas

Vilnius, 2014

TURINYS

ĮVADAS..... 3
1. ASMENS DUOMENŲ APSAUGOS MATERIALUSIS IR FORMALUSIS ASPEKTAI..... 6
2. EUROPOS SĄJUNGOS IR NACIONALINIS TEISINIS REGULIAVIMAS ASMENS DUOMENŲ APSAUGOS SRITYJE..... 13
2.1. Asmens duomenų apsaugos reguliavimas Europos Sąjungoje 13
2.2. Asmens duomenų apsaugos reguliavimas Lietuvoje 17
3. ASMENS DUOMENŲ APSAUGA ELEKTRONINIŲ RYŠIŲ SRITYJE..... 21
3.1. Bendrieji asmens duomenų tvarkymo aspektai 21
3.2. Direktyvos 2006/24/EB nuostatų įgyvendinimas 24
4. IŠANKSTINIO MOKĖJIMO SIM KORTELIŲ REGISTRAVIMO GALIMYBIŲ ANALIZĖ 34
4.1. Išankstinio mokėjimo SIM kortelių registravimo būtinumas 34
4.2. Europos Sąjungos šalių patirtis registruojant išankstinio mokėjimo SIM korteles 40
4.3. Išankstinio mokėjimo SIM kortelių registravimo galimybės tyrimo rezultatai 45
IŠVADOS..... 54
PASIŪLYMAI..... 56
LITERATŪRA..... 58
ANOTACIJA LIETUVIŲ IR ANGLŲ KALBOMIS..... 65
SANTRAUKA LIETUVIŲ KALBA..... 66
SANTRAUKA ANGLŲ KALBA..... 68
PRIEDAI..... 69
PATVIRTINIMAS APIE ATLIKTO DARBO SAVARANKIŠKUMĄ..... 70

ĮVADAS

Magistro baigiamojo darbo aktualumas. Pastaraisiais dešimtmečiais vis greitėjantis informacinių technologijų vystymasis, spartėjanti globalizacija ir milžiniški informacijos srautai pakeitė žmonijos suvokimą apie duomenų perdavimą. Tai jau nėra kadaise mums buvęs įprastas ir lengvai kontroliuojamas materialusis keitimasis informacija. Šiomis dienomis informacija vis rečiau įgauna materialųjį pavidalą, nes apsikeitimas informaciniais ištekliais įprastai vyksta virtualioje erdvėje. Tai yra sudėtingai kontroliuojamas procesas. Akivaizdu, kad teisė į asmens duomenų apsaugą šiame kontekste tampa vienu aktualiausių klausimų sprendimu, į kurį nuolatos ieškoma tiek nacionaliniu, tiek Europos Sąjungos mastu, nes tai, visų pirma, siejama su žmogaus teisių užtikrinimu.

Visose srityse, kur žmonių veikla apima informacinių technologijų naudojimą, susiduriama su duomenų tvarkymo teisėtumo ir jų saugumo užtikrinimo problema. Todėl yra labai svarbu nubrėžti aiškią ribą tarp žmogaus teisės į privatumą bei teisės gauti ir skleisti informaciją. Suvokus informacinių technologijų keliamus pavojus, žmonija vis aktyviau imasi priemonių sukurti saugų bei efektyvų teisinio reguliavimo mechanizmą užtikrinant asmens duomenų apsaugą, tačiau neretai toks reguliavimas nespėja kartu su informacinių technologijų progresu.

Kadangi visuomeniniai santykiai asmens duomenų apsaugos srityje yra labai plati tema, pagrindinis dėmesys darbe skiriamas asmens duomenų apsaugos užtikrinimui, teikiant elektroninių ryšių paslaugas. Detalus tokių santykių nagrinėjimas yra sąlygotas vis dažnėjančių diskusijų visuomenėje dėl judriojo ryšio išankstinio mokėjimo SIM kortelių registracijos būtinumo. Vienu aktualiausių teisės aktų, nustatančiu pagrindinius principus užtikrinant asmens duomenų apsaugą elektroninių ryšių srityje, laikytina Europos Parlamento ir Tarybos direktyva 2006/24/EB dėl duomenų, generuojamų arba tvarkomų teikiant viešai prieinamas elektroninių ryšių paslaugas arba viešuosius ryšių tinklus, saugojimo ir iš dalies keičianti Direktyvą 2002/58/EB. Todėl pasirinkta tema nagrinėjama žvelgiant per šios direktyvos reguliavimo prizmę ir analizuojant jos santykį su nacionaliniais teisės aktais asmens duomenų apsaugos srityje. Gautos išvados ir pateikti siūlymai darbe grindžiami atlikto tyrimo dėl išankstinio mokėjimo SIM kortelių registravimo būtinumo duomenimis.

Magistro baigiamojo darbo tyrimo objektas – Europos Sąjungos ir nacionalinės teisės reguliacinių mechanizmų ypatumai asmens duomenų apsaugos srityje ir šių ypatumų sąlygotos galimybės privalomai registruoti judriojo ryšio išankstinio mokėjimo SIM korteles Lietuvoje.

Magistro baigiamojo darbo hipotezė – Europos Sąjungos ir nacionalinis teisinis reguliavimas asmens duomenų apsaugos srityje sudaro palankias sąlygas privalomai judriojo ryšio išankstinio mokėjimo SIM kortelių registracijai Lietuvoje.

Magistro baigiamojo darbo tikslas – atskleisti Europos Sąjungos ir nacionalinio teisinio reguliavimo asmens duomenų apsaugos srityje ypatumus juos nagrinėjant per elektroninių ryšių srities prizmę ir pateikti moksline, teisinio reguliavimo ir atlikto tyrimo medžiaga pagrįstas galimybes registruoti judriojo ryšio išankstinio mokėjimo SIM korteles.

Magistro baigiamojo darbo uždaviniai:

1. atskleisti esminius Europos Sąjungos ir nacionalinės teisės asmens duomenų apsaugos aspektus;
2. ištirti lyginamuoju požiūriu asmens duomenų apsaugos elektroninių ryšių srityje ypatumus nacionalinėje ir Europos Sąjungos teisėje;
3. ištirti ir įvertinti judriojo ryšio išankstinio mokėjimo SIM kortelių registravimo praktiką Europos Sąjungos šalyse;
4. išanalizuoti judriojo ryšio išankstinio mokėjimo SIM kortelių registravimo galimybes Lietuvoje;

Magistro baigiamojo darbo tyrimo metodai:

Siekdami visapusiškos nagrinėjamos temos analizės, magistro baigiamajame darbe naudosimės tiek *empiriniais*, tiek *teoriniais* tyrimo metodais kaip tyrimo objekto pažinimo būdais, ypatingą dėmesį skirdami kokybiniam tyrimo metodui.

Tyrimui magistro baigiamajame darbe atlikti pasirinkti du empiriniai tyrimo metodai – tai *tradicinis dokumentų analizės metodas*, kuris taikomas nagrinėjant Europos Sąjungos ir nacionalinės teisės šaltinius, siekiant visapusiškai atskleisti asmens duomenų apsaugos teisinio reguliavimo mechanizmą elektroninių ryšių srityje. Pagrindiniai nagrinėjami Europos Sąjungos teisės aktai yra Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, Europos Parlamento ir Tarybos direktyva 97/66/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos telekomunikacijų sektoriuje, Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje ir Europos Parlamento ir Tarybos direktyva 2006/24/EB dėl duomenų, generuojamų arba tvarkomų teikiant viešai prieinamas elektroninių ryšių paslaugas arba viešuosius ryšių tinklus, saugojimo ir iš dalies keičiančios Direktyvą 2002/58/EB. Vertinant nacionalinės teisės ypatumus nagrinėjamos Asmens duomenų teisinės apsaugos ir Elektroninių ryšių įstatymų bei su šių įstatymų reguliavimo sritimi susijusių poįstatyminių teisės aktų nuostatos; taip pat *apklausos metodas,* kurį

atliekant 204 respondentams elektroniniu būdu pateiktas parengtas klausimynas dėl judriojo ryšio išankstinio mokėjimo SIM kortelių registravimo galimybių, o gauti duomenys apibendrinti ir pateiktos motyvuotos išvados.

Analizuojant pasirinktą temą taikomi šie tyrimo metodai: *indukcinis* ir *dedukcinis metodai* naudojami analizuojant ir vertinant kryptingai pateikiamą informaciją asmens duomenų apsaugos srityje, t. y. apžvelgiama asmens duomenų apsaugos instituto samprata, pateikiami jo ypatumai, kurie vertinami per elektroninių ryšių srities prizmę, jais grindžiant galimybę privalomai registruoti judriojo ryšio išankstinio mokėjimo SIM korteles Lietuvoje; *lyginamuoju istoriniu metodu* trumpai apžvelgiama asmens duomenų apsaugos instituto vystymosi raida; *lyginamojo metodo* pagalba lyginami *dokumentų analizei* pasirinkti aukščiau minėti Europos Sąjungos ir nacionalinės teisės aktai, nustatytas jų tarpusavio santykis; naudojant *kritikos metodą* pateikiami Europos Sąjungos ir nacionalinės teisės reguliavimo trūkumai*; sisteminės analizės metodas* taikomas analizuojant judriojo ryšio išankstinio mokėjimo SIM kortelių praktiką Europos Sąjungos šalyse. Vertinant išankstinio mokėjimo SIM kortelių registravimo galimybes Lietuvoje, taip pat naudojamas *prognozavimas*.

1. ASMENS DUOMENŲ APSAUGOS MATERIALUSIS IR FORMALUSIS ASPEKTAI

Pradėdami nagrinėti pasirinktą temą, manytume, svarbu apibrėžti asmens duomenų apsaugos sampratą, jos vystymosi raidą ir šiuos visuomeninius santykius reguliuojančius teisinius instrumentus. Tinkamo elgesio standartai yra formuluojami normų arba principų pavidalu, t. y. turi atitinkamą formą, kurios atsiradimas yra sąlygotas tam tikrų išorės veiksnių. Todėl siekdami glaustumo ir konkretumo, temos dalyką įvardinsime dviem aspektais – *materialiuoju* ir *formaliuoju*.

Nagrinėdami asmens duomenų apsaugos materialųjį aspektą, trumpai apžvelgsime visuomeninius interesus ir visuomenės egzistavimo sąlygas, dėl kurių asmens duomenų apsauga tapo aktuali ir tokio pobūdžio visuomeniniai santykiai turėjo būti formalizuoti, t. y. paversti teisės norma.

Nagrinėdami asmens duomenų apsaugą formaliuoju aspektu apžvelgsime jos, kaip elgesio taisyklės išorinį pavidalą, kuriuo ši norma pateikiama visuomenei, t. y. trumpai išnagrinėsime asmens duomenų apsaugos instituto virsmo elgesio norma mechanizmą, jos vidinę struktūrą ir sampratos įvairovę. Be to, apžvelgsime poveikio priemones, kurios yra taikomos už šios elgesio taisyklės pažeidimą.

Asmens duomenų apsaugos sritis yra pakankamai nauja, nors tam tikrų jos formavimosi užuomazgų galima įžvelgti jau gilioje senovėje. Net Biblijoje gausu asmens teisės į privatumą pasireiškimo pavyzdžių, tačiau tais laikais privatumas nebuvo suvokiamas kaip socialinė vertybė.[1] Akivaizdu, kad tuo metu asmens duomenų apsauga nebuvo suprantama taip, kaip ją suvokia šiuolaikinė visuomenė, tačiau visuomeninius santykius, susijusius su asmenų teise į privatumą buvo bandyta reguliuoti ir anuomet. Pažymėtina, kad istoriškai pirma ėmė formuotis privatumo samprata ir pagrindinis dėmesys buvo kreipiamas į asmens privatumo apsaugą. Todėl galima teigti, kad asmens duomenų apsaugos koncepcijos ištakos slypi asmens teisėje į privatumą.

Pirmuosius rašytinius teisės į privatumą įgyvendinimo pavyzdžius randame Anglijos teisinėje sistemoje. 1361 m. Anglijos taikos teisėjas išdavė sankciją sekiotojų ir pasiklausinėtojų areštui, o 1765 m. Lordas Camdenas panaikino įėjimo į privačius namus ir jų apieškojimo orderį,

[1] Civilka M. *Asmens duomenų apsauga tarptautinėje ir EB teisėje* [interaktyvus]. Vilnius: Vilniaus universitetas Teisės fakultetas,2001[žiūrėta2013-10-09]. http://www.scribd.com/doc/24045929/Mindaugas-Civilka-Asmens-duomen%C5%B3-apsauga-tarptautin%C4%97je-ir-EB-teis%C4%97je-2001-LT-Baltracker-net.

kuriame nurodė, kad „Nėra jokios teisės normos, kuri leistų tokius dalykus; tokiu atveju mūsų visuomenės nariai prarastų bet kokį komfortą ir apsaugą“.[2]

Reikėtų paminėti, kad Švedijoje asmens privatumo samprata formavosi taip pat labai sparčiai ir 1776 m. Švedijos parlamentas priėmė aktą „Dėl priėjimo prie viešųjų registrų“, kur buvo nustatytas reikalavimas visą valstybinių institucijų turimą informaciją naudoti tik teisėtiems tikslams. Tokiu būdu galima teigti, kad šiuo dokumentu jau buvo formalizuota teisė ne tik į privatumą, tačiau ir į asmens duomenų apsaugą, kas tuo metu buvo labai pažangu. 1858 m. Prancūzija uždraudė privačių/asmeninių faktų viešą publikavimą ir už šio reikalavimo pažeidimą nustatė griežtas baudas.

Tačiau nežiūrint į aukščiau minimus privatumo ir asmens duomenų apsaugos formavimosi pavyzdžius, M. Civilkos teigimu, „teisinės privatumo šaknys glūdi JAV“[3]. 1890 m. S. Warren ir L. Brandeis parašė darbą „Teisė į privatumą“ (*angl. The right to privacy*), kur teisę į privatumą apibūdino, kaip teisę būti paliktam vienam. Esminis šio darbo išskirtinumas istoriniu požiūriu yra tas, kad jame pirma kartą teisė į privatumą buvo išreikšta kaip socialinė vertybė.

Iki duomenų perdavimo tinklų infrastruktūros atsiradimo visuomenės susirūpinimas asmens duomenų apsauga nebuvo didelis. Tai sąlygojo dideli informacijos administravimo kaštai, kas sudarė nepalankias aplinkybes pažeidimams asmens duomenų apsaugos srityje plisti. Tačiau vystantis informacinėms technologijoms, atsirado galimybė asmens duomenis tvarkyti automatizuotu būdu. Asmens duomenų apsaugos užtikrinimas ėmė reikalauti greitų ir inovacinių sprendimų, visuomenėje ėmė augti susirūpinimas dėl galimų asmens duomenų apsaugos pažeidimų. Atsiradus internetui ir mobiliai telekomunikacijai šis susirūpinimas sustiprėjo dar labiau.

Europos Sąjungos teisinio reguliavimo pagrindai asmens duomenų apsaugos srityje buvo nustatyti dar 1948 m. Visuotinėje žmogaus teisių deklaracijoje. Šios deklaracijos 12 straipsnyje nustatytas principas, kad „*niekas neturi patirti savavališko kišimosi į jo privatumą, šeimos gyvenimą, buitį ar susirašinėjimą arba kėsinimosi į jo garbę ir reputaciją. Kiekvienas turi teisę į įstatymo apsaugą nuo tokio kišimosi arba kėsinimosi*“. Vėliau ši nuostata buvo plėtojama 1950 m. Europos žmogaus teisių ir pagrindinių laisvių konvencijos 8 straipsnyje, kur teigiama, kad „*kiekvienas turi teisę į tai, kad būtų gerbiamas jo asmeninis ir jo šeimos gyvenimas, buto neliečiamybė ir susirašinėjimo slaptumas*“.

N. Točickienė nurodo, kad „modernios asmens duomenų apsaugos koncepcijos formavimosi pradžia galima laikyti 1968 m. Europos Tarybos ir Europos bendradarbiavimo ir plėtros

[2] *Ibid,* [žiūrėta 2013-10-10].
[3] Civilka M., *supra* note 1.

organizacijos žengtą žingsnį, kai Europos Tarybos parlamentinė asamblėja rekomendacijoje Ministrų kabinetui iškėlė klausimą, ar šiuolaikinių technologijų ir mokslo pasaulyje Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija ir valstybių narių nacionaliniai teisės aktai pakankamai apsaugo privataus gyvenimo neliečiamybę“[4]. Tokiu būdu buvo išreikštas poreikis ir reikalingumas užtikrinti teisę į asmeninės informacijos apsaugą. Netrukus Austrija, Danija, Prancūzija, Vokietija, Liuksemburgas, Norvegija, Švedija, Portugalija, Ispanija priėmė įstatymus dėl asmens duomenų apsaugos[5].

Asmens duomenų apsaugos pagrindines kryptis dėl privatumo apsaugos ir duomenų judėjimo valstybėms narėms 1980 m. nustatė Europos bendradarbiavimo ir plėtros organizacija (EBPO). Atsižvelgdama į vis spartesnį pasaulio ekonominį ir demokratijos vystymąsi, EBPO savo rekomendacijoje pasiūlė valstybėms narėms nacionalinių įstatymų leidybos srityje apsaugoti asmens privatumą bei nesudaryti kliūčių laisvam informacijos judėjimui.

1981 m. sausio 28 d. buvo priimta Europos Tarybos konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu, kur nustatyti pagrindiniai asmens duomenų apsaugos principai: „asmens duomenų rinkimo ir tvarkymo sąžiningumo, teisėtumo ir tikslingumo, duomenų tvarkymo saugumo, duomenų subjekto teisių ir garantijų, duomenų valdytojo atsakomybės, specialios ypatingų duomenų apsaugos“[6].

1995 m. spalio 24 d. Europos Parlamentas ir Taryba priėmė direktyvą (95/46/EB) dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo. Tokiu būdu buvo pašalintos laisvo duomenų perdavimo kliūtys, nepakenkiant duomenų saugumui. Vėliau, 2002 m. liepos 12 d., Europos Parlamentas ir Taryba priėmė direktyvą (2002/58/EB) dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje dėl asmenų privatumo apsaugos telekomunikacijų sektoriuje. Taip pat vienu svarbiausių dokumentų asmens duomenų apsaugos reguliavimui laikytina 2006 m. kovo 15 d. Europos Parlamento ir Tarybos priimta direktyva (2006/24/EB) dėl duomenų, generuojamų arba tvarkomų teikiant viešai prieinamas elektroninių ryšių paslaugas arba viešuosius ryšių tinklus, saugojimo. Išsamiau šių direktyvų nuostatos, reguliavimo ypatumai ir kiti su jomis susiję klausimai nagrinėjami sekančioje darbo dalyje.

Duomenų apsaugos svarbą Europos Sąjungoje pabrėžė ir 2000 m. gruodžio 8 d. paskelbta Europos Sąjungos pagrindinių teisių chartija, kurios 8 straipsnis įtvirtino asmens teisę į savo

[4] Točickienė N. Asmens duomenų apsaugos reglamentavimas Europos Sąjungos ir Lietuvos Respublikos teisėje. *Jurisprudencija*. 2003, 44(36): 115.
[5] Išsamiau apie šiose valstybėse asmens duomenų reglamentavimą bus kalbama kitose darbo dalyse.
[6] Konvencija „Dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108)“. *Valstybės žinios*. 2001, Nr. 32-1059.

duomenų apsaugą. V. Valančius ir S. Kavalnė teigia, kad „kiekvienas žmogus turi teisę į savo asmens duomenų apsaugą. Tokie duomenys apdorojami sąžiningai tam tikrais nurodytais tikslais, atitinkamam asmeniui sutinkant arba remiantis kitais įstatymu numatytais teisėtais pagrindais. Kiekvienas asmuo turi teisę susipažinti su surinktais apie jį duomenimis ir reikalauti tuos duomenis ištaisyti. Kaip laikomasi šių taisyklių, kontroliuoja nepriklausoma institucija“[7].

Svarbu pažymėti, kad praėjus daugiau kaip trims dešimtmečiams nuo 1980 m. EBPO rekomendacijų, iš esmės nebuvo priimtas nei vienas solidus bei šiuolaikines visuomenės vystymosi tendencijas atitinkantis tarptautinis dokumentas. Šio darbo autorė mano, kad tokia padėtis susidarė todėl, kad teisinio reguliavimo mechanizmai nėra tokie „imlūs“ naujovėms ir nespėja vystytis taip greitai, kaip tai daro informacinių technologijų sritis. 1981 m. Europos Tarybos konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu taip pat jau neaprėpia visų santykių asmens duomenų apsaugos srityje, nes yra nukreipta į jos priėmimo metu vykusių apsikeitimo asmens duomenimis ir jų tvarkymo automatizuotu būdu ypatumus. Net direktyva (95/46/EB) dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo tik iš dalies atitiko to meto visuomenės poreikius asmens duomenų apsaugos srityje, nors ir buvo laikoma pažangia. To meto spartus internetinio ryšio vystymasis sukėlė tikrą perversmą informacinių technologijų ir apsikeitimo informacija srityje. Toks staigus informacinių technologijų proveržis priimant to meto teisės aktus asmens duomenų apsaugos srityje numatytas nebuvo.

Kalbant apie asmens duomenų apsaugą formaliuoju aspektu, reikėtų išskirti dvi kategorijas: *duomenų apsauga* ir *duomenų saugumas*[8]. Lietuvių kalboje žodis „*duomenys*“ (*duomuo*) reiškia „*kas duota, kuo remiamasi, darant išvadas*“[9]. Žodis „*apsauga*“ reiškia „*apsaugojimą, gynimą*“[10]. Žodis „*saugus*“ reiškia „*nekeliantis pavojų, nepavojingas, apsaugotas nuo pavojaus*“[11]. Kadangi darbe kalbama apie asmens duomenų apsaugą, manytume, taip pat svarbu apibrėžti ir asmens sąvoką. Lietuvių kalboje žodis „*asmuo*“ reiškia „*žmogus, kaip atskiras individas*“[12].

Vertinant sampratas, galime teigti, kad duomenų apsauga sietina su asmens duomenimis, t. y. duomenų apsauga savyje suponuoja draudimą skelbti, platinti ir kitaip disponuoti asmens duomenimis be jo sutikimo, o duomenų saugumas yra suvokiamas kaip apsauginė funkcija, kaip priemonių rinkinys užtikrinti turimos informacijos apsaugą. Tai gali būti daroma informaciją

[7] Valančius V., Kavalnė S. *Europos Sąjungos teisės įgyvendinimas Lietuvos administracinėje teisėje*. Vilnius: VĮ Registrų centras, 2009, p. 201.
[8] Keras A., Kurapka E., Petrauskas R. *Informacinės visuomenės kūrimo, informacinių technologijų taikymo ir informacinių technologijų teisės plėtros tendencijos Europos Sąjungoje*. Vilnius: 2001, p. 42.
[9] Keinys S. *Dabartinės lietuvių kalbos žodynas. Septintasis leidimas*. Vilnius: Lietuvių kalbos institutas, 2012, p. 138.
[10] *Ibid.*, p. 32.
[11] *Ibid.*, p. 677.
[12] *Ibid.*, p. 43.

koduojant, šifruojant ar kitokiais būdais imantis priemonių apsaugoti turimus duomenis. Svarbu pažymėti, kad visi asmens duomenų apsaugą reglamentuojantys tiek nacionaliniai, tiek tarptautiniai teisės aktai nustato ne duomenų saugumo, bet fizinių asmenų duomenų apsaugos reikalavimus. Kalbant konkrečiau, šie teisės aktai reguliuoja ne pačią duomenų apsaugą, kaip procesą, bet pačių fizinių asmenų, kaip duomenų subjektų apsaugą. Plačiąja prasme, asmens duomenų apsaugos esmė – apsaugoti žmonių teises. Pagrindinis jos tikslas yra užtikrinti, kad asmens duomenys būtų apdorojami taip, kad būtų užtikrinamas žmogaus privatumas ir kitos su tuo susijusios žmogaus teisės.

Lietuvoje asmens duomenų apsaugos sąvoka yra apibrėžta Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatyme (ADTAĮ). Europos Sąjungos mastu asmens duomenų sąvoka šiuo metu yra apibrėžta trijuose teisės aktuose:

- 1980 m. EBPO rekomendacijoje dėl asmens privatumo apsaugos ir asmens duomenų judėjimo tarp valstybių narių gairių.
- 1981 m. Europos Parlamento ir Tarybos konvencijoje dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu.
- Direktyvoje (95/46/EB) dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo.

ADTAĮ 2 straipsnio 1 dalyje teigiama, kad asmens duomenys yra „bet kuri informacija, susijusi su fiziniu asmeniu – duomenų subjektu, kurio tapatybė yra žinoma arba gali būti tiesiogiai ar netiesiogiai nustatyta pasinaudojant tokiais duomenimis kaip asmens kodas, vienas arba keli asmeniui būdingi fizinio, fiziologinio, psichologinio, ekonominio, kultūrinio ar socialinio pobūdžio požymiai“[13].

Pagal direktyvos 95/46/EB 2 straipsnį 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 ir netiesiogiai, ypač pasinaudojus nurodytu asmens identifikavimo kodu arba vienu ar keliais to asmens fizinei, fiziologinei, protinei, ekonominei, kultūrinei ar socialinei tapatybei būdingais veiksniais“[14].

Nagrinėdami aukščiau pateiktas sąvokas matome, kad jos iš esmės yra identiškos ir jų turinys yra labai platus. Pažymėtina, kad sąvokose pateikiama informacijos apimtis asmeniui apibūdinti yra

[13] Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas. *Valstybės Žinios*. 1996, Nr. 63-1479.
[14] Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo. [1995] OL L 281/ 31.

ne visuomet būtina. Analizuojant pateiktas asmens duomenų sąvokas esminiais jų požymiais reikėtų laikyti *tiesioginį* ir *netiesioginį* asmens tapatybės nustatymo kriterijus, t. y. asmens duomenys yra vertinami pagal jų santykį su duomenų subjektu. Net netiesiogiai su asmeniu susijusi informacija gali būti vertinama kaip asmens duomenys, nes ji gali būti glaudžiai susijusi su kitais tiesioginiais asmens duomenimis[15].

Reikėtų skirti sąvokas „asmeninė informacija“ ir „asmens duomenys“. „Asmeninė informacija asmens duomenimis gali virsti tik tuomet, kai jos pagalba tampa įmanoma identifikuoti konkretų asmenį“[16]. Nagrinėdami pateiktas sąvokas šiuo aspektu matome, kad čia asmens duomenys skirstomi į dvi kategorijas: asmenį apibūdinančius duomenis (identifikatorius) ir kitus duomenis. Tokį skirstymą M. Civilka įvardina kaip „sąryšio/santykio koncepciją“[17]. Identifikatoriai tiesiogiai nurodo konkretų asmenį. Šiai grupei galime priskirti asmens kodą, registracijos numerį ar kitus duomenis, nurodančius konkretų duomenų subjektą. Visi duomenys, identifikatoriaus pagalba susieti su asmens duomenų subjektu, tampa asmens duomenimis. Nesant identifikatoriaus, duomenys praranda asmens duomenų statusą, nors ir yra susiję su tam tikru asmeniu.

1981 m. Europos Parlamento ir Tarybos konvencija dėl asmenų apsaugos, susijusios su automatizuotu asmens duomenų apdorojimu ir 1980 m. EBPO rekomendacija dėl asmens privatumo apsaugos ir asmens duomenų judėjimo tarp valstybių narių gairių pateikia gerokai siauresnes asmens duomenų sąvokas. Jose teigiama, kad asmens duomenimis yra bet kokia informacija, susijusi su identifikuotu ar identifikuotinu asmeniu. Pagrindinė šios sąvokos mintis yra ta, kad čia asmuo tam tikros informacijos pagalba turi būti identifikuojamas lengvai ir nesudėtingai, t. y. nepasitelkiant kažkokių ypatingų/sofistikuotų priemonių ar metodų/būdų.[18] Matome, kad skirtingai nuo ADTAĮ ir direktyvos 95/46/EB, čia asmens duomenų kriterijumi nurodoma tik galimybė identifikuoti konkretų asmenį pagal tam tikrą turimą informaciją. Nors šioje sąvokoje nėra minima tiesioginio ar netiesioginio asmens nustatymo galimybė, tačiau, N. Točickienės teigimu, pagal šią sąvoką „identifikuojamas fizinis asmuo yra tas, kurio tapatybė gali būti nustatyta tiesiogiai ir netiesiogiai, ypač pasinaudojus nurodytu asmens identifikavimo kodu arba vienu ar keliais to asmens fizinei, fiziologinei, protinei, ekonominei, kultūrinei ar socialinei tapatybei būdingais veiksniais“[19]. Manytume, kad ši sąvoka yra pakankamai siaura, nes pateikė neišsamų visų požymių asmeniui

[15] Lietuvos vyriausiojo administracinio tesimo 2010 m. vasario 1 d. nutartis administracinėje byloje Nr. A-444-270/2010; Lietuvos vyriausiojo administracinio tesimo 2011 m. gruodžio 16 d. nutartis administracinėje byloje Nr. N^{62}-2266/2011.
[16] Civilka M. *Asmens duomenų apsaugos teisinis reguliavimas interneto kontekste* [interaktyvus] [žiūrėta 2013-10-20]. <http://media.search.lt/ GetFile.php?OID=92932&FID=269994>.
[17] Civilka M., *supra* note 1 [žiūrėta 2013-10-20].
[18] *Ibid.*
[19] Točickienė N., *supra* note 4, p. 116.

nustatyti sąrašą ir nenurodė kitų duomenų (ne identifikatorių), kurie taip pat gali padėti nustatyti konkretų asmenį.

Plačiau apie asmens duomenų apsaugos teisinį reguliavimą kalbama sekančioje darbo dalyje.

Siekdami apibendrinti šioje dalyje pateiktą informaciją galime teigti, kad asmens duomenų apsaugos, kaip instituto vystymasis buvo sąlygotas visuomenės modernizacijos ir globalaus pasaulio raidos tendencijų. Akivaizdu, kad nuolatinis informacinių technologijų progresas ir vis didėjantis jų skverbimasis į asmeninį žmonių gyvenimą paskatino valstybes imtis priemonių apsaugoti asmenų teisę į privatų gyvenimą ir užtikrinti jų asmens duomenų apsaugą teisinio reguliavimo priemonėmis. Tokios priemonės buvo nustatytos Europos Sąjungos kompetentingoms institucijoms priėmus direktyvą 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo reguliavimo, kur pirmą kartą buvo imtasi priemonių Europos Sąjungos mastu sureguliuoti asmens duomenų apsaugos visuomeninius santykius ir nustatant aiškią kryptį tolimesniam tokių santykių reguliavimo vystymui.

2. EUROPOS SĄJUNGOS IR NACIONALINIS TEISINIS REGULIAVIMAS ASMENS DUOMENŲ APSAUGOS SRITYJE

Pirmojoje darbo dalyje apžvelgėme asmens duomenų apsaugos formavimosi priežastis, visuomeninius santykius, kurie sudarė sąlygas asmens duomenų apsaugos reguliavimo būtinumui bei išsiaiškinome asmens duomenų sąvokos struktūrą ir elementus. Kadangi toliau pasirinkta tema nagrinėjama žvelgiant formaliuoju aspektu, manytume, svarbu apžvelgti Europos Sąjungos teisinio reguliavimo ypatumus asmens duomenų apsaugos srityje ir tokio reguliavimo santykį su nacionalinės teisės normomis, analizuojant svarbiausius asmens duomenų apsaugą reglamentuojančius teisės aktus.

2.1. Asmens duomenų apsaugos reguliavimas Europos Sąjungoje

Kaip matyti ankstesnėje darbo dalyje, Europos Sąjungos mastu asmens duomenų apsaugos reguliavimas yra nustatytas pakankamai išsamiai ir aiškiai. Atsižvelgdamos į tokį Europos Sąjungos imperatyvų reikalavimą atkreipti dėmesį į šią problemą ir matydamos kylančias grėsmes asmens duomenų apsaugos srityje, dauguma valstybių ėmėsi reguliuoti visuomeninius santykius asmens duomenų apsaugos srityje nacionaliniu mastu.

Kaip jau buvo minėta, Europos Sąjungoje yra keletas teisės aktų, reguliuojančių asmens duomenų apsaugos klausimus, tačiau svarbiausiu laikytina direktyva 95/46/EB. Šis dokumentas atvertė naują puslapį asmens duomenų apsaugos istorijoje, padarė didelę įtaką kitų valstybių įstatymų leidybai, detalizavo bei naujai apibrėžė asmens duomenų apsaugos principus. Šiuo metu direktyva yra solidžiausias bei išsamiausias asmens duomenų apsaugą užtikrinantis dokumentas Europos Sąjungoje.

Išskirtinė šios direktyvos savybė yra tai, kad ji reguliuoja santykius ne tik Europos Sąjungos viduje, bet nustato elgesio taisykles ir trečiosioms šalims, tokioms kaip Norvegija, Lichtenšteinas ar Islandija, kurios prie Europos ekonominės erdvės prisijungė 1992 m. Šioje direktyvoje yra nustatytas draudimas perduoti asmens duomenis trečiosioms šalims. Toks perdavimas yra galimas tik tuomet, jei trečioji šalis užtikrina atitinkamą perduodamų asmens duomenų apsaugos lygį, kuris privalo atitikti esantį Europos Sąjungos narėse. Tačiau tolygaus apsaugos lygio samprata direktyvoje nėra apibrėžta. Be to, pats apsaugos lygis trečiosiose valstybėse yra skirtingas. Asmens duomenų apsaugos lygio tolygumą kiekvienu konkrečiu atveju vertina Europos Komisija, atsižvelgdama į visas su asmens duomenų tvarkymu susijusias aplinkybes, o ypač į asmens duomenų prigimtį,

tvarkymo tikslą, trukmę, asmens duomenų kilmės valstybę ir paskirties valstybę, teisės normas bei saugumo priemones, galiojančias trečiojoje valstybėje. Remiantis direktyvos nuostatomis sudaryta darbo grupė pasiūlė, vertinant apsaugos tolygumo lygį, atsižvelgti taip pat į teisės aktų, reglamentuojančių asmens duomenų apsaugą, įgyvendinimo priemones trečiojoje valstybėje.[20] Esant tokiam reguliavimui, ir norėdamos gauti asmens duomenis, trečiosios valstybės turėjo suderinti savo teisinį asmens duomenų apsaugos reglamentavimą su Europos Sąjungos teise tam, kad jų asmens duomenų apsaugos lygis atitiktų Europos Sąjungos lygį.

Direktyva iškėlė du pagrindinius tikslus:

- apsaugoti Žmogaus laisves ir pagrindines teises, ypač susijusias su asmens privačiu gyvenimu tvarkant asmens duomenis;
- nevaržyti ir nedrausti laisvo asmens duomenų judėjimo tarp valstybių narių dėl priežasčių, susijusių su asmens duomenų apsauga.

N Točickienės teigimu, „šių tikslų įgyvendinimas, direktyvos kūrėjų nuomone, galėtų būti pasiektas, suvienodinant privataus gyvenimo apsaugos, tvarkant asmens duomenis, lygį visose valstybėse narėse“[21]. Kaip matome, „iš vienos pusės direktyva siekia apsaugoti fizinių asmenų pagrindines teises bei laisves tvarkant asmens duomenis, tačiau iš kitos pusės, nevaržo ir nedraudžia laisvo asmens duomenų judėjimo tarp valstybių narių“[22].

M. Civilka pažymi, kad direktyva palieka laisvę valstybėms narėms pačioms apsispręsti dėl jos reguliavimo mąsto perkėlimo į nacionalinę teisę. Direktyvos ketvirto straipsnio pirmojoje dalyje sakoma, jog: „kiekviena valstybė narė taiko nacionalines nuostatas, kurias ji priima pagal šią direktyvą, kai tvarkomi asmens duomenys“. A, b ir c punktuose išdėstomos sąlygos, kuriomis remiantis minėtasis straipsnis galioja. Duomenų valdytojas turi vadovautis tos šalies teisės aktais, kurios teritorijoje jis veikia nepriklausomai nuo to, ar jo filialai yra vienoje valstybėje narėje, ar keliose valstybėse narėse, ar jis tik naudojasi valstybės narės techniniais resursais, siekdamas vykdyti operacijas su asmens duomenimis.[23]

Kalbant apie šią direktyvą, būtina paminėti 29 straipsnio darbo grupę[24], kaip pirmą praktinę direktyvos sukurto mechanizmo išraišką. Darbo grupės narių veikla yra nepriklausoma ir konsultacinio pobūdžio. Vertinant darbo grupės veiklą galima teigti, kad ji yra išties sėkminga. Tai

[20] Točickienė N., *supra* note 4, p. 117.
[21] *Ibid.*, p. 116.
[22] Kiškis M., *et. al. Teisės informatika ir informatikos teisė*. Vilnius: Mykolo Romerio universitetas, 2006., p. 120
[23] Civilka M., *supra* note 1.
[24] 29 straipsnio darbo grupė buvo įkurta 1996 m. vadovaujantis Direktyvos 95/46/EB 29 straipsniu, siekiant harmonizuoti Europos Sąjungos teisę asmens duomenų apsaugos srityje. Tai nepriklausomas Europos patariamasis organas duomenų apsaugos ir privatumo klausimais.

aiškiai matyti iš to, kaip vystėsi Europos Sąjungos teisinis reguliavimas asmens duomenų apsaugos srityje. Reikėtų pažymėti, kad plečiantis Europos Sąjungai, plečiasi ir šios darbo grupės veiklos sritis, nes būtina suderinti Europos Sąjungos ir naujų valstybių narių teisines sistemas ir pritaikyti jas prie direktyvos nuostatų. Darbo grupę sudaro kiekvienos valstybės narės paskirtos priežiūros institucijos ar institucijų atstovas, Bendrijos institucijoms ir organams įsteigtos valdžios institucijos ar institucijų atstovas ir Europos Komisijos atstovas. Lietuvai šioje Darbo grupėje atstovauja Valstybinės duomenų apsaugos inspekcijos atstovai.

Siekiant suvokti Europos Sąjungos asmens duomenų apsaugos mechanizmą, reikia apžvelgti taip vadinamus „trečiosios kartos“ teisės aktus (sui generis – *aut. pastaba)* šioje srityje. Internetui vis labiau skverbiantis į visuomeninį mūsų gyvenimą, jam keičiant ekonominio ir politinio bendradarbiavimo sąlygas, atsirado būtinybė teisiškai sureguliuoti elektroninių ryšių srityje atsirandančius teisinius santykius. Technologinio progreso pateikti iššūkiai suformavo atitinkamus socialinius lūkesčius. Atsižvelgdama į tai, Europos Komisija parengė pranešimą Tarybai bei Europos Parlamentui dėl naujos kartos interneto bei prioritetinių veiksmų pereinant prie naujo interneto protokolo IPv6 bei 2002 m. liepos 12 d., priėmė direktyvą (2002/58/EB) dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje, pakeitusią 1997 m. direktyvą 97/66/EB dėl asmens duomenų apdorojimo ir privatumo apsaugos telekomunikacijų sektoriuje ir papildančią direktyvos 95/46/ES reguliavimo mastą. Ši direktyva papildo jau esamą Europos Sąjungos asmens duomenų apsaugos mechanizmą ir sureguliuoja asmens duomenų tvarkymo procesus elektroninių ryšių srityje.

Direktyva įpareigoja valstybes nares užtikrinti per viešųjų ryšių tinklą ir viešai teikiamas elektroninių ryšių paslaugas pranešimų ir su jais susijusių tinklo srauto duomenų konfidencialumą. Valstybės narės turi priimti teisės aktus, draudžiančius pasiklausyti, slapta prisijungti, išsaugoti ar kitaip perimti bei kontroliuoti pranešimus ir su jais susijusius tinklo srauto duomenis, išskyrus atvejus, jei tai yra būtina, valstybės saugumui ir gynybai, viešajai tvarkai užtikrinti, taip pat užkardyti kriminalinius veiksmus ar neteisėtų elektroninių ryšių sistemų naudojimą.

Viena iš svarbiausių duomenų apsaugos užtikrinimo problemų yra duomenų saugojimo infrastruktūros sukūrimas. Be abejo, tam yra būtinas ir aiškus teisinis reguliavimas. Sureguliuoti tokius procesus Europos Sąjungos mastu pabandyta Europos Parlamentui ir Tarybai priėmus direktyvą (2006/24/EB) dėl duomenų, generuojamų arba tvarkomų teikiant viešai prieinamas elektroninių ryšių paslaugas arba viešuosius ryšių tinklus, saugojimo. Ja buvo nustatytos duomenų saugojimo taisyklės, siekiant skubiai spręsti saugumo problemas, išryškėjusias po didelio masto teroristinių išpuolių 2004 m. Madride ir 2005 m. Londone. Direktyva nėra tiesiogiai taikoma

valstybėse narėse, tačiau nustato bendrus tikslus, kurių šios turinčios siekti, kad būtų suderinti Europos Sąjungos institucijų sprendimai ir nacionalinės teisės numatytas reguliavimas.

Direktyva atskleidė trapią ribą tarp asmens privatumo ir viešojo intereso. Informacinėje visuomenėje, siekiant užtikrinti jos saugumą, būtina peržiūrėti asmens privatumo sampratą ir kad teisė į privatų gyvenimą nėra absoliuti, kai kalbama apie tokias grėsmes, kaip terorizmas ar organizuotas nusikalstamumas. Žinoma, tam yra būtina nustatyti aiškias ribas ir sukurti tokius teisinius įrankius, kurių pagalba būtų pasiekti maksimalūs tikslai su kaip įmanoma mažesniais asmens privatumo suvaržymais. Direktyva parodė, kad valstybės kišimasis į piliečių gyvenimą yra neišvengiamas ir kad išlaikyti pusiausvyrą tarp privataus gyvenimo neliečiamumo ir efektyvaus valstybės funkcionavimo tampa vis sudėtingiau. Plačiau apie šią direktyvą kalbama kitoje darbo dalyje.

Kaip vieną svarbiausių būdų reguliuojant asmens duomenų apsaugos klausimus, reikėtų paminėti Ministrų komiteto rekomendacijas valstybėms narėms, kuriose pasisakoma dėl tam tikrų aktualių problemų ir kokiu būdu tos problemos galėtų būti sprendžiamos. Tam tikru teisės aktu sukurtas reguliavimas ne visuomet yra vienodai suprantamas valstybėse narėse ir sukelia taikymo problemų, be to, kaip minėta ankstesnėje dalyje, informacinės technologijos vystosi taip sparčiai, kad teisinis reguliavimas būna pasenęs jau priėmus teisės aktą. Galime teigti, kad taip nutiko ir su direktyva (95/46/EB) dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo. Nors šios direktyvos priėmimas buvo sąlygotas spartaus technologinio progreso ir su tuo susijusio asmens duomenų apsaugos mechanizmo būtinumo, tačiau iškart priėmus šią direktyvą, tapo reikalingu tam tikrus procesus reguliuoti išsamiau. Kompetentingos Europos Sąjungos institucijos priėmė rekomendacijas, kuriomis elektroninių ryšių tinklų naudotojams ir tiekėjams bandyta pagelbėti nustatyti pagrindinius privatumo užtikrinimo principus. Šiuo požiūriu svarbiausia yra Ministrų komiteto rekomendacija Nr. R (99). Šia rekomendacija penkioms valstybėms narėms buvo nustatyti duomenų apsaugos principai internete. Be to, joje nurodomos priemonės, mažinančios trečiųjų asmenų galimybę prieiti prie interneto naudotojo asmens duomenų bei bendrosios saugumo priemonės interneto naudotojams. Taip pat atkreipiamas dėmesys į dalinio anonimiškumo išlaikymą, kodavimo priemones, slapyvardžių naudojimą, tinkamą paslaugų teikėjo pasirinkimą ir kt. Rekomendacijoje interneto tiekėjams nurodomos jų pareigos vartotojų atžvilgiu asmens duomenų apsaugos aspektu, nurodomi paslaugų tiekėjo darbo su tvarkomais asmens duomenimis principai ir ypatumai. Rekomendacijoje pabrėžiama asmens pareiga pačiam pasirūpinti savo asmens duomenų saugumu. Pažymėtina, kad rekomendacija surašyta labai apibendrintai ir jai

trūksta konkretumo, tačiau manytume, kad tuo buvo siekiama universalesnės rekomendacijos formuluočių taikymo galimybės.

Dar viena aktuali rekomendacija asmens duomenų apsaugos srityje yra Ministrų komiteto rekomendacija Nr. R (95). Šioje rekomendacijoje keturioms valstybėms narėms yra teikiamos rekomendacijos dėl automatizuoto duomenų tvarkymo telekomunikacijų ypatumų, pažymima tokio tvarkymo nauda, pateikiamos galimos grėsmių asmens duomenų saugumui tvarkant asmens duomenis automatizuotai. Čia pateikti duomenų tvarkymo principai taikomi elektroninių ryšių operatoriams ir paslaugų tiekėjams, kurių veikla susijusi su asmens duomenų tvarkymu. Reikėtų pažymėti, kad rekomendacijoje pateikiami jau 1981 m. Europos Tarybos konvencijoje dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu ir kituose Europos Sąjungos teisės aktuose nustatyti privatumo ir asmens duomenų apsaugos principai, tačiau jie apibrėžiami žvelgiant per telekomunikacijų prizmę.

Vertinant Ministrų komiteto rekomendacijas valstybėms narėms pagal jų paskirtį, galima teigti, kad jomis taisomos Europos teisinio reglamentavimo taikymo spragos ir šalinamos skirtingo interpretavimo galimybės. Svarbu pažymėti, kad rekomendacijos nėra imperatyvaus pobūdžio dokumentai, tačiau tinkamas ir savalaikis rekomendacijų formulavimas ir pateikimas suteikia galimybę Europos Sąjungos kompetentingoms institucijoms ar jos piliečiams išvengti asmens duomenų apsaugos pažeidimų.

Apibendrinant galime teigti, kad priėmus direktyvą 95/46/EB Europos Sąjunga žengė didelį žingsnį asmens duomenų apsaugos reguliavimo srityje. Asmens duomenų apsaugai tapus viena iš prioritetinių sričių buvo priimti kiti teisės aktais, kuriais buvo bandoma žengti koja kojon su vis spartėjančia informacinių technologijų raida. Tačiau apmaudu, kad iš pažiūros modernūs svarstomi teisinio reguliavimo instrumentai neretai juos priėmus pasirodydavo esą atgyvenę ir jų reguliavimo sritis neapimdavo visų aktualių asmens duomenų apsaugos aspektų. Taip nutiko ir su direktyva 95/46/EB, nors ji laikyta pažangiausiu to meto asmens duomenų apsaugą reguliuojančiu teisės aktu.

2.2. Asmens duomenų apsaugos reguliavimas Lietuvoje

Išnagrinėję Europos Sąjungos teisinio reguliavimo asmens duomenų apsaugos srityje ypatumus, šioje dalyje apžvelgsime asmens duomenų apsaugos vystymosi raidą, problemas ir tendencijas Lietuvoje.

Lietuvai įstojus į Europos Sąjungą, pastarosios teisinė sistema tapo sudedamąja Lietuvos teisinės sistemos dalimi. Tokiu būdu vienu iš pagrindinių uždavinių tapo Europos Sąjungos teisės

aktų inkorporavimas į nacionalinę teisę. Šios srities derinimas buvo numatytas net dvejose derybinėse pozicijose: „*Laisvė teikti paslaugas*“ ir „*Teisingumo ir vidaus reikalai*“.[25] Stojimo į Europos Sąjungą sutartis įsigaliojo 2004 m. gegužės 1 d. Šios sutarties IX priede yra pateiktos priemonės ir laikinos išimtys dėl Bendrijos teisės įgyvendinimo. Pažymėtina, kad dėl asmens duomenų apsaugos ir telekomunikacijų srities jokių išimčių numatyta nebuvo. Tai parodo šio klausimo aktualumą ir Europos Sąjungos požiūrį į šių nuostatų perkėlimą į nacionalinę teisę. Visi Europos Sąjungos teisės aktai asmens duomenų apsaugos ir elektroninių ryšių srityse turėjo būti perkelti į nacionalinę teisę iki 2004 m. gegužės 1 d. Tokiu būdu asmens duomenų apsaugos klausimai elektroninių ryšių srityje buvo sureguliuoti priėmus Elektroninių ryšių įstatymą ir Asmens duomenų teisinės apsaugos įstatymo pakeitimo įstatymą, kur jis išdėstytas nauja redakcija.

Reikėtų pažymėti, kad duomenų apsaugos teisinis reguliavimas Lietuvoje pradėtas dar 1996 m. priėmus Asmens duomenų teisinės apsaugos įstatymą, kurį sudarė tik 14 straipsnių, nustatančių kai kuriuos bendruosius principus dėl duomenų tvarkymo ir nuostatas dėl duomenų subjektų teisių. Šiame įstatyme trūko teisėto tvarkymo kriterijų apibrėžimo bei sąžiningo tvarkymo principų. Asmens duomenų teisinės apsaugos įstatymas iš esmės buvo peržiūrėtas 2000 m. ir praplėstas iki 29 straipsnių. To tikslas buvo įgyvendinti direktyvą 95/46/EB ir 1981 m. Europos Tarybos konvenciją dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu. Taigi, ADTAĮ 3 straipsnis buvo papildytas sąžiningo tvarkymo principais, kurie buvo įtvirtinti minėtoje konvencijoje ir direktyvoje, o 5 straipsnis buvo papildytas bendrųjų ir ypatingų asmens duomenų teisėto tvarkymo kriterijais, kurie įtvirtinti direktyvos 7 ir 8 straipsniuose. Be to, ADTAĮ buvo papildytas detaliomis nuostatomis dėl priežiūros institucijos kompetencijos duomenų apsaugos srityje.

Trečią kartą ADTAĮ buvo keičiamas 2004 m. balandžio 13 d. ir šie pakeitimai buvo susiję su Lietuvos stojimu į Europos Sąjungą 2004 m. gegužės mėn. Čia įstatymas buvo papildytas detaliais išankstinės patikros nuostatais (22 straipsnis). Be to, Valstybinė duomenų apsaugos inspekcija buvo įvardinta kaip priežiūros institucija asmens duomenų apsaugos klausimais ir buvo pakeistas jos statusas – ji tapo atskaitinga ne Valdymo reformų ir savivaldybių reikalų ministerijai, o tiesiogiai Vyriausybei. Šiais pakeitimais į ADTAĮ buvo įtrauktos ir tik Lietuvai būdingos nuostatos – 16 straipsnis, reglamentuojantis asmens duomenų tvarkymą asmens mokumui įvertinti ir įsiskolinimui valdyti.

Reikėtų paminėti, kad 1998 m. buvo papildytas Administracinių teisės pažeidimų kodeksas, kur nustatyta administracinė atsakomybė už neteisėtą asmens duomenų tvarkymą, kliudymą

[25] Točickienė N., *supra* note 4, p. 118.

asmeniui susipažinti su savo duomenimis. 2000 m. priimtas Baudžiamasis kodeksas įtvirtino baudžiamąją atsakomybę už neteisėtą informacijos apie privatų gyvenimą rinkimą, atskleidimą ir panaudojimą. 2001 m. Lietuva ratifikavo Europos Tarybos konvenciją dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108). Išsami informacija apie šalis, ratifikavusias šią konvenciją pateikiama 1 priede.

2001 m. Europos Komisija savo nuolatiniame pranešime apie Lietuvos pasirengimą narystei Europos Sąjungoje pažymėjo, kad Lietuva padarė didelę pažangą duomenų apsaugos srityje, kad Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas iš esmės atitinka direktyvą 95/46/EB, tačiau atkreipė dėmesį į tai, kad kai kurios įstatymo nuostatos turi būti tikslinamos.

Siekiant suderinti Lietuvos Respublikos teisės aktus su direktyvos 97/66/EB nuostatomis buvo pataisytas tuo metu santykius elektroninių ryšių srityje reglamentavęs Telekomunikacijų įstatymas.

Kaip minėta, Lietuvoje duomenų apsaugos priežiūrą vykdo Valstybinė duomenų apsaugos inspekcija, kurios „paskirtis – prižiūrėti duomenų valdytojų veiklą tvarkant asmens duomenis, kontroliuoti asmens duomenų tvarkymo teisėtumą, užkirsti kelią duomenų tvarkymo pažeidimams, užtikrinti duomenų subjekto teisių apsaugą“[26]. Valstybinė duomenų apsaugos inspekcija atsakinga už ADTAĮ (išskyrus 8 ir 35^1 straipsnius), Lietuvos Respublikos asmens duomenų, tvarkomų vykdant policijos ir teisminį bendradarbiavimą baudžiamosiose bylose, teisinės apsaugos įstatymo, Lietuvos Respublikos elektroninių ryšių įstatymo nuostatų, reglamentuojančių asmens duomenų tvarkymą ir privatumo apsaugą. Lietuvos Respublikos Vyriausybė 2004 m. gruodžio 6 d. nutarimo Nr. 1593 „Dėl įgaliojimų suteikimo įgyvendinant Lietuvos Respublikos elektroninių ryšių įstatymą“ 4 punktu įgaliojo Valstybinę duomenų apsaugos inspekciją „vykdyti elektroninių ryšių paslaugų naudotojų privataus gyvenimo neliečiamumo užtikrinimo kontrolę“[27].

2009 m. kovo 15 d. įsigaliojus Elektroninių ryšių įstatymo pakeitimui buvo praplėsta Valstybinės duomenų apsaugos inspekcijos kompetencija, kadangi Elektroninių ryšių įstatymo devintojo skirsnio nuostatos jau taikomos ne tik fiziniams, bet ir juridiniams asmenims. Atsižvelgiant į tai, išsiplėtė Valstybinės duomenų apsaugos inspekcijos atliekamų duomenų tvarkymo ir privatumo apsaugos tikrinimų, prašymų ir skundų nagrinėjimo bei konsultacijų teikimo elektroninių ryšių srityje apimtys. O atsižvelgiant į Elektroninių ryšių įstatymo 65 straipsnio 2 dalį ir

[26] Lietuvos Respublikos Vyriausybės 2011 m. rugpjūčio 24 d. nutarimas Nr. 987 „Dėl Lietuvos Respublikos Vyriausybės 2001 m. rugsėjo 25 d. nutarimo Nr. 1156 „Dėl Valstybinės duomenų apsaugos inspekcijos struktūrinės reformos, įgaliojimų suteikimo, Valstybinės duomenų apsaugos inspekcijos nuostatų patvirtinimo ir su tuo susijusių Lietuvos Respublikos Vyriausybės nutarimų dalinio pakeitimo“ pakeitimo“. *Valstybės žinios*. 2011, Nr. 107-5058.
[27] Lietuvos Respublikos Vyriausybės 2004 m. gruodžio 6 d. nutarimas Nr. 1593 „Dėl įgaliojimų suteikimo įgyvendinant Lietuvos Respublikos elektroninių ryšių įstatymą“. *Valstybės žinios*. 2004, Nr. 177-6569.

66 straipsnio 4 dalį, atitinkamai padidėjo ir jos veiklos apimtys prižiūrint Elektroninių ryšių įstatymo 1 priede išvardintų duomenų saugojimo ir naudojimo teisėtumą.

Lietuvos Respublikos Vyriausybės 2009 m. liepos 22 d. nutarimu Nr. 788 „Dėl Lietuvos Respublikos Vyriausybės 2004 m. gruodžio 6 d. nutarimo Nr. 1593 „Dėl įgaliojimų suteikimo įgyvendinant Lietuvos Respublikos elektroninių ryšių įstatymą „pakeitimo“ Valstybinę duomenų apsaugos inspekciją įgaliojo „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“[28].

Matome, kad esminiai pokyčiai asmens duomenų apsaugos srityje Lietuvoje prasidėjo nuo jos įstojimo į Europos Sąjungą. Iki tol asmens duomenų apsauga Lietuvoje buvo reguliuojama paviršutiniškai, todėl tuo metu galiojantys teisės aktai neužtikrino visapusiškos asmens duomenų apsaugos. Vienu svarbiausių teisės aktų, kuris moderniomis priemonėmis ėmėsi reguliuoti aptariamus visuomeninius santykius, laikytina Asmens duomenų teisinės apsaugos įstatymo nauja redakcija. Nagrinėjant tiek šio įstatymo, tiek kitų šį įstatymą įgyvendinančių teisės aktų nuostatas matyti, kad juose atsispindi Europos Sąjungos asmens duomenų apsaugos reguliaciniai mechanizmai ir jos nustatytos kryptys.

[28] S*upra* note 27.

3. ASMENS DUOMENŲ APSAUGA ELEKTRONINIŲ RYŠIŲ SRITYJE

3.1.Bendrieji asmens duomenų tvarkymo aspektai

Kadangi pasirinkta darbo tema nagrinėjama žvelgiant per elektroninių ryšių prizmę, tikslinga išnagrinėti asmens duomenų apsaugos reguliavimo santykį su Elektroninių ryšių įstatymo nuostatomis ir su juo susijusiais Europos Sąjungos teisės aktais tiek, kiek tai apima asmens duomenų tvarkymo ypatumus elektroninių ryšių srityje.

Prieš įsigaliojant naujai bendrai Europos Sąjungos elektroninių ryšių reguliavimo sistemai, duomenų apsauga šioje srityje buvo reguliuojama Europos Parlamento ir Tarybos direktyva (97/66/EB) dėl asmens duomenų tvarkymo ir privatumo apsaugos telekomunikacijų sektoriuje. Šioje direktyvoje buvo sukonkretinti direktyvoje 95/46/EB nustatyti principai, kurie direktyvoje 97/66/EB jau buvo pateikiami kaip elgesio taisyklės taikomos telekomunikacijų srityje. 1999 m. buvo peržiūrėtos telekomunikacijų sritį reglamentuojančios direktyvos[29], siekiant optimizuoti šios srities valdymą. 2002 m. buvo priimta nauja elektroninių ryšių reguliavimo sistema, kuri apėmė Pagrindų direktyvą (2002/21/EB), Prieigos direktyvą (2002/19/EB), Leidimų direktyvą (2002/20/EB), Universaliųjų paslaugų ir paslaugų gavėjų teisių direktyvą (2002/22/EB) ir Konkurencijos direktyvą (2002/77/EB).[30] Po atliktos apžiūros direktyvos 97/66/EB nuostatos buvo peržiūrėtos ir pakoreguotos į to meto informacinės pažangos tendencijas. Todėl Europos Parlamentas ir Taryba priėmė direktyvą 2002/58/EB kaip naujos bendros reguliavimo sistemos sudėtinę dalį.

Direktyvos 2002/58/EB 3 straipsnyje pasakyta, kad ji taikoma ,,asmens duomenims tvarkyti teikiant Bendrijoje viešai prieinamas elektroninių ryšių paslaugas viešaisiais ryšių tinklais"[31]. Pats terminas ,,elektroninių ryšių paslauga" yra apibrėžtas Pagrindų direktyvoje 2002/21/EB kaip ,,paslauga, paprastai teikiama už atlygį, kuri visa ar didžiąja dalimi susideda iš signalų perdavimo elektroninių ryšių tinklais, įskaitant telekomunikacijų paslaugas ir perdavimo paslaugas tinklais, naudojamais transliavimui, išskyrus elektroniniais ryšių tinklais ir paslaugomis perduodamo turinio teikimo ar redakcinės jo kontrolės paslaugas; į šią paslaugą neįeina informacinės visuomenės paslaugos, apibrėžtos Direktyvos 98/34/EB 1 straipsnyje, kurios visos ar didžiąja dalimi susideda iš signalų perdavimo elektroninių ryšių tinklais".

[29] Taip vadinama "Peržiūra 99"
[30] Duomenų apsauga telekomunikacijų sektoriuje [interaktyvus] [žiūrėta 2013-11-11]. <http://www.ada.lt/images/cms/File/Duomenu%20apsauga%20 telekomunikaciju%20sektoriuje%281%29>.
[31] Europos Parlamento Ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių). [2002] OL L 201/37.

Svarbu pažymėti, kad direktyva 2002/58/EB apima tik duomenų tvarkymą teikiant Bendrijoje viešai prieinamas elektroninių ryšių paslaugas viešaisiais ryšių tinklais, t. y. ji netaikoma tiems duomenims, kurie tvarkomi uždarose vartotojų grupėse, privačiuose tinkluose, išskyrus tuos atvejus, kai tokie tinklai turi prieigą prie viešųjų ryšių tinklų.

Pagal savo pobūdį direktyva 2002/58/EB yra suvienodinimo teisės aktas ir vadovaujasi Europos Bendrijų Sutarties vidaus rinkos nuostatomis, todėl direktyvos tikslai yra susiję su laisvo duomenų, įrangos ir paslaugų judėjimo užtikrinimu. Direktyvos 1 straipsnyje sakoma, kad jos tikslai yra ,,užtikrinti vienodą pagrindinių teisių ir laisvių apsaugos lygį, ypač teisę į privatumą, susijusį su asmens duomenų tvarkymu elektroninių ryšių sektoriuje“ ir „užtikrinti laisvą tokių duomenų judėjimą ir laisvą elektroninių ryšių įrangos ir paslaugų judėjimą Bendrijoje“[32].

Kaip buvo minėta ankstesnėse darbo dalyse, Europos Sąjungos teisės aktai, susiję su asmens duomenų apsauga ir elektroninių ryšių reguliavimu, į nacionalinę teisę buvo perkelti Lietuvoje priėmus Asmens duomenų teisinės apsaugos įstatymo pakeitimo įstatymą ir Elektroninių ryšių įstatymą.

ADTAĮ 2 straipsnio 4 dalis duomenų tvarkymą apibrėžia kaip „bet kurį su asmens duomenimis atliekamą veiksmą: rinkimą, užrašymą, kaupimą, saugojimą, klasifikavimą, grupavimą, jungimą, keitimą (papildymą ar taisymą), teikimą, paskelbimą, naudojimą, logine ir (arba) aritmetines operacijas, paiešką, skleidimą, naikinimą ar kitokį veiksmą arba veiksmų rinkinį“[33].

Direktyvos 95/46/EB 2 straipsnio b punktas nustato, kad asmens duomenų tvarkymas „reiškia bet kurią operaciją ar operacijų rinkinį, automatiniais 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“[34].

ADTAĮ pateiktas „duomenų tvarkymo“ sąvokos apibrėžimas, iš esmės, atitinka direktyvos 95/46/EB nustatytą apibrėžimą. Nors ADTAĮ įtvirtinti ne visi direktyvoje 95/46/EB sąvokos elementai („operacijų rinkinys“, „automatiniais arba neautomatiniais būdais“), tačiau jie nėra esminiai. Vadovaujantis abiem šiais teisės aktais, bet kokia su duomenimis atliekama operacija yra tvarkymas. Tai labai plati sąvoka ir nepriklauso nuo naudojamų metodų. Duomenų tvarkymas yra viena pagrindinių sąvokų, naudojamų ir ADTAĮ ir direktyvoje 95/46/EB. Svarbu pažymėti, kad

[32] *Supra* note 14.
[33] S*upra* note 13.
[34] *Supra* note 14.

kiekvienas duomenų tvarkymo veiksmas turi būti pagristas arba ADTAĮ, arba kito specialaus įstatymo nuostatomis.

Pagrindinius reikalavimus asmens duomenų tvarkymui nustato ADTAĮ 3 straipsnis, kuriame sakoma, kad „duomenys turi būti:

- renkami apibrėžtais ir teisėtais tikslais ir toliau nebūtų tvarkomi tikslais, nesuderinamais su nustatytaisiais prieš renkant asmens duomenis;
- tvarkomi tiksliai, sąžiningai ir teisėtai;
- tikslūs ir, jei reikia dėl asmens duomenų tvarkymo, nuolat atnaujinami; netikslūs ar neišsamūs duomenys turi būti ištaisyti, papildyti, sunaikinti arba sustabdytas jų tvarkymas;
- tapatūs, tinkami ir tik tokios apimties, kuri būtina jiems rinkti ir toliau tvarkyti;
- saugomi tokia forma, kad duomenų subjektų tapatybę būtų galima nustatyti ne ilgiau, negu to reikia tiems tikslams, dėl kurių šie duomenys buvo surinkti ir tvarkomi“[35].

Išvardinti duomenų tvarkymo reikalavimai atitinka direktyvos 95/46/EB 6 straipsnyje nustatytuosius, tačiau nuo 2011 m. rugsėjo 11 d. jie papildyti reikalavimu, kad duomenys turi būti „tvarkomi pagal šiame ir kituose atitinkamą veiklą reglamentuojančiuose įstatymuose nustatytus aiškius ir skaidrius asmens duomenų tvarkymo reikalavimus“. ADTAĮ nustatyti duomenų tvarkymo reikalavimai kyla iš normų, kurios iš pradžių buvo nustatytos Europos Tarybos konvencijos dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu 5 straipsnyje, kurias įtvirtino direktyvos 95/46/EB duomenų tvarkymo principai.

Kaip jau minėta, ADTAĮ nustato tik bendruosius asmens duomenų tvarkymo reikalavimus, o specialiuosius nustato kiti atitinkamas visuomeninio gyvenimo sritis reglamentuojantys įstatymai. Taip pagal ADTAĮ 15 straipsnį „asmens duomenys elektroninių ryšių srityje tvarkomi vadovaujantis Elektroninių ryšių įstatymu ir šiuo įstatymu“[36]. Nors ADTAĮ asmens duomenų apsaugą elektroninių ryšių srityje nukreipia į Elektroninių ryšių įstatymą, už kurio įgyvendinimą bendrai yra atsakinga Lietuvos Respublikos ryšių reguliavimo tarnyba, tačiau Valstybinės duomenų apsaugos inspekcijos kompetencija dėl duomenų apsaugos išlieka ir elektroninių ryšių srityje. Svarbu tai, kad nors Elektroninių ryšių įstatymas nenustato jokių duomenų apsaugos reikalavimų elektroninių ryšių srityje, tačiau bendrieji, išdėstyti ADTAĮ, yra taikomi, išskyrus, jei yra numatytos specialios išimtys.

Asmens duomenų tvarkymą Elektroninių ryšių įstatyme reglamentuoja 66 straipsnio nuostatos. Apie kiekvieną asmens duomenų tvarkymo atvejį elektroninių ryšių tiekėjui privalu

[35] *Op. cit.* 13.
[36] *Supra* note 13.

pranešti Valstybinei duomenų apsaugos inspekcijai. Juose asmens duomenis tvarkyti gali tik įgalioti asmenys ir tik tiek, kiek to reikia elektroninių ryšių tiekėjo tiesioginėms funkcijoms vykdyti.

Duomenų tvarkymas elektroninių ryšių srityje yra neatsiejamas su registrais ir informacinėmis sistemomis, nes būtent jose šie duomenys yra kaupiami. Specialus įstatymas tokioms duomenų kaupimo priemonėms yra Registrų įstatymas, kur *tvarkymas* apibrėžiamas kaip „bet kurie su registro duomenimis atliekami veiksmai: duomenų rinkimas, užrašymas, kaupimas, saugojimas, klasifikavimas, grupavimas, jungimas, keitimas (papildymas ar taisymas), teikimas, paskelbimas, naudojimas, loginės ir (ar) aritmetinės operacijos, duomenų paieška, naikinimas ir kiti veiksmai“[37]. Reikia pažymėti, kad jame taip pat nėra nustatyta bendrų reikalavimų asmens duomenų tvarkymui, kuriuos reglamentuoja ADTAĮ, tačiau tų santykių, kurių pastarojo reguliavimo sritis neapima, reglamentuoja būtent Registrų įstatymo nuostatos.

ADTAĮ 4 straipsnis nustato, kad „asmens duomenys saugomi ne ilgiau, negu to reikalauja duomenų tvarkymo tikslai. Kai asmens duomenys nebereikalingi jų tvarkymo tikslams, jie turi būti sunaikinami, išskyrus tuos, kurie įstatymų nustatytais atvejais turi būti perduoti valstybės archyvams“[38]. Tokiu būdu yra nukreipiama į Elektroninių ryšių įstatymą, kuris yra speciali norma asmens duomenų saugojimui elektroninių ryšių srityje. Elektroninių ryšių įstatymas nustato, kad sukaupti abonentų ar registruotų elektroninių ryšių paslaugų naudotojų srauto duomenys gali būti saugomi ne ilgiau kaip 6 mėnesius.

Viena pagrindinių kategorijų užtikrinant asmens duomenų apsaugą elektroninių ryšių srityje yra teisėtas asmens duomenų tvarkymas. Pagrindiniai asmens duomenų tvarkymo principai buvo nustatyti direktyvoje 95/46/EB, kurie vėliau sukonkretinti direktyva 97/66/EB, kur jau pateikiami kaip elgesio taisyklės, taikomos telekomunikacijų srityje. Lietuvoje asmens duomenų tvarkymas yra apibrėžtas ADTAĮ, tačiau jame nustatyti tik bendrieji asmens duomenų tvarkymo reikalavimai, o specialiuosius nustato kiti atitinkamas visuomeninio gyvenimo sritis reglamentuojantys įstatymai.

3.2. Direktyvos 2006/24/EB nuostatų įgyvendinimas

Nagrinėjant asmens duomenų apsaugos ypatumus elektroninių ryšių srityje tiek Europos Sąjungos, tiek nacionaliniu mastu, esminiu teisės aktu reikėtų laikyti direktyvą 2006/24/EB. Nors ši direktyva vertinama nevienareikšmiškai ir ją priėmus netilo diskusijos dėl jos tinkamo taikymo galimybių, tačiau šios direktyvos svarba yra sąlygota jos reguliuojamų visuomeninių santykių

[37] Lietuvos Respublikos registrų įstatymas. *Valstybės žinios*. 1996, Nr. 86-2043.
[38] *Op. cit.* 13.

ypatumų. Minėtos direktyvos nuostatos šiame darbe pabrėžiamos todėl, kad jos tiesiogiai susijusios su pasirinkta nagrinėjama tema. Būtent direktyvos 2006/24/EB nuostatomis grįstas nacionalinis teisinis reguliavimas elektroninių ryšių srityje turės būti papildomas, siekiant įpareigoti elektroninių ryšių tiekėjus registruoti išankstinio mokėjimo SIM korteles. Konkreti tokio registravimo galimybių analizė pateikta kitose darbo dalyse, tačiau šioje dalyje svarbu apibrėžti direktyvos 2006/24/EB taikymo ypatumus ir jos santykį su nacionaline teise.

Elektroninių ryšių teikėjai vykdydami savo veiklą tvarko asmens duomenis. Ši procedūra jiems būtina siekiant užtikrinti ryšio perdavimą, sąskaitų pateikimą, atsiskaitymus už tinklų sujungimą, rinkodaros vykdymą ir kitas su jų veikla susijusias funkcijas. Tokių būdu yra tvarkomi šie duomenys: ryšio šaltinis, paskirties vieta, data, laikas, trukmė ir tipas, taip pat vartotojo naudojama ryšio įranga ir, judriojo ryšio telefonijos atveju, įrangos vieta. Vadovaujantis direktyvos 2002/58/EB nuostatomis, tokie duomenys iš esmės turėtų būti sunaikinti arba pakeisti taip, kad taptų anoniminiais, kai tokių duomenų nereikia pačiam elektroninių ryšių teikėjui. Prieš įsigaliojant direktyvai 2006/24/EB, nacionalinės valdžios institucijos elektroninių ryšių teikėjų prašydavo suteikti prieigą prie tokių duomenų.

Europos Sąjungos mastu duomenų saugojimo ir naudojimo teisėsaugos tikslais klausimas pirmą kartą bandytas spręsti priėmus direktyvą 97/66/EB, kur valstybėms narėms buvo numatyta galimybė priimti tokias priemones, kurių reikėjo siekiant užtikrinti visuomenės saugumą, gynybą arba viešąją tvarką, taip pat valstybės ekonominę gerovę, jeigu veikla buvo siejama su valstybės saugumo reikalais, ir baudžiamuoju persekiojimu.

Vėliau ši nuostata buvo plėtojama direktyvoje 2002/58/EB, kur valstybėms narėms numatyta galimybė priimti būtinas priemones nukrypstant nuo ryšių konfidencialumo principo. Joje taip pat buvo numatyta galimybė atitinkamomis sąlygomis saugoti duomenis, suteikti prieigą prie jų ir juos naudoti teisėsaugos institucijų veiklai. Šios direktyvos 15 straipsnio 1 dalyje valstybėms narėms suteikta galimybė apriboti teises į privatumą ir pareigas, taip pat ribotą laikotarpį saugoti duomenis, jeigu toks ribojimas yra „būtina, tinkama ir adekvati demokratinės visuomenės priemonė, skirta apsaugoti nacionalinį saugumą (t. y. valstybės saugumą), gynybą, visuomenės saugumą, taip užkardant, tiriant ir nustatant baudžiamąsias veikas ar neteisėtą elektroninių ryšių sistemos naudojimą“[39].

Direktyvų 97/66/EB ir 2002/58/EB nuostatos dėl duomenų saugojimo kai kurioms valstybėms narėms sukėlė tam tikrų nepatogumų. Šių valstybių elektroninių ryšių teikėjai turėjo

[39] *Supra* note 31.

pirkti duomenų saugojimo įrangą ir papildomai įdarbinti darbuotojų duomenų paieškai teisėsaugos institucijoms atlikti. Reikėtų pažymėti, kad tokie direktyvų reikalavimai sąlygojo situaciją, kai elektroninių ryšių teikėjai savo verslo modelį ėmė orientuoti į išankstinio mokėjimo paslaugas, kur duomenų kaupti neprivaloma arba jų kaupiama mažiau, pradėjo taikyti didesnius paslaugų tarifus.

Todėl direktyva 2006/24/EB įpareigojo valstybių narių elektroninių ryšių paslaugų teikėjus saugoti srauto ir vietos nustatymo duomenis nuo šešių mėnesių iki dvejų metų sunkių nusikaltimų tyrimo, atskleidimo ir baudžiamojo persekiojimo tikslu. Svarbu pažymėti, kad nei direktyvoje 2002/58/EB, nei direktyvoje 2006/24/EB neapibrėžta „sunkaus nusikaltimo sąvoka“, todėl sunku atskirti priemones, kurių valstybės narės turėjo imtis, kad perkeltų direktyvoje 2006/24/EB nustatytus duomenų saugojimo įpareigojimus, ir bendrojo pobūdžio valstybių narių praktiką duomenų saugojimo srityje, kuri leidžiama direktyvos 2002/58/EB 15 straipsnio 1 dalimi.

Priėmus direktyvą 2006/24/EB, jos teisinis pagrindas buvo užginčytas Europos Teisingumo Teisme.[40] Tokio ginčo motyvas buvo, kad šios direktyvos pagrindinis tikslas buvo sunkių nusikaltimų tyrimas, atskleidimas ir baudžiamasis persekiojimas, o ne vidaus rinkos kūrimas ir veikimas, kaip nustatyta Europos bendrijos steigimo sutarties 95 straipsnyje, kuriuo grindžiama direktyva 2006/24/EB. Tačiau Teismas nusprendė, kad direktyva reglamentuoja operacijas, kurios nesusijusios su policijos ir teismų bendradarbiavimu baudžiamosiose bylose, ir kad ja nėra suderinamas nei kompetentingų nacionalinių teisėsaugos institucijų prieigos prie duomenų klausimas, nei šių duomenų naudojimo ir keitimosi jais šiose institucijose klausimas. Todėl jis priėjo prie išvados, kad direktyva iš esmės skirta atitinkamo vidaus rinkos sektoriaus operatorių veiklai. Atsižvelgdamas į tai, Teismas pripažino, kad direktyvos teisinis pagrindas tinkamas[41].

Siekiant užtikrinti efektyvų direktyvos 2006/24/EB nuostatų perkėlimą į nacionalinė teisę, pagal 29 straipsnį sukurta darbo grupė siūlė atsižvelgti į šias apsaugos priemones:

- „Tikslo nurodymas: duomenys turėtų būti saugojami tik konkretiems tikslams, todėl būtina tiksliai apibrėžti „sunkaus nusikaltimo sąvoką“. Tolesnis duomenų tvarkymas turėtų būti draudžiamas arba griežtai ribojamas konkrečiomis apsaugos priemonėmis.
- Leidimo naudotis duomenimis ribojimas: duomenys turėtų būti prieinami tik konkrečiai paskirtoms teisėsaugos institucijoms, kai to reikia direktyvoje minėtiems nusikaltimams tirti, atskleisti ir baudžiamosioms byloms kelti. Pageidautinas tokių institucijų sąrašo viešas skelbimas.

[40] Europos Sąjungos Teisingumo Teismo raidos ir veiklos 2009 m. ataskaita [interaktyvus]. 2010 [žiūrėta 2013-11-25]. <http://curia.europa.eu/jcms/upload/docs/application/pdf/2010-05/ra09_activite_cour_final_lt.pdf>.
[41] Byla C-301/06 *Airija prieš Parlamentą ir Tarybą* [2006] I-00593.

Duomenų paieška turėtų būti registruojama, o registracijos įrašai turėtų būti prieinami priežiūros institucijoms, kad jos galėtų veiksmingai vykdyti priežiūrą.

- Duomenų mažinimas: saugotinų duomenų turėtų būti kuo mažiau, o keisti duomenų sąrašą būtų galima tik tuomet, kai tai būtina.
- Duomenų paieška: direktyvoje minėtų nusikaltimų tyrimas, atskleidimas ir baudžiamosios bylos iškėlimas neturėtų reikšti plataus masto duomenų paieškos, grindžiamais saugomais duomenimis apie žmonių, kurie nėra teisėsaugos institucijų įtariami padarę nusikaltimą, keliavimo ir bendravimo būdus.
- Teisminis ir (arba) nepriklausomos institucijos vykdomas leidimo naudotis duomenimis tyrimas: leidimas naudotis duomenis turėtų būti patvirtinamas teisminių institucijų kiekvienu atveju, išskyrus šalis, kurių teisės aktais numatoma konkreti nepriklausomos instancijos patvirtinama galimybė naudotis duomenimis. Tam tikrais atvejais turėtų būti nurodyta, kokie būtent duomenys reikalingi konkrečiai nagrinėjamai bylai.
- Paslaugų teikėjų duomenų saugojimo tikslai: remiantis Duomenų saugojimo direktyva, viešųjų elektroninių ryšių ar tinklų paslaugų teikėjams neturi būti leista vien tik viešosios tvarkos tikslais saugomu duomenų tvarkyti kitais, ypač asmeniniais, tikslais.
- Sistemų atskyrimas: viešosios tvarkos tikslais saugomų duomenų sistemos turėtų būti atskirtos nuo verslo tikslais naudojamų sistemų.
- Saugumo priemonės: turėtų būti nustatyti minimalūs paslaugų teikėjų ir organizacinio saugumo priemonių standartai, kuriuose turėtų būti išsamiau apibrėžti bendrieji Duomenų saugojimo direktyvos reikalavimai“[42].

Valstybės narės direktyvą 2006/24/EB privalėjo perkelti iki 2007 m. rugsėjo 15 d., suteikiant galimybę iki 2009 m. kovo 15 d. atidėti direktyvos taikymą duomenų, susijusių su prieiga prie interneto, interneto telefonija ir interneto elektroniniu paštu, saugojimui. Pažymėtina, kad ne visos šalys direktyvos 2006/24/EB nuostatas laiku perkėlė į nacionalinę teisę. Kaip pavyzdį galima paminėti Europos Komisijos sprendimą prieš Švediją, kuriame Europos Teisingumo Teismas pripažino, kad per nustatytą terminą nepriėmusi Direktyvai 2006/24/EB įgyvendinti būtinų įstatymų ir kitų teisės aktų, Švedijos Karalystė neįvykdė įsipareigojimų pagal šią direktyvą[43]. Tokiu būdu

[42] Pagal 29 straipsnį įkurtos duomenų apsaugos darbo grupės nuomonė Nr. 3/2006 apie 2006 m. vasario 21 d. Tarybos priimtą Europos Parlamento ir Tarybos direktyvą 2006/24/EB dėl duomenų, generuojamų arba tvarkomų teikiant viešai prieinamas elektroninių ryšių paslaugas arba viešuosius ryšių tinklus, saugojimo ir iš dalies pakeičiančią Direktyvą 2002/58/EB [interaktyvus]. 2006 [žiūrėta 2013-12-01].

[43] Byla C-270/11, *Švedijos Karalystė prieš Europos Komisiją* [2013].

Švedijos Karalystė buvo įpareigota sumokėti Europos Komisijai į „Nuosavų Europos Sąjungos išteklių“ sąskaitą vienkartinę 3 mln. EUR sumą ir apmokėti bylinėjimosi išlaidas.

Remiantis Europos Komisijos ataskaita[44], Lietuva, kaip ir devynios kitos valstybės narės (Bulgarija, Estija, Airija, Graikija, Ispanija, Liuksemburgas, Vengrija, Nyderlandai, Suomija), nacionalinėje teisėje apibrėžė sunkaus nusikaltimo sąvoką, nurodydamos minimalią laisvės atėmimo bausmę, galimybę taikyti laisvės atėmimo bausmę arba nusikalstamų veikų, apibrėžtų kituose nacionaliniuose teisės aktuose, sąrašą. Aštuonios valstybės narės (Belgija, Danija, Prancūzija, Italija, Latvija, Lenkija, Slovakija, Slovėnija) reikalauja, kad duomenys būtų saugomi ne tik sunkių nusikaltimų, bet ir visų nusikalstamų veikų tyrimo, atskleidimo ir baudžiamojo persekiojimo tikslais, taip pat nusikaltimų prevencijos tikslais arba apskritai dėl nacionalinio arba valstybės ir (arba) visuomenės saugumo. Keturių valstybių narių (Kipro, Maltos, Portugalijos, Jungtinės Karalystės) teisės aktuose nurodyti „sunkūs nusikaltimai“ arba „sunkūs teisės pažeidimai“ nepateikiant jų apibrėžčių. Tikslesnė informacija pateikiama 2 priede.

Vertinant elektroninių ryšių teikėjams nustatytą reikalavimą saugoti duomenis, dvi valstybės narės (Suomija ir Jungtinė Karalystė) nereikalauja, kad jie saugotų duomenis. Tokia pozicija grindžiama teigimu, kad elektroninių ryšių teikėjų ir valstybės patiriamos sąnaudos yra didesnės nei siekiama nauda tiriant nusikalstamas veikas. Keturios valstybės narės (Latvija, Liuksemburgas, Nyderlandai, Lenkija) įvedė alternatyvias administracines tvarkas.

Direktyvos 2006/24/EB 4 straipsnyje pasakyta, kad „valstybės narės patvirtina priemones siekdamos užtikrinti, kad pagal šią direktyvą saugomi duomenys kompetentingoms nacionalinėms institucijoms būtų teikiami tik konkrečiais atvejais ir laikantis nacionalinės teisės. Atsižvelgiant į Europos Sąjungos teisės ar viešosios tarptautinės teisės ir visų pirma EŽTK, kaip ją aiškina Europos žmogaus teisių teismas, atitinkamas nuostatas, kiekviena valstybė narė, laikydamasi būtinumo ir proporcingumo reikalavimų, savo nacionalinėje teisėje nustato tvarką ir sąlygas, kurių turi būti laikomasi siekiant gauti prieigą prie saugomų duomenų.[45]“

Europos Komisijos ataskaitoje teigiama, kad visose valstybėse narėse prieigą prie saugomų duomenų turi nacionalinės policijos tarnybos ir, išskyrus bendrosios teisės jurisdikcijos šalis (Airiją ir Jungtinę Karalystę), prokuratūros. Keturiolika valstybių narių kaip kompetentingas institucijas nurodo saugumo arba žvalgybos arba ginkluotųjų pajėgų tarnybas. Šešios valstybės narės nurodo

---

44 Europos Komisijos ataskaita Tarybai ir Europos Parlamentui dėl Duomenų saugojimo direktyvos (Direktyva 2006/24/EB) taikymo vertinimo [interaktyvus]. Briuselis, 2011 [žiūrėta 2013-12-04]. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:LT:PDF>.

45 Europos Parlamento Ir Tarybos direktyva 2006/24/EB dėl duomenų, generuojamų arba tvarkomų teikiant viešai prieinamas elektroninių ryšių paslaugas arba viešuosius ryšių tinklus, saugojimo ir iš dalies keičianti Direktyvą 2002/58/EB. [2006] OL L 105/54.

mokesčių ir (arba) muitinės institucijas, o trys – sienos apsaugos institucijas. Viena valstybė narė prieigą prie duomenų suteikia kitoms valdžios institucijoms, jeigu joms tokią prieigą specialiais tikslais leidžiama turėti pagal antrinius teisės aktus. Vienuolikoje valstybių narių kaskart prašant prieigos prie saugomų duomenų reikia gauti teismo leidimą. Trijose valstybėse narėse dažniausiai reikia teismo leidimo. Kitose keturiose valstybėse narėse reikia gauti ne teisėjo, bet vyresniojo pareigūno leidimą. Dviejose valstybėse narėse vienintelė sąlyga – prašymas turi būti pateiktas raštu.[46] Išsamesnė informacija apie kompetentingų insitucijų prieigą prie saugomų duomenų pateikiama 3 priede.

Pagal direktyvos 2006/24/EB nuostatas, valstybės narės privalo užtikrinti, kad 5 straipsnyje nurodytų kategorijų duomenys būtų saugomi ne trumpiau kaip šešis mėnesius ir ne ilgiau kaip dvejus metus. Dėl ypatingų aplinkybių ir pranešus Komisijai, valstybės narės gali pratęsti ilgiausią saugojimo laikotarpį. Nagrinėjant duomenų saugojimo praktiką valstybėse narėse matyti, kad penkiolika valstybių narių visų kategorijų duomenims nustatė vieną laikotarpį: viena valstybė narė (Lenkija) nurodo dvejų metų saugojimo laikotarpį, viena (Latvija) – 1,5 m., dešimt (Bulgarija, Danija, Estija, Graikija, Ispanija, Prancūzija, Nyderlandai, Portugalija, Suomija, Jungtinė Karalystė) – vienerius metus, o trys (Kipras, Liuksemburgas, Lietuva) – šešis mėn. Penkios valstybės narės skirtingų kategorijų duomenims nustatė skirtingus saugojimo laikotarpius: dvi valstybės narės (Airija, Italija) nurodo dvejų metų laikotarpį fiksuotojo ir judriojo ryšio telefonijos duomenims ir vienerių metų laikotarpį interneto prieigos, interneto elektroninio pašto ir interneto telefonijos duomenims; viena valstybė narė (Slovėnija) nurodo 14 mėn. telefonijos duomenims ir 8 mėn. su internetu susijusiems duomenims; viena valstybė narė (Slovakija) nurodo vienerius metus fiksuotojo ir judriojo ryšio telefonijos duomenims ir šešis mėn. su internetu susijusiems duomenims; viena valstybė narė (Malta) nurodo vienerius metus fiksuotojo, judriojo ryšio ir interneto telefonijos duomenims ir šešis mėn. interneto prieigos ir interneto elektroninio pašto duomenims. Viena valstybė narė (Vengrija) saugo visus duomenis vienerius metus, išskyrus duomenis apie nesėkmingus skambučius, kurie saugomi tik šešis mėn. Viena valstybė narė (Belgija) nenurodė jokių duomenų saugojimo laikotarpių, taikomų direktyvoje nustatytiems duomenims.[47] Išsami informacija apie tai pateikiama 4 priede.

Iš pateiktų duomenų matyti, kad dauguma valstybių narių taiko skirtingą elektroninių ryšių duomenų saugojimo praktiką. Direktyvos 2006/24/EB nuostatos to nedraudžia, tačiau tokia skirtinga

[46] *Supra* note 44.
[47] *Supra* note 44.

praktika gali sukelti nepatogumų tiek elektroninių ryšių tiekėjams, tiek jų paslaugomis besinaudojantiems asmenims, kurie veikia keliose valstybėse narėse.

Direktyvos 2006/24/EB 7 straipsnis nustato, kad „nepažeisdama nuostatų, priimtų pagal Direktyvą 95/46/EB ir Direktyvą 2002/58/EB, kiekviena valstybė narė užtikrina, kad viešai prieinamų elektroninių ryšių paslaugų arba viešojo ryšių tinklo teikėjai pagal šią direktyvą saugomų duomenų atveju laikytųsi bent šių duomenų saugumo principų:

- saugomi duomenys turi būti tokios pačios kokybės ir jiems taikomi tokie patys saugumo ir apsaugos reikalavimai kaip ir tinkle esantiems duomenims;
- duomenims taikomos tinkamos techninės ir organizacinės priemonės, kad duomenys būtų apsaugoti nuo atsitiktinio ar neteisėto sunaikinimo, atsitiktinio praradimo ar pakeitimo, neleistino ar neteisėto saugojimo, tvarkymo, naudojimo ar atskleidimo;
- duomenims taikomos tinkamos techninės ir organizacinės priemonės siekiant užtikrinti, kad prieigą prie jų galėtų gauti tik specialiai įgaliotas personalas;
- duomenys, išskyrus tuos, prie kurių buvo gauta prieiga ir kurie buvo išsaugoti, pasibaigus saugojimo laikotarpiui sunaikinami.[48]“

Valstybės narės, įgyvendindamos direktyvos 2006/24/EB nuostatas privalo užtikrinti, kad 5 straipsnyje nurodyti duomenys būtų saugomi taip, kad kompetentingų institucijų reikalavimu saugomi duomenys ir visa kita reikalinga informacija, susijusi su tais duomenimis, būtų nedelsiant perduota. Valstybės narės taip pat yra įpareigotos paskirti vieną ar kelias valdžios institucijas, atsakingas už duomenų saugumo principų laikymosi stebėjimą valstybių narių teritorijoje. Direktyvoje įtvirtintas tokių institucijų nepriklausomumo principas.

Europos Komisijos ataskaitoje nurodoma, kad penkiolika valstybių narių perkėlė visus duomenų saugumo principus į atitinkamus teisės aktus. Keturios valstybės narės (Belgija, Estija, Ispanija, Latvija) perkėlė du arba tris šiuos principus, tačiau nenustatė aiškių duomenų sunaikinimo pasibaigus saugojimo laikotarpiui nuostatų. Dvi valstybės narės (Italija, Suomija) nustatė duomenų sunaikinimo nuostatas. Dvidešimt dvi valstybės narės yra paskyrusios už principų taikymo stebėseną atsakingą priežiūros instituciją.[49] Išsami informacija dėl duomenų saugumo principų taikymo, saugomų duomenų laikymo sąlygų ir priežiūros institucijų paskyrimo valstybėse narėse pateikima 5 priede.

2009 m. spalio mėn. Rumunijos Konstitucinis Teismas, 2010 m. kovo mėn. Vokietijos Konstitucinis Teismas ir 2011 m. kovo mėn. Čekijos Konstitucinis Teismas panaikino įstatymus,

[48] *Supra* note 45.
[49] *Supra* note 44.

kuriais direktyva 2006/24/EB perkeliama į šių valstybių teisę, remdamiesi tuo, kad teisės aktai prieštaravo konstitucijai.[50]

Rumunijos Konstitucinis Teismas savo sprendime nustatė, kad į asmenų pagrindines laisves gali būti kišamasi tik tuo atveju, jeigu valstybė nustato tinkamos ir pakankamos apsaugos priemonės. Teismas taip pat nustatė, kad direktyvos 2006/24/EB perkėlimo įstatymo taikymo sritis ir tikslas buvo neaiškūs, nebuvo nustatyta pakankamų apsaugos priemonių ir nusprendė, kad nuolatinė teisinė pareiga saugoti visus srauto duomenis šešis mėnesius prieštaravo Europos žmogaus teisių konvencijos 8 straipsnyje nustatytoms teisei į privatumą ir teisei naudotis saviraiškos laisve.

Vokietijos Konstitucinis Teismas direktyvos 2006/24/EB nuostatos gali pažeisti asmenų laisvę naudotis pagrindinėmis teisėmis ir kad saugant tokius duomenis smarkiai apribojama teisė į privatumą, todėl juos saugoti gali būti leidžiama tik labai išimtinėmis aplinkybėmis. Teismo manymu, šešių mėnesių saugojimo laikotarpis yra viršutinė galima leistina riba. Tokie duomenys gali būti teikiami kompetentingoms valstybės institucijoms tik sunkaus nusikaltimo tyrimo arba grėsmės visuomenės saugumui atvejais.

Čekijos Konstitucinis Teismas panaikino direktyvos 2006/24/EB perkėlimo teisės aktus remdamasis tuo, kad juose nebuvo pakankamai aiškiai ir tiksliai suformuluotos kišamosi į naudojimąsi pagrindinėmis teisėmis sąlygos. Teismas nusprendė, kad perkėlimo teisės aktuose pateikta kompetentingų institucijų, kurios gali prieiti prie duomenų ir juos naudoti, apibrėžtis, tokios prieigos ir naudojimo procedūros buvo nepakankamai aiškios, kad būtų galima užtikrinti duomenų vientisumą ir konfidencialumą. Tai sąlygotų galimą valdžios institucijų piktnaudžiavimą valdžia.

Direktyvos 2006/24/EB nuostatų atitikimas nacionalinei teisei taip pat buvo svarstytos Bulgarijoje, Kipre ir Vengrijoje.[51]

Europos duomenų apsaugos priežiūros pareigūnas P. Hustinxas savo nuomonėje nurodė išsakė savo nuomonę, jog „direktyva 2006/24/EB nepasiektas pagrindinis jos tikslas suderinti su duomenų saugojimu susijusius teisės aktus. Toks derinimo trūkumas yra žalingas visoms susijusioms šalims: piliečiams, verslo subjektams ir teisėsaugos institucijoms. Jo teigimu, direktyva neatitinka teisės į privatumą ir duomenų apsaugą reikalavimų dėl tokių priežasčių:

- nepakankamai įrodytas direktyvoje numatytas būtinumas saugoti duomenis;
- duomenų saugojimą buvo galima reglamentuoti mažiau ribojant privatumą;
- direktyvai trūksta nuspėjamumo[52].[53]

[50] *Ibid.*
[51] *Supra* note 44.

P. Hustinxas taip pat pateikė išvadą, kad direktyva 2006/24/EB neatitinka teisės į privatumą ir duomenų apsaugą reikalavimų, nes joje nepakankamai įrodytas būtinumas saugoti duomenis bei duomenų saugojimą buvo galima reglamentuoti mažiau ribojant privatumą. Tokiu būdu, Europos duomenų apsaugos priežiūros pareigūnas ragina apsvarstyti visas alternatyvas, įskaitant galimybę panaikinti direktyvą *per se*. Būsima Duomenų saugojimo direktyva svarstytina tik esant susitarimui dėl poreikio turėti Europos Sąjungos taisykles vidaus rinkos ir policijos bei teismų bendradarbiavimo baudžiamosiose bylose požiūriu ir, jeigu atliekant poveikio vertinimą gali būti pakankamai įrodytas Europos Sąjungos palaikomo ir reguliuojamo duomenų saugojimo būtinumas, įskaitant atidų alternatyvių priemonių apsvarstymą. Tokia priemonė turėtų atitikti tokius pagrindinius reikalavimus:

- ji turėtų būti visapusiška ir tikrai suderinti taisykles, susijusias su pareiga saugoti duomenis, taip pat su duomenų prieiga ir tolesniu jų naudojimu kompetentingose institucijose;
- ji turėtų būti išsami, t. y. turėti aiškų ir tikslų tikslą, be to, reikėtų panaikinti direktyvos 2002/58/EB 15 straipsnio 1 dalyje paliktą teisinę spragą;
- ji turėtų būti proporcinga ir neviršyti to, kas yra būtina.[54]

Nagrinėjant direktyvos 2006/24/EB nuostatas, taip pat kyla neaiškumų dėl jų santykio su Europos žmogaus teisių konvencija. Akivaizdu, kad direktyvos siekiami tikslai – kova su terorizmu ir organizuotu nusikalstamumu yra labai aktualūs, tačiau esant teisinio reguliavimo nesuderinamumui gali sudaryti prielaidas netinkamam teisės normų taikymui. Vadovaujantis direktyvos nuostatomis ir pradėjus kaupti visus srauto ir vietos nustatymo duomenis, asmenims atimama teisė koreguoti savo elgesį dėl to, kad duomenys apie juos yra kaupiami nuolat. Taip pat lieka neaiškus pagal šią direktyvą kaupiamų ir ypatingų asmens duomenų santykis, nes net kai kurie srauto duomenų elementai gali atskleisti pakankamai daug informacijos apie asmenį, kurios tvarkymui keliami sugriežtinti reikalavimai pagal kitus teisės aktus. Iš elektroninio laiško antraštės ar iš asmens skambučių tam tikrais telefono numeriais galima gauti informacijos apie tą asmenį ir

---

[52] Nuspėjamumo reikalavimas kyla iš EŽTK 8 straipsnio 2 dalyje ir ES pagrindinių teisių chartijos 52 straipsnio 1 dalyje nustatyto bendro reikalavimo, kad ribojimas turi būti numatytas įstatymo. EŽTT teigimu, tai reiškia, kad priemonės teisinis pagrindas turi būti įstatymas ir ji turėtų atitikti teisės viršenybės principą. Tai reiškia, kad teisė yra tinkamai prieinama ir nuspėjama.

[53] Europos duomenų apsaugos priežiūros pareigūno nuomonė dėl Duomenų saugojimo direktyvos (Direktyva 2006/24/EB) taikymo vertinimo ataskaitos, kurią Komisija pateikė Tarybai ir Europos Parlamentui. [2011] OL C 279/01.

[54] Kelios valstybės narės yra pasinaudojusios 15 straipsnio 1 dalimi ir 15 straipsnio 1 dalies b punktu, kad pagal direktyvą 2006/24/EB saugomus duomenis panaudotų ir kitais tikslais. Europos duomenų apsaugos priežiūros pareigūnas tai pavadino „teisine spraga“, kliudančia direktyvos 2006/24/EB tikslui, t. y. sudaryti pramonei vienodas sąlygas.

dalis jos pagal 1950 m. Europos žmogaus teisių ir pagrindinių laisvių konvenciją bei direktyvą 2002/58/EB gali būti priskiriama ypatingųjų asmens duomenų grupei.

Dar prieš direktyvos 2006/24/EB priėmimą, 2005 m. spalio 21 d. Nr. 113, 29 straipsnio darbo grupė išsakė nuomonę, kad šios direktyvos nuostatos turės rimtų pasekmių ir kad saugoti ryšių duomenis siekiant kovoti su sunkiais nusikaltimais yra beprecedentis ir vertintinas kaip istorinis įvykis, tačiau tai gali stipriai įtakoti kiekvieno europiečio gyvenimą ir kelti grėsmę žmonių pagrindinėms laisvėms, kurių apsaugai Europos Sąjungoje skiriama tiek daug dėmesio. Darbo grupė pažymėjo, kad valstybės narės privalo imtis visų priemonių užtikrinti kaip įmanoma mažesnį poveikį žmonių privatumui įgyvendinant direktyvos nuostatas. Darbo grupė taip pat pažymėjo, kad direktyvos prevencinės priemonės nėra galutinai suderintos, stokoja tinkamų ir konkrečių priemonių ryšių duomenims apsaugoti ir sudaro sąlygas skirtingam šios direktyvos nuostatų interpretavimui ir perkėlimui į nacionalinę teisę.[55]

Apibendrinant galime teigti, kad nors direktyva 2006/24/EB vertinama nevienareikšmiškai, nes dalis direktyvos nuostatų, reikalaujančių tam tikrą laiką saugoti srauto bei vietos nustatymo duomenis, sudaro sąlygas visiškam asmenų sekimui, tačiau žiūrint iš visuomenės poreikių, ypatingai visuomenės saugumo užtikrinimo pusės, tokie reikalavimai yra pakankamai aiškūs ir suprantami. Visuomenės susirūpinimas, kad dėl tokių direktyvos nuostatų valstybė nepagrįstai skverbsis į privatų asmenų gyvenimą, tokių duomenų laikymas yra perteklinis ir teigiamos įtakos užtikrinant visuomenės saugumą neturės, yra nepagrįstos. Akivaizdu, kad direktyvos nuostatos nesuteikia teisinio pagrindo kaupti asmenų susižinojimo turinio. Tačiau vien tik srauto duomenų kaupimo pakanka, kad būtų galima padidinti nusikalstamų veikų tyrimo efektyvumą. Reikėtų pažymėti, kad srauto ir vietos nustatymo duomenų kaupimas yra vienas iš kovos su terorizmo apraiškomis būdų. Tokiu būdu direktyvos reguliavimo sritis pereina iš visuomenės saugumo užtikrinimo į nacionalinio saugumo užtikrinimą.

[55] Nuomonė Nr. 3/2006 apie 2006 m. vasario 21 d. Tarybos priimtą Europos Parlamento ir Tarybos direktyvą 2006/24/EB dėl duomenų, generuojamų arba tvarkomų teikiant viešai prieinamas elektroninių ryšių paslaugas arba viešuosius ryšių tinklus, saugojimo ir iš dalies pakeičiančią Direktyvą 2002/58/EB [interaktyvus]. 2006 [žiūrėta 2013-12-21].
<http://ec.europa.eu/justice/policies/ privacy/docs/wpdocs/ 2006/wp119_lt.pdf>.

4. IŠANKSTINIO MOKĖJIMO SIM KORTELIŲ REGISTRAVIMO GALIMYBIŲ ANALIZĖ

4.1.Išankstinio mokėjimo SIM kortelių registravimo būtinumas

Teisėsaugos institucijos privalo žinoti ir sekti informacinių technologijų kitimo procesus, kad jos nebūtų naudojamos nusikalstamoms veikoms daryti. Duomenų saugojimas yra viena iš baudžiamojo persekiojimo priemonių, kurias naudodamos teisėsaugos institucijos gali efektyviai spręsti esamas nusikalstamumo problemas, atsirandančias dėl nusikalstamų veikų įvairovės, apimties ir kitų veiksnių. Į direktyvos 2006/24/EB taikymo sritį nėra įtraukta keleto vis dažniau naudojamų ryšių būdų. Kaip vieną iš tokių galima paminėti didelių įmonių naudojamus virtualiuosius privačius tinklus, kurių pagalba vartotojams suteikiama prieiga prie interneto per vieną tinklų sietuvą naudojant tą patį IP adresą. Tačiau ši problema sprendžiama diegiant naują technologiją, leisiančią paskirstyti IP adresus atskiriems virtualiųjų privačių tinklų naudotojams.

Dar viena aktuali problema yra judriojo ryšio telefonijos naudotojai, kurie naudojasi išankstinio mokėjimo paslaugomis. Jų skaičius Europos Sąjungos valstybėse narėse skiriasi. Išankstinio mokėjimo SIM kortelėmis, dažnai naudojasi nusikalstamas veikas darantys asmenys tam, kad būtų sudėtingiau nustatyti jų tapatybę. Vis labiau Europos Sąjungos mastu kalbama, kad būtina imtis priemonių, pagal kurias būtų reikalaujama registruoti išankstinio mokėjimo SIM korteles. Danija, Ispanija, Italija, Graikija, Slovakija ir Bulgarija jau priėmė tokias priemones. Kitos valstybės narės (Lenkija, Kipras, Lietuva) tokioms priemonėms pritaria ir artimiausiu metu imsis veiksmų joms įgyvendinti. Sprendžiant šią problemą taip pat būtina atsižvelgti į sunkumus, kurie gali tokias priemones padaryti mažiau efektyvias, pavyzdžiui, tapatybės vagystės atveju arba kai SIM kortelę nusiperka trečiasis asmuo, arba kai naudotojas naudojasi tarptinklinio ryšio paslaugomis su trečioje šalyje pirkta kortele.

Dar 2008 m. lapkričio 27 d. Europos Sąjungos vidaus reikalų ministrai patvirtino Europos Sąjungos Tarybos išvadas dėl kovos su nusikalstamu ir anoniminiu elektroninių ryšių naudojimu, kur išreiškė susirūpinimą dėl išankstinio mokėjimo kortelių naudojimo nusikalstamiems tikslams.[56] Taryba savo išvadas pateikė atsižvelgdama į direktyvos 2002/58/EB ir direktyvos 2006/24/EB nuostatų įgyvendinimo praktiką. Išvadoje pabrėžta, kad nors minėtų direktyvų nuostatos yra labai svarbios tiek duomenų, gaunamų teikiant elektroninių ryšių paslaugas, apsaugai, tiek tokių duomenų

[56] Europos Sąjungos Tarybos išvados dėl kovos su nusikalstamu elektroninių ryšių naudojimu ir anoniminiu jų naudojimu (Nr. 12694/4/10) [interaktyvus]. Briuselis, 2008 [žiūrėta 2013-12-20].

saugojimui nusikaltimų tyrimų tikslais, tačiau jos neužkerta kelio organizuoto nusikalstamumo grupuotėms, siekiančioms vykdyti nusikalstamas veikas Europos Sąjungos teritorijoje, naudotis tuo, kad įgyvendinamas laisvo asmenų judėjimo principas ir plėtojami elektroniniai ryšiai (ir ypač judrusis ryšys), t.y. kompetentingos institucijos negali nustatyti išankstinio mokėjimo SIM korteles naudojančių judriojo ryšio telefonų naudotojų tapatybės. Tai sudaro galimybes nusikalstamas veikas darantiems asmenims visiškai nebaudžiamai bendrauti su kitais tą pačią nusikalstamą veiką padariusiais asmenimis ar bendrininkais. Taryba taip pat pažymėjo, kad tokiu būdu gali būti sudarytos palankesnės sąlygos tarpvalstybiniam nusikalstamumui, nes naudojantis tarptinkliniu ryšiu nacionalinio operatoriaus įregistruoto telefono linijos abonento tapatybė yra nežinoma priimančiosios šalies operatoriui, registruotam paskirties šalyje, neatsižvelgiant į tai, ar linija veikia abonentinės sutarties, ar išankstinio mokėjimo SIM kortelės pagrindu.

Lietuvos kompetentingos teisėsaugos institucijos užkardant ir atskleidžiant nusikalstamas veikas aktyviai naudojasi iš elektroninių ryšių paslaugų teikėjų gaunama informacija, tačiau praktikoje nuolat iškyla sunkumų nustatant išankstinio mokėjimo SIM kortelių naudotojus. Asmenys, planuodami ir vykdydami nusikalstamas veikas, dažniausiai naudojasi „Labas“, „Pildyk“, „Ežys“ ir kitomis išankstinio mokėjimo SIM kortelėmis, kurias, kartu su judriojo ryšio telefonų aparatais, keičia kasdien, o kartais ir keletą kartų per dieną. Tokia situacija labai apsunkina ir sulėtina vykdomus kriminalinės žvalgybos tyrimus ar baudžiamąjį persekiojimą, nes minėtų kortelių naudotojų asmenybėms nustatyti gaištamas laikas, o surinkti duomenys praranda aktualumą. Todėl intensyviau naudojant elektroninius ryšius, duomenys apie elektroninių ryšių įvykius įgauna vis didesnę reikšmę ir yra svarbi nusikalstamų veikų, ypač organizuoto nusikalstamumo ir korupcijos tyrimo, atskleidimo ir baudžiamojo persekiojimo priemonė.

Elektroninių ryšių įstatymo 65 straipsnio 2 dalyje teigiama, kad „siekiant užtikrinti, kad duomenys būtų prieinami sunkių ir labai sunkių nusikaltimų, kaip jie apibrėžti Lietuvos Respublikos baudžiamajame kodekse, tyrimo, atskleidimo ir baudžiamojo persekiojimo tikslais, viešųjų ryšių tinklų ir (ar) viešųjų elektroninių ryšių paslaugų teikėjai privalo išsaugoti ir įstatymų nustatyta tvarka neatlygintinai teikti kompetentingoms institucijoms jų generuojamus arba tvarkomus šio Įstatymo 1 priede išvardytus duomenis“[57]. Čia minimame 1 priede yra išvardinti duomenys, kuriuos elektroninių ryšių paslaugų tiekėjai privalo registruoti, tačiau jame nėra įpareigojimo ūkio subjektams, teikiantiems elektroninių ryšių paslaugas, kaupti išankstinių elektroninių ryšių paslaugų vartotojų duomenų, nes šie duomenys nėra reikalingi operatorių veiklai vykdyti.

[57] Lietuvos Respublikos elektroninių ryšių įstatymas. *Valstybės žinios*. 2004, Nr. 69-2382.

Šio darbo autorė mano, kad siekiant spręsti susidariusią problemą dėl išankstinio mokėjimo elektroninių ryšių paslaugų vartotojų tapatybių nustatymo, tikslinga papildyti Elektroninių ryšių įstatymą ir numatyti, kad ūkio subjektai, teikiantys elektroninių ryšių paslaugas, privalėtų kaupti išankstinio mokėjimo paslaugų vartotojų duomenis ir įstatymų nustatyta tvarka tokius duomenis teiktų kriminalinės žvalgybos subjektams, ikiteisminio tyrimo įstaigoms, prokurorams ar teismams. Galimas tokio teisinio reguliavimo pavyzdys pateikiamas 6 priede.

Iš esmės tokių duomenų kaupimas yra susijęs su asmens duomenų tvarkymu, kurį reglamentuoja ADTAĮ, tačiau minėto įstatymo 15 straipsnyje pasakyta, kad „asmens duomenys elektroninių ryšių srityje tvarkomi vadovaujantis Elektroninių ryšių įstatymu ir šiuo įstatymu“[58], t. y. ADATĮ nustato bendruosius asmens duomenų tvarkymo principus, o specialiuosius reikalavimus tokio pobūdžio tvarkomiems duomenims nustato Elektroninių ryšių įstatymas. Bendrieji asmens duomenų tvarkymo reikalavimai aptarti ankstesnėje darbo dalyje, todėl šioje darbo dalyje išsamiau jų nenagrinėsime, tačiau svarbu pažymėti, kad vertinant nagrinėjamos problemos praktinius aspektus, sunkumų gali kilti ne su asmens duomenų tvarkymu, o su jų saugumo užtikrinimu. Asmens duomenų tvarkymas Lietuvoje yra aiškiai ir griežtai reglamentuotas. Elektroninių ryšių operatoriai yra užsiregistravę asmens duomenų tvarkytojais Asmens duomenų valdytojų valstybės registre, kurio nuostatai patvirtinti Lietuvos Respublikos Vyriausybės 2008 m. lapkričio 12 d. nutarimu Nr. 1163 „Dėl Lietuvos Respublikos Vyriausybės 2002 m. vasario 20 d. nutarimo Nr. 262 „Dėl asmens duomenų valdytojų valstybės registro nuostatų ir duomenų valdytojų pranešimo apie duomenų tvarkymą taisyklių patvirtinimo „pakeitimo“ ir turi teisę tvarkyti asmens duomenis, kuriuos gauna vykdydami savo veiklą, tačiau gautų duomenų saugumo reikalavimai aiškiai jokiame teisės akte nėra apibrėžti. ADTAĮ 30 straipsnio 1 dalyje nustatyta, kad „duomenų valdytojas ir duomenų tvarkytojas privalo įgyvendinti tinkamas organizacines ir technines priemones, skirtas apsaugoti asmens duomenims nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo. Minėtos priemonės turi užtikrinti tokį saugumo lygį, kuris atitiktų saugotinų asmens duomenų pobūdį ir jų tvarkymo keliamą riziką, ir turi būti išdėstytos rašytinės formos dokumente (duomenų valdytojo patvirtintose asmens duomenų tvarkymo taisyklėse, duomenų valdytojo ir duomenų tvarkytojo sudarytoje sutartyje ir pan.).[59]“

Šio darbo autorė mano, kad tokia formuluotė yra pakankamai abstrakti ir neapibrėžta, nes joje yra daug galimo skirtingo vertinimo elementų. Čia yra tik nustatyta prievolė užtikrinti duomenų saugumą, tačiau aiškūs kriterijai saugumo lygmeniui nėra nustatyti, t. y. net ir menkiausios saugumo

[58] *Supra* note 13.
[59] *Ibid.*

priemonės gali būti veiksmingos tvarkomiems duomenims apsaugoti iki to momento, kol saugumo sistema bus pažeista ir tvarkomais duomenimis bus pasinaudota neteisėtai. Registrų ir informacinių sistemų steigimą Lietuvos Respublikoje reglamentuoja Registrų įstatymas ir Lietuvos Respublikos Vyriausybės 2004 m. balandžio 19 d. nutarimas Nr. 451 „Dėl valstybės informacinių sistemų steigimo ir įteisinimo taisyklių patvirtinimo“, tačiau šie teisės aktai taikomi tik valstybės registrams ir informacinėms sistemoms, todėl galime teigti, kad valstybiniame sektoriuje asmens duomenų tvarkymo reikalavimai, jų saugumo užtikrinimo priemonės yra reglamentuotos tinkamai. Tačiau privačių juridinių asmenų steigiamų informacinių sistemų asmens duomenims tvarkyti jokie specialūs teisės aktai nereglamentuoja, todėl jų veikloje galimi įvairūs teisinio reguliavimo interpretavimai. Autorė mano, kad tokia padėtis sąlygoja, kad juridinių asmenų tvarkomi asmens duomenys nėra saugūs ir tai sudaro sąlygas galimam jų neteisėtam tvarkymui.

Kaip alternatyva elektroninių ryšių subjektų naudojamoms duomenų apie klientus tvarkymo sistemoms galėtų būti sukurta automatizuotas duomenų tvarkymo registras, tvarkomas tam įgaliotos valstybės institucijos. Prie šio registro turėtų prieigą elektroninių ryšių subjektai, kompetentingos valstybės institucijos ir įstaigos. Tokiu būdu, šio registro veiklą reglamentuotų Registrų įstatymas ir, šio darbo autorės manymu, tai būtų pakankamai efektyvus ir skaidrus duomenų tvarkymo būdas.

Nagrinėjamu atveju elektroninių ryšių operatoriai jau turi sukūrę informacines sistemas, kuriose tvarko savo klientų (elektroninių ryšių naudotojų) asmens duomenis. Asmuo, panorėjęs tapti judriojo ryšio paslaugos naudotoju, atvyksta į juridinio asmens įsteigtą atstovybę ir sudaręs paslaugos teikimo sutartį tampa judriojo ryšio operatoriaus klientu. Išankstinio judriojo ryšio paslaugų teikimas pagrįstas kitais principais. Čia asmuo bet kurioje prekybos vietoje anonimiškai įsigijęs išankstinio mokėjimo SIM kortelę tampa judriojo ryšio operatoriaus klientu ir gali naudotis judriuoju ryšiu. Apie tokias korteles įsigyjančius asmenis šiuo metu nėra renkami jokie duomenys. Taip pat nėra ribojamas tokių kortelių įsigijimo amžius.

Akivaizdu, kad įvedus ribojimus įsigyti išankstinio mokėjimo korteles, elektroninių ryšių operatoriams reikės iš dalies keisti savo verslo modelį. Siekiant užtikrinti asmens duomenų apsaugą, išankstinio mokėjimo SIM kortelės negalės būti parduodamos bet kurioje vietoje, kur nėra galimybių saugiai tvarkyti asmens duomenis. Šiuo metu tokios kortelės parduodamos ir prekybos centrų kasose, kioskuose, degalinėse ir pan. Dėl nuolatinio pirkėjų srauto abejotina, ar yra galimybė efektyviai surinkti būtinus kaupti asmens duomenis tokioje prekybos vietoje. Pavyzdžiui, sunku įsivaizduoti, kad pirkėjai prie kasos lauks, kol pardavėja nurašys (suves į informacinę sistemą) asmens, perkančio išankstinio mokėjimo kortelę, duomenis. Tai pat abejotina, ar elektroninių ryšių

operatoriai iškart sugebės sukurti modernią infrastruktūrą, tvarkyti asmens duomenis operatyviai bet kurioje prekybos vietoje. Akivaizdu, kad tokie veiksmai reikalaus nemažai ir papildomų lėšų.

Autorė mano, kad pirmame etape, elektroninių ryšių operatoriai išankstinio mokėjimo paslaugos teikimą privalės perkelti į savo atstovybes, kur jau yra sukurta asmens duomenų tvarkymo infrastruktūra ir tokius duomenis šiuo metu gali tvarkyti efektyviausiai. Siekdami neprarasti išankstinio mokėjimo paslaugos paklausos ir suteikdami mažiau nepatogumų klientams, elektroninių ryšių operatoriai turės steigti daugiau atstovybių. Tačiau tai yra ne šio darbo uždavinys, todėl plačiau elektroninių ryšių operatorių verslo galimybės nagrinėjamu klausimu nėra aptariamos.

Vienu iš būdų griežtinant prekybą išankstinio mokėjimo SIM kortelėmis autorė siūlo galimybę tokias korteles įsigyti bet kurioje prekybos vietoje taip, kaip yra šiuo metu, tačiau aktyvuoti tokią SIM kortelę būtų galima tik atvykus į atitinkamo operatoriaus atstovybę. Asmens duomenų apsaugos klausimu šis pasiūlymas yra analogiškas prieš tai aptartam ir aktualus tik verslumo užtikrinimo aspektu, todėl išsamiau aptariamas nėra.

Siekiant mažinti administracinę ir finansinę naštą elektroninių ryšių paslaugų teikėjams, svarstytina galimybė licencijuoti išankstinio mokėjimo SIM kortelių pardavimą, jeigu jas parduotų ne pats elektroninių ryšių paslaugos teikėjas.

Lietuvos Respublikos civilinio kodekso 2.77 straipsnyje pasakyta, kad „įstatymų nustatytais atvejais juridiniai asmenys gali imtis tam tikros rūšies veiklos tik gavę įstatymų nustatyta tvarka išduotą licenciją“. Šio kodekso 2.78 straipsnyje nurodyta, kad „Kiekvienai įstatymų nustatytai licencijuojamai veiklos rūšiai Vyriausybė tvirtina licencijavimo taisykles, jeigu kiti įstatymai nenustato ko kita“[60]. Prieš įvedant apribojimus tokiai verslo rūšiai, būtina įvertinti, ar nėra nepagrįstai įtvirtinti suvaržymai ūkio subjektams, pageidaujantiems prekiauti išankstinio mokėjimo SIM kortelėmis.

Įtvirtinus prekybos išankstinio mokėjimo SIM kortelėmis licencijavimą, sumažėtų būtinos investicijos išankstinio mokėjimo paslaugos privalomo registravimo įgyvendinimui elektroninių ryšių tiekėjams. Tačiau šiuo atveju susiduriama su dar didesne grėsme, nei galimas elektroninių ryšių paslaugos teikėjo netinkamas asmens duomenų tvarkymas. Kaip jau buvo minėta šioje dalyje, visi elektroninių ryšių tiekėjai yra stambūs ūkio subjektai, sukūrę tam tikrą jau veikiančią infrastruktūrą. Akivaizdu, kad jų finansinės galimybės leidžia jiems užtikrint tvarkomų asmens duomenų saugumą. Tačiau kyla pagrįstų abejonių, ar tokią apsaugą galėtų užtikrinti licencijas įsigiję

[60] Lietuvos Respublikos civilinis kodeksas. *Valstybės žinios*. 2000, Nr. 74-2262.

„tarpininkai“, kuriems reikėtų viską kurti nuo pradžių, siekiant užtikrinti asmens duomenų teisinio reguliavimo nuostatų įgyvendinimą jų veikloje.

Nustatant tam tikrus teisinio reguliavimo įrankius ir siekiant, kad nustatytų elgesio taisyklių būtų laikomasi, būtina numatyti ir atitinkamas poveikio priemones už šių taisyklių pažeidimą. Todėl autorė pažymi, kad būtina papildyti Lietuvos Respublikos administracinių teisės pažeidimų kodeksą, nustatant administracinę atsakomybę už prekybos išankstinio mokėjimo kortelėmis paslaugų teikimo tvarkos pažeidimą. Galimas tokio teisinio reguliavimo pavyzdys pateikiamas 7 priede.

Kaip vieną iš būdų šiai problemai spręsti autorė nurodo galimybę ją nagrinėti Europos Sąjungos mastu taip, kaip, pavyzdžiui, tarptinklinio judriojo telefono ryšio paslaugų tarifai buvo suvienodinti ir sureguliuoti visoje Europos Sąjungoje priėmus 2007 m. birželio 27 d. Europos Parlamento ir Tarybos reglamentą (EB) Nr. 717/2007 dėl tarptinklinio ryšio per viešuosius judriojo ryšio tinklus Bendrijoje, iš dalies keičiantis direktyvą 2002/21/EB, su paskutiniais pakeitimais, padarytais 2009 m. birželio 18 d. Europos Parlamento ir Tarybos reglamentu (EB) Nr. 544/2009.

Autorė mano, kad sėkmingai atlikti teisinio reguliavo pakeitimus, susijusius su nagrinėjama problema, taip pat yra būtina surengti viešas konsultacijas su ūkio subjektais, teikiančiais elektroninių ryšių paslaugas. Šių paslaugų teikėjai, remdamiesi tuo, kad Lietuvoje 52,4 proc.[61] judriojo ryšio vartotojų naudojasi būtent išankstinio mokėjimo paslauga, tikėtina, priešinsis siūlomiems nustatyti reikalavimams.

Prieš inicijuojant Elektroninių ryšių įstatymo pataisas taip pat tikslinga išanalizuoti elektroninių ryšių paslaugų teikėjų ir/ar Ryšių reguliavimo tarnybos turimą judriojo ryšio rinkos statistiką (esant galimybei taip pat pasitelkti ir kriminalinių tyrimų statistiką), siekiant įvertinti, kiek paklausos sumažėjimas būtų sąlygotas galimybių daryti nusikalstamas veikas apsunkinimo ir kiek dėl vartotojams kylančių nepatogumų.

Autorė taip pat pažymi, kad siekiant, jog siūlomas teisinis reguliavimas būtų efektyvus, turi būti užregistruotos visos veikiančios išankstinio mokėjimo SIM kortelės. Akivaizdu, kad norint tai efektyviai padaryti, būtina numatyti tam tikras poveikio priemones (pvz. turimų kortelių galiojimo nutraukimą) asmenims, kurie atsisako registruoti savo turimą išankstinio mokėjimo SIM kortelę.

Efektyviam ir sklandžiam išankstinio mokėjimo SIM kortelių registravimui, Elektroninių ryšių įstatymo pakeitimo įstatyme būtina nustatyti pereinamąjį laikotarpį, per kurį turi būti užregistruotos visos jau naudojamos kortelės. Tai sumažintų administracinę ir finansinę naštą

[61] Lietuvos Respublikos ryšių reguliavimo tarnybos Strategijos departamento Ekonominės analizės skyriaus 2012 m. gruodžio 7 d. pateikta ataskaita Nr. LD-2274 [interaktyvus]. 2013 [žiūrėta 2014-02-01]. http://www.rrt.lt/lt/apzvalgos-ir-ataskaitos/elektroniniu-rysiu-sektoriaus-mzkm/httpwww.rrt.ltltapzvalgos-ir-ataskaitoselektroniniu-7n66.html.

elektroninių ryšių tiekėjams, be to parodytų siekiamo teisinio reguliavimo efektyvumą, suteiktų galimybę daryti atitinkamas išvadas ir, esant būtinumui, teisinį reguliavimą tobulinti. Autorės nuomone, būtų pakankamas 12 mėnesių laikotarpis. Atlikto tyrimo rezultatai šiuo klausimu pateikti paskutinėje darbo dalyje.

Darbo autorė atkreipia dėmesį ir į grėsmes, kurios neišvengiamai atsiras nustačius įpareigojimą kaupti asmenų, įsigyjančių išankstinio mokėjimo SIM korteles, duomenis:

- ūkio subjektų, teikiančių elektroninių ryšių paslaugas, įpareigojimas kaupti išankstinio mokėjimo paslaugų gavėjų duomenis, uždės papildomą administracinę ir finansinę naštą šiems ūkio subjektams bei sąlygos jų galimybių konkuruoti su užsienio valstybių elektroninių ryšių paslaugų teikėjais susilpnėjimą. Gali didėti išankstinio mokėjimo SIM kortelių platinimo sąnaudos bei mažėti tokių kortelių paklausa;
- įvedus tokį įpareigojimą, Lietuvos vartotojams bus apribotos judriojo ryšio paslaugų pasirinkimo galimybės;
- taip pat egzistuoja galimybė pasinaudoti kaimyninių valstybių elektroninių ryšių paslaugų teikėjų parduodamomis išankstinio mokėjimo SIM kortelėmis;
- siekdami įsigyti išankstinio mokėjimo SIM korteles asmenys galės pasinaudoti trečiųjų asmenų pagalba, t. y. jų prašymų tokias korteles galės nupirkti kitas asmuo.

Apibendrinant galima teigti, kad pagrindinės kryptys, siekiant nustatyti privalomą išankstinio mokėjimo SIM kortelių registraciją yra: prekybos išankstinio mokėjimo SIM kortelėmis veiklos licencijavimas; galimybė įsigyti išankstinio mokėjimo SIM korteles tik atitinkamuose elektroninių ryšių tiekėjų atstovybėse; galimybė išankstinio mokėjimo SIM kortelę įsigyti bet kurioje pardavimo vietoje, tačiau aktyvuoti ją tik elektroninių ryšių tiekėjo prekybos atstovybėje ar licenciją gavusioje pardavimo vietoje. Tačiau visais šiais išvardintais atvejais lieka svarstytinas tvarkomų asmens duomenų saugumo užtikrinimo mechanizmas, kuris kiekvienu atveju priklausys nuo pasirinkto išankstinio mokėjimo SIM kortelių registravimo būdo.

4.2. Europos Sąjungos šalių patirtis registruojant išankstinio mokėjimo SIM korteles

Siekiant išanalizuoti Europos Sąjungos valstybių narių patirtį registruojant judriojo ryšio išankstinio mokėjimo SIM korteles, autorė kreipėsi į Valstybinę duomenų apsaugos inspekciją dėl tokios informacijos gavimo. Toliau darbe pateikiama apibendrinta informaciją iš tų valstybių, kurios atsiliepė į Valstybinės duomenų apsaugos inspekcijos kreipimąsi ir pateikė prašomus duomenis.

Valstybinė duomenų apsaugos inspekcija elektroniniu paštu išsiuntė paklausimus į 34 šalis (Europos Sąjungos ir kitų Europos valstybių kompetentingas institucijas asmens duomenų apsaugos srityje). Paklausimuose buvo prašoma pateikti informaciją, ar jų šalyse kaupiami išankstinio mokėjimo paslaugos naudotojų duomenys ir kokie teisės aktai reglamentuoja tokių duomenų rinkimą. Taip pat buvo prašoma pateikti informaciją, kokie asmens duomenų elementai yra tvarkomi, kada šie duomenys yra renkami, ar paslaugų teikėjai turi teisę daryti asmens tapatybę patvirtinančių dokumentų kopijas.

Apibendrinus 18 valstybių pateiktus duomenis (likusios valstybės informacijos nepateikė – *aut. pastaba*) paaiškėjo, kad vieningos praktikos šiuo klausimu nėra. Vienose valstybėse išankstinio mokėjimo paslaugos naudotojų duomenys yra kaupiami, o jų kaupimą reglamentuoja Elektroninių ryšių įstatymas (Italija, Makedonija, Graikija, Federalinis telekomunikacijų įstatymas (Vokietija) arba įstatymas Dėl elektroninių ryšių (Albanija, Vengrija). Kitos informaciją pateikusios šalys (Austrija, Lenkija, Olandija, Islandija, Čekija, Malta ir Slovėnija, Latvija ir kt.) teigė, kad jų šalyje Elektroninių ryšių įstatymas ar kiti teisės aktai nenumato pareigos rinkti tokius duomenis.

Reikėtų pažymėti, kad kai kurios šalys (Airija ir Moldova) nurodė, jog šiuo metu jose nėra įtvirtintas reikalavimas saugoti išankstinio mokėjimo SIM kortelių naudotojų duomenis, tačiau artimiausioje ateityje toks reikalavimas bus įtvirtintas, nes kompetentingos valstybės institucijos jau parengė nacionalinių įstatymų projektus arba artimiausiu metu ketina juos parengti. Airijos pateiktoje informacijoje teigiama, kad ateityje planuojama rinkti išankstinio mokėjimo paslaugos naudotojų vardus, pavardes, gyvenamosios vietos ir elektroninio pašto adresus. Moldovoje jau parengtas nacionalinio įstatymo projektas, leisiantis rinkti tokius duomenis.

Iš pateiktos informacijos matyti, kad valstybėse yra renkami skirtingi išankstinio mokėjimo paslaugos SIM kortelių naudotojų duomenys ir skirtingi tokių duomenų kiekiai. Pavyzdžiui, Italijoje prieš aktyvuojant tokią SIM kortelę, padaroma asmens tapatybę patvirtinančio dokumento kopija. Vokietijoje yra nustatytas privalomų saugoti duomenų sąrašas: judriojo ryšio telefono IMEI[62], IMSI[63], MSISDN[64] numeriai, išankstinio mokėjimo paslaugos naudotojo vardas, pavardė, gyvenamosios vietos adresas ir gimimo data. Vokietijoje galima daryti asmens tapatybę patvirtinančio dokumento kopijas, tačiau iškart po tapatybės patvirtinimo jos turi būti sunaikintos. Albanijoje kaupiami šie išankstinio mokėjimo paslaugos naudotojo duomenys: vardas, pavardė, gyvenamosios vietos adresas, gimimo data, asmens kodas, judriojo ryšio telefono IMEI, SIM

62 International Mobile Equipment Identity (angl.)
63 International Mobile Subscriber Identity (angl.)
64 Mobile Station International Subscriber Directory Number (angl.)

kortelės numeris, padaroma asmens tapatybę patvirtinančio dokumento kopija, kuri pridedama prie paraiškos įsigyti išankstinio mokėjimo SIM kortelę. Graikijoje kaupiami šie išankstinio mokėjimo paslaugos naudotojo duomenys: vardas, pavardė, gimimo data, gyvenamosios vietos adresas, nacionalinis mokesčių mokėtojo registracijos numeris, judriojo ryšio telefono IMEI ir IMSI bei padaroma asmens tapatybę patvirtinančio dokumento kopija.

Asmens tapatybę patvirtinančių dokumentų kopijos, pagal pateiktą šalių informaciją, daromos Albanijoje, Italijoje, Graikijoje ir Vokietijoje.

Kaimyninėse šalyse Lenkijoje, Latvijoje ir Estijoje nėra teisės aktų, reglamentuojančių išankstinio mokėjimo SIM kortelių naudotojų duomenų rinkimą. Estijos Elektroninių ryšių aktas nustato, kad tuo atveju, kai naudojama išankstinio mokėjimo SIM kortelė, turi būti išsaugoma kortelės aktyvavimo data, tikslus laikas bei vietovės, kurioje kortelė buvo aktyvuota, Cell ID[65] žyma. Latvijos Elektroninių ryšių įstatymas numato pareigą kaupti išankstinio mokėjimo SIM kortelių srauto duomenis.

Toliau darbe pateikta apibendrinta atskirų šalių pateikta informacija apie jose taikomą išankstinio mokėjimo paslaugos naudotojų registravimo praktiką.

Albanija. Elektroninių ryšių naudotojų duomenų tvarkymą šioje valstybėje reglamentuoja 2008 m. įstatymas Dėl elektroninių ryšių. Apie elektroninių ryšių naudotoją kaupiama tokia informacija: vardas, pavardė, skambučio duomenų įrašas, gyvenamosios vietos adresas, gimimo data, asmens kodas, telefono numeris, SIM kortelės numeris, padaroma asmens tapatybę patvirtinančio dokumento kopija, kuri pridedama prie paraiškos gauti SIM kortelę. Šie duomenys registruojami prieš aktyvuojant kortelę. Duomenis apie skambučius pradedami kaupti aktyvavus kortelę.

Italija. Reikalavimas saugoti išankstinio mokėjimo kortelių naudotojų duomenis Italijoje nustatytas 2003 m. Elektroninių ryšių įstatyme. Prieš aktyvuojant išankstinio mokėjimo SIM kortelę, padaroma jos naudotojo asmens tapatybę patvirtinančio dokumento kopija.

Makedonija. Galimybė gauti saugoti išankstinio mokėjimo SIM kortelių naudotojų duomenis nustatyta Makedonijos elektroninių ryšių įstatyme. Prieš įsigyjant išankstinio mokėjimo kortelę, gali būti daroma asmens tapatybę patvirtinančio dokumento kopija, tačiau tam sutikimą turi duoti kortelę siekiantis įsigyti asmuo.

Vengrija. Reikalavimas saugoti išankstinio mokėjimo kortelių naudotojų duomenis nustatytas 2003 m. Įstatyme dėl elektroninių ryšių. Paslaugų tiekėjams turi būti sudaroma galimybė

[65] Cell identity (angl.)

tvarkyti galutinių naudotojų ir abonentų asmens duomenis elektroninių ryšių paslaugoms teikti, nustatyti ir pakeisti sutarčių turinį, stebėti sutarčių vykdymo įgyvendinimą, sąskaitų ar skundų pateikimo ir nagrinėjimo klausimams spręsti.

Graikija. 2009 m. rugpjūčio mėn. įsigaliojo įstatymas, kuris nustatė išankstinio mokėjimo SIM kortelių naudotojų duomenų privalomą kaupimą. Duomenys pradedami kaupti prieš įsigyjant SIM kortelę. Visiems iki įstatymo priėmimo dienos išankstinio mokėjimo SIM korteles įsigijusiems asmenims buvo nurodyta užsiregistruoti ir pateikti savo asmens duomenis iki 2010 m. birželio 30 d., t. y. paliktas 9 mėn. pereinamasis laikotarpis jau naudojamoms kortelėms užregistruoti. Tiems, kurie to nepadarė iki nurodytos datos, buvo nutrauktas paslaugos tiekimas. Graikijoje renkami šie išankstinio mokėjimo SIM kortelių naudotojų duomenys: vardas, pavardė, gimimo data, gyvenamosios vietos adresas, nacionalinis mokesčių mokėtojo registracijos numeris, judriojo ryšio telefono IMEI ir IMSI. Taip pat padaroma asmens tapatybę patvirtinančio asmens dokumento kopija.

Vokietija. Reikalavimas saugoti išankstinių mokėjimo paslaugų naudotojų duomenis nustatytas Federaliniame telekomunikacijų įstatyme. Yra privaloma išsaugoti asmens tapatybę patvirtinančius duomenis, gali būti saugomi srauto duomenys. Jie registruojami prieš parduodant išankstinio mokėjimo SIM kortelę. Vokietijoje nustatytas toks privalomų registruoti duomenų sąrašas: vardas, pavardė, gimimo data, gyvenamosios vietos adresas, judriojo ryšio telefono IMEI, IMSI, MSISDN. Taip pat daroma asmens tapatybę patvirtinančio dokumento kopija, tačiau po tapatybės patvirtinimo ji iškart privalo būti sunaikinta.

Moldova. Šiuo metu Moldovoje nėra teisės akto, įpareigojančio elektroninių ryšių tiekėjus kaupti išankstinio mokėjimo paslaugos naudotojų duomenis, tačiau 2011 m. kompetentingos institucijos parengė tokio įstatymo projektą. Šio projekto derinimo metu yra iškilę ginčų su Moldovos duomenų apsaugos priežiūros institucija, kuri išreiškė prieštaravimą tokios reguliavimui, nes jie pažeidžia duomenų subjekto teisę į privatumą.

Airija. Šiuo metu reikalavimo saugoti išankstinio mokėjimo SIM kortelių naudotojų duomenis šioje valstybėje nėra, tačiau artimiausiu metu planuojama įpareigoti elektroninių ryšių operatorius saugoti tokių asmenų vardą, pavardę, gyvenamosios vietos ir elektroninio pašto adresus.

Estija. Estijos elektroninių ryšių aktas nenumato galimybės kaupti išankstinio mokėjimo paslaugos naudotojų duomenų, tačiau straipsnis, įpareigojantis saugoti srauto duomenis nustato, kad tuo atveju, kai naudojama išankstinio mokėjimo SIM kortelė, turi būti išsaugomi šie duomenys: kortelės aktyvavimo data, tikslus laikas bei vietovės, kurioje kortelė buvo aktyvuota, Cell ID žyma.

Latvija. Šioje valstybėje nėra teisės akto, nustatančio pareigą kaupti išankstinio mokėjimo SIM kortelių naudotojų duomenis, tačiau tokias korteles naudojantys asmenys turi galimybė patys užsiregistruoti jų naudotojais. Latvijos elektroninių ryšių įstatymas nustato pareigą kaupti elektroninių ryšių srauto duomenis.

Islandija, Austrija, **Lenkija**, **Olandija**, **Kipras**, **Čekija**, **Malta** ir **Slovėnija**. Šiuo metu šiose jų valstybėse elektroninių ryšių tiekėjams nėra nustatyta pareiga kaupti išankstinio mokėjimo SIM kortelių naudotojų duomenis.

1 lentelė. Apibendrinta valstybių pateikta informacija apie jose kaupiamus išankstinio mokėjimo SIM kortelių naudotojų asmens duomenis

Valstybė/ Registruojami duomenys	Vardas, pavardė	Gimimo data	Gyvenamosios vietos adresas	Asmens kodas	Kita	Ar daroma asmens tapatybę patvirtinančio dokumento kopija
Albanija	+	+	+	+	Skambučio duomenys, SIM informacija	+
Italija	-	-	-	-	-	-
Makedonija	-	-	-	-	-	+
Vengrija	+	+	+	+	-	-
Graikija	+	+	+	-	Nac. mokėtojo reg. Nr.. IMEI, IMSI	+
Vokietija	+	+	+	-	IMEI. IMSI, MSISDN	+
Moldova (*plan.*)	-	-	-	-	-	-
Airija (*plan.*)	+	-	+	-	el. paštas	-
Estija	-	-	-	-	-	-
Latvija	-	-	-	-	-	-

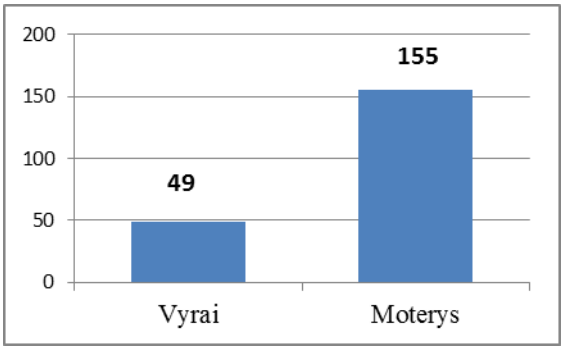
Islandija	-	-	-	-	-	-
Austrija	-	-	-	-	-	-
Lenkija	-	-	-	-	-	-
Olandija	-	-	-	-	-	-
Kipras	-	-	-	-	-	-
Čekija	-	-	-	-	-	-
Malta	-	-	-	-	-	-
Slovėnija	-	-	-	-	-	-

4.3. Išankstinio mokėjimo SIM kortelių registravimo galimybės tyrimo rezultatai

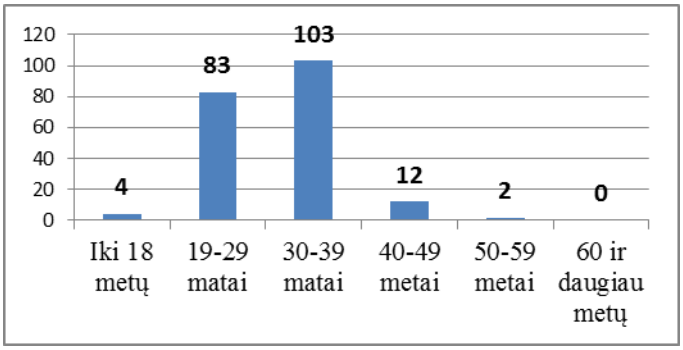
Siekiant visapusiškai nustatyti, ištirti ir įvertinti judriojo ryšio išankstinio mokėjimo SIM kortelių registravimo galimybes Lietuvoje autorė elektroniniu būdu atliko apklausą, kurioje dalyvavo 204 respondentai. Respondentų atsakymai buvo susisteminti, apibendrinti, pateikti toliau darbe. Taip pat apibendrinus gautus duomenis buvo suformuoti konkretūs, tyrimo rezultatais pagrįsti siūlymai dėl judriojo ryšio išankstinio mokėjimo SIM kortelių privalomos registracijos galimybių.

Atliktoje apklausoje dalyvavo 49 vyrai (24 proc.) ir 155 moterys (7 proc.) (1 pav.). Didžiąją dalį respondentų sudarė asmenų nuo 19 iki 29 metų (40,7 proc.) ir nuo 30 iki 39 metų (50,5 proc.) amžiaus grupės (2 pav.).

1 pav. Apklausoje dalyvavusių respondentų lytis

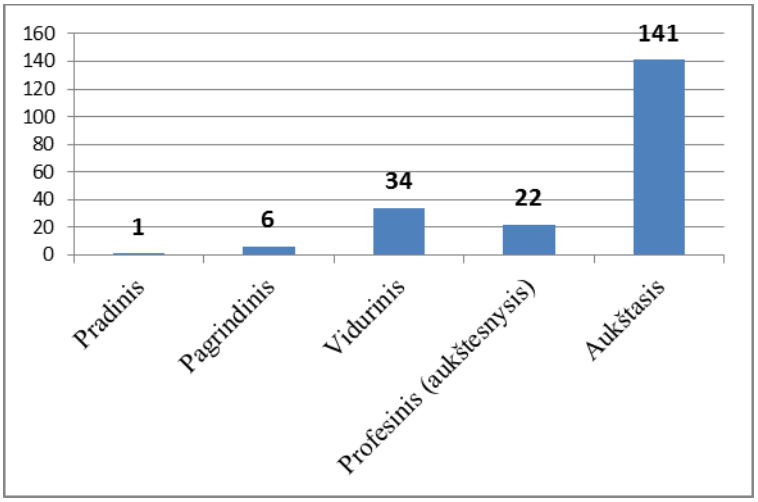


2 pav. Apklausoje dalyvavusių respondentų amžius

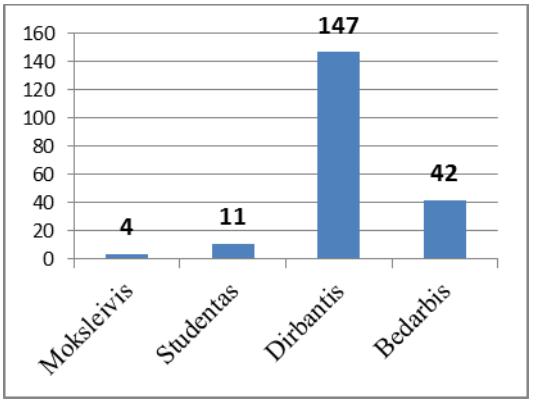


Dauguma respondentų turi aukštąjį išsilavinimą ir yra dirbantys. Tokių respondentų atitinkamai buvo 141 (69,1 proc.) ir 147 asmenys (72,1 proc.) (3 ir 4 pav.).

3 pav. Apklausoje dalyvavusių respondentų išsilavinimas



4 pav. Apklausoje dalyvavusių respondentų veikla

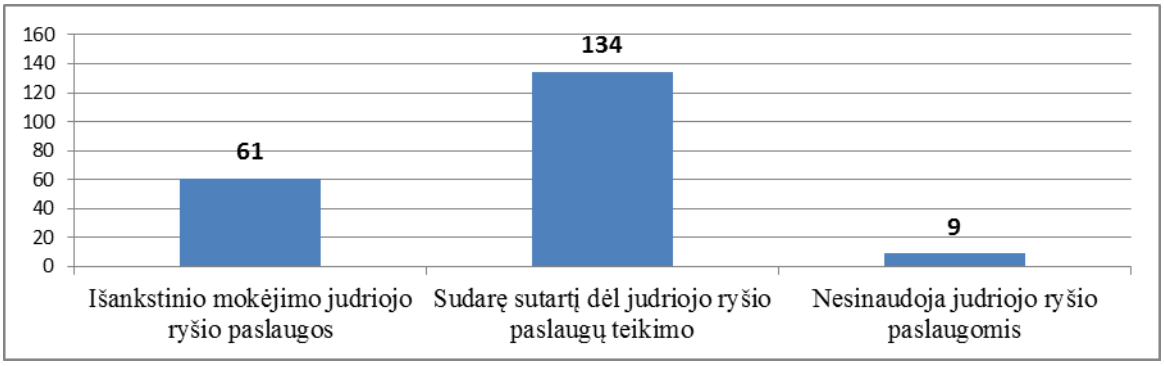


Apibendrinus gautus duomenis matyti, kad iš 204 asmenų 134 (65,7 proc.) yra sudarę sutartis dėl judriojo ryšio paslaugų teikimo ir tik 61 asmuo (29,9 proc.) naudojasi judriojo ryšio išankstinio mokėjimo paslaugomis. 9 asmenys (4,4 proc.) nurodė, kad mobiliojo ryšio paslaugomis nesinaudoja (5 pav.). Iš esmės, šie duomenys prieštarauja Ryšių reguliavimo tarnybos pateiktiems duomenims apie judriojo ryšio išankstinio mokėjimo paslaugos paplitimą šalyje, kur nurodoma, kad 52,4 proc.[66] judriojo ryšio vartotojų naudojasi būtent išankstinio mokėjimo paslauga. Autorės manymu, tai sietina su tuo, kad dauguma respondentų yra dirbantys ir aukštąjį išsilavinimą turintys

[66] *Supra* note 61.

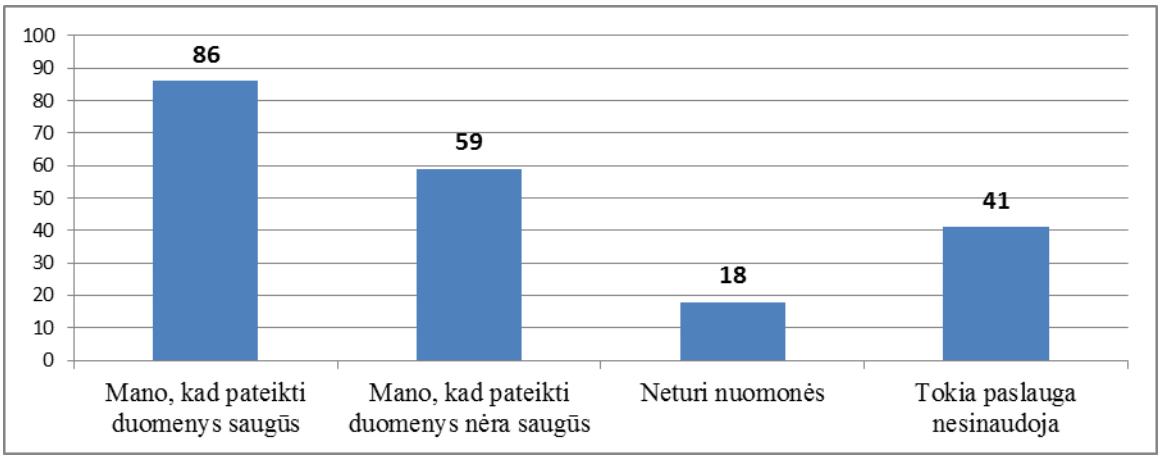
asmenys. Tai sąlygoja, jog jie turi nuolatinį pajamų šaltinį, yra užtikrinti galimybe tinkamai mokėti nefiksuotas įmokas už suteiktas paslaugas, t. y. judriojo ryšio paslaugų pasirinkimui didelę įtaką turi asmens socialinė padėtis.

5 pav. Respondentų naudojamų ryšio paslaugų pobūdis



Atsakydami į klausimą apie jų pateiktų asmens duomenų saugumą, sutartis dėl judriojo ryšio paslaugų teikimo sudarę 86 respondentai (42,2 proc.) nurodė, kad yra įsitikinę dėl savo asmens duomenų saugumo. 59 respondentai (28,9 proc.) nurodė, kad nėra įsitikinę dėl savo pateiktų asmens duomenų saugumo (6 pav.)

6 pav. Respondentų, sudariusių sutartį dėl judriojo ryšio paslaugų teikimo nuomonė apie jų pateiktų asmens duomenų saugumą

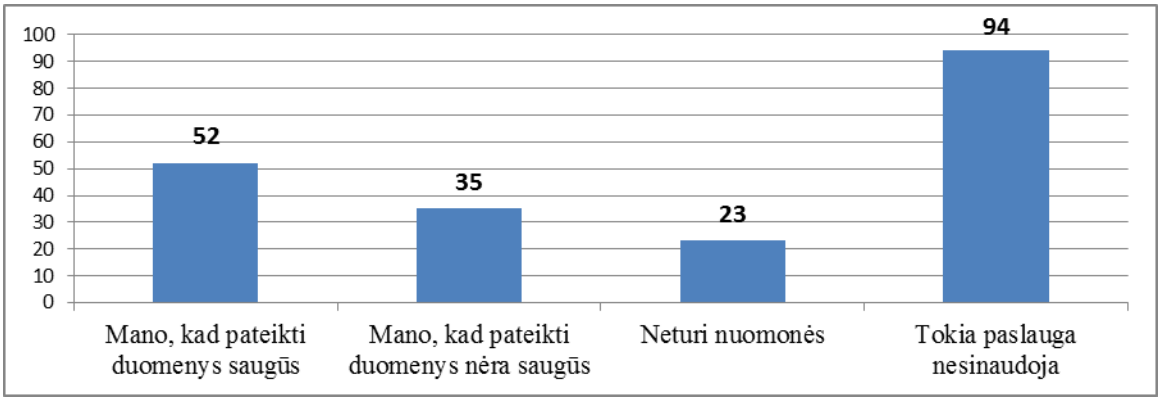


Didesnė dalis asmenų, kurie naudojasi judriojo ryšio išankstinio mokėjimo paslauga taip pat nurodė, kad jeigu būtų nuspręsta registruoti judriojo ryšio išankstinio mokėjimo SIM korteles, jų teiktini asmens duomenys būtų saugūs. Tokių asmenų buvo 52 (25,5 proc.) iš tų, kurie naudojasi šia

paslauga. 35 asmenys (17,2 proc.) nurodė, kad jų manymu jų pateiktini asmens duomenys nebūtų saugūs (7 pav.).

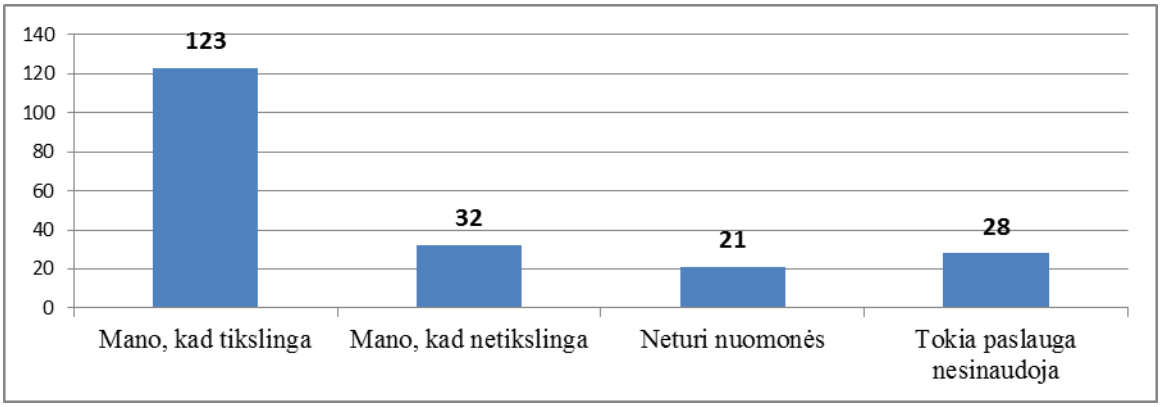
Apibendrinus 6 ir 7 pav. pateiktą informaciją matyti, kad asmens duomenų apsaugos institutas visuomenei nėra naujiena ir didesnė visuomenės dalis mano, kad privatus sektorius pajėgus užtikrinti asmens duomenų saugumą, o valstybė sugebės šį procesą sukontroliuoti.

7 pav. Respondentų nuomonė dėl jų asmens duomenų saugumo jei būtų registruojamos judriojo ryšio išankstinio mokėjimo SIM kortelės



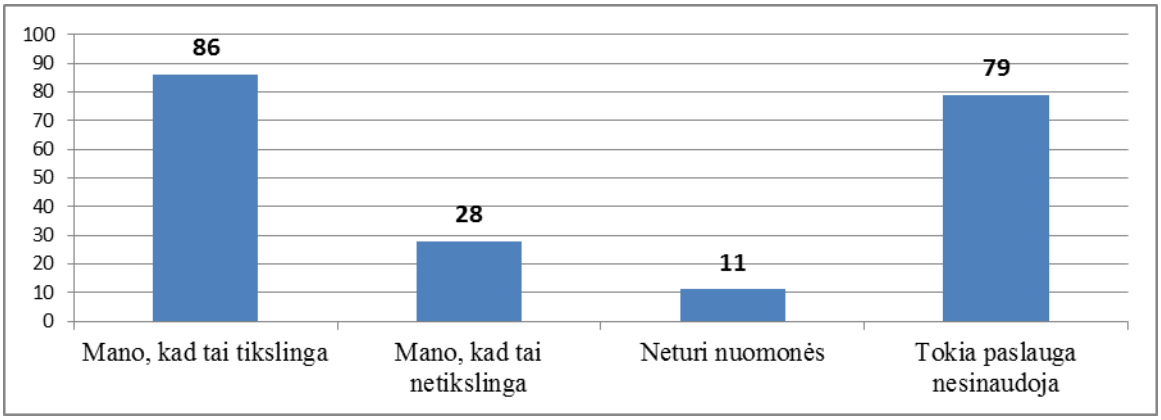
Įdomu tai, kad 123 respondentai (60,3 proc.) iš tų, kurie yra sudarę sutartis dėl judriojo ryšio paslaugų teikimo ir 86 respondentai (42,2 proc.) iš tų, kurie naudojasi judriojo ryšio išankstinio mokėjimo paslaugomis nurodė, kad visos judriojo ryšio išankstinio mokėjimo SIM kortelės turi būti užregistruotos (8 ir 9 pav.). Atitinkamai 32 (15,7 proc.) ir 28 (13,7 proc.) respondentų nurodė priešingai.

8 pav. Respondentų, sudariusių sutartį dėl judriojo ryšio paslaugų teikimo nuomonė apie privalomą judriojo ryšio išankstinio mokėjimo SIM kortelių registraciją



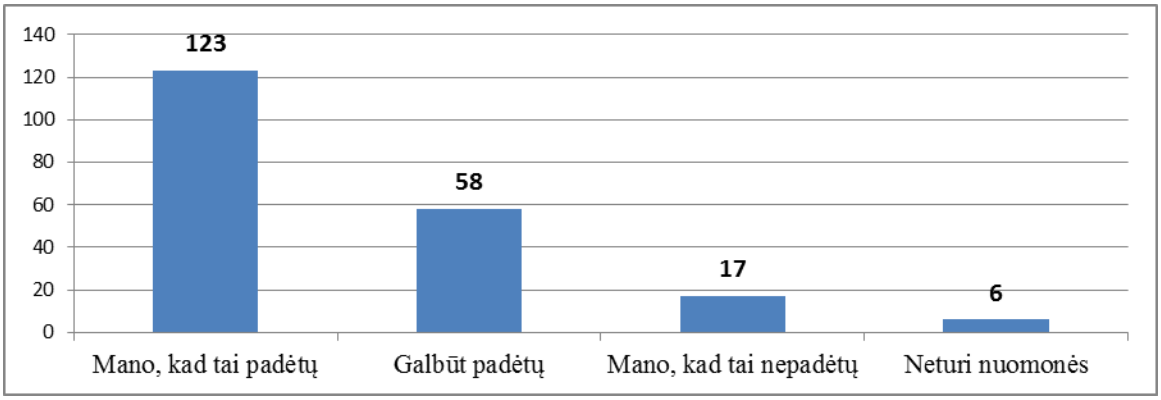
Darbo autorės manymu tai, kad didesnė dalis besinaudojančiųjų judriojo ryšio išankstinio mokėjimo paslaugomis palaiko privalomą judriojo ryšio išankstinio mokėjimo SIM kortelių registraciją parodo, kad visuomenė yra pasirengusi pokyčiams elektroninių ryšių srityje, net jeigu papildomas asmens duomenų kaupimas sąlygos didesnį asmens privatumo ribojimą.

9 pav. Respondentų, besinaudojančių judriojo ryšio išankstinio mokėjimo paslauga, nuomonė apie privalomą judriojo ryšio išankstinio mokėjimo SIM kortelių registraciją



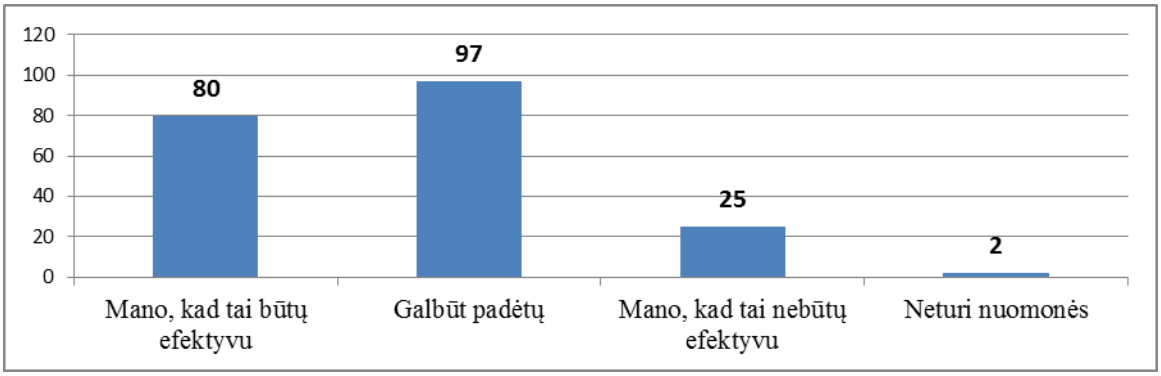
Aukščiau pateiktus teiginius papildo ir 10 pav. nurodyti duomenys, kur 123 respondentai (60,3 proc.) nurodė, kad privaloma judriojo ryšio išankstinio mokėjimo SIM kortelių registracija padėtų sumažinti nusikalstamų veikų skaičių, kai nusikalstamoms veikoms padaryti naudojamos judriojo ryšio priemonės). Tokios registracijos naudą užkardant nuskalstamas veikas aptarėme ankstesniuose skyriuose.

10 pav. Respondentų nuomonė apie tai, ar judriojo ryšio išankstinio mokėjimo SIM kortelių registracija padėtų mažinti nusikalstamų veikų skaičių



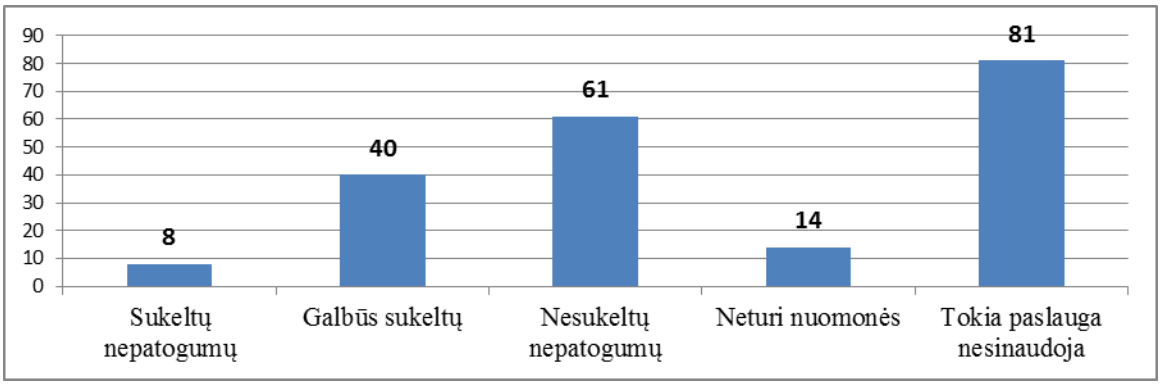
Atsižvelgiant į tai, kad judriojo ryšio išankstinio mokėjimo paslauga itin paplitusi tarp paauglių, respondentams buvo užduotas klausimas, ar privaloma judriojo ryšio išankstinio mokėjimo SIM kortelių registracija padėtų kontroliuoti paauglius. 80 respondentų (39,2 proc.) nurodė, kad tai būtų efektyvu ir 97 respondentai (47,5 proc.) nurodė, kad galbūt tai padėtų. Tik 25 respondentai (12,3 proc.) nurodė, kad tai nebus efektyvu (11 pav.).

11 pav. Respondentų nuomonė apie tai, ar judriojo ryšio išankstinio mokėjimo SIM kortelių registracija padėtų kontroliuoti paauglius



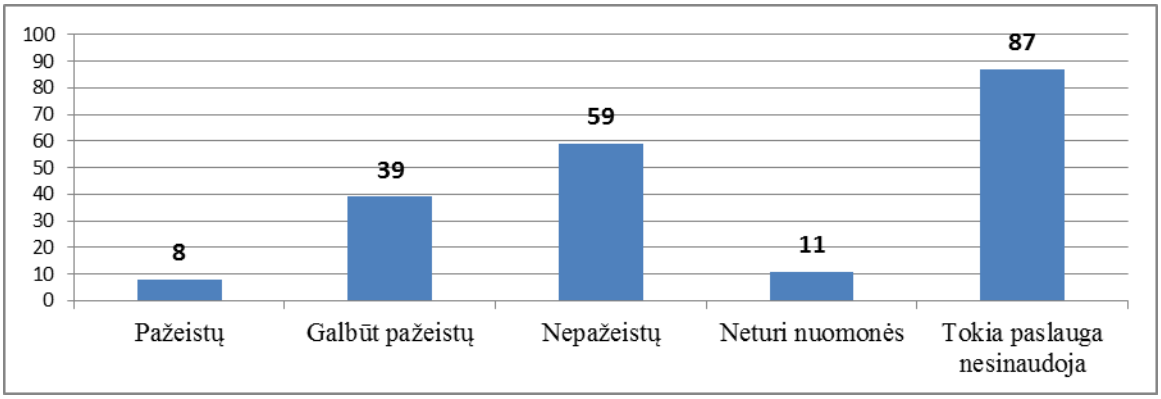
Vertinant galimai iškilsiančius nepatogumus, jeigu būtų nuspręstą privalomai registruoti judriojo ryšio išankstinio mokėjimo SIM korteles respondentams, kurie naudojasi judriojo ryšio išankstinio mokėjimo paslauga buvo užduotas klausimas, ar jiems tai sukeltų nepatogumų. 61 respondentas (29,9 proc.) nurodė, kad jiems tai nepatogumų nesukeltų. Vis tik 40 respondentų (19,6 proc.) nurodė, kad galimai jiems nepatogumų kiltų ir 8 respondentai (3,9 proc.) nurodė esą įsitikinę dėl kilsiančių nepatogumų (12 pav.).

12 pav. Respondentų, kurie naudojasi judriojo ryšio išankstinio mokėjimo paslauga, nuomonė, ar judriojo ryšio išankstinio mokėjimo SIM kortelių registracija jiems sukeltų nepatogumų



Nežiūrint į tai, kad įvedus privalomą judriojo ryšio išankstinio mokėjimo SIM kortelių registraciją neišvengiamai būtų kaupiami papildomi asmens duomenys, kas sąlygotų asmenų teisės į privatumą mažėjimą, 59 respondentai (28,9 proc.), kurie naudojasi judriojo ryšio išankstinio mokėjimo paslauga nurodė, kad tokiu būdu jų teisė į privatumą pažeista nebūtų. 39 respondentai (19,1 proc.) nurodė, kad jų teisė į privatumą galbūt būtų pažeista ir tik 8 respondentai (3,9 proc.) nurodė, kad jų teisės būtų suvaržytos (13 pav.).

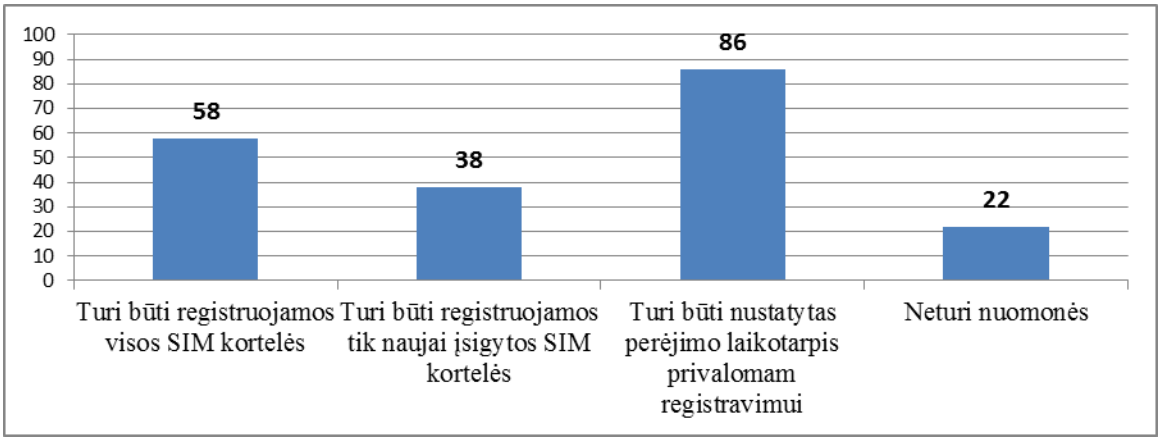
13 pav. Respondentų, kurie naudojasi judriojo ryšio išankstinio mokėjimo paslauga nuomonė, ar judriojo ryšio išankstinio mokėjimo SIM kortelių registracija pažeistų jų teisę į privatumą



Vertinant 12 ir 13 pav. pateiktus skaičius į atsakymus „*galbūt*“ ir „*neturiu nuomonės*“ matyti, kad respondentams trūksta informacijos apie privalomos judriojo ryšio išankstinio mokėjimo SIM kortelių registracijos modelius, mechanizmą ir kitais su tuo susijusiais klausimais, nes didelė dalis respondentų nėra įsitikinę dėl jiems galimai atsirasiančių įpareigojimų mąsto.

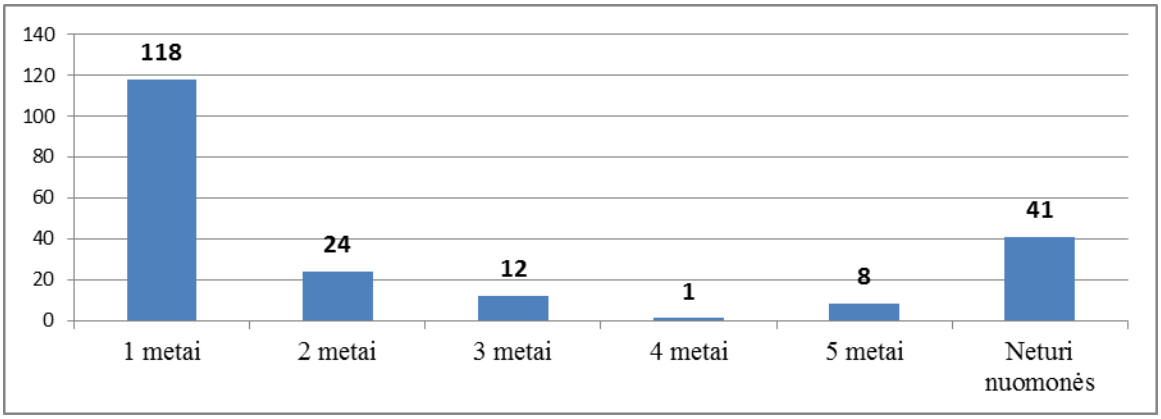
Siekiant nustatyti respondentų nuomonę dėl privalomo judriojo ryšio išankstinio mokėjimo SIM kortelių registracijos būdo, jiems buvo pateikti keturi galimi (labiausiai tikėtini) tokios registracijos modeliai. 58 respondentai (28,4 proc.) nurodė, kad nedelsiant turi būti užregistruotos visos rinkoje esančios judriojo ryšio išankstinio mokėjimo SIM kortelės. 38 respondentai (18,6 proc.) nurodė, kad registruojamos turi būti tik naujai įsigytos SIM kortelės, o 22 respondentai (10,8 proc.) nurodė, kad nuomonės neturi. Daugiausiai respondentų – 86 (42,2 proc.) kaip optimaliausią privalomos judriojo ryšio išankstinio mokėjimo SIM kortelių registracijos modelį nurodė, kad turi būti nustatytas pereinamasis laikotarpis tokių kortelių registracijai (14 pav.).

14 pav. Respondentų nuomonė apie tai, kokiu būdu turėtų būti registruojamos judriojo ryšio išankstinio mokėjimo SIM kortelės



Įvertinus tai, kad dauguma respondentų labiausiai tinkamu privalomos judriojo ryšio išankstinio mokėjimo SIM kortelių registracijos modeliu pasirinko pereinamojo laikotarpio nustatymą, itin aktualia tapo respondentų nuomonė apie tokio laikotarpio ilgumą. Didžioji dalis – 118 respondentų (57,8 proc.) nurodė, kad turėtų būti nustatytas 1 metų pereinamasis laikotarpis (15 pav.). Nežiūrint į judriojo ryšio išankstinio mokėjimo paslaugos paplitimą Lietuvoje ir rinkoje esančių šios paslaugos SIM kortelių kiekį, autorė taip pat mano, kad 1 metų pereinamasis laikotarpis yra pakankamas tokioms kortelėms užregistruoti.

15 pav. Respondentų nuomonė, koks pereinamasis laikotarpis turėtų būti nustatytas judriojo ryšio išankstinio mokėjimo SIM kortelių registracijai

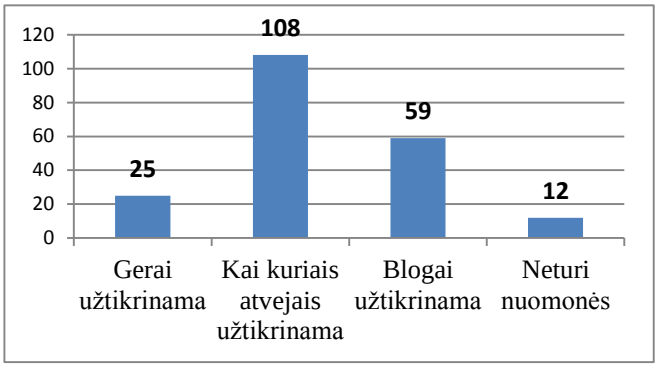


Siekiant visapusiškai atskleisti judriojo ryšio išankstinio mokėjimo SIM kortelių registracijos galimybes, autorė nusprendė, jog yra tikslinga įvertinti ir respondentų nuomonę apie asmens duomenų apsaugos būklę Lietuvoje. Todėl respondentams buvo užduoti du bendro pobūdžio klausimai, kaip jų manymu Lietuvoje užtikrinama asmens duomenų apsauga ir ar jie yra susidūrę su atvejais, kai asmens duomens duomenimis buvo pasinaudota neteisėtai.

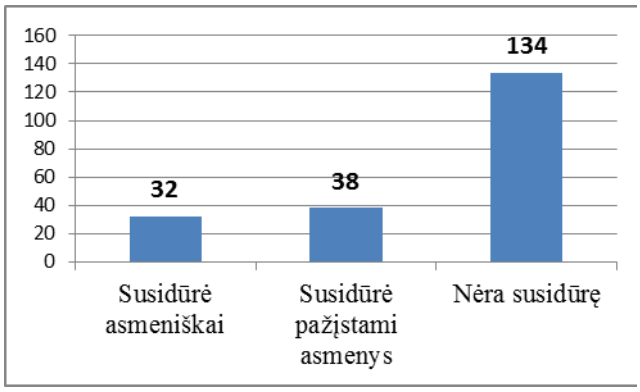
Vertinant gautus atsakymus matyti, kad tik 25 respondentai (12,3 proc.) mano, kad asmens duomenys Lietuvoje visais atvejais saugomi tinkamai. Net 108 respondentai (52,9 proc.) nurodė, kad asmens duomenys Lietuvoje tinkamai saugomi tik kai kuriais atvejais, o 59 respondentai (28,9 proc.) nurodė, kad jie saugomi netinkamai (16 pav.). Šie duomenys parodo, kad visuomenė iki galo nėra patenkinta ir įžvelgia trūkumų kompetentingų institucijų veikloje.

Tai patvirtina žemiau (17 pav.) pateikti duomenys, kur nurodyta, kad net trečdalis respondentų asmeniškai ar artimoje aplinkoje yra susidūrę su neteisėtu asmens duomenų panaudojimu. Atitinkamai tokių respondentų buvo 32 (15,7 proc.) ir 38 (18,6 proc.).

16 pav. Respondentų nuomonė, kaip Lietuvoje užtikrinama asmens duomenų apsauga



17 pav. Respondentų patirtis apie tai, ar jie buvo susidūrę su neteisėtu asmens duomenų panaudojimu



Apibendrinant atlikto tyrimo metu gautus duomenis teigtina, kad visuomenė aiškiai suvokia privalomos judriojo ryšio išankstinio mokėjimo SIM kortelių registracijos būtinumą ir galimą tokios registracijos naudą užtikrinant visuomenės saugumą. Nežiūrint į tai, kad tokia registracija šia paslauga besinaudojantiems asmenims neišvengiamai sukels nepatogumų ir ėmus kaupti papildomus asmens duomenis apribos jų teisę į privatumą, visuomenė yra pasirengusi tokiems pokyčiams ir juos palaiko. Nusikalstamų veikų užkardymas, socialiai rizikingiausių visuomenės grupių papildoma kontrolė yra pagrindinės sritys, kurioms privaloma judriojo ryšio išankstinio mokėjimo SIM kortelių registracija darys didžiausią įtaką. Taip pat iš pateiktos informacijos galima daryti išvadą, kad kompetentingoms valstybės institucijos privalo imtis papildomų priemonių asmens duomenų apsaugos srityje, nes didelė visuomenės dalis vis dar abejoja tinkamu asmens duomenų apsaugos užtikrinimu ir yra susidūrę su neteisėtu asmens duomenų tvarkymu.

IŠVADOS

1. Pirmą kartą Europos Sąjungos mastu teisinio reguliavimo priemonėmis apsaugoti asmenų teisę į privatų gyvenimą ir užtikrinti jų asmens duomenų apsaugą bei nustatyti aiškią kryptį tolimesniam tokių santykių vystymuisi imtasi priėmus direktyvą 95/46/EB. Nors po šios direktyvos priėmimo asmens duomenų apsauga tapo viena iš prioritetinių sričių, tačiau teisinis reguliavimas šioje srityje ne visuomet spėdavo su laiku, nes naujai priimti teisės aktai neretai pasirodydavo esą atgyvenę iškart tik juos priėmus. Taip nutiko ir su direktyva 95/46/EB, nors ji laikytina pažangiausiu to meto asmens duomenų apsaugą reguliuojančiu teisės aktu.

2. Svarbiausiu teisės aktu, reguliuojančių asmens duomenų apsaugą elektroninių ryšių srityje, yra direktyva 2006/24/EB. Nors ji vertinama nevienareikšmiškai, nes dalis direktyvos nuostatų, reikalaujančių tam tikrą laiką saugoti srauto bei vietos nustatymo duomenis, sudaro sąlygas visiškam asmenų sekimui, tačiau žiūrint iš visuomenės poreikių, ypatingai visuomenės saugumo užtikrinimo pusės, tokie reikalavimai yra pakankamai aiškūs ir suprantami. Visuomenės susirūpinimas, kad dėl tokių direktyvos nuostatų valstybė nepagrįstai skverbsis į privatų asmenų gyvenimą, tokių duomenų laikymas yra perteklinis ir teigiamos įtakos užtikrinant visuomenės saugumą neturės, yra nepagrįstas. Direktyvos nuostatos nesuteikia teisinio pagrindo kaupti asmenų susižinojimo turinio. Tačiau vien tik srauto duomenų kaupimo yra pakankama, kad padidinti nusikalstamų veikų tyrimo efektyvumą. Reikėtų pažymėti, kad srauto ir vietos nustatymo duomenų kaupimas yra viena iš kovos su terorizmo apraiškomis būdų. Tokiu būdu, direktyvos reguliavimo sritis pereina iš visuomenės saugumo užtikrinimo į nacionalinio saugumo užtikrinimą.

3. Lietuvoje esminiai pokyčiai asmens duomenų apsaugos srityje prasidėjo nuo jos įstojimo į Europos Sąjungą ir priėmus Asmens duomenų teisinės apsaugos įstatymo naują redakciją. Iki tol asmens duomenų apsauga Lietuvoje reguliuota paviršutiniškai, todėl tuo metu galiojantys teisės aktai neužtikrino visapusiškos asmens duomenų apsaugos. Tačiau iš atliktos respondentų apklausos matyti, kad ir esamas teisinis reguliavimas šioje srityje nėra visiškai efektyvus, nes tik 12,3 proc. respondentų nurodė, kad asmens duomenys Lietuvoje visais atvejais saugomi tinkamai, o net 52,9 proc. pasisakė, kad jie tinkamai saugomi tik kai kuriais atvejais ir 28,9 proc. nurodė, kad jie saugomi netinkamai. Taip pat net trečdalis respondentų asmeniškai ar artimoje aplinkoje yra susidūrę su neteisėtu asmens duomenų panaudojimu. Todėl darytina išvada, kad visuomenė iki galo nėra užtikrinta savo asmens duomenų saugumu ir įžvelgia trūkumų kompetentingų institucijų veikloje.

4. Siekiant įtvirtinti privalomą judriojo ryšio išankstinio mokėjimo SIM kortelių registraciją, būtina keisti esamą teisinį reguliavimą. Tam būtina pakeisti Elektroninių ryšių įstatymo

1 priedą, kur būtina nurodyti kauptinų duomenų sąrašą bei papildyti Administracinių teisės pažeidimų kodeksą, nustatant administracinę atsakomybę už prekybos judriojo ryšio išankstinio mokėjimo SIM kortelėmis paslaugų teikimo tvarkos pažeidimą.

5. Pagrindinės kryptys, siekiant nustatyti privalomą išankstinio mokėjimo SIM kortelių registraciją yra: prekybos išankstinio mokėjimo SIM kortelėmis veiklos licencijavimas; galimybė įsigyti išankstinio mokėjimo SIM korteles tik atitinkamuose elektroninių ryšių tiekėjų atstovybėse; galimybė išankstinio mokėjimo SIM kortelę įsigyti bet kurioje pardavimo vietoje, tačiau aktyvuoti ją tik elektroninių ryšių tiekėjo prekybos atstovybėje ar licenciją gavusioje pardavimo vietoje. Tačiau visais šiais išvardintais atvejais lieka svarstytinas tvarkomų asmens duomenų saugumo užtikrinimo mechanizmas, kuris kiekvienu atveju priklausys nuo pasirinkto išankstinio mokėjimo SIM kortelių registravimo būdo.

6. Vertinant Europos Sąjungos šalių narių ir kitų Europos valstybių patirtį registruojant išankstinio mokėjimo SIM korteles matyti, kad jose yra renkami skirtingi išankstinio mokėjimo paslaugos SIM kortelių naudotojų duomenys ir skirtingi tokių duomenų kiekiai.

7. Siekiant atlikti išsamesnį tyrimą atlikta anketinė apklausa, kurios metu 204 respondentams elektroniniu būdu buvo pateiktas klausimynas dėl judriojo ryšio išankstinio mokėjimo SIM kortelių registravimo galimybių. Išanalizavus ir apibendrinus apklausos metu surinktą medžiagą, prieita prie išvados, kad visuomenė aiškiai suvokia privalomos judriojo ryšio išankstinio mokėjimo SIM kortelių registracijos būtinumą ir galimą tokios registracijos naudą užtikrinant visuomenės saugumą. Tai patvirtina faktas, kad 60,3 proc. iš tų asmenų, kurie yra sudarę sutartis dėl judriojo ryšio paslaugų teikimo ir 42,2 proc. iš tų, kurie naudojasi judriojo ryšio išankstinio mokėjimo paslaugomis nurodė, kad visos judriojo ryšio išankstinio mokėjimo SIM kortelės turi būti užregistruotos (8 ir 9 pav.).

8. Nežiūrint į tai, kad judriojo ryšio išankstinio mokėjimo SIM kortelių registracija šia paslauga besinaudojantiems asmenims neišvengiamai sukels nepatogumų ir ėmus kaupti papildomus asmens duomenis bus apribota jų teisę privatumą, visuomenė yra pasirengusi tokiems pokyčiams, nes didesnė dalis respondentų (29,9 proc.) to nesureikšmina ir apklausos metu vis tik pasisakė, kad jiems tai nepatogumų nesukeltų (12 pav.).

9. Išanalizavus 204 respondentų atsakymus, prieita išvada, kad tinkamiausias judriojo ryšio išankstinio mokėjimo SIM kortelių registracijos būdas yra pereinamojo laikotarpio nustatymas. Taip pat vertinant tokio laikotarpio ilgumą nustatyta, kad dauguma respondentų (57.8 proc.) optimaliu laiko 1 metų pereinamąjį laikotarpį. Šie duomenys patvirtino autorės darbe tyrimo metu išsakytą poziciją.

PASIŪLYMAI

Išanalizavus nacionalinio ir Europos Sąjungos teisinio reguliavimo ypatumus elektroninių ryšių srityje, apibendrinus Europos Sąjungos valstybių narių patirtį registruojant judriojo ryšio išankstinio mokėjimo SIM korteles bei vadovaudamasi atlikto magistro baigiamojo darbo tyrimo medžiaga autorė teikia šiuos pasiūlymus dėl galimybių registruoti išankstinio mokėjimo SIM korteles Lietuvoje:

1. Teisingumo, Vidaus ar Susisiekimo ministerijoms siūlyti parengti Elektroninių ryšių įstatymo pakeitimo įstatymo projektą, kur papildant 1 priedą numatyti, kad ūkio subjektai, teikiantys elektroninių ryšių paslaugas, privalėtų kaupti išankstinio mokėjimo paslaugų vartotojų duomenis ir įstatymų nustatyta tvarka tokius duomenis teiktų kriminalinės žvalgybos subjektams, ikiteisminio tyrimo įstaigoms, prokurorams ar teismams. Kartu papildyti Administracinių teisės pažeidimų kodeksą nustatant administracinę atsakomybę už prekybos judriojo ryšio išankstinio mokėjimo SIM kortelėmis paslaugų teikimo tvarkos pažeidimą.

2. Projekto rengėjas turi surengti viešas konsultacijas su ūkio subjektais, teikiančiais elektroninių ryšių paslaugas, nes Lietuvoje 52,4 proc. judriojo ryšio vartotojų naudojasi būtent judriojo ryšio išankstinio mokėjimo paslauga ir siūlomi pakeitimai neišvengiamai sudarys organizacinių sunkumų, taip pat pareikalaus papildomų lėšų išankstinio mokėjimo SIM kortelių registracijai užtikrinti.

3. Projekto rengėjas turi atlikti judriojo ryšio rinkos vertinimą (esant galimybei taip pat pasitelkti ir kriminalinių tyrimų statistiką), siekiant nustatyti, kiek galimas išankstinio mokėjimo paslaugos paklausos mažėjimas yra sąlygotas galimybių daryti nusikalstamas veikas apsunkinimo ir kiek dėl vartotojams kylančių nepatogumų įtvirtinus privalomą judriojo ryšio išankstinio mokėjimo SIM kortelių registraciją.

4. Projekto rengėjui siūlyti inicijuoti privalomo judriojo ryšio išankstinio mokėjimo SIM kortelių registracijos klausimą svarstyti Europos Sąjungos mastu.

5. Projekto rengėjui svarstyti galimybę judriojo ryšio išankstinio mokėjimo SIM korteles registruoti vienu iš šių modelių: įvesti prekybos išankstinio mokėjimo SIM kortelėmis veiklos licencijavimą; nustatyti galimybę įsigyti išankstinio mokėjimo SIM korteles tik atitinkamuose elektroninių ryšių tiekėjų atstovybėse; nustatyti galimybę išankstinio mokėjimo SIM korteles įsigyti bet kurioje pardavimo vietoje, tačiau aktyvuoti jas tik elektroninių ryšių tiekėjo prekybos atstovybėje ar licenciją gavusioje pardavimo vietoje.

6. Nustatyti vienerių metų pereinamąjį laikotarpį, per kurį privalės būti registruojamos visos judriojo ryšio išankstinio mokėjimo kortelės. Šis laikotarpis sudarys galimybę kontroliuoti vykdomo proceso eigą ir daryti pagrįstas išvadas dėl jo būtinumo ir galimybių jį tobulinti.

LITERATŪROS SĄRAŠAS

Lietuvos Respublikos teisės aktai:

1. Lietuvos Respublikos Konstitucija. *Valstybės žinios*. 1992, Nr. 33-1014.
2. Lietuvos Respublikos Konstitucijos papildymo Konstituciniu aktu „Dėl Lietuvos Respublikos narystės Europos Sąjungoje“ ir Lietuvos Respublikos Konstitucijos 150 straipsnio papildymo įstatymas. *Valstybės žinios*. 2004, Nr. 111-4123.
3. Lietuvos Respublikos administracinių teisės pažeidimų kodeksas. *Valstybės žinios*. 1985, Nr. 1-1.
4. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas. *Valstybės žinios*. 1996, Nr. 63-1479.
5. Lietuvos Respublikos baudžiamasis kodeksas. *Valstybės žinios*. 2000, Nr. 89-2741.
6. Lietuvos Respublikos baudžiamojo proceso kodeksas. *Valstybės Žinios*. 2002, Nr. 37-1341.
7. Lietuvos Respublikos civilinis kodeksas. *Valstybės žinios*. 2000, Nr. 74-2262.
8. Lietuvos Respublikos elektroninių ryšių įstatymas. *Valstybės žinios*. 2004, Nr. 69-2382.
9. Lietuvos Respublikos gyventojų registro įstatymas. *Valstybės žinios*. 1999, Nr. 28-793.
10. Lietuvos Respublikos įstatymas „Dėl Konvencijos dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108) su Europos Tarybos ministrų komiteto priimtomis pataisomis ratifikavimo“. *Valstybės žinios*. 2001, Nr. 32-1055.
11. Lietuvos Respublikos kriminalinės žvalgybos įstatymas. *Valstybės žinios*. 2012, Nr. 122-6093.
12. Lietuvos Respublikos operatyvinės veiklos įstatymas. *Valstybės žinios*. 2002, Nr. 65-2633.
13. Lietuvos Respublikos registrų įstatymas. *Valstybės žinios*. 1996, Nr. 86-2043.
14. Lietuvos Respublikos teisėkūros pagrindų įstatymas. *Valstybės žinios*. 2012, 110-5564.
15. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas. *Valstybės žinios*. 2011, Nr. 163-7739.
16. Lietuvos Respublikos valstybės registrų įstatymas. *Valstybės žinios*. 1996, Nr. 86-2043.
17. Lietuvos Respublikos viešojo administravimo įstatymas. *Valstybės žinios*. 1999, Nr. 60-1945.
18. Lietuvos Respublikos Vyriausybės 1994 m. rugpjūčio 11 d. nutarimas Nr. 728 „Dėl Lietuvos Respublikos Vyriausybės darbo reglamento patvirtinimo“. *Valstybės žinios*. 1994, Nr. 63-1238.
19. Lietuvos Respublikos Vyriausybės 2000 m. kovo 27 d. nutarimas Nr. 349 „Dėl asmens duomenų valdytojų valstybės registro įsteigimo ir šio registro nuostatų patvirtinimo“. *Valstybės žinios*. 2000, Nr. 27-721.

20. Lietuvos Respublikos Vyriausybės 2004 m. balandžio 19 d. nutarimas Nr. 451 „Dėl valstybės informacinių sistemų steigimo ir įteisinimo taisyklių patvirtinimo“. *Valstybės žinios*. 2004, Nr. 58-2061.
21. Lietuvos Respublikos Vyriausybės 2004 m. balandžio 19 d. nutarimas Nr. 451 “Dėl valstybės informacinių sistemų steigimo ir įteisinimo taisyklių patvirtinimo“. *Valstybės žinios*. 2004, Nr. 58-2061.
22. Lietuvos Respublikos Vyriausybės 2004 m. gruodžio 6 d. nutarimas Nr. 1593 „Dėl įgaliojimų suteikimo įgyvendinant Lietuvos Respublikos elektroninių ryšių įstatymą“. *Valstybės žinios*. 2004, Nr. 177-6569.
23. Lietuvos Respublikos Vyriausybės 2008 m. lapkričio 12 d. nutarimas Nr. 1163 „Dėl Lietuvos Respublikos Vyriausybės 2002 m. vasario 20 d. nutarimo Nr. 262 „Dėl asmens duomenų valdytojų valstybės registro nuostatų ir duomenų valdytojų pranešimo apie duomenų tvarkymą taisyklių patvirtinimo“ pakeitimo“. *Valstybės žinios*. 2008, Nr. 133-5137.
24. Lietuvos Respublikos Vyriausybės 2009 m. liepos 22 d. nutarimas Nr. 788 „Dėl Lietuvos Respublikos Vyriausybės 2004 m. gruodžio 6 d. nutarimo Nr. 1593 „Dėl įgaliojimų suteikimo įgyvendinant Lietuvos Respublikos elektroninių ryšių įstatymą“ pakeitimo“. *Valstybės žinios*. 2009, Nr. 90-3858.
25. Lietuvos Respublikos Vyriausybės 2011 m. rugpjūčio 24 d. nutarimas Nr. 987“Dėl Lietuvos Respublikos Vyriausybės 2001 m. rugsėjo 25 d. nutarimo Nr. 1156 „Dėl Valstybinės duomenų apsaugos inspekcijos struktūrinės reformos, įgaliojimų suteikimo, Valstybinės duomenų apsaugos inspekcijos nuostatų patvirtinimo ir su tuo susijusių Lietuvos Respublikos Vyriausybės nutarimų dalinio pakeitimo“ pakeitimo“. *Valstybės žinios*. 2011, Nr. 107-5058.
26. Teisės aktų projektų rengimo rekomendacijos, patvirtintos Lietuvos Respublikos teisingumo ministro 2013 m. gruodžio 23 d. įsakymu Nr. 1R-298 „Dėl teisės aktų projektų rengimo rekomendacijų patvirtinimo“. *Valstybės žinios*. 2013, Nr. 137-6952.

Europos Sąjungos ir tarptautiniai dokumentai

27. 1980 m. rugsėjo 23 d. EBPO Rekomendacija dėl asmens privatumo apsaugos ir asmens duomenų judėjimo tarp valstybių narių gairių [interaktyvus]. 1980, C(80)58/FINAL [žiūrėta 2013-11-10].
<http://acts.oecd.org/Instruments/ShowInstrumentView.aspx?InstrumentID=114&InstrumentPID=312&Lang=en&Book=False>.

28. Europos duomenų apsaugos priežiūros pareigūno nuomonė dėl Duomenų saugojimo direktyvos (Direktyva 2006/24/EB) taikymo vertinimo ataskaitos, kurią Komisija pateikė Tarybai ir Europos Parlamentui. [2011] OL C 279/01.
29. Europos Komisijos ataskaita Tarybai ir Europos Parlamentui dėl Duomenų saugojimo direktyvos (Direktyva 2006/24/EB) taikymo vertinimo [interaktyvus]. Briuselis, 2011 [žiūrėta 2013-12-04].
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:LT:PDF>.
30. Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo. [1995] OL L 281/ 31.
31. Europos Parlamento ir Tarybos direktyva 97/66/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos telekomunikacijų sektoriuje. [1998] OL L 24/1.
32. Europos Parlamento ir Tarybos direktyva 2002/19/EB 2002 m. kovo 7 d. dėl elektroninių ryšių tinklų ir susijusių priemonių sujungimo ir prieigos prie jų (Prieigos direktyva). [2002] OL L 108/7.
33. Europos Parlamento ir Tarybos direktyva 2002/20/EB 2002 m. kovo 7 d. dėl elektroninių ryšių tinklų ir paslaugų-leidimo (Leidimų direktyva). [2002] OL L 108/21.
34. Europos Parlamento ir Tarybos direktyva 2002/21/EB 2002 m. kovo 7 d. Dėl elektroninių ryšių tinklų ir paslaugų bendrosios reguliavimo sistemos (Pagrindų Direktyva). [2002] OL L 108/33.
35. Europos Parlamento ir Tarybos direktyva 2002/22/EB 2002 m. kovo 7 d. dėl universaliųjų paslaugų ir paslaugų gavėjų teisių, susijusių su elektroninių ryšių tinklais ir paslaugomis (Universaliųjų paslaugų direktyva). [2002] OL L 108/51.
36. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių). [2002] OL L 201/37.
37. Europos Parlamento Ir Tarybos direktyva 2006/24/EB dėl duomenų, generuojamų arba tvarkomų teikiant viešai prieinamas elektroninių ryšių paslaugas arba viešuosius ryšių tinklus, saugojimo ir iš dalies keičianti Direktyvą 2002/58/EB. [2006] OL L 105/54.
38. Europos Parlamento ir Tarybos direktyva 2009/136/EB 2009 m. lapkričio 25 d. iš dalies keičianti Direktyvą 2002/22/EB dėl universaliųjų paslaugų ir paslaugų gavėjų teisių, susijusių su elektroninių ryšių tinklais ir paslaugomis, Direktyvą 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje ir Reglamentą (EB) Nr.

2006/2004 dėl nacionalinių institucijų, atsakingų už vartotojų apsaugos teisės aktų vykdymą. Bendradarbiavimo. [2009] OL L 337/11.

39. Europos parlamento ir Tarybos reglamentas (EB) Nr. 544/2009 2009 m. birželio 18 d. iš dalies keičiantis Reglamentą (EB) Nr. 717/2007 dėl tarptinklinio ryšio per viešuosius judriojo telefono ryšio tinklus Bendrijoje ir Direktyvą 2002/21/EB dėl elektroninių ryšių tinklų ir paslaugų bendrosios reguliavimo sistemos. [2009] OL L 167/12.
40. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 717/2007 2007 m. birželio 27 d. dėl tarptinklinio ryšio per viešuosius judriojo ryšio tinklus Bendrijoje, iš dalies keičiantis Direktyvą 2002/21/EB. [2007] OL L 171/32.
41. Komisijos direktyva 2002/77/EB 2002 m. rugsėjo 16 d. dėl konkurencijos elektroninių ryšių tinklų ir paslaugų rinkose (Tekstas svarbus EEE). [2002] OL L 249/21.
42. Europos Sąjungos pagrindinių teisių chartija. [2010] C 83/391.
43. Europos Sąjungos Tarybos išvados dėl kovos su nusikalstamu elektroninių ryšių naudojimu ir anoniminiu jų naudojimu (Nr. 12694/4/10) [interaktyvus]. Briuselis, 2008 [žiūrėta 2013-12-20].
<http://register.consilium.europa.eu/pdf/lt/08/st12/st12694-re04.lt08.pdf>.
44. Europos Sąjungos Teisingumo Teismo raidos ir veiklos 2006 m. ataskaita [interaktyvus]. 2007 [žiūrėta 2013-11-25].
<http://curia.europa.eu/jcms/upload/docs/application/pdf/2008-09/06_cour_activ_2008-09-29_13-54-7_165.pdf>.
45. Europos Sąjungos Teisingumo Teismo raidos ir veiklos 2007 m. ataskaita [interaktyvus]. 2008 [žiūrėta 2013-11-25].
<http://curia.europa.eu/jcms/upload/docs/application/pdf/2008-09/07_cour_activ_2008-09-29_14-12-37_968.pdf>.
46. Europos Sąjungos Teisingumo Teismo raidos ir veiklos 2008 m. ataskaita [interaktyvus]. 2009 [žiūrėta 2013-11-25].
<http://curia.europa.eu/jcms/upload/docs/application/pdf/2009-03/ra08_lt_cj_act.pdf>.
47. Europos Sąjungos Teisingumo Teismo raidos ir veiklos 2009 m. ataskaita [interaktyvus]. 2010 [žiūrėta 2013-11-25].
<http://curia.europa.eu/jcms/upload/docs/application/pdf/2010-05/ra09_activite_cour_final_lt.pdf>.
48. Europos Sąjungos Teisingumo Teismo raidos ir veiklos 2010 m. ataskaita [interaktyvus]. 2011 [žiūrėta 2013-11-25].

<http://curia.europa.eu/jcms/upload/docs/application/pdf/2011-05/ra2010_activite_cour_final_lt.pdf>.

49. Europos Sąjungos Teisingumo Teismo raidos ir veiklos 2011 m. ataskaita [interaktyvus]. 2012 [žiūrėta 2013-11-25]. <http://curia.europa.eu/jcms/upload/docs/application/pdf/2012-06/ra2011_activite_cour_lt.pdf>.
50. Europos Sąjungos Teisingumo Teismo raidos ir veiklos 2012 m. ataskaita [interaktyvus]. 2013 [žiūrėta 2013-11-25]. <http://curia.europa.eu/jcms/upload/docs/application/pdf/2013-04/192685_2012_6020_cdj_ra_2012_lt_proof_01.pdf>.
51. Europos žmogaus teisių ir pagrindinių laisvių konvencija. *Valstybės žinios*. 1995, Nr. 40-987.
52. Konvencijos dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu papildomas protokolas dėl priežiūros institucijų ir valstybės sienas kertančių duomenų srautų. *Valstybės žinios*. 2004, Nr. 36-1187.
53. Ministrų komiteto rekomendacija Nr. R (99) 5 valstybėms narėms dėl privatumo apsaugos internete [interaktyvus]. 1999 [žiūrėta 2013-11-28]. <http://portalas.ada.lt/images/cms/File/Rekomendacijos%20ministru%20tarybos/R_99_%205%20priv_aps_intern_rekom.pdf>.
54. Ministrų komiteto rekomendacija Nr. R (95) 4 valstybėms narėms dėl privatumo apsaugos telekomunikacijų paslaugų srityje, ypač telefoninio ryšio paslaugose [interaktyvus]. 1998 [žiūrėta 2013-11-28]. <http://portalas.ada.lt/images/cms/File/Rekomendacija%20Nr.%20R%20%2895%29%204.pdf>.
55. Nuomonė Nr. 3/2006 apie 2006 m. vasario 21 d. Tarybos priimtą Europos Parlamento ir Tarybos direktyvą 2006/24/EB dėl duomenų, generuojamų arba tvarkomų teikiant viešai prieinamas elektroninių ryšių paslaugas arba viešuosius ryšių tinklus, saugojimo ir iš dalies pakeičiančią Direktyvą 2002/58/EB [interaktyvus]. 2006 [žiūrėta 2013-12-21]. <http://ec.europa.eu/justice/policies/ privacy/docs/wpdocs/ 2006/wp119_lt.pdf>.
56. Pagal 29 straipsnį įkurtos duomenų apsaugos darbo grupės nuomonė Nr. 3/2006 apie 2006 m. vasario 21 d. Tarybos priimtą Europos Parlamento ir Tarybos direktyvą 2006/24/EB dėl duomenų, generuojamų arba tvarkomų teikiant viešai prieinamas elektroninių ryšių paslaugas arba viešuosius ryšių tinklus, saugojimo ir iš dalies pakeičiančią Direktyvą 2002/58/EB [interaktyvus]. 2006 [žiūrėta 2013-12-01].

<http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp119_lt.pdf>

57. Visuotinė žmogaus teisių deklaracija. *Valstybės žinios*. 2006, Nr. 68-2497.

Specialioji literatūra:

58. Civilka M. *Asmens duomenų apsauga tarptautinėje ir EB teisėje* [interaktyvus]. Vilnius: Vilniaus universitetas Teisės fakultetas, 2001 [žiūrėta 2013-10-09]. <http://www.scribd.com/doc/24045929/Mindaugas-Civilka-Asmens-duomen%C5%B3-apsauga-tarptautin%C4%97je-ir-EB-teis%C4%97je-2001-LT-Baltracker-net>.
59. Civilka M. *Asmens duomenų apsaugos teisinis reguliavimas interneto kontekste* [interaktyvus] [žiūrėta 2013-10-20]. <http://media.search.lt/ GetFile.php?OID=92932&FID=269994>.
60. Duomenų apsauga telekomunikacijų sektoriuje [interaktyvus] [žiūrėta 2013-11-11]. <http://www.ada.lt/images/cms/File/Duomenu%20apsauga%20 telekomunikaciju%20sektoriuje%281%29>.
61. Keras A., Kurapka E., Petrauskas R. *Informacinės visuomenės kūrimo, informacinių technologijų taikymo ir informacinių technologijų teisės plėtros tendencijos Europos Sąjungoje*. Vilnius: 2001.
62. Kiškis M., *et. al*. *Teisės informatika ir informatikos teisė*. Vilnius: Mykolo Romerio universitetas, 2006.
63. Lietuvos Respublikos ryšių reguliavimo tarnybos Strategijos departamento Ekonominės analizės skyriaus 2012 m. gruodžio 7 d. pateikta ataskaita Nr. LD-2274 [interaktyvus]. 2013 [žiūrėta 2014-02-01]. http://www.rrt.lt/lt/apzvalgos-ir-ataskaitos/elektroniniu-rysiu-sektoriaus-mzkm/httpwww.rrt.ltltapzvalgos-ir-ataskaitoselektroniniu-7n66.html.
64. Točickienė N. Asmens duomenų apsaugos reglamentavimas Europos Sąjungos ir Lietuvos Respublikos teisėje. *Jurisprudencija*. 2003, 44(36).
65. Valančius V., Kavalnė S. *Europos Sąjungos teisės įgyvendinimas Lietuvos administracinėje teisėje*. Vilnius: VĮ Registrų centras, 2009, p. 201.

Teismų praktika:

66. Byla C-301/06 *Airija prieš Parlamentą ir Tarybą* [2006] I-00593.
67. Byla C-270/11, *Švedijos Karalystė prieš Europos Komisiją* [2013].
68. Lietuvos vyriausiojo administracinio tesimo 2010 m. vasario 1 d. nutartis administracinėje byloje Nr. A-444-270/2010.

69. Lietuvos vyriausiojo administracinio tesimo 2010 m. vasario 1 d. nutartis administracinėje byloje Nr. N[62]-2266/2011.

Interneto tinklapių adresai:

70. Lietuvos aukščiausiasis teismas – www.lat.lt
71. Lietuvos vyriausiasis administracinis teismas – www.lvat.lt
72. Nacionalinė teismų administracija – www.teismai.lt
73. Lietuvos Respublikos Seimas – www.lrs.lt
74. Vidaus reikalų ministerija – www.vrm.lt
75. Valstybinė duomenų apsaugos inspekcija – www.ada.lt
76. Tarptautinės ekonominio bendradarbiavimo ir plėtros organizacijos tinklapis – www.oecd.org
77. Teisinės informacijos centras – www.infolex.lt
78. Žmogaus teisių stebėjimo institutas – www.hrmi.lt
79. Informatikos ir ryšių departamentas prie VRM – www.ird.lt
80. Ryšių reguliavimo tarnyba – www.rrt.lt
81. Asmens duomenų valdytojų Valstybės registras – http://db.ada.lt/
82. Portalas EUROPA – www.europa.eu

ANOTACIJA

Macienė V. Asmens duomenų apsauga nacionalinėje ir Europos Sąjungos teisėje/Teisės magistro baigiamasis darbas. Vadovas - **P**rof. dr. Algimantas Urmonas. –Vilnius: Mykolo Romerio universitetas, Teisės fakultetas, 2014.

Magistro baigiamajame darbe pasitelkus mokslinio tyrimo metodus analizuojami Europos Sąjungos teisės asmens duomenų apsaugos ypatumai, apžvelgiant jos formavimosi priežastis, raidą, sąveiką su nacionaliniu asmens duomenų apsaugos reguliavimu plačiąja prasme, tiek pasirinkus siauresnę tyrimo kryptį – elektroninių ryšių srityje. Tai pat atskleidžiama būtinybė registruoti judriojo ryšio išankstinio mokėjimo SIM korteles ir pateikiamos tokios registracijos galimybės Lietuvoje. Visas tyrimas grindžiamas atlikta Europos Sąjungos valstybių narių, taip pat kitų Europos valstybių praktika bei atliktos respondentų apklausos duomenimis.

Pagrindiniai žodžiai: Asmens duomenų apsauga, privatumas, elektroniniai ryšiai, judriojo ryšio išankstinio mokėjimo paslauga, SIM kortelė.

ANNOTATION

Macienė V. The personal data protection in the national and the European Union Law/MA thesis in Law. Supervisor Assoc. Prof. Dr. Algimantas Urmonas. – Vilnius: University of Mykolas Romeris, Faculty of Law, 2014.

The MA paper, applying the methods of scientific research, analyzes the specifics of personal data protection in the European Union Law, covering the reasons of its formation, development, interaction with the national regulations in personal data protection from the overall point of view, as well as the in the area of electronic connections. The work also proves the necessity to register the mobile connection pre-paid SIM cards and presents the possibilities of such registration in Lithuania. The research is based on the experience of the European Union state members and other European countries, as well as the data of the conducted respondents' poll.

Key words: personal data protection, privacy, electronic connections, mobile connection pre-paid service, SIM cards.

SANTRAUKA

Macienė V. Asmens duomenų apsauga nacionalinėje ir Europos Sąjungos teisėje/Teisės magistro baigiamasis darbas. Vadovas - Prof. dr. Algimantas Urmonas. –Vilnius: Mykolo Romerio universitetas, Teisės fakultetas, 2014.

Magistro baigiamajame darbe mokslinių tyrimo metodų pagalba detaliai analizuojamas asmens duomenų apsaugos institutas tiek nacionalinėje, tiek Europos Sąjungos teisėje. Nors darbe didžiausias dėmesys skiriamas asmens duomenų apsaugai elektroninių ryšių srityje, tačiau siekiant magistro baigiamojo darbo visapusiškumo ir išbaigtumo, aptariami taip pat ir esminiai asmens duomenų apsaugos instituto raidos aspektai, teisinio reguliavimo ypatumai Europos Sąjungos mastu. Visa nagrinėjama medžiaga darbe turi aiškiai apibrėžtą tikslą – pasinaudojus užsienio šalių patirtimi ir atlikto turimo medžiaga įvertinti judriojo ryšio išankstinio mokėjimo SIM kortelių registracijos galimybes Lietuvoje, nepažeidžiant tokios paslaugos vartotojų teisių į jų asmens duomenų apsaugą.

Pirmojoje darbo dalyje apžvelgiama asmens duomenų apsaugos samprata tiek materialiuoju, tiek formaliuoju aspektais, t. y. nagrinėjami visuomeniniai santykiai, sąlygoję asmens duomenų apsaugos instituto atsiradimą ir formavimąsi bei aptariama asmens duomenų apsaugos instituto vidinė struktūra.

Antrojoje dalyje pereinama prie asmens duomenų apsaugos ypatumų nagrinėjimo tiek nacionalinėje tiek Europos Sąjungos teisėje, apžvelgiami šią sritį reguliuojantys pagrindiniai teisės aktai, jų reguliavimo mastas ir tarpusavio sąveika. Tokia analizė yra aktuali siekiant suvokti bendrą asmens duomenų apsaugos užtikrinimo mastą Europos Sąjungoje ir jo poveikį nacionaliniam asmens duomenų apsaugos sureguliavimui.

Trečiojoje dalyje analizuojami asmens duomenų apsaugos ypatumai elektroninių ryšių srityje, nes tai yra tiesiogiai susiję su praktiniais pasirinktos magistro baigiamojo darbo temos aspektais. Ypatingas dėmesys čia skiriamas direktyvos 2006/24/EB dėl duomenų, generuojamų arba tvarkomų teikiant viešai prieinamas elektroninių ryšių paslaugas arba viešuosius ryšių tinklus, saugojimo ir iš dalies keičianti Direktyvą 2002/58/EB reguliavimo sričiai.

Ketvirtojoje dalyje atskleidžiamas judriojo ryšio išankstinio mokėjimo SIM kortelių registravimo būtinumas ir analizuojama Europos Sąjungos valstybių narių, taip pat kitų Europos valstybių patirtis registruojant išankstinio mokėjimo SIM korteles. Tyrimo medžiaga grindžiama atliktos respondentų apklausos duomenimis dėl judriojo ryšio išankstinio mokėjimo SIM kortelių registravimo galimybių Lietuvoje.

Magistro baigiamasis darbas užbaigiamas pateikiant atlikto tyrimo išvadas dėl asmens duomenų apsaugos sureguliavimo būklės tiek Europos Sąjungoje, tiek ir nacionalinėje teisėje bei pateikiamos išvados dėl judriojo ryšio išankstinio mokėjimo SIM kortelių registravimo galimybių. Šiam tikslui pasiekti atlikta anketinė apklausa, kurios metu 204 respondentams elektroniniu būdu pateiktas klausimynas dėl judriojo ryšio išankstinio mokėjimo SIM kortelių registravimo galimybių.

Apibendrinus ir susisteminus tyrimo metu išanalizuotą medžiagą ir taip pat pateikiami aiškiai apibrėžti pasiūlymai dėl aptariamų visuomeninių santykių reguliavimo tobulinimo ir labiausiai visuomenės poreikius atitinkantys judriojo ryšio išankstinio mokėjimo SIM kortelių registravimo modeliai bei jų formalizavimo būdai.

SUMMARY

Macienė V. The personal data protection in the national and the European Union Law/MA thesis in Law. Supervisor Assoc. Prof. Dr. Algimantas Urmonas. – Vilnius: University of Mykolas Romeris, Faculty of Law, 2014.

The MA thesis in great details analyzes the institute of personal data protection both in the national and in the European Union Law. Although the paper focuses on the data protection in the area of electronic connections, however, aiming for the versatility and thoroughness of the work, the essential aspects of the institute of personal data protection are discussed as well as the specifics of legal regulations in the European Union. All the material examined in this paper has a specific objective – to assess the possibility of mobile connection pre-paid SIM cards registration in Lithuania without the breach of right to the protection of their personal data of the users of this service.

The first part of this paper analyzes both the material and formal aspects of the concept of personal data protection i.e. social relationships, resulting in personal data protection institute's appearance and formation, are examined as well as the internal structure of the personal data protection institute.

The second part of the MA paper moves to the specifics of personal data protection investigation both in the national and the European Union Law, the basic legal acts regulating this area are discussed as well as their scale and interaction. Such analysis is applicable in trying to comprehend the overall scale of ensuring the personal data protection in the European Union and its impact on the national regulations of personal data protection.

The third part analyzes the specifics of personal data protection in the sphere of electronic connections due to their direct relation to the practical aspects of the topic, chosen for the MA thesis. Special attention is paid to the 2006/24/EB Directive for the protection of data, generated or processed providing electronic connection services accessible to the common public or public connection routes, that partly changes the 2002/58/EB Directive in the regulation area.

The fourth part of the paper shows necessity of the mobile connection pre-paid SIM cards' registration and analyzes the experience of the European Union member states as well as other European countries, registering the pre-paid SIM cards. The research material is based on the poll, conducted on the topic of mobile connection SIM card registration possibilities in Lithuania.

The MA paper is finished by submitting the conclusions of the research conducted on the personal data protection regulation's state both in the European Union and in the national Law. What is more, the conclusions on mobile connection pre-paid SIM cards registration possibilities are provided.

After summing up and systemizing all the data, analyzed during this research, the paper also provides clearly defined proposal on the issue of improving the regulation of discussed social relationships as well as the models of registration of mobile connection pre-paid SIM cards that meet the needs of the society the best and means of their formalizing.