Vilniaus universiteto Teisės fakulteto
Viešosios teisės katedra

Leilos Abi Chaker
V kurso, tarptautinės ir Europos Sąjungos teisės
Studijų šakos studentės

Magistro darbas

Daiktų interneto (IoT) reguliavimas pagal ES Bendrąjį duomenų apsaugos reglamentą
Regulation of the Internet of Things (IoT) under the EU General Data Protection Regulation

Vadovas: asist. dr. Julius Zaleskis

Recenzentė: asist. dr. Agnė Juškevičiūtė-Vilienė

Vilnius
2021

ANOTACIJA IR PAGRINDINIAI ŽODŽIAI

Šiame darbe analizuojamos pagrindinių Bendrojo duomenų apsaugos reglamento nuostatų taikymas daiktų interneto technologijomis tvarkomiems asmens duomenims. Nagrinėjamas Bendrajame duomenų apsaugos reglamente įtvirtintų duomenų apsaugos teisės principų, iš jų kylančių duomenų subjektų teisių, kitų svarbiausių reikalavimų įgyvendinimas, kai asmens duomenys yra renkami ir tvarkomi daiktų interneto technologijomis.

Pagrindiniai žodžiai: daiktų internetas, Bendrasis duomenų apsaugos reglamentas, duomenų apsaugos teisė.

This work analyses the application of the main provisions of the General Data Protection Regulation to personal data processed on the Internet of Things. The implementation of the principles of data protection law enshrined in the General Data Protection Regulation, the rights of data subjects arising from them, and other essential requirements when personal data are collected and processed on the Internet of Things are examined.

Keywords: Internet of Things (IoT), General Data Protection Regulation (GDPR), data protection law.

TURINYS

ĮŽANGA

Nagrinėjamos temos aktualumas. Daiktų internetas yra tinklas, kuriame fiziniai objektai sujungti tarpusavyje, žmonių ir objektų bendravimas vyksta per fizinius objektus, o valdymas vykdomas virtualiai (Zalieckaitė, L., Žilinskas, 2015, p. 104). Pats daiktų interneto terminas buvo pirmą kartą paminėtas tik 1999 metais (Ashton, 2009). Nuo to laiko technologijos itin stipriai pasikeitė, o išmanieji įrenginiai, tokie kaip išmanieji namų asistentai, išmanieji laikrodžiai ar apyrankės, dulkių siurbliai robotai, išmaniosios namų stebėjimo kameros, tapo mūsų visų kasdienybe.

Daiktų internetas pasižymi duomenų apie asmens elgesį, jo įpročius (t. y. asmens duomenų) rinkimu. Vis didėjant vartojamų įrenginių, prijungtų prie interneto, įvairovei, tokie prietaisai tampa vis populiaresni, o renkamų bei daiktų interneto technologijomis tvarkomų asmens duomenų įvairovė taip pat plinta. Tokioms technologijoms tampant mūsų kasdienybe, neužtikrinus tinkamo reguliavimo, kyla pavojus asmens teisei į privatumą, o kartu ir asmens duomenų apsaugos teisės įgyvendinimui. Asmenys gali jaustis stebimi, nesaugiai. Ir tai, jog asmens teisė į privatumą bus pažeista, yra reali galimybė. To puikus pavyzdys yra 2018 metų įvykis Oregone, JAV. Pora savo namuose naudojo išmanųjį namų asistentą "Alexa". Šis prietaisas, kaip ir dauguma kitų išmaniųjų namų asistentų, yra valdomas balsu ir užprogramuotas reaguoti į tam tikras balso komandas. Įrenginio vartotojai bendraujant su savo vyru namuose, „Alexa" galimai išgirdo kelias balso komandas, į kurias buvo užprogramuota reaguoti, kol galiausiai išgirstus atskirus pokalbio fragmentus priėmė kaip komandą įrašyti vykstantį pokalbį ir išsiųsti jį kaip žinutę vyro kontaktų sąraše esantiems darbuotojams (Chokshi, 2018). Tokiu būdu buvo pažeista sutuoktinių teisė į privatumą, kartų į duomenų apsaugos teisę.

Teisių užtikrinimui taip pat pasitikėjimo tarp įrenginių gamintojų ar kitų duomenų valdytojų ir išmaniųjų prietaisų vartotojų skatinimui Europos Sąjungoje (toliau – ES) svarbiausiu teisės aktu tapęs Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). OJ L 119 (toliau – BDAR). Šiuo teisės aktu yra užtikrinami duomenų apsaugos principai bei iš jų kylančios duomenų subjektų teisės ar kiti reikalavimai. BDAR pasižymi technologiniu neutralumu, tai užtikrina, jog jame numatytos teisės normos išliks aktualios ir galimos taikyti, nepaisant nenuspėjamos technologijų kaitos. Dėl šios BDAR savybės darbe yra nagrinėjamas svarbiausių ir aktualiausių BDAR

normų įgyvendinimas, kai asmens duomenų tvarkymas yra vykdomas daiktų interneto technologijomis.

Darbo tikslas. Šio darbo tikslas yra išnagrinėti, kokiu mastu ir kaip ES Bendrasis duomenų apsaugos reglamentas yra taikomas daiktų internetui bei jo taikymo problematiką.

Darbo uždaviniai. Magistrinio darbo tikslo įgyvendinimui yra keliami šie darbo uždaviniai:

1) atskleisti interneto sampratą ir jo savybes, turinčias įtakos duomenų apsaugos teisės užtikrinimui;
2) išnagrinėti, kokius pavojus žmogaus teisėms kelia daiktų internetas, įskaitant teisę į asmens duomenų apsaugą;
3) įvertinti, kokia apimtimi BDAR yra taikomas daiktų internetui;
4) išanalizuoti svarbiausius daiktų internetui taikomus BDAR reikalavimus;
5) nustatyti, kokie iššūkiai kyla taikant BDAR daiktų interneto kontekste.

Objektas ir tyrimo metodai. Šiame darbe yra nagrinėjamos BDAR pagrindinės nuostatos, taikomos daiktų internetui. Darbe apsiribojama pagrindinėmis ir daugiausiai iššūkių daiktų internete įgyvendinti keliančiomis nuostatomis. Analizuojama BDAR taikymo apimtis daiktų interneto technologijomis tvarkomiems duomenims, nagrinėjant BDAR nuostatas, apibrėžiančias duomenų valdytojo, tvarkytojo sąvokas, duomenų subjekto sąvoką bei nustatančias teritorinį BDAR taikymą. Šios normos svarbios siekiant nustatyti, kokiais atvejais daiktų interneto technologijomis tvarkomų asmens duomenų tvarkymui taikomas BDAR. Taip pat nagrinėjama BDAR įtvirtintų duomenų apsaugos teisės principų realizavimas daiktų internete. Darbe analizuojami visi BDAR įtvirtinti principai: teisėtumo, sąžiningumo ir skaidrumo, duomenų tvarkymo tikslo apribojimo, duomenų kiekio mažinimo, duomenų tikslumo, duomenų saugojimo trukmės ribojimo, duomenų saugumo, atskaitomybės bei pritaikytosios ir standartizuotosios duomenų apsaugos. BDAR įtvirtintais duomenų apsaugos principais grindžiamos visos kitos BDAR įtvirtintos normos. Dėl šios priežasties darbe svarbu išnagrinėti, kaip šie principai taikomi daiktų internetui. Magistro darbe yra nagrinėjamos principais grindžiamos duomenų subjektų teisės bei jų įgyvendinimo problemos. Aptariamos visos pagrindinės BDAR numatytos teisės: teisė būti informuotam apie duomenų tvarkymą, teisė nesutikti su duomenų tvarkymu, teisė apriboti duomenų tvarkymą, teisė būti pamirštam, teisė susipažinti su duomenimis ir juos ištaisyti, teisė į duomenų perkeliamumą. Identifikuojama šių teisių sąsaja su duomenų apsaugos teisės principais bei kaip šios teisės įgyvendinamos daiktų internete. Galiausiai nagrinėjami kiti svarbiausi reikalavimai daiktų interneto

technologijomis vykdomam duomenų tvarkymui. Pagrindinis reikalavimas yra turėti teisėtą asmens duomenų tvarkymo pagrindą. Šiuo reikalavimu užtikrinamas principų ir duomenų subjektų teisių įgyvendinimas. Daiktų interneto technologijomis vykdomam skaidriam duomenų tvarkymui užtikrinti svarbūs reikalavimai yra pareiga pranešti apie duomenų saugumo pažeidimą, poveikio duomenų apsaugai vertinimas bei pareiga turėti duomenų apsaugos pareigūną. Daiktų interneto technologijomis tvarkomi dideli kiekiai asmens duomenų, dažnu atveju tai yra specialiųjų kategorijų duomenys, duomenys yra tvarkomi automatizuotomis priemonėmis, vykdomas profiliavimas. Dėl šių daiktų interneto savybių darbe pasirinkta nagrinėti daiktų interneto kontekste aktualiausius ir svarbiausius BDAR reikalavimus.

Darbo tikslui pasiekti yra pasitelkiami šie tyrimo metodai:

- lingvistinis. Pasinaudojant lingvistiniu metodu yra aiškinamos tam tikros BDAR įtvirtintos sąvokos. Taip pat aiškinama daiktų interneto sąvoka, iš kurios išvedami daiktų interneto požymiai, kurie daro įtaką duomenų apsaugos teisės, o svarbiausia, BDAR taikymui.
- Istorinis. Istoriniu metodu yra analizuojamas technologijų vystymasis, prie daiktų interneto prijungtų įrenginių raida ir plėtra.
- Teleologinis. Šiuo metodu yra siekiama atskleisti BDAR leidėjo, duomenų apsaugos teisės tikslus. Kartu su loginiu metodu technologiškai neutralios BDAR normos susiejamos su daiktų internetu.
- Sisteminis. Sisteminiu metodu yra analizuojamos BDAR normos (principai, duomenų subjektų teisės, kiti svarbūs reikalavimai), jų sąsaja su kitomis BDAR normomis, duomenų apsaugos teisės principais.

Darbo originalumas. Darbo originalumui pabrėžti yra svarbu paminėti, jog Lietuvoje, nei magistriniuose darbuose, nei moksliniuose straipsniuose daiktų interneto reguliavimas pagal BDAR nebuvo nagrinėtas. Pagrindinis šaltinis nagrinėjantis BDAR normas yra J. Zaleskio monografija „Europos Sąjungos Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė“ (Zaleskis, 2019), kuria yra remiamasi šiame darbe. Tačiau atskirai, kaip BDAR reguliavimas taikomas daiktų internetui, darbų nėra. Lietuvoje magistriniuose darbuose buvo nagrinėtos pačio BDAR normos (ar jų taikymas atskirose srityse, tačiau ne daiktų internete). Taip pat yra magistrinių darbų, kurie nagrinėja daiktų internetą iš technologinės pusės, tačiau šiuose darbuose, žinoma, teisės aktai nėra nagrinėjami.

ES mastu yra nemažai mokslinių darbų, straipsnių, kurie nagrinėja daiktų interneto problematiką duomenų apsaugos teisės kontekste (daugiausiai šiame darbe remiamasi S.

Wachter straipsniais (Watcher, 2017), (Wachter, 2018)). Taip pat yra mokslinių straipsnių nagrinėjančių tik konkrečios daiktų interneto srities (pavyzdžiui, išmaniųjų namų) ir BDAR normų įgyvendinimo probleminius aspektus. Autoriaus S. R. Suppan 2017 metais tema „Duomenų apsauga daiktų internetui“ (angl. „*Data Protection for the Internet of Things*“) parašyta daktaro disertacija Regensburgo universitete, Vokietijoje[1]. Šioje disertacijoje daiktų internetas yra labiau nagrinėjamas iš technologinės pusės, pateikiami konkretūs technologiniai siūlymai siekiant užtikrinti asmenų privatumą. Taip pat 2020 metais parašyta Faiza Loukil daktaro disertacija Lyon universitete, Prancūzijoje, kurios tema „Naujo duomenų privatumu pagrįsto daiktų interneto požiūrio link“ (angl. *Towards a new data privacy-based approach for IoT*“)[2]. Disertacija aptaria tik mažą dalį BDAR numatytų normų (skaidrumo principą ir sutikimą kaip teisėto duomenų tvarkymo pagrindą). Dauguma magistrinių darbų nagrinėjančių daiktų internetą ir jo saugumą yra parašyti nagrinėjant technologinę šio darbo pusę. 2018 metais Lisabonos universitete buvo apgintas L. P. Santos magistrinis darbas labai panašia tema, kaip šis „Asmens duomenų ir privatumo apsauga ES plintant daiktų internetui“ (angl. „*Protecting Personal Data and Privacy in the EU in the Rise of the Internet of Things*“)[3], tačiau darbo objektu nėra tik BDAR normos ir darbas taip pat yra labiau orientuotas į technologinę pusę, nors teisės normos taip pat gan išsamiai aptariamos. Šis magistro darbo nuo tokių mokslinių ar magistro darbų išsiskiria tuo, jog darbe yra nagrinėjama bendrai daiktų interneto ir BDAR svarbiausių teisės normų (sistemiškai išskiriant aktualiausias daiktų internetui BDAR normas) sąveika.

Svarbiausi šaltiniai. Darbe pagrindinis nagrinėjamas šaltinis kaip teisės aktas yra BDAR. BDAR normų išaiškinimui, pritaikymui daiktų internetui yra remiamasi *soft law* šaltiniais. Taip pat analizuojant BDAR normas bei jų taikymą daiktų interneto kontekste pasiremta teisės doktrina (įvairių mokslininkų darbais ir straipsniais). ES Teisingumo Teismas (toliau – ESTT) konkrečios praktikos dėl BDAR normų taikymo daiktų internetui nėra suformulavęs, tačiau ESTT praktika buvo remiamasi aiškinant tam tikrų BDAR normų bendro taikymo ypatumus.

[1]Prieiga internetu: https://epub.uni-regensburg.de/37113/1/Dissertation%20-%20Data%20Protection%20in%20the%20Internet%20of%20Things%20-%20Santiago%20Reinhard%20Suppan%20-%20August%202017%20-%20Contributed.%20pdf.
[2]Prieiga internetu: https://hal.archives-ouvertes.fr/tel-02496151/document.
[3]Prieiga internetu: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwj2w_f-yYvwAhUpxosKHQ4mC-AQFjAAegQIAhAD&url=https%3A%2F%2Ffenix.tecnico.ulisboa.pt%2FdownloadFile%2F1407770020546701%2FProtecting%2520Personal%2520Data%2520and%2520Privacy%2520in%2520the%2520EU%2520in%2520the%2520Rise%2520of%2520the%2520Internet%2520of%2520Things.pdf&usg=AOvVaw2sA5ReuiZak45OqMt5v9Z2.

Šiame darbe pagrindiniais *soft law* šaltiniai yra ES Duomenų apsaugos direktyvos 29 straipsniu įsteigtos Darbo grupės asmenų apsaugai tvarkant asmens duomenis (toliau – ES 29 straipsnio darbo grupė) išleistos nuomonės ir gairės, daugiausiai remiamasi ES 29 str. darbo grupės nuomone dėl naujausių daiktų interneto pokyčių[4].

Remiantis teisės doktrina ir nagrinėjant BDAR normų taikymą daiktų internetui didžiausias dėmesys buvo skiriamas šių mokslininkų darbams: N. Ni Loideain (Ni Loideain, 2018), S. Wachter (Wachter, 2017), (Wachter, 2018), S. Eskens (Eskens, 2016) (šių autorių darbai orientuoti į daiktų interneto ir BDAR taikymo daiktų internetui ypatumus, probleminius aspektus) J. Zaleskio (Zaleskis, 2019) (šio autoriaus darbais remiamasi aiškinant duomenų apsaugos teisės ypatumus, atskiras BDAR normas).

[4]Pilnas pavadinimas: ES 29 str. duomenų apsaugos darbo grupė 2014 m. rugsėjo 16 d. Nuomonė Nr. 8/2014 dėl naujausių daiktų interneto pokyčių Nr. WP 223.

1. DAIKTŲ INTERNETAS IR JO TEISINIO REGULIAVIAMO ŠALTINIŲ SISTEMA

1.1. Daiktų interneto samprata

Daiktų interneto (angliškai – *Internet of things (IoT*)) idėja buvo paminėta jau 1926 m., kai inžinierius Nikola Tesla Collier žurnalui duotame interviu išreiškė: „Puikiai pritaikius belaidį ryšį, visa žemė bus paversta didžiulėmis smegenimis, kurios iš tikrųjų yra tikros ir ritmiškos visumos dalelės ..... ir įrankiai, kuriais galėsime tai padaryti bus ypatingai paprasti, palyginti su dabartiniu mūsų telefonu. Vyras galės nešiotis vieną savo liemenės kišenėje.“ (Vermesan *et al*., 2012, p. 24). Iš esmės tai apibūdina daiktų interneto veikimo principą. Objektams ir programoms susiejus jų surinktus duomenis, visi mūsų kasdienybėje naudojami įrenginiai tampa vis paprastesni naudoti. J. Gubbi ir kiti daiktų internetą apibūdina kaip jutimo ir įjungimo įtaisų tarpusavio sujungimą, suteikiantį galimybę dalytis duomenimis visose platformose per vieningą sistemą, sukuriant bendrą veiklos vaizdą, leidžiantį diegti novatoriškas programas. Tai pasiekiama taikant sklandų visur aptikimą, duomenų analizę ir informacijos pateikimą, o debesų kompiuterija yra vienijanti sistema (Gubbi, et. al., 2013 cituota Jusas, 2017, p. 16). Taigi, daiktų internetas paprasčiau gali būti apibūdintas kaip tinklas tarp fizinių objektų, kuriuo šie objektai (daiktai) gali dalintis surinktais duomenimis. Šie fiziniai objektai yra laikomi išmaniaisiais ir gali rinkti tam tikrus duomenis. Tokiais „išmaniaisiais“ daiktais gali būti laikomi įvairaus pobūdžio daiktai nuo įprastų daiktų su jutikliais, buitinės technikos iki automobilių (European Parliamentary Research Service, 2015, p. 2). Tikriausiai Nikola Tesla dar 1926 m. kalbėdamas apie belaidį ryšį ir jo pritaikymą, nenumanė, jog taip greitai tokia jo vizija taps realybe, įgyvendinama per daiktų internetą.

Duomenys dažniausiai yra renkami siekiant užtikrinti, jog daikto atliekamos funkcijos būtų kuo naudingiau pritaikytos vartotojo poreikiams. Beveik kiekvienas duomuo, surenkamas naudojant objektą, gali būti panaudojamas. Susiejant įrenginius, programas ir jų surinktus duomenis tarpusavyje į vieną vartotojo tapatybę, tokių prietaisų ar paslaugų naudojimas gali būti individualizuotas, atsižvelgiant į vartotojo elgesį, preferencijas naudojant įrenginius ir iš tokių duomenų padarytas išvadas (Schermer, 2011 cituota Wachter, 2018, p. 10). Pavyzdžiui, kartais net duomuo, kaip tam tikras vartotojas naudoja lempos jungiklį (kaip jį įjungia / išjungia, kokiu metu dažniausiai įjungia / išjungia), tampa labai vertingu jį susiejus su kitais to paties vartotojo iš kitų programų ar objektų surinktais duomenimis.

Akivaizdu, jog internetu ar aplikacijomis valdomų objektų kasdieniniame gyvenime vis daugėja ir vis daugiau jų tampa neatsiejama gyvenimo dalimi. 2020 metų statistikos duomenimis, net dešimt procentų Lietuvoje gyvenančių suaugusių asmenų naudojo bent vieną prie interneto prijungtą namų apsaugos sistemą, apšvietimo, energijos valdymo sistemą, buitinį prietaisą ar virtualųjį asistentą savo namų ūkyje. Tarp tokių prietaisų gali būti namų apsaugos sistemos, dūmų detektoriai, saugumo kameros, durų spynos, automatiniai dulkių siurbliai, šaldytuvai, kavos aparatai ar kiti prie interneto prijungti prietaisai (Oficialiosios statistikos portalas, 2020). Vis didėjančiai prie interneto prijungtų prietaisų paklausai įtakos turi tai, jog elektronika kuriama vis mažesnė ir pigesnė, tokiu būdu ji tampa labiau įperkama bei patogesnė vartotojams (Misra, *et al*. 2021, p. 76).

Kažkada tik paprastoms žinutėms išsiųsti naudotas internetas dabar yra naudojamas prijungti prie plačios įvairovės išmaniųjų prietaisų. Toks pasikeitimas įvyko per keletą dešimtmečių. Sparčiai daiktų interneto plėtrai įtaką dariusiems faktoriams galima priskirti: technologijas, padėjusias pamatus susietoms sistemoms, palankų visuomenės požiūrį į besivystančias technologijas bei akivaizdžią naudą, kurią šios technologijos suteikia. Anot autorių S. Misra, A. Mukherjee, ir A. Roy, šiuolaikinis daiktų internetas pasiekė dabartinę stadiją šiais etapais (Misra, *et al*. 2021, p. 77-82)[5]:

1) bankomatai. Jie yra susieti su vartotojo banko sąskaita (patikrinę vartotojo tapatybę ir jo sąskaitą per specialiai užkoduotą kortelę, išduoda grynuosius pinigus). Bankomatai buvo sukurti vartotojų patogumui - užtikrinti, jog net ir banko nedarbo metu jų klientai galėtų pasinaudoti grynųjų pinigų išsiėmimo paslauga. Pirmasis prie interneto prijungtas bankomatas pradėjo veikti jau 1974 metais.

2) Žiniatinklis. Globaliu mastu veikiantis žiniatinklis yra pasaulinė keitimosi informacija ir komunikacijos platforma. Pirmą kartą žiniatinklis pradėjo veikti 1991 metais.

3) Išmanieji skaitikliai. Pirmasis išmanusis skaitiklis buvo galios matuoklis, pradėjęs veikti 2000 m.

4) Skaitmeninės spynos. Šiandienos skaitmeninės spynos yra itin pažengusios technologine prasme, jas valdyti (atrakinti / užrakinti) galima naudojant išmaniuosius telefonus.

5) „Prijungta“ sveikatos priežiūra (angl. *connected healthcare*). Sveikatos priežiūros prietaisai jungiasi prie ligoninių, gydytojų ir artimųjų susietų išmaniųjų įrenginių, prietaisų, kad įspėtų juos apie ekstremalias medicinos situacijas ir paragintų imtis prevencinių

[5]Kiekvienas raidos etapas sąlygojo tapačios daiktų interneto rūšies atsiradimą.

priemonių. Tokie prietaisai gali būti paprasti nešiojami prietaisai, stebintys paciento širdies ritmą ir pulsą, taip pat įprasti medicinos prietaisai, kaip monitoriai ligoninėse.

6) „Prijungtos“ transporto priemonės (angl. *connected vehicles*). Tokios transporto priemonės gali prisijungti prie interneto ar komunikuoti su kitomis transporto priemonėmis arba net su jose esančiais jutikliais. Šios transporto priemonės gali pačios atlikti diagnostinius tyrimus ir pranešti savininkui apie galimus gedimus.

7) Išmanieji miestai. Tai pažangių jutimo, stebėjimo ir valdymo sistemų diegimas visame mieste. Pažangi miesto infrastruktūra leidžia suvienodinti ir sinchronizuoti operacijas bei skleisti duomenis, siekiant pagerinti suteikiamas paslaugas, pavyzdžiui, stovėjimo aikštelėse, viešajame transporte ir pan.

8) „Smart Dust“ - tai yra mikroskopiniai kompiuteriai. Mažesni nei smėlio grūdeliai, galimi pritaikyti įvairiose srityse, pavyzdžiui, išmatuoti dirvožemyje esančias chemines medžiagas ar net nustatyti žmogaus organizmo problemas.

9) Išmaniosios gamyklos. Jos gali savarankiškai stebėti daugumą gamyklos procesų, taip sumažinant žmogaus padaromų klaidų skaičių.

10) Galiausiai, UAV (nepilotuojami orlaiviai) (angl. *unmanned aerial vehicles*).

ES 29 straipsnio darbo grupė daugiausiai dėmesio reikalaujančius asmens duomenis renkančius ir tvarkančius daiktų interneto įrenginius dėl jų saugumo išskyrė į tris pagrindines kategorijas (ES 29 straipsnio darbo grupė, 2014, p. 5-6):

1) dėvimi kompiuteriniai prietaisai (angl. *Wearable Computing*). Tai kasdieniai daiktai, kuriuos galime dėvėti ant kūno, pavyzdžiui, laikrodis, akiniai ar net rūbai. Žinoma, šių daiktų funkcijos yra kur kas platesnės nei įprastų, prie interneto neprijungtų daiktų, nors iš išvaizdos išmaniosios daiktų versijos yra beveik neatskiriamos nuo savo pirmtakių. Dėvimi kompiuteriniai prietaisai gali turėti įmontuotas kameras, mikrofonus, jutiklius, galinčius rinkti įvairius duomenis apie asmens įpročius.

2) Kiekybinio įvertinimo (angl. *Quantified Self*). Tai prietaisai, gebantys įvertinti ir pateikti vartotojui duomenis apie jo įpročius, gyvenimo būdą. Tai gali būti įvairūs prietaisai: išmaniosios apyrankės, sekančios asmens aktyvumą, išmanieji žiedai, analizuojantys asmens miego kiekybę ir kokybę, išmaniosios svarstyklės, išmanieji laikrodžiai, galintys nustatyti asmens kraujospūdį ar net deguonies kiekį kraujyje. Ilgainiui, prietaisai analizuodami tokius duomenis gali padaryti tam tikras išvadas apie asmens fizinę bei psichologinę sveikatą. Žinoma, dauguma tokių prietaisų gali būti priskiriami ir prie pirmosios išskirtos kategorijos – dėvimų kompiuterinių prietaisų, dėl pačių vartotojų patogumo.

3) Namų automatika („domotika“) (angl. *domotics*). Tai išmanieji prietaisai naudojami namų ūkyje ar ofisuose. Tai gali būti įvairūs įprastai namuose naudojami prietaisai, nuo kavos aparato iki žoliapjovės. Daugiausiai paplitę namų įrenginiai yra išmanieji asistentai (garsiakalbiai) (angl. *smart assistant*), dūmų detektoriai, saugumo kameros, durų spynos, automatiniai dulkių siurbliai, šaldytuvai, termostatai, apšvietimo sistemos (Oficialiosios statistikos portalas, 2020).

Atsižvelgiant į tai, kas išdėstyta, galime daryti išvadas, jog, pradedant nuo labai paprastų technologijų įvedimo į kasdieninį gyvenimą bei su laiku vis tobulėjant technologijoms, daiktų internetas pamažu apėmė beveik visas gyvenimo sritis ir šiuo metu gali būti pritaikomas bet kur. Plačios įrenginių galimybės rinkti įvairaus pobūdžio su asmeniu susijusius duomenis gali sukelti tam tikrų su asmens saugumu susijusių iššūkių.

1.2. Daiktų interneto keliami iššūkiai bei jų sąsaja su duomenų apsauga

Daiktų internetas, kaip aptarta anksčiau, pasižymi bet kokių duomenų, susijusių su prietaiso naudojimu, rinkimu. Nors būtent ši daiktų interneto savybė atneša didžiausią naudą ir palengvina kiekvienos dienos prietaisų, įrenginių naudojimą, tačiau kelia ir tam tikrų iššūkių. Suprantama, kad, esant įvairaus pobūdžio dideliam duomenų kiekiui, kyla ir rizikų bei problemų. Surinkus duomenis iš įvairių prietaisų, gali kilti grėsmė ir šių objektų vartotojo teisėms, tokioms kaip teisei į privatumą ar teisei į asmens duomenų apsaugą.

Teisė į privatumą yra užtikrinama tarptautiniu lygiu. Tai yra viena iš pamatinių žmogaus teisių. Visuotinė žmogaus teisių deklaracija numato, 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.*“ (Visuotinė žmogaus teisių deklaracija, 1948). Naudojant daiktų internetą ir netinkamai valdant jo surenkamus duomenis kartais galima rizika, jog būtent ši asmens teisė gali būti pažeista. Daiktų interneto įrenginiai renka įvairius duomenis realiu laiku, kurie gali būti susiję su vartotojo buvimo vieta, finansais, sveikata, kontaktais, veikla. Iš surinktų duomenų galima sudaryti asmens „profilį“ (profiliavimas[6]) apie jo įpročius, elgesio pokyčius. Visi šie duomenys gali būti saugomi, analizuojami ir prieinami kitiems tinkle esantiems įrenginiams ar net kitiems vartotojams. Turint tokius su asmeniu susijusius

[6]Profiliavimas – procedūra, galinti apimti daugiau kaip vieną statistinės dedukcijos operaciją. Jis dažnai taikomas žmonių savybėms prognozuoti naudojant iš įvairių šaltinių gautus duomenis, siekiant padaryti kokias nors išvadas dėl asmens, remiantis kitų, statistiniu požiūriu panašių asmenų savybėmis (ES 29 straipsnio darbo grupė, 2017b, p. 7).

duomenis, yra gan lengva sudaryti asmens profilį apie jo asmeninį privatų gyvenimą, kurio asmuo galbūt nenorėtų atskleisti.

Būtent vienas iš pagrindinių teisės į privatumą elementų yra asmens teisė neatskleisti tam tikros informacijos apie savo asmeninį privatų gyvenimą (Janis, *et al*., 2000 cituota Maras, 2015, p. 102). Naudojant daiktų internetą, gali būti atvejų, kai nuo paties vartotojo nepriklauso, ar tokia informacija išliks „slapta“. Taip gali būti pažeista vartotojo teisė į privatumą (Maras, 2015, p. 102). Taigi, kartais daiktų interneto savybė rinkti kuo įvairesnius duomenis apie asmenį, asmens įpročius gali pažeisti pastarojo teisę į privatumą. Pavyzdžiui, vokiečių mokslininkai atliko eksperimentą, kaip prisijungus prie vieno įrenginio galima gauti duomenis iš kito įrenginio, prijungto prie daiktų interneto. Šio tyrimo metu mokslininkai nustatė, kad išmanieji skaitikliai[7] gali stebėti vartotojų elgesį. Energijos suvartojimo duomenys, perduodami komunalinių paslaugų įmonei, leidžia įsibrauti, identifikuoti ir stebėti įrangą vartotojų namuose (pvz., televizorių, šaldytuvą, skrudintuvą ir orkaitę). Tyrimo metu taip pat buvo nustatyta, kad esant tam tikram imties dažniui įmanoma net nustatyti, kokį kanalą tuo metu rodė namuose esantis televizorius. Taip pat galima nustatyti garso ir vaizdo turinį rodomą per televizorių (Greveler, 2012, p. 1).

Daiktų interneto saugumas yra pažeidžiamas, kadangi veikia bevieliu ryšiu (Zalieckaitė, *et al*., 2015, p. 111). Dėl šios priežasties gali atsirasti įsilaužimų rizika. Įrenginiai, neturintys būtinų apsaugos priemonių, tampa dar lengviau pasiekiami įsilaužėliams. Įsilaužus, į netinkamas rankas gali patekti įvairaus pobūdžio duomenys, surinkti iš prietaisų. Priklausomai nuo duomenų pobūdžio, vėliau įsilaužėlis gali juos netinkamai panaudoti ir taip sukelti pavojų vartotojui, ypač jeigu duomenys yra susiję su vartotojo medicinine informacija, finansiniais duomenimis (Maras, 2015, p. 100). Tokiu būdu gali būti įvykdyta asmens tapatybės vagystė. Kai vartotojui nėra pranešama, jog įvyko įsilaužimas, pažeidžiama asmens teisė žinoti apie įvykusį pažeidimą, apie tai, ar naudojami ir kur naudojami apie jį surinkti duomenys, kuriuos jis norėtų laikyti neatskleistus.

Asmens teisei į privatumą pavojus dažai gali kilti ir dėl kitų asmenų teisės į privatumą, privataus asmeninio ir šeimos gyvenimo negerbimo. Teisė į privataus gyvenimo gerbimą ir duomenų apsaugos teisė, nors ir glaudžiai susijusios, vis dėl to yra dvi atskiros teisės. Duomenų apsaugos teisė yra platesnė ir taikoma, kai yra tvarkomi asmens duomenys (Europos Sąjungos pagrindinių teisių agentūra; Europos Taryba, 2019, p. 18). Dėl asmens duomenų, kuriuos renka daiktų internetas, tvarkymo, kyla iššūkių asmens teisei į privatų

[7]Tokie skaitikliai Vokietijoje yra įdiegti visuose šalyje esančiuose elektros tinkluose.

gyvenimą. Todėl galima teigti, jog siekiant apsaugoti teisę į privatumą, daiktų internetui turi būti taikomas duomenų apsaugos teisinis reguliavimas.

Sunkumų sklandžiam ir saugiam daiktų interneto naudojimui gali kelti ir duomenų apsaugos teisės reguliavimo nesilaikymas. Pagrindiniai iššūkiai taikant duomenų apsaugos teisę daiktų internetui išskiriami šie: minimizavimas, tikslų apribojimas, duomenų saugojimas / ištrynimas, automatizuotas sprendimų priėmimas / profiliavimas (įskaitant diskriminaciją) ir saugumo reikalavimai (Wachter, 2018, p. 9). Plačiau apie šiuos iššūkius bus aptariama tolimesnėse darbo dalyse.

Tam, jog daiktų internetas būtų naudojamas saugiai, nepažeidžiant asmenų teisės į privatų gyvenimą ir duomenų apsaugos teisės, yra svarbu užtikrinti tinkamą duomenų apsaugos reguliavimą bei jo taikymą.

1.3. Daiktų interneto duomenų apsaugos reguliavimo sistema

Kadangi asmens teisei į privatumą iššūkių kelia daiktų interneto savybė rinkti asmens duomenis, kaip ir aptarta anksčiau, šios srities reguliavimui turėtų būti taikomos asmens duomenų apsaugą reguliuojančios teisės normos. Šiame skyriuje bus aptariami svarbiausi asmens duomenų apsaugos teisės šaltiniai, taip pat pagrindiniai teisės šaltiniai, įtvirtinantys teisę į privatumą.

Teisės doktrinoje teisės šaltiniai gali būti skirstomi pagal tam tikras klasifikacijas į atskiras rūšis. Remiantis bendriems teisės šaltiniams taikoma klasifikacija, galima išskirti ir daiktų internetui taikomos duomenų apsaugos teisės šaltinius. Darbe bus aptariama duomenų apsaugos teisės šaltinių klasifikacija pagal tai, kokiai teisės sistemai šie šaltiniai priklauso, aptariant tiek pirminius, tiek antrinius ir *soft law* šaltinius. Pagal tai, kokiai teisės sistemai priklauso, duomenų apsaugos teisės šaltiniai gali būti skirstomi į tris pagrindines rūšis: tarptautinės duomenų apsaugos teisės šaltiniai, ES duomenų apsaugos teisės šaltiniai bei nacionaliniai duomenų apsaugos teisės šaltiniai[8] (Zaleskis, 2019, p. 60).

Pirmiausia aptarsiu tarptautinės duomenų apsaugos teisės šaltinius. Kaip ir visos tarptautinės viešosios teisės, tarptautiniais duomenų apsaugos teisės šaltiniais galima laikyti tarptautines sutartis, tarptautinius papročius, *jus cogens* principus, teismų praktiką, autoritetingų specialistų doktriną, kaip tai išskirta Tarptautinio Teisingumo Teismo statute (Tarptautinio Teisingumo Teismo statutas, 1946). Taip pat vienašaliai valstybių aktai bei antriniai teisės šaltiniai, kaip tarptautinių organizacijų rezoliucijos, *soft law* šaltiniai ir kiti.

[8]Šiame skyriuje aptariant nacionalinius duomenų apsaugos teisės šaltinius dėmesys bus skiriamas Lietuvos nacionalinei teisei.

(Shaw, 2008 cituota Zaleskis, 2019, p. 63). Svarbu paminėti, jog bendrų šaltinių, taikomų tarptautiniu mastu ir turinčių privalomąją galią valstybėms, reglamentuojančių tarptautinę duomenų apsaugos teisę kaip atskirą teisę, nėra. Jungtinių Tautų sistemoje asmens duomenų apsauga nepripažįstama pagrindine teise, tačiau yra pripažįstama teisė į privatumą (Europos Sąjungos pagrindinių teisių agentūra; Europos Taryba, 2019, p. 21), kuri yra svarbi daiktų interneto ir visos duomenų apsaugos teisės kontekste. Teisė į privatumą, kaip vienas iš duomenų apsaugos teisės tikslų, užtikrinama keliuose tarptautiniuose teisės šaltiniuose. Pirmasis tarptautinis teisės aktas, užtikrinęs teisę į privatumą, buvo 1948 m. priimta Visuotinė žmogaus teisių deklaracija. Vėliau priimtas ir kitas Jungtinių Tautų dokumentas, užtikrinantis teisę į privatumą – Jungtinių Tautų (toliau – JT) pilietinių ir politinių teisių paktas. Teisė į privatumą taip pat užtikrinama ir 1950 m. Europos Tarybos (toliau – ET) išleista Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija (toliau – EŽTK). Užtikrinant teisių ir laisvių, numatytų EŽTK, gerbimą, buvo įsteigtas ir Europos Žmogaus Teisių Teismas, kurio kompetencijai priklauso ir bylų, susijusių su dėl daiktų interneto atsiradusių teisių pažeidimu, sprendimas. Asmens duomenų apsauga užtikrinama per šios konvencijos 8 straipsnį. Vėliau ET priėmė ir kitą teisės aktą – Konvenciją dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu. Daiktų interneto technologijomis duomenys yra tvarkomi automatizuotu būdu, kas taip pat kelia tam tikrų duomenų apsaugos teisės užtikrinimo iššūkių, tad ši konvencija yra itin svarbus tarptautiniu lygiu (ne tik ES lygiu) taikomas teisės šaltinis. Taip pat yra ir antrinių teisės šaltinių, detaliau aptariančių duomenų apsaugos teisės reguliavimą tarptautiniu mastu. Nuo 2013 m. JT buvo išleistos rezoliucijos, aptariančios teisės į privatumą iššūkius skaitmeniniame amžiuje (Europos Sąjungos pagrindinių teisių agentūra; Europos Taryba, 2019, p. 22). Bene svarbiausias tarptautinis *soft law* šaltinis yra Ekonominio bendradarbiavimo ir plėtros organizacijos (toliau – EBPO) privatumo gairės, kuriose įtvirtinti pagrindiniai duomenų apsaugos teisės principai (Zaleskis, 2019, p. 66). Įvairias gaires ir rekomendacijas dėl duomenų apsaugos yra pateikusi ir ET.

Technologijų plėtra bei duomenų apsaugos teisės įtvirtinimas tarptautiniu lygiu paskatino ieškoti sprendimų šios teisės apsaugai ir ES lygmeniu. Pirminis ir bene pagrindinis teisės šaltinis, pripažįstantis duomenų apsaugos teisę, yra ES pagrindinių teisių chartija, kurios 8 straipsnis įtvirtina kiekvieno asmens teisę į duomenų apsaugą. Teisę į duomenų apsaugą reguliuoja ir direktyvos. Svarbiausia šiuo atveju yra iki 2018 m. galiojusi Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (toliau – ES duomenų apsaugos direktyva). Ši direktyva buvo pagrindas ir dabartiniam reguliavimui – BDAR.

Svarbu yra paminėti ir ES 29 straipsnio darbo grupės nuomones bei rekomendacijas dėl duomenų apsaugos teisės ir daiktų interneto reguliavimo. Daiktų interneto reguliavimui ir šiam darbui aktualiausi šie *soft law* šaltiniai: ES 29 straipsnio darbo grupės nuomonės, gairės ir kiti ES duomenų apsaugos direktyvos normas aiškinantys dokumentai, Europos duomenų apsaugos valdybos (toliau – EDAV) nuomonės ir rekomendacijos, Europos duomenų apsaugos priežiūros pareigūno nuomonės bei ESTT praktika.

Vienintelis būtent daiktų interneto technologijoms skirtas ES 29 straipsnio darbo grupės parengtas *soft law* šaltinis yra ES 29 str. darbo grupės nuomonė dėl naujausių daiktų interneto pokyčių. Šioje nuomonėje yra aiškinamos atskiros, BDAR įtvirtintos normos (asmens duomenų, duomenų subjekto, valdytojo, tvarkytojos sąvokos, kaip jos siejamos su daiktų internetu, duomenų apsaugos principų taikymas daiktų interneto technologijomis vykdomam asmens duomenų tvarkymui, svarbiausios daiktų interneto vartotojo – duomenų subjekto teisės). Kiti ES 29 straipsnio darbo grupės parengti dokumentai, ypač aktualūs daiktų interneto technologijomis tvarkomų asmens duomenų reguliavimui, yra ES 29 straipsnio darbo grupės automatizuoto atskirų sprendimų priėmimo ir profiliavimo gairės. Asmens duomenų tvarkymas daiktų interneto technologijomis yra atliekamas automatizuotomis priemonėmis (įskaitant profiliavimą), šios gairės analizuoja aktualias BDAR normas tokiam asmens duomenų tvarkymui. Taip pat svarbios kitos ES 29 straipsnio darbo grupės rekomendacijos dėl atskirų asmens duomenų apsaugos principų, duomenų subjekto teisių, reikalavimų duomenų valdytojui reikalavimų įgyvendinimo, gali būti taikomos duomenis tvarkant daiktų interneto technologijomis (pavyzdžiui, skaidrumo užtikrinimo gairės, teisės į duomenų perkeliamumą gairės ir kt.). Priėmus BDAR, ES 29 straipsnio darbo grupę pakeitė BDAR pagrindu įsteigta Europos duomenų apsaugos valdyba. Pastaroji toliau sistemingai *soft law* šaltiniais aiškina BDAR įtvirtintą reguliavimą. Pavyzdžiui, gairėmis dėl BDAR teritorinės taikymo srities (Europos duomenų apsaugos valdyba, 2019), detalizuojama BDAR norma, reguliuojanti teritorinį BDAR taikymą. Šiomis gairėmis galima naudotis ir siekiant nustatyti, ar tam tikromis daiktų interneto technologijomis atliekamas asmens duomenų tvarkymas patenka į BDAR reguliavimo sritį ir ar daiktų interneto vartotojo teisės bus užtikrintos būtent pagal šį teisės aktą. ESTT atskiros praktikos dėl BDAR normų taikymo daiktų internetui dar nėra suformavusi, tačiau, yra išvysčiusi praktiką aiškindama BDAR normas bei jų taikymą. Tokius ESTT sprendimus galima pritaikyti ir siekiant nustatyti, kaip ESTT aiškinamos normos turėtų būti taikomos daiktų internetui.

Lietuva, kaip Jungtinių Tautų ir EŽTK narė, nacionalinėje teisėje taip pat atsižvelgia į minėtą tarptautiniu mastu nustatytą reguliavimą. Teisę į privatumą užtikrina aukščiausiąją

teisinę galią turintis teisės šaltinis – Lietuvos Respublikos Konstitucija (22 straipsnis). Tapusi ES nare, Lietuva įsipareigojo taikyti ES teisės aktus nacionalinėje teisėje bei atsižvelgia į tarptautinius bei ES antrinius teisės šaltinius. Tik nacionaliniu mastu duomenų apsaugos teisei reguliuoti yra priimtas Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas (toliau – Duomenų apsaugos įstatymas), taikomas kartu su BDAR (Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo Nr. I-1374 pakeitimo įstatymas, 2018), jis yra aktualiausias šiam darbui įstatymo galią turintis nacionalinės teisės šaltinis. Šiam įstatymui, kaip ir Tarptautiniu ir ES lygiu priimtiems duomenų apsaugą reguliuojantiems teisės aktams, yra būdingas technologinis neutralumas. Atskirai daiktų internetą reguliuojančio įstatymo galią turinčio nacionalinės teisės šaltinio nėra. Tačiau nuostatos, numatytos Duomenų apsaugos įstatyme, kaip ir kituose teisės šaltiniuose yra taikomos daiktų internetui kaip bendrasis teisės šaltinis. Žinoma pagrindiniu duomenų apsaugos teisę reguliuojančiu teisės aktu lieka BDAR, kuris nacionalinėje teisinėje sistemoje yra taikomas tiesiogiai. Taip pat Lietuvoje duomenų apsaugos teisės kontekste yra svarbūs poįstatyminiai teisės aktai – Valstybinės duomenų apsaugos inspekcijos (toliau – VDAI) direktoriaus įsakymais patvirtinti teisės aktai, kuriais įgyvendinamas BDAR (Zaleskis, 2019, p. 81). VDAI taip pat teikia rekomendacijas ir konsultacijas, kurios taikomos kaip *soft law* šaltiniai. Kaip nacionalinis teisės šaltinis yra ir teismų praktika, tačiau daiktų interneto kontekste Lietuvoje teismų praktika nėra suformuota.

2. BENDROJO DUOMENŲ APSAUGOS REGLAMENTO TAIKYMO DAIKTŲ INTERNETUI APIMTIS

2.1. Asmens duomenų sąvoka pagal Bendrąjį duomenų apsaugos reglamentą

BDAR 2 straipsnis numato, jog BDAR yra taikomas asmens duomenų tvarkymui visiškai arba iš dalies atliekamam automatizuotomis priemonėmis, ir asmens duomenų, kurie sudaro susisteminto rinkinio dalį ar yra skirti ją sudaryti, tvarkymui ne automatizuotomis priemonėmis (BDAR 2 str.). Svarbu nustatyti, kokia informacija sudaro asmens duomenis, bei kokiu būdu jie yra tvarkomi, tam, jog galėtume nustatyti, ar BDAR nuostatos yra tinkamos taikyti daiktų internetui. Šiuo atveju svarbu atkreipti dėmesį, jog BDAR taikomas asmens duomenų tvarkymui automatizuotomis priemonėmis. Būtent tokiu būdu yra tvarkomi daiktų interneto duomenys.

Asmens duomenų sąvoka yra įtvirtinta BDAR 4 straipsnyje, kuriame nurodoma, jog asmens duomenys suprantami kaip bet kokia informacija apie fizinį asmenį, kurio tapatybė yra nustatyta arba galima (tiesiogiai ar netiesiogiai) nustatyti pagal identifikatorių, asmens identifikavimo numerį, buvimo vietos duomenis ir interneto identifikatorių arba pagal vieną ar kelis to fizinio asmens fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar socialinės tapatybės požymius (BDAR 4 str.). Kadangi daiktų interneto renkami duomenys gali būti įvairaus pobūdžio, svarbu identifikuoti, kurie iš jų gali būti laikomi asmens duomenimis ir taip numatyti, kokia apimtini yra taikomas BDAR.

Duomenų apsaugos sąvoka, apibrėžta ES duomenų apsaugos direktyvoje, liko nepakeista ir BDAR. ES 29 straipsnio darbo grupės nuomonėje dėl asmens duomenų sąvokos (ES 29 straipsnio darbo grupė, 2007, p. 5) yra išskirti keturi asmens duomenų sąvokos elementai:

1) bet kuri informacija,
2) informacija, susijusi su asmeniu,
3) fizinis asmuo, kurio tapatybė yra nustatyta arba gali būti nustatyta,
4) fizinis asmuo.

Kiekvienas iš šių elementų bus aptartas plačiau, siejant su daiktų interneto renkama informacija.

Kalbant apie „bet kurios informacijos“ aspektą, ES 29 straipsnio darbo grupė pabrėžia, kad tokia formuluote teisės aktų leidėjas siekia nustatyti kuo platesnę asmens duomenų sąvokos apimtį. Tai apima ir biometrinius duomenis. Tokiais duomenimis yra laikomi ne tik biologinės, fiziologinės savybės (pavyzdžiui, piršto antspaudas ar akies

rainelės struktūra), bet ir gyvenimo ypatumai, tam tikri asmens įpročiai, veiksmai. (ES 29 straipsnio darbo grupė, 2007, p. 6). Būtent tokio pobūdžio duomenys, kaip aptarta anksčiau, yra renkami daiktų interneto (pavyzdžiui, šviesos jungiklio naudojimo įpročiai). Pastarojo renkamus duomenis apie asmens įrenginio naudojimo įpročius pagal tokį išaiškinimą galima būtų priskirti prie „bet kurios informacijos“.

Informacija, susijusi su asmeniu, reiškia, jog konkreti informacija gali būti susieta su konkrečiu asmeniu, todėl svarbiausias yra tikslo elementas. Yra išskiriama, kad tikslo elementas atsiranda, kai duomenys bus naudojami siekiant įvertinti arba nagrinėti asmens padėtį ar elgesį arba daryti jiems įtaką (ES 29 straipsnio darbo grupė, 2007, p. 10). Daiktų interneto technologijomis duomenys renkami tikslu išanalizuoti tam tikrus asmens įpročius, elgesį ir iš duomenų sudarytas išvadas vėliau pritaikyti asmeniui naudojant prietaisą. Taigi, galima teigti, jog daiktų interneto renkama informacija yra susijusi su asmeniu.

Trečiasis asmens duomenų sąvoką apibūdinantis elementas – duomenimis nustatyta arba gali būti nustatyta fizinio asmens tapatybė. Nagrinėjant, ar iš duomenų galima nustatyti asmens tapatybę, svarbu suprasti, jog asmens tapatybė gali būti nustatyta ne tik iš asmens vardo, pavardės ar asmens kodo (tiesioginis tapatybės nustatymas). ESTT praktikoje yra išaiškinta, jog tam, kad informacija būtų laikoma asmens duomenimis, nebūtina, kad ji pati savaime leistų nustatyti atitinkamo asmens tapatybę. Taip pat reikėtų atsižvelgti į visas priemones, kuriomis galėtų pasinaudoti duomenų valdytojas ar bet kuris kitas asmuo minėto asmens tapatybei nustatyti (*Breyer*, 2014, 41-44 punktai). Iš teismo išaiškinimo galima suprasti, jog asmens tapatybė gali būti atpažinta ir pagal naudojamą IP adresą, radijo dažnio atpažinimo žymenis, taikomųjų programų, priemonių ir protokolų interneto identifikatorius (Zaleskis, 2019, p. 95). Tokie identifikatoriai yra naudojami daiktų internete. Renkant ir dalinantis informacija daiktų interneto technologijomis, galimas asmens profiliavimas, taip sudarant galimybę nustatyti asmens tapatybę. ES 29 straipsnio darbo grupė taip pat išskiria, kad net duomenis apie asmenis, kuriuos ketinama tvarkyti tik įgyvendinus pseudonimizaciją ar net anonimizavimo metodus, gali tekti laikyti asmens duomenimis (ES 29 str. duomenų apsaugos darbo grupė, 2014, p. 11).

Paskutinis elementas, išskirtas reguliavime, yra tai, jog duomenys yra susiję su fiziniu asmeniu. Atsižvelgiant į teisės akto leidėjo tikslą, reguliavimas taikomas tik su fiziniais asmenimis susijusių duomenų tvarkymui. Vadinasi, daiktų interneto renkami duomenys turi būti būtinai siejami su fiziniu asmeniu, kad konkrečiu atveju būtų taikomos BDAR nuostatos.

Taip pat BDAR išskiria specialių kategorijų asmens duomenis, kurie yra draudžiami tvarkyti, išskyrus tam tikras išimtis. Prie specialių kategorijų asmens duomenų yra priskiriami duomenys, atskleidžiantys rasinę ar etninę kilmę, politines pažiūras, religinius ar filosofinius įsitikinimus ar narystę profesinėse sąjungose, taip pat genetiniai duomenys, biometriniai duomenys, siekiant konkrečiai nustatyti fizinio asmens tapatybę, sveikatos duomenys arba duomenys apie fizinio asmens lytinį gyvenimą ir lytinę orientaciją. (BDAR, 9 str. 1.d.). Tokie duomenys gali būti gaunami ne tik tiesiogiai iš duomenų subjekto. Daiktų interneto technologijomis tvarkomų duomenų valdytojai, vykdydami profiliavimą, gali gauti specialiųjų kategorijų duomenis juos išvedant iš kitų duomenų, kurie patys nėra specialių kategorijų duomenys, bet tokiais tampa, kai sujungiami su kitais duomenimis (ES 29 str. duomenų apsaugos darbo grupė, 2017b, p. 16).

Apibendrinant, pagal BDAR pateiktą apibrėžimą daiktų interneto tvarkomus duomenis galima laikyti asmens duomenimis. Todėl, daiktų interneto duomenys turėtų būti tvarkomi pagal BDAR numatytą reguliavimą.

2.2. Duomenų valdytojas, tvarkytojas, jų vaidmuo daiktų internete

BDAR pateikia šią duomenų valdytojo sąvoka: fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuris vienas ar drauge su kitais nustato duomenų tvarkymo tikslus ir priemones[9]. Yra numatyta galimybė duomenų valdytojui paskirti duomenų tvarkytoją, kuris duomenų valdytojo vardu tvarkys asmens duomenis (BDAR 4 str.). Ne visuomet gali būti atskiras duomenų tvarkytojas, kartais duomenų tvarkymą atlieka pats duomenų valdytojas. Svarbu, kad tokiu atveju, kai yra paskiriamas duomenų tvarkytojas, pareiga užtikrinti, kad duomenys būtų tvarkomi laikantis BDAR nuostatų, išlieka duomenų valdytojui[10]. Net ir paskyrus asmens duomenų tvarkytoją, didžioji dalis BDAR reguliavimo yra orientuojama į duomenų valdytoją, kuriam tenka pagrindinė našta įgyvendinant BDAR normas.

Daiktų interneto veikimas dėl savo savybių (duomenų dalinimosi ir pan.) savaime sudaro sąlygas bendram kelių suinteresuotų šalių, tokių kaip įrenginių gamintojų, socialinių platformų, trečiųjų šalių programų, įrenginių skolintojų ar nuomininkų, duomenų tarpininkų ar duomenų platformų, įsikišimui (ES 29 str. duomenų apsaugos darbo grupė, 2014, p. 11). Esant suinteresuotų šalių daugetui, yra svarbu nustatyti kiekvienos šalies

[9]Toliau, atsižvelgiant į darbo kontekstą, aptariami atvejai, kai duomenų tvarkymo tikslai ir priemonės nėra nustatyti Europos Sąjungos arba valstybės narės teisės.
[10]Atskaitomybės principas nagrinėjamas trečioje darbo dalyje.

vaidmenį, o svarbiausia – duomenų valdytojo. Nustatyti, kas yra duomenų valdytojas, yra itin svarbu įvertinant galimos atsakomybės ribas.

Prietaisų, naudojamų daiktų internetui, gamintojai, kurdami prietaisus, dažniausiai yra atsakingi ir už šių prietaisų operacinės sistemos ar programinės įrangos sukūrimą, naudojimą. Įrenginių gamintojai nustato tokios programinės įrangos funkcijas, kokius duomenis rinks, kaip ir kokiu tikslu jie bus naudojami (ES 29 str. duomenų apsaugos darbo grupė, 2014, p. 11). Pavyzdžiui, išmaniųjų asistentų, išmaniųjų laikrodžių gamintojas „Apple“ šiuose ir kituose įrenginiuose naudoja savo operacinę sistemą „IOS“. Kurdama įrenginius bei juose naudojamas operacines sistemas daiktų interneto bendrovė gali nustatyti, kokie asmens duomenys tuo įrenginiu bus renkami / tvarkomi bei kokiu tikslu tai bus atliekama. Tačiau, ne visuomet įrenginio gamintojas ir operacinės sistemos bendrovė sutampa, pavyzdžiui, išmaniųjų įrenginių gamintojas „Samsung“ savo įrenginiuose (pavyzdžiui, išmaniajame televizoriuje) naudoja vienos didžiausių operacinės sistemos daiktų internetui kūrėjo „Tizen“ operacinę sistemą („Samsung“ internetinis puslapis, 2020). Net ir kitų bendrovių teikiamas operacines sistemas pasirinkę išmaniųjų įrenginių gamintojai, atsižvelgdami į kuriamo įrenginio ypatybes ir siekdami užtikrinti kuo sklandesnį įrenginio vartojimą, patys nusprendžia, kokie duomenys turėtų būti tvarkomi. Taigi, pagal BDAR pateiktą duomenų valdytojo sąvoką, kuria numatoma, kad duomenų valdytojas nustato duomenų tvarkymo tikslus ir priemones, įrenginių gamintojai laikomi duomenų valdytojais.

Duomenų valdytojais galima laikyti ir socialinius tinklus. Dažnu atveju, daiktų interneto prietaisų vartotojas nusprendžia pasidalinti daiktų interneto duomenimis socialinėje erdvėje (ES 29 str. duomenų apsaugos darbo grupė, 2014, p. 11). Pavyzdžiui, sporto metu išmaniąja apyranke surinktais asmens duomenimis bei prietaiso padarytomis išvadomis asmuo gali nuspręsti pasidalinti socialiniuose tinkluose. Šiuo atveju duomenys yra perduodami tam tikram socialiniam tinklui, kuris pasirenka, kokiu tikslu ir kaip šiuos duomenis valdys[11]. Tokiu būdu socialinis tinklas tampa duomenų valdytoju.

Kartais, tikslu gauti prieigą prie įrenginio renkamų ir sisteminamų duomenų, duomenų subjektas turi naudoti trečiųjų šalių sukurtas programėles. Tokių programėlių įdiegimas nėra būtinas, kad įrenginys tinkamai veiktų, vartotojas turi teisę pasirinkti, ar nori įdiegti tokią programėlę. Šios programėlės, dažnai naudodamos aplikacijų programavimo sąsajas (API)[12], gali gauti įrenginio gamintojo turimus duomenis. Tokiu būdu programėlės

[11]Dažniausiai, socialiniai tinklai iš tokių duomenų padarytomis išvadomis naudojasi marketingo tikslais, siekdami pateikti kuo labiau tam vartotojui tinkančias reklamas.
[12]API (angl. *Application Programming Interface)* – aplikacijos programavimo sąsaja, suteikiama kompiuterinės sistemos ar programos, kad būtų galima apsikeisti duomenimis su kita programa.

kūrėjas tampa duomenų valdytoju. Pavyzdžiui, namų draudimo bendrovė sukuria programėlę, kad galėtų patikrinti, ar jų klientų priešgaisrinės sistemos yra teisingai įrengtos (ES 29 str. duomenų apsaugos darbo grupė, 2014, p. 12). Taigi, programėlės kūrėjai nustato, kaip ir kokie duomenys bus naudojami, patys nustato šių duomenų tvarkymo tikslą.

Kiti tretieji asmenys, kurie nėra programėlių kūrėjai ar įrenginių gamintojai, tam tikrais atvejais gali būti laikomi duomenų valdytojais. Pavyzdžiui, sveikatos draudimo bendrovės suteikia savo klientams žingsniamačius, kad galėtų stebėti jų fizinį aktyvumą ir taip įvertinti draudiminio įvykio riziką bei nustatyti jiems taikomų draudimo įmokų dydžius (ES 29 str. duomenų apsaugos darbo grupė, 2014, p. 12). Tokiu atveju draudimo kompanija numato pati, kokiu tikslu ji renka duomenis, ir taip tampa duomenų valdytoju. Kiti tretieji asmenys, kurie nėra programų kūrėjai ar įrenginių gamintojai patys nesprendžia, kokie duomenys bus renkami. Jie gali būti laikomi tik tų asmens duomenų, kuriuos jie patys nusprendžia tvarkyti atskirai savo iškeltiems tikslams, valdytojais. Dažniau tokie tretieji asmenys yra laikomi duomenų tvarkytojais, jeigu yra atsakingi tik už duomenų valdytojų (įrenginių gamintojų) nustatytais tikslais surinktų duomenų tvarkymą.

Kai kurie daiktų interneto įrenginiai yra sukuriami taip, jog nesidalintų duomenimis su kitais įrenginiais. Jie turi atskirą duomenų tvarkymo erdvę. Tačiau net ir tokiu atveju, įrenginių gamintojai neapriboja galimybės susieti įrenginio tvarkomų duomenų su išmaniuosiuose telefonuose ar planšetiniuose kompiuteriuose esančiomis platformomis. Tokios platformos irgi gali būti laikomos duomenų valdytojais, jeigu platformose duomenys yra renkami jų pačių nustatytiems tikslams.

Pagal išnagrinėtus atvejus, gali taip pat būti taikomas ir bendro valdymo institutas. Atsižvelgiant į tai, jog daiktų interneto technologijomis duomenų valdytojai gali dalintis iš skirtingų įrenginių surinktais ir tvarkomais duomenimis tokio instituto įgyvendinimo galimybė yra labai tikėtina. Šio instituto taikymui reikalingas dviejų ar daugiau duomenų valdytojų tarpusavio susitarimas, skaidriu būdu nustatant kiekvieno jų atsakomybės ribas (BDAR, 26 str. 1 d.).

Akivaizdu, jog norint nustatyti, ar suinteresuotas asmuo (kurių daiktų internete gali būti ne vienas) yra duomenų valdytojas, svarbu identifikuoti, ar egzistuoja BDAR numatyti duomenų valdytoją apibrėžiantys elementai: duomenų valdytojas nustato duomenų tvarkymo tikslą bei nustato duomenų tvarkymo priemones. Vis dėlto, daiktų interneto bendrovės (įrenginių gamintojai) yra laikomi duomenų valdytojais, kadangi jie, atsižvelgdami į bendrovių teikiamas paslaugas, nustato duomenų tvarkymo tikslą bei duomenų tvarkymo priemones.

2.3. Duomenų subjektas

Kaip ir aptarta anksčiau darbe, asmens duomenų apsaugos teisinio reguliavimo paskirtis yra užtikrinti fizinio asmens teisę į asmens duomenų apsaugą. BDAR duomenų subjektu laiko asmenį, kurio tapatybę (tiesiogiai ar netiesiogiai) galima nustatyti (BDAR 4 str.). Duomenų apsaugos teisė reguliuoja būtent duomenų subjektu laikomo asmens teises ir pareigas, dėl to yra svarbu nustatyti, kas yra duomenų subjektas daiktų interneto kontekste.

Daiktų internete duomenų subjektu dažniausiai galima laikyti įrenginių ar prietaisų vartotojus, savininkus (ES 29 str. duomenų apsaugos darbo grupė, 2014, p. 13). Žinoma, yra atvejų, kai tuo pačiu įrenginiu naudojasi keli asmenys, pavyzdžiui, namuose įdiegta išmaniąja spyna naudojasi visi namuose gyvenantys asmenys. Esant keliems to paties prietaiso vartotojams, visi jie vis tiek bus laikomi duomenų subjektais. ES 29 straipsnio darbo grupė pabrėžia, jog ES duomenų apsaugos taisyklių taikymą lemia ne prietaiso ar terminalo nuosavybės teisės, o pats asmens duomenų tvarkymas, kad ir koks asmuo būtų susijęs su šiais duomenimis (ES 29 str. duomenų apsaugos darbo grupė, 2014, p. 13).

Taigi, bet kuris asmuo, kurio duomenys yra tvarkomi daiktų interneto technologijomis, yra laikomas duomenų subjektu pagal ES duomenų apsaugos teisę, užtikrinant jo teises, numatytas BDAR.

2.4. Teritorinis Bendrojo duomenų apsaugos reglamento taikymas

Aptarus duomenų valdytoją, tvarkytoją bei duomenų subjektą, svarbu identifikuoti BDAR galiojimą erdvėje. Teritorinė taikymo sritis įtvirtinta BDAR 3 straipsnyje, kuriuo numatyti trys atvejai, kada taikomas reglamentas asmens duomenų tvarkymui.

BDAR taikomas asmens duomenų tvarkymui, kai asmens duomenis Europos ES tvarko duomenų valdytojo arba duomenų tvarkytojo buveinė, vykdydama savo veiklą, neatsižvelgiant į tai, ar duomenys tvarkomi ES, ar ne (BDAR 3 str. 1d.). Šia nuostata yra užtikrinama, kad BDAR būtų taikomas duomenų valdytojo arba duomenų tvarkytojo vykdomam duomenų tvarkymui, kai tokią veiklą vykdo ES duomenų valdytojo arba duomenų tvarkytojo buveinė, nepaisant faktinės duomenų tvarkymo vietos (Europos duomenų apsaugos valdyba, 2019, p. 5). Duomenų valdytojas arba duomenų tvarkytojas turi turėti buveinę ES[13]. Faktiškai duomenys gali būti tvarkomi duomenų valdytojo /

[13] „Buveinė“, tiek ES aktuose, tiek ESTT praktikoje aiškinama plačiai. Ar yra buveinė yra nustatoma kiekvienu konkrečiu atveju, atsižvelgiant į šiuos faktorius: a) reali ir veiksminga, net ir minimali veikla; b) stabili struktūra, nepaisant teisinės jos formos (Europos duomenų apsaugos valdyba, 2019, p. 7).

tvarkyto, kuris yra įsisteigęs užsienyje, bet turi buveinę ES. Šiuo atveju, kaip išaiškino ESTT, yra svarbu nustatyti, kad asmens duomenys tvarkomi „įmonės veiklos kontekste“, kai įmonės veikla yra neatskiriamai susijusi su jos įsteigimo veikla (*Google Spain ir Google*, 2014, 56 punktas). Vadinasi, atsižvelgiant į šią BDAR nuostatą, duomenų valdytojui ar tvarkytojui reikės laikytis BDAR numatyto duomenų apsaugos teisinio reguliavimo, jeigu šis ES turi savo buveinę, kuri vykdo veiklą. Taigi, BDAR daiktų interneto atveju bus taikomas tuo atveju, kai jų valdytojas, dažniausiai, įrenginių, prietaisų gamintojas, turi buveinę ES. Pavyzdžiui, Vokietijoje įsisteigusi viena didžiausių daiktų interneto įmonių „Infarm“, kuri užsiima vertikalių ūkių miestuose kūrimu, turi tvarkyti duomenis kaip duomenų valdytoja, laikydamasi BDAR nuostatų, kadangi yra įsikūrusi ES valstybėje narėje. Kitos didelės išmaniuosius įrenginius ir / ar operacines programas daiktų internetui suteikiančios bendrovės, kurios įkurtos ar turi buveinę ES: „Apple“ (buveinė Airijoje), „Bosch IoT Sensor Company“ (buveinė Vokietijoje), „Cisco“ (buveinė Nyderlanduose), „Huawei“ (buveinė Vokietijoje), IBM (buveinė Prancūzijoje, teikia paslaugas, susijusias su debesų kompiuterija), Microsoft (buveinė Prancūzijoje, taip pat teikia paslaugas daiktų internetui, susijusias su debesų kompiuterija), „Nokia“ (įsikūrusi Suomijoje), „Siemens IoT Analytics Company“ (įsikūrusi Vokietijoje). Visos šios bendrovės, įsikūrusios ar įsteigusios buveines ES, yra įpareigotos, kaip duomenų valdytojos, asmens duomenų tvarkymą atlikti pagal BDAR nuostatas.

Antrojoje aptariamo straipsnio dalyje, numatomas eksteritorialus BDAR taikymas – duomenų valdytojams ar duomenų tvarkytojams, kurie nėra įsikūrę ES. BDAR taikomas asmens duomenų tvarkymui, kai ES esančių duomenų subjektų asmens duomenis tvarko ES neįsisteigęs duomenų valdytojas arba duomenų tvarkytojas ir duomenų tvarkymo veikla yra susijusi su prekių arba paslaugų siūlymu tokiems duomenų subjektams ES arba elgesio, kai jie veikia ES, stebėsena (BDAR 3 str. 2 d.). Duomenų subjekto vieta, kuri turi būti ES, yra kriterijus, lemiantis pareigą laikytis BDAR nustatyto reguliavimo[14]. Europos duomenų apsaugos valdyba išskiria dvi sąlygas, norint nustatyti, ar taikytina BDAR 3 straipsnio 2 dalis: pirma, ar duomenų tvarkymas yra susijęs su ES esančių duomenų subjektų asmens duomenimis, ir, antra, ar duomenų tvarkymas yra susijęs su prekių ar paslaugų siūlymu arba duomenų subjektų elgesio stebėsena ES (Europos duomenų apsaugos valdyba, 2019, p. 14). Siekiant nustatyti, ar duomenų valdytojas arba duomenų tvarkytojas siūlo prekes ar paslaugas ES esantiems duomenų subjektams, reikėtų įsitikinti, ar akivaizdu, kad tas

[14]Duomenų subjekto tautybė pilietybė ar kitas teisinis statusas negali būti Reglamento teritorinio taikymo sritį ribojantis arba apribojantis veiksnys, o duomenų subjekto vieta turi būti nustatoma kiekvienu konkrečiu atveju, būtent duomenų valdytojo ar duomenų tvarkyto veiklos vykdymo momentu (Europos duomenų apsaugos valdyba, 2019, p. 14).

duomenų valdytojas arba duomenų tvarkytojas numato teikti paslaugas duomenų subjektams ES (BDAR preambulė 23 p.). Tokiam tikslui nustatyti, įstatymų leidėjas nurodo, kad užtenka, jog paslauga būtų teikiama ES vartojama kalba, o ne tik trečiosios valstybės, kurioje įsisteigęs duomenų valdytojas, kalba. Pavyzdžiui, Jungtinėse Amerikos Valstijose įsisteigusios įmonės „Apple Inc.“ gaminamas išmanusis laikrodis „Apple Watch“ turi virš 40 kalbos pasirinkimų, tarp kurių yra ir tik ES valstybėse narėse vartojamos kalbos, pavyzdžiui, olandų, suomių, danų, vokiečių, italų ir kitos („Apple“ internetinis puslapis). Taip pat BDAR, kaip tai nurodyta nagrinėjamoje nuostatoje, gali būti taikomas, kai duomenų tvarkymas susijęs su duomenų subjekto elgesio stebėsena. „Google Nest“ bendrovė, neturinti buveinės ES, laikantis eksteritorialus BDAR taikymo taip pat turėtų ES vartotojų asmens duomenis tvarkyti pagal BDAR normas. Pati bendrovė yra numačiusi, jog jų įrenginiai yra skirti ne tik regionui, kuriame yra įsikūrusi (JAV), bet ir ES vartotojams, suteikdama galimybę įsigyti juos ES valstybėse narėse („Google“ internetinis puslapis). Jų įrenginiai, pavyzdžiui, išmanusis namų asistentas, pasižymi savybėmis stebėti vartotojo elgesį. Dėl šių priežasčių šios bendrovės suteikiamomis technologijomis vykdomas asmens duomenų tvarkymas turėtų atitikti BDAR nuostatas. Atsižvelgus į daiktų interneto ypatybę rinkti duomenis tikslu stebėti duomenų subjekto elgesį ir taip pritaikyti įrenginių naudojimą duomenų subjektui, galima daryti išvadą, jog beveik visais atvejais, duomenų subjektui esant ES valstybėje narėje tokių duomenų tvarkymui bus taikomas BDAR.

Taigi, norint nustatyti, ar BDAR yra taikomas vienu ar kitu atveju, svarbu pirmiau nustatyti, kas yra duomenų subjektas, duomenų valdytojas (ir duomenų tvarkytojas, jeigu jie skiriasi). BDAR nuostatos bus taikomos tik tiems valdytojams (ir / arba tvarkytojams), kurie turi buveinę ES arba duomenų valdytojams (ir / arba tvarkytojams), kurie nėra įsikūrę ES, tačiau jų asmens duomenų tvarkymo veikla susijusi su prekių ar paslaugų siūlymu arba duomenų subjektų elgesio stebėsena ES ir tvarkomi ES teritorijoje esančių duomenų subjektų asmens duomenys.

3. PAGRINDINIAI DUOMENŲ APSAUGOS PRINCIPAI IR JŲ TAIKYMAS DAIKTŲ INTERNETUI

Nustačius, kokiu mastu taikomas BDAR, galima aptarti duomenų subjekto, duomenų valdytojo, duomenų tvarkytojo teises ir pareigas. Svarbiausias duomenų apsaugos teisės nuostatas apibūdina principai, įtvirtinti BDAR 5 straipsnyje.

3.1. Teisėtumo, sąžiningumo ir skaidrumo principas

Kaip pirmasis principas BDAR įtvirtintas teisėtumo, sąžiningumo ir skaidrumo principas.

Teisėtumo principas reikalauja, kad duomenų valdytojas turėtų teisėtą pagrindą duomenų tvarkymui (galimi teisėto duomenų tvarkymo pagrindai įtvirtinti BDAR 5 straipsnyje[15]) ir duomenis tvarkytų teisėtai, t. y. laikantis kitų BDAR ar kituose teisės aktuose numatytų reikalavimų[16]. Turėti teisėtą pagrindą duomenų tvarkymui yra itin svarbu atsižvelgiant į tai, kad daiktų interneto renkami ir tvarkomi duomenys naudojami duomenų subjektų profiliavimui (Eskens, 2016, p. 28-29)[17].

Sąžiningumo ir skaidrumo principo[18] tarp duomenų subjekto ir duomenų valdytojo užtikrinimui (kartu užtikrinant, jog atliekamas profiliavimas yra teisėtas), manoma, jog reikalinga, kad duomenų subjektas visuomet turėtų galimybę žinoti, kokie duomenys ir kaip yra tvarkomi. Daiktų interneto atveju tai itin sunku, tačiau savaime nepaneigia šių principų užtikrinimo svarbos. Daiktų interneto technologijomis nuolatos renkami ir tvarkomi itin dideli kiekiai duomenų, apie ką pats duomenų subjektas gali net nežinoti (Wachter, 2018, p. 9). Daiktų interneto įrenginių jutikliai yra suprogramuoti taip, jog duomenų subjektas kuo mažiau pastebėtų jų veikimą. Tokiu atveju, duomenų valdytojui tampa itin sudėtinga įgyvendinti jam nustatytą pareigą užtikrinti, kad duomenų subjektas būtų visuomet informuotas apie su duomenų subjektu susijusių duomenų rinkimą ir tvarkymą (ES 29 str. duomenų apsaugos darbo grupė, 2014, p. 16). Pagrindiniai su skaidrumu susiję BDAR reikalavimai yra įtvirtinti prie nuostatų, reglamentuojančių duomenų subjekto teises: 12 straipsnyje nustatomos bendrosios taisyklės, taikomos:

[15]Plačiau BDAR įtvirtinti pagrindai teisėtam duomenų tvarkymui bus aptariami šios dalies tolimesniame skyriuje.
[16]Kitais teisės norminiais aktais gali būti laikomi ir specialieji teisės norminiai aktai, kurie numato specialiąsias teisės normas, taikomas kartu su BDAR.
[17]Vienas iš specifinių daiktų interneto požymių yra galimybė iš apie asmenį surinktų duomenų sudaryti šio asmens (duomenų subjekto) profilį. Tokio profiliavimo duomenų subjektas beveik nekontroliuoja, dėl to yra itin svarbu užtikrinti, kad duomenys būtų tvarkomi laikantis aptariamo principo.
[18]Sąžiningumo ir skaidrumo principai yra glaudžiai susiję, tai galime matyti ir iš BDAR preambulėje pateikiamo šių principo paaiškinimo (Eskens, 2016, p. 27), dėl to šie principai bus nagrinėjami kartu.

informacijos apie duomenų subjektus teikimui; ryšių palaikymui su duomenų subjektais dėl jų teisių įgyvendinimo; ryšių palaikymui dėl duomenų saugumo pažeidimų[19] (ES 29 str. duomenų apsaugos darbo grupė, 2016, p. 6). Užtikrinant skaidrumo principo įgyvendinimą duomenų valdytojas (ypač įrenginių gamintojas) turėtų informuoti, kaip planuoja vykdyti savo veiklą, kad būtų užtikrintos duomenų subjekto teisės ir duomenų subjektas nesijaustų stebimas ar negalinčiu kontroliuoti, kokius su juo susijusius duomenis tvarkys duomenų valdytojas (Wachter, 2017, p. 19).

Taigi, šio principo įgyvendinimui svarbiausias aspektas yra duomenų subjekto teisė žinoti, kokie ir kokiu tikslu su juo susiję duomenys yra renkami. Duomenų subjektui susipažinus su duomenų tvarkymu, kurį atlieka duomenų valdytojas, bus užtikrintas ne tik teisėtumo, sąžiningumo bet ir skaidrumo principas, ypač kai tvarkomi duomenys yra jautrūs (priskirtini prie specialių kategorijų duomenų) (pavyzdžiui, išmaniosios apyrankės renkami duomenys apie asmens sveikatą).

3.2. Tikslo apribojimo principas

BDAR duomenų valdytojui kaip pareigą įtvirtina duomenų tvarkymo tikslo apribojimą. Šiuo principu užtikrinama, kad duomenys būtų renkami aiškiais, apibrėžtais tikslais ir toliau netvarkomi su tikslais nesuderinamu būdu (BDAR 5 str. 1 d. b p.). Šiuo principu siekiama užtikrinti, kad daiktų interneto vartotojas – duomenų subjektas, turėtų galimybę sužinoti, kokiais tikslais bus tvarkomi jo duomenys, ir turėtų galimybę nuspręsti, ar patikėti savo duomenis duomenų valdytojui (ES 29 str. duomenų apsaugos darbo grupė, 2014, p. 16).

Svarbus šio principo įgyvendinimo aspektas yra tai, kad duomenų rinkimo ir tvarkymo tikslas turi būti apibrėžtas dar prieš pradedant duomenų rinkimą. Tik tokiu būdu bus užtikrinamos duomenų subjekto teisės. Šio principo įgyvendinimas padeda užtikrinti ir anksčiau nagrinėto teisėtumo, sąžiningumo ir skaidrumo principo laikymąsi. Daiktų interneto vartotojams duomenų valdytojas (įrenginių gamintojas) turėtų iš anksto nurodyti, kad įrenginių renkami duomenys bus naudojami profiliavimui, nors profiliavimas kaip duomenų rinkimo ir tvarkymo tikslas negali būti įvardijamas (Eskens, 2016, p. 30). Daiktų internete gali kilti sunkumų įgyvendinant šį principą, kai įrenginių jutikliai yra sujungiami ar prijungiami nauji duomenys, surinkti iš kitų įrenginių, kartu šiuos duomenis naudojant ir profiliavimui. Taip duomenų valdytojas gali gauti duomenų, kurių rinkimas ir tvarkymas

[19]Šios su skaidrumo principu susijusios duomenų subjekto teisės bus analizuojamos ketvirtoje darbo dalyje „Duomenų subjekto teisės, jų pritaikymas naudojant daiktų internetą“.

nebuvo numatytas (Wachter, 2018, p. 10). Tam, kad duomenų subjekto teisės liktų nepažeistos, jam apie tokias technines galimybes turėtų būti pranešama arba tokiu būdu gauti duomenys turėtų būti tvarkomi tik gavus asmens sutikimą.

Daiktų interneto technologijomis renkami ir tvarkomi asmens duomenys gali būti susieti su didžiaisiais duomenis (angl. *Big Data*) ir jų atliekama analize. Kadangi tiek daiktų interneto sklandžiam veikimui, tiek didžiųjų duomenų analizei yra būdinga rinkti kuo didesnį kiekį duomenų, tai prieštarauti tikslo apribojimo principui. Tai atspindi didžiųjų duomenų analizės, kaip sklandaus ir nuoseklaus proceso, reikšmę, kai analizuojant duomenis naudojant daug skirtingų algoritmų, nustatomos netikėtos koreliacijos, dėl kurių duomenys gali būti naudojami naujiems tikslams. Manoma, kad tikslo ribojimo principas riboja didžiųjų duomenų analizę vykdančių šalių laisvę daryti šiuos atradimus ir naujoves (Information Commisioner's Office, 2017, p. 37). Išskiriami du analizės atlikimo atvejai: duomenis tvarkančios organizacijos nori aptikti informacijos tendencijas ir koreliacijas arba organizacijos yra suinteresuotos išanalizuoti asmens elgesį. Pirmuoju atveju, siekiant užtikrinti tikslo apribojimo principo įgyvendinimą yra rekomenduojama įgyvendinti funkcinį atskyrimą - duomenų valdytojai turi garantuoti duomenų konfidencialumą ir saugumą bei imtis visų būtinų techninių ir organizacinių priemonių, kad užtikrintų funkcinį atskyrimą. Asmens duomenų konfidencialumo ir saugumo užtikrinimas lemia, ar duomenys galės būti naudojami ir rinkodaros ar kitais tikslais. Antruoju atveju, kai organizacijos analizė yra nukreipta į asmeninį vartotojo požiūrį, elgesį, teisėtam duomenų tvarkymui reikės laisvo, konkretaus, informuoto ir nedviprasmiško asmens sutikimo, kitaip tolesnis duomenų naudojimas negali būti laikomas suderinamu su tikslo apribojimo principu (ES 29 str. duomenų apsaugos darbo grupė, 2013, p. 46). Galima teigti, jog esminis faktorius duomenų rinkimo ir tvarkymo suderinamumui su tikslo apribojimo principu yra skaidrumo principo užtikrinimas, t. y. vartotojas turi būti informuotas ir pateikti savo sutikimą, jog su juo susiję duomenys būtų naudojami vieniems ar kitiems tikslams.

Taigi, šiam principui užtikrinti, išmaniųjų įrenginių gamintojas (duomenų valdytojas) turi potencialiam vartotojui aiškiai pateikti informaciją, kokiu tikslu ir kaip šio vartotojo (duomenų subjekto) duomenys bus renkami.

3.3. Duomenų kiekio mažinimo principas

Su duomenų tvarkymo tikslo apribojimo principu yra glaudžiai susijęs duomenų kiekio mažinimo principas. Šiuo principu užtikrinama, kad duomenų valdytojas (dažniausiai, įrenginių gamintojas) įrenginiais rinktų tik tokius duomenis, kurie yra būtini, kad būtų

įgyvendinti numatyti duomenų tvarkymo tikslai (BDAR 5 str. 1 d. c p.). Vadinasi, duomenų valdytojai gali rinkti tik tokius duomenis, kurie yra būtini užtikrinti, kad vartotojas – duomenų subjektas galėtų tinkamai naudotis daiktų interneto įrenginiu ar kita paslauga (Wachter, 2018, p. 10).

Daiktų interneto savybė yra rinkti kuo didesnį kiekį ir įvairių duomenų. Tokiu būdu įrenginių gamintojai, programų kūrėjai užtikrina, jog įrenginys bus visapusiškai pritaikytas vartotojo poreikiams. Dėl šios priežasties įrenginių gamintojams ar kitiems duomenų valdytojams kyla iššūkis užtikrinti duomenų kiekio mažinimo principą. Šio principo įgyvendinimas gali netgi sudaryti kliūtį daiktų interneto plėtrai. Nepaisant to, prioritetas turėtų būti skiriamas duomenų subjekto teisių apsaugai ir šio principo įgyvendinimui (ES 29 str. duomenų apsaugos darbo grupė, 2014, p. 16).

Minėtos problemos sprendimui ES 29 straipsnio darbo grupė išaiškino, jog esant situacijai, kai asmens duomenys nėra būtini duomenų valdytojo nustatyto tikslo įgyvendinimui ir teikiant konkrečią daiktų interneto paslaugą, duomenų subjektui turėtų būti suteikta galimybė šią paslaugą gauti anonimiškai (ES 29 str. duomenų apsaugos darbo grupė, 2014, p. 17). Tokiu būdu duomenų subjektas gali toliau naudotis daiktų interneto teikiamais privalumais nepažeidžiant jo teisių, o duomenų valdytojas nepažeidžia jam įstatymu nustatytų pareigų.

3.4. Duomenų tikslumo principas

Duomenų valdytojas turi užtikrinti, kad jo tvarkomi duomenys nuolatos būtų tikslūs (BDAR 5 str. 1 d. d p.). Tai yra, duomenys turi būti teisingi, o ar duomenys iš tikrųjų tokie yra, turi tikrinti duomenų valdytojas. Jeigu duomenys nėra teisingi, duomenų valdytojas turi juos ištrinti.

Daiktų internete pagrindiniais duomenų valdytojais laikomi įrenginių ir programų kūrėjai. Laikantis šio principo, jie yra įpareigojami sukurti tokias duomenų valdymo programas, kurios leistų nuolatos tikrinti, ar surinkti asmens duomenys yra tikslūs, teisingi. Dažniausiai įrenginiu, prijungtu daiktų internetu, naudojasi daugiau nei vienas asmuo. Siekiant užtikrinti duomenų tikslumo principo įgyvendinimą svarbu, kad, naudojantis įrenginiu, duomenų subjektas patvirtintų savo tapatybę (Wachter, 2018, p. 11). Tokiu būdu būtų nustatoma, kad surinkti asmens duomenys yra būtent apie konkretų duomenų subjektą, yra teisingi ir tikslūs. Jeigu duomenys būtų tvarkomi nenustačius, kuris asmuo naudojasi įrenginiu / programa, gali kilti grėsmė, kad renkami / tvarkomi duomenys ne apie asmenį, kurį duomenų valdytojas laiko duomenų subjektu tuo konkrečiu atveju, todėl būtų pažeistas

šis principas. Duomenų tikslumo principą galima sieti su standartizuotosios duomenų apsaugos principu, įtvirtintu BDAR 25 straipsnyje. Šis principas reiškia, kad daiktų interneto išmanieji įrenginiai ir jiems naudoti skirtos programos turėtų būti sukurtos taip, jog būtų išvengta nereikalingo duomenų tvarkymo (ES 29 str. darbo grupė, 2015 cituota Zaleskis, 2019, p. 139).

Duomenų valdytojas turi užtikrinti ne tik asmens duomenų tikslumą, bet ir jų saugumą (saugumo principas). Kaip minėta darbo pirmoje dalyje, daiktų internete dėl technologijų pažangumo bei tvarkomų duomenų jautrumo gali kilti grėsmė, jog teisėtai renkami ir tvarkomi asmens duomenys gali „patekti į netinkamas rankas“. Kad taip neįvyktų yra atsakingas duomenų valdytojas. Duomenų valdytojas turi užtikrinti, kad asmens duomenys būtų tvarkomi saugiai, pritaikius tam reikalingas technines ar organizacines priemones (BDAR 5 str.1 d. f p.). Vadinasi, įrenginių / programų kūrėjai turėtų užtikrinti ne tik tai, kad jų gaminami produktai ir teikiamos paslaugos nuolatos garantuotų asmens duomenų tikslumą, bet ir tokių duomenų saugų tvarkymą. Tam taip pat reikalinga, kad daiktų interneto įrenginių / programų kūrėjai pasitelktų specialias programas ar kitas priemones, kuriomis būtų užtikrintas šio principo įgyvendinimas. Tai gali tapti iššūkiu tiems įrenginiams, kurie paremti paprastesnėmis programomis ir veikia, pavyzdžiui, per bevielio interneto (*WiFi*) ryšį ir dėl to negali užtikrinti, kad duomenys būtų šifruojami, tokiu būdu duomenys nėra tvarkomi saugiai[20] (Wachter, 2018, p. 11). Taigi, kad duomenys būtų tvarkomi saugiai, reikalingas pačių daiktų interneto įrenginių / programų kūrėjų ar gamintojų indėlis į saugesnių prietaisų ir programų kūrimą.

3.5. Saugojimo trukmės apribojimo principas

Tarp BDAR įtvirtintų duomenų apsaugos teisės principų yra numatytas ir asmens duomenų saugojimo trukmės apribojimo principas. Šis principas taip pat siejamas su antruoju aptartu tikslo apribojimo principu. Saugojimo trukmės apribojimo principas numato, kad duomenų valdytojas asmens duomenis laikytų ir asmens tapatybė galėtų būti nustatoma tik tokį laikotarpį, kuris yra būtinas duomenų valdytojo apsibrėžtam asmens duomenų rinkimo ir tvarkymo tikslui įgyvendinti (BDAR 5 str. 1 d. e p.).

Šiam tikslui įgyvendinti taip pat kiekvienas suinteresuotas asmuo (duomenų valdytojas ar kiti tretieji asmenys), veikiantis daiktų internete, turėtų periodiškai tikrinti, ar asmens duomenys vis dar yra reikalingi apsibrėžto tikslo įgyvendinimui. Tai turėtų būti

[20]Tai nereiškia, kad norint užtikrinti tvarkomų asmens duomenų saugumą būtinas jų šifravimas. Norima pabrėžti, kad naudojant paprastesnio veikimo įrenginius asmens duomenų saugumą išsaugoti yra sudėtingiau.

vertinama kiekvienu konkrečiu atveju, atsižvelgiant į tikslą, pavyzdžiui, neturėtų būti saugoma informacija, kurią vartotojas pats ištrina savo paskyroje. Kai vartotojas nenaudoja paslaugos ar programos nustatytą laiką, vartotojo profilis turėtų būti nustatytas kaip neaktyvus, po kurio laiko tokia visa turima informacija turėtų būti apskritai ištrinama ir duomenų valdytojo (ES 29 str. duomenų apsaugos darbo grupė, 2014, p. 17). Atkreiptinas dėmesys, kad siekiant užtikrinti duomenų subjekto teises, apie tokius duomenų valdytojo veiksmus turėtų būti pranešama duomenų subjektui. Galima pastebėti, kad šio principo įgyvendinimas gali koreliuoti su duomenų subjekto BDAR numatytomis teisėmis, pavyzdžiui su teise būti pamirštam.

Apibendrinant, saugojimo trukmės apribojimo principas yra glaudžiai susijęs su tikslo apribojimo principu, abiejų šių principų įgyvendinimui duomenų valdytojas turėtų nusistatyti aiškius duomenų rinkimo ir tvarkymo tikslus, apie kuriuos duomenų subjektas – įrenginių vartotojas, turėtų žinoti, duomenys turėtų būti tvarkomi tik šio tikslo įgyvendinimui. Jeigu tikslui įgyvendinti duomenų nebereikia, jie turėtų būti ištrinti, o tai įrenginių ir programų kūrėjai turėtų užtikrinti nuolatine priežiūra.

3.6. Atskaitomybės principas

BDAR 5 straipsnio 2 dalyje atskirai išskirtas atskaitomybės principas. Tai bene svarbiausias BDAR įtvirtintas principas, kuriuo įgyvendinamas BDAR tikslas – apsaugoti duomenų subjekto teises. Kaip jau minėta anksčiau darbe, itin svarbu yra kiekvienu konkrečiu atveju nustatyti duomenų valdytoją, kadangi būtent duomenų valdytojui yra numatyta atskaitomybė ne tik užtikrinti visų anksčiau išnagrinėtų principų laikymąsi, bet ir tuo pačiu jis turi sugebėti įrodyti, kad šių principų yra laikomasi (BDAR 5 str. 2 d.). Šį principą išplečia BDAR 24 ir 25 straipsniai.

Atskaitomybės principe, kaip tai apibrėžiama ir pačiame reglamente, išskiriami du aspektai:

1) reikalaujama organizacijose taikyti tinkamą vidaus politiką ir priemones, skirtas užtikrinti, kad būtų laikomasi esminių duomenų apsaugos teisės principų ir prievolių (Zaleskis, 2019, p. 135). Tai praplečia BDAR 24 straipsnis, kuriame išaiškinama, kad duomenų valdytojas turi įgyvendinti tinkamas technines ir organizacines priemones bei atitinkamą duomenų apsaugos politiką, kad užtikrintų ir galėtų įrodyti, kad duomenys tvarkomi laikantis BDAR (BDAR 24 str. 1 d.). Kaip jau minėta anksčiau darbe, prie atskirai aptartų principų, siekiant užtikrinti jų laikymąsi, reikalingas duomenų valdytojo – išmaniųjų įrenginių ir programų kūrėjų indėlis. Jau nuo pat įrenginių ir programų kūrimo

pradžios turėtų būti atsižvelgiama į turimus įgyvendinti principus. Tokius reikalavimus išmaniųjų įrenginių ir / ar programų gamintojams kelia ir pritaikytosios duomenų apsaugos principas, įtvirtintas BDAR 25 straipsnyje. Pritaikytosios duomenų apsaugos principas reiškia, kad duomenų apsauga turi būti įtraukta į visą technologijos gyvavimo ciklą: ankstyvąją kūrimo stadiją, rengimą galutiniam naudojimui, taikymą, šalinimą (ES 29 str. darbo grupė, 2015 cituota Zaleskis, 2019, p. 139).

2) Duomenų valdytojas turi turėti vidinius mechanizmus, kad galėtų suinteresuotiems asmenims įrodyti duomenų tvarkymo atitiktį BDAR (priežiūros institucijoms) (Zaleskis, 2019, p. 135). Šio aspekto įgyvendinimui ypatingai svarbus duomenų valdytojo bendradarbiavimas su priežiūros institucija – jos prašymu duomenų valdytojas turėtų pateikti reikiamus dokumentus, įrodančius, kad duomenų tvarkymas yra atliekamas nepažeidžiant BDAR nustatyto reguliavimo (BDAR preambulės 82 p.). Pavyzdžiui, dažniausiai daiktų internete duomenys yra tvarkomi gavus duomenų subjekto sutikimą (pradėjus naudoti išmanųjį įrenginį vartotojas duoda sutikimą rinkti ir tvarkyti to įrenginio galimus surinkti duomenis), tokiu atveju įrenginio gamintojas privalo turėti įrodymą, kad duomenys buvo surinkti ir tvarkomi sutikimo pagrindu, o priežiūros institucijai to pareikalavus, pateikti jai šį įrodymą.

Apibendrinant galima daryti išvadą, jog tiek šio, tiek kitų aptartų principų įgyvendinimui yra itin svarbus duomenų valdytojų – išmaniųjų prietaisų ir jiems veikti reikalingų programėlių kūrėjų indėlis, siekiant kurti ne tik pelningus, bet ir vertus vartotojo pasitikėjimo produktus, tuo pačiu užtikrinant geriausius duomenų subjekto interesus.

4. DUOMENŲ SUBJEKTO TEISĖS, JŲ PRITAIKYMAS NAUDOJANT DAIKTŲ INTERNETĄ

Iš ankstesnėje dalyje aptartų principų galima pastebėti, jog BDAR, kaip ir visos duomenų apsaugos teisės, tikslas – apsaugoti duomenų subjektą, užtikrinant jo teises tvirtu teisiniu reguliavimu. Principais įtvirtintos duomenų subjekto teisės yra praplečiamos atskiruose BDAR straipsniuose.

4.1. Teisė būti informuotam apie duomenų tvarkymą

BDAR 12 straipsnyje nurodyta, jog duomenų valdytojas yra atsakingas, kad duomenų subjektui būtų pateikta BDAR 13 ir 14 straipsniuose nurodytą informacija, o ši būtų pateikta glausta, skaidria, suprantama ir lengvai prieinama forma, aiškia ir paprasta kalba. Informacija turi būti teikiama rašytine ar kita forma (daiktų internete dažniausiai naudojama elektroninė forma) (BDAR 12 str. 1 d.). BDAR 13 straipsnis reglamentuoja atvejus, kai asmens duomenys yra renkami tiesiogiai iš duomenų subjekto – išmaniojo įrenginio vartotojo, o 14 straipsnis – atvejus, kai duomenys renkami netiesiogiai iš duomenų subjekto. Duomenų valdytojas turi pareigą bet kuriuo iš aptartų atvejų duomenų subjektui pateikti panašią informaciją. Visus informavimo reikalavimus galima išskirti į bendruosius, kuriais numatoma, kokią informaciją privaloma pateikti duomenų subjektams visais atvejais, ir specialiuosius, kuriais numatoma, kokia papildoma informacija turi būti pateikta duomenų subjektui tam tikrais numatytais atvejais (Zaleskis, 2019, p. 165).

Duomenų subjektui visuomet turi būti pateikiama informacija apie: duomenų valdytojo tapatybę ir kontaktinius duomenis (BDAR 13 str. 1 d. a p., 14 str. 1 d. a p.); duomenų tvarkymo tikslus bei teisinį duomenų tvarkymo pagrindą (BDAR 13 str. 1 d. c p., 14 str. 1 d. c p.); duomenų saugojimo laikotarpį (BDAR 13 str. 2 d. a p., 14 str. 2 d. a p.); duomenų subjekto teises (BDAR 13 str. 2 d. b p., 14 str. 2 d. c p.); teisę pateikti skundą priežiūros institucijai (BDAR 13 str. 2 d. d p., 14 str. 2 d. e p.).

Atvejai, kai duomenų teisėto tvarkymo pagrindas yra sutikimas, priskiriami prie specialiųjų duomenų subjektų informavimo atvejų, kai duomenų valdytojas be bendrosios informacijos yra įpareigotas pateikti papildomą informaciją. Kaip minėta anksčiau, tai dažniausiai daiktų internete taikomas asmens duomenų teisėto tvarkymo pagrindas. Tokiu atveju (įskaitant ir kai sutikimu tvarkomi specialių kategorijų duomenys), duomenų valdytojas yra įpareigojamas duomenų gavimo metu išmaniojo įrenginio vartotojui pateikti

informaciją, jog šis turi teisę bet kuriuo metu atšaukti sutikimą tvarkyti su jo asmeniu susijusius duomenis (BDAR 13 str. 2 d. c p., 14 str. 2 d. d p.) (teisė būti pamirštam).

Taip pat prie atskirų atvejų, kai taikomi specialieji subjektų informavimo reikalavimai, yra priskiriami atvejai, kai esama automatizuoto sprendimų priėmimo (įskaitant profiliavimą). Kadangi, daiktų internetas pasižymi profiliavimu, daiktų interneto technologijomis renkamų ir tvarkomų duomenų tvarkymui ši BDAR norma ypatingai svarbi užtikrinant sąžiningumo ir skaidrumo principus. Įrenginių gamintojai ar kiti duomenų valdytojai, atliekantys daiktų interneto technologijomis automatizuotą sprendimų priėmimą ir / ar profiliavimą, duomenų valdytojas įpareigojami pateikti duomenų subjektui loginį automatizuoto sprendimų priėmimo (įskaitant profiliavimo) pagrindimą, tokio tvarkymo reikšmę bei galimas pasekmes duomenų subjektui (BDAR 13 str. 2 d. f p., 14 str. 2 d. g p.). Atsižvelgdamas į tokį reguliavimą, duomenų valdytojas taip pat turėtų informuoti duomenų subjektą, ar duomenų valdytojas sudaręs asmens profilį juo ketina dalytis su kitomis organizacijomis, o duomenis gavusi įmonė turėtų informuoti asmenį apie šio profilio naudojimo tikslus ir apie tai, iš kokio šaltinio ji gavo informaciją, taip pat informuoti apie asmens teisę nesutikti su tokiu duomenų tvarkymu (ES 29 str. duomenų apsaugos darbo grupė, 2017b, p. 17).

Taigi, išmaniųjų įrenginių gamintojas, kaip duomenų valdytojas daiktų internete, be bendraisiais reikalavimais numatomos privalomos pateikti informacijos, vartotojui turi taip pat pateikti informaciją apie tai, jog vartotojas bet kuriuo metu turi teisę atšaukti sutikimą tvarkyti su jo asmeniu susijusius duomenis. Taip pat vartotojui turi būti suteikiama informacija, visų pirma, kad naudojamu įrenginiu ir jo renkamais duomenis gali būti ir / ar yra atliekamas profiliavimas, loginį jo pagrindą, tokio duomenų tvarkymo reikšmę bei galimas pasekmes duomenų subjektui (BDAR 13 str. 2 d. f p., 14 str. 2 d. g p.).

Visa reikalinga informacija yra pateikiama pranešimais, kurie dažnai vadinami privatumo pranešimais (arba privatumo politikomis (angl. *privacy policies*). BDAR nenumato, kokiu būdu visa duomenų subjektui teiktina informacija turi būti pateikta. Duomenų valdytojas, priimdamas sprendimą dėl tinkamų informacijos pateikimo būdų ir formos turėtų atsižvelgti į visas duomenų rinkimo ir tvarkymo aplinkybes (ES 29 straipsnio darbo grupė, 2016, p. 15). Idealiu atveju, pranešimas būtų pateikiamas vartotojui per naudojamą išmanųjį įrenginį. Taip duomenų subjektui nekiltų sunkumų ir visa reikalinga žinoti informacija būtų vienoje vietoje.

Tačiau, daiktų internete privatumo pranešimai ne visuomet yra patogūs. Kadangi dažniausiai profiliavimas atliekamas iš kelių kartu prijungtų įrenginių, kiekvienas jų turėtų pateikti privatumo pranešimą (Eskens, 2016, p. 36). Tai nėra patogu nei įrenginių

gamintojui, nei vartotojui. Kaip minėta anksčiau, daiktų interneto įrenginiai vis labiau panašėja į įprastus neišmaniuosius daiktus. Daugelis daiktų interneto įrenginių galimai turės tik mažą ekraną (pavyzdžiui, išmanusis termostatas, išmanusis laikrodis) arba net neturės ekrano ar kitos vartotojo sąsajos, kurioje vartotojai galėtų perskaityti privatumo politiką ir pateikti sutikimą, dėl to vartotojas turėtų būti informuojamas kitais būdais (Peppet, 2014 cituota Eskens, 2016, p. 37). Sparčiai keičiantis ir tobulėjant technologijoms, akivaizdu, kad ir privatumo pranešimai keičiasi. Gamintojas būtų įpareigotas nuolatos pateikti naujus pranešimus. Tokiais atvejais privatumo pranešimai galėtų būti teikiami kitais šaltiniais, pavyzdžiui, pateikiant privatumo pranešimus ne per patį išmanųjį įrenginį, bet per prie įrenginio prijungtą programėlę ar internetinę svetainę, kuria vartotojas gali naudotis kitu prietaisu (išmaniuoju telefonu, kompiuteriu ar pan.). Bet kuriuo atveju, privatumo pranešimai turėtų būti teikiami aiškia ir suprantam forma. Deja, dažnai tai nėra įgyvendinama, privatumo pranešimuose esanti informacija pateikiama ilgomis, sudėtingomis ir įprastam vartotojui sunkiai suprantamomis frazėmis. Pavyzdžiui, buvo atliktas tyrimas dėl didžiųjų daiktų interneto įrenginių gamintojų „Google Home“ (dabar – „Google Nest“) ir „Amazon Alexa“ pateikiamų privatumo pranešimų sudėtingumo. Buvo tiriamas teksto sudėtingumas, ilgis bei kiti aspektai. Buvo nustatyta, jog nors „Google Home“ privatumo pranešimas yra ilgesnis, tačiau jo tekstas yra suprantamesnis paprastam vartotojui (tekstas suprantamas net pagrindinį išsilavinimą turinčiam asmeniui). „Amazon Alexa“ privatumo pranešime tekstas buvo trumpesnis, bet – sudėtingesnis. Privatumo pranešime pateiktą tekstą galėtų suprasti tik aukštąjį išsilavinimą turintis asmuo (Shayegh, Ghanavati, 2017, p. 107).

Taigi, išmaniųjų įrenginių gamintojas ne visuomet gali užtikrinti, kad, kaip rekomenduoja ES 29 straipsnio darbo grupė, visa informacija būtų pateikiama vienoje vietoje. Tačiau gamintojas, kaip duomenų valdytojas, vis tiek privalo imtis aktyvių veiksmų, kad duomenų subjektui būtų pateikta aptarta informacija arba duomenų subjektas būtų nukreiptas į nuorodą, kur gali susipažinti su jam teiktina informacija (pavyzdžiui, naudodamas tiesioginę nuorodą, greitojo atsako (QR) kodą ir t.t.) (ES 29 straipsnio darbo grupė, 2016, p. 13).

4.2. Teisė nesutikti su duomenų tvarkymu

Duomenų valdytojui neužtikrinus duomenų subjekto teisės būti informuotam apie duomenų tvarkymą, būtų pažeistos ir kitos duomenų subjekto teisės. Viena iš šių teisių yra duomenų subjekto teisė nesutikti su duomenų tvarkymu. BDAR 21 straipsnis įtvirtina, kad

duomenų subjektas turi teisę dėl su juo konkrečiu atveju susijusių priežasčių bet kuriuo metu nesutikti, kad su juo susiję asmens duomenys būtų tvarkomi, kai toks duomenų tvarkymas vykdomas pagal 6 straipsnio 1 dalies e (duomenų valdytojas tvarko duomenis vykdydamas viešosios valdžios funkcijas arba siekdamas atlikti užduotį viešosios tvarkos labui) arba f (kai tvarkyti duomenis būtina siekiant teisėtų duomenų valdytojo arba trečiosios šalies interesų) punktus, įskaitant profiliavimą remiantis tomis nuostatomis.

Vartotojas gali prieštarauti daiktų interneto atliekamam duomenų tvarkymui, įskaitant profiliavimui tik tuo atveju, jeigu duomenys buvo renkami ir tvarkomi vykdant užduotį viešojo intereso labui, atliekant viešosios valdžios funkcijas, teisėtais duomenų valdytojo ar trečiosios šalies interesais. Taigi, jeigu duomenys, kaip dažniausiai ir būna daiktų internete, tvarkomi sutikimo, kaip teisėto asmens duomenų tvarkymo pagrindu, tokiu atveju duomenų subjektas teisę nesutikti su duomenų tvarkymu ir atliekamu profiliavimu praranda. Šiuo atveju, ES 29 straipsnio darbo grupė pabrėžia, jog vis dėlto turėtų būti numatytas reguliavimas, kad duomenų subjektas bet kokiu bet kurio prietaiso naudojimo atveju galėtų būti užtikrintas (žinoma, tai įpareigotų ir įrenginių bei programų gamintojus kurti įrangą atsižvelgiant į tokį reguliavimą), jog galės atsisakyti ar nesutikti su tolimesniu tam tikrų ar visų asmens duomenų, kuriuos tas įrenginys gali rinkti, rinkimu ir tvarkymu (ES 29 str. duomenų apsaugos darbo grupė, 2014, p. 19).

Taip pat vartotojas gali nesutikti su atliekamu duomenų tvarkymu, įskaitant profiliavimą ir kai jis atliekamas tiesioginės rinkodaros tikslais (BDAR 21 str. 2 d.) (nesvarbu, kokiu teisiniu pagrindu šie duomenys yra tvarkomi). Tokiu atveju vartotojas gali bet kuriuo metu nesutikti arba nutraukti jau duotą sutikimą duomenų tvarkymui (įskaitant ir profiliavimui), kiek jis bus susijęs su tiesiogine rinkodara. Ši duomenų subjekto teisė yra absoliuti ir skirtingai nei BDAR 21 straipsnio 1 dalyje nurodytais atvejais, duomenų valdytojas negalės toliau tvarkyti duomenų, remdamasis viršesniais už duomenų subjekto interesais (Wachter, 2017, p. 13).

Duomenų subjekto apsauga nuo neteisėto profiliavimo taip pat yra įtvirtinta ir BDAR 22 straipsnyje. Duomenų subjektas turi teisę, kad jam nebūtų taikomas tik automatizuotu duomenų tvarkymu, įskaitant profiliavimą, grindžiamas sprendimas, dėl kurio jam kyla teisinės pasekmės arba kuris jam panašiu būdu daro didelį poveikį (BDAR 22 str. 1 d.). Kaip ir BDAR 21 straipsnyje numatytos teisės įgyvendinimo atveju, taip ir BDAR 22 straipsnyje įtvirtintos teisės įgyvendinimas priklauso nuo paties duomenų subjekto, tai yra pats duomenų subjektas nusprendžia, ar pasinaudos šia teise (Bygrave, 2001 cituota Eskens, 2016, p. 41). Ja nepasinaudojus, duomenų valdytojui – įrenginių gamintojui, jeigu žinoma duomenų tvarkymas atliekamas turint teisinį pagrindą, išlieka

teisė atlikti profiliavimą. Kadangi daiktų interneto technologijomis asmens duomenys gali būti renkami iš skirtingų šaltinių (įrenginių) ir įvairaus pobūdžio, atliekamas profiliavimas gali tapti palankia „erdve“ diskriminacijos atsiradimui[21] (Peppet, 2014, p. 111). Dėl profiliavimo keliamo pavojaus teisės doktrinoje yra išskiriama nuomonė, kad tai reguliuojančios teisės normos turėtų būti griežtesnės (Bygrave, 2001 cituota Eskens, 2016, p. 41). Darbo autorės nuomone, dabartinis reguliavimas yra pakankamas duomenų subjekto teisėms užtikrinti, kol daiktų interneto vartotojui yra aiškiai pateikiama informacija, jog pastarasis turi teisę nesutikti su tam tikrų duomenų tvarkymu (BDAR numatytais atvejais) ir jam suteikiama galimybė aiškiai ir patogiai pateikti nesutikimą su jo duomenų tvarkymu.

4.3. Teisė apriboti duomenų tvarkymą

Kita duomenų subjekto teisė – teisė apriboti duomenų tvarkymą. Duomenų subjektas gali prašyti duomenų valdytojo apriboti duomenų tvarkymą, kai: ginčijamas asmens duomenų tikslumas, tvarkymas yra neteisėtas ir duomenų subjektas prašo riboti asmens duomenų naudojimą, o ne ištrinti; duomenys turi būti saugomi teisiniams reikalavimams pareikšti ar apginti arba laukiama sprendimo dėl teisėtų duomenų valdytojo interesų, svarbesnių už duomenų subjekto interesus (BDAR 18 str. 1 d.). Tokiais atvejais duomenų valdytojas privalo pranešti apie tokį asmens duomenų tvarkymo apribojimą visiems duomenų gavėjams, kuriems buvo atskleisti duomenys (BDAR 19 str.).

Išmaniųjų įrenginių gamintojai, siekdami užtikrinti šią duomenų subjekto teisę bei atsižvelgdami į duomenų tikslumo ir standartizuotosios duomenų apsaugos principus, kurdami įrenginius privalo numatyti galimybę ir sukurti itin palankias sąlygas vartotojui tinkamai įgyvendinti jam suteiktas teises. Tai yra, naudojant įrenginį vartotojui turėtų būti aišku, kad jis gali pateikti prašymą apriboti duomenų tvarkymą. Taip pat įrenginiai ir programos turėtų būti kuriamos taip, kad pateikus prašymą dėl duomenų tvarkymo ribojimo, neliktų galimybės toliau tvarkyti asmens duomenis ar juos skleisti, sistemoje turi būti aiškiai nurodyta, kad asmens duomenų tvarkymas yra apribotas (BDAR preambulės 67 p.).

Taigi, siekiant užtikrinti duomenų subjekto teisę apriboti duomenų tvarkymą daiktų interneto technologijomis – itin svarbus pačių technologijų kūrėjų vaidmuo ir

[21]Viena iš diskriminacijos rūšių gali būti ekonominė diskriminacija. Daiktų interneto surinkti milžiniški asmeninės informacijos kiekiai gali tapti pajamų gausinimo priemonėmis, nes leidžia atsižvelgiant į stebėtą elgesį labiau suasmeninti kainų pasiūlymus (ypač – sveikatos draudimo sektoriuje) (Europos duomenų apsaugos priežiūros pareigūnas, 2015, p. 8). Pavyzdžiui, susiejus duomenis, kokiose vietose asmuo lankosi, kiek laiko miega, jo mitybos įpročius, galima sudaryti tam tikrą profilį, apibūdinantį asmens gyvenimo būdą (ar yra linkęs į alkoholizmą, kokia finansinė padėtis) ar net rasę (Peppet, 2014, p. 111).

standartizuotosios duomenų apsaugos principo įgyvendinimas. Technologijų kūrėjai turėtų sudaryti visas sąlygas vartotojui, kad šis bet kuriuo įrenginio naudojimo metu galėtų apriboti su juo susijusių duomenų tvarkymą. Teisė apriboti duomenų tvarkymą, kaip ir teisė nesutikti su duomenų tvarkymu, yra įgyvendinama tik pačio duomenų subjekto iniciatyva.

4.4. Teisė būti pamirštam

Iš duomenų kiekio mažinimo ir duomenų saugojimo trukmės apribojimo principų BDAR išskiria duomenų subjekto teisę reikalauti duomenų valdytojo ištrinti su juo susijusius duomenis (BDAR 17 str. 1 d.). Ši teisė dar kitaip įvardijama kaip teisė būti pamirštam. Vienintelis ir pakankamas pagrindas duomenų subjektui pasinaudoti nagrinėjama teise – paties duomenų subjekto pozicija, kad jo asmens duomenys tvarkomi neteisėtai ar nesąžiningai. Nereikalaujama, kad kuri nors institucija patvirtintų, kad duomenų subjekto įtarimai dėl jo asmens duomenų tvarkymo neteisėtumo ar nesąžiningumo pagrįsti (Petraitytė, 2013, p. 263). Įrodyti, kad duomenų tvarkymas yra teisėtas, teks duomenų valdytojams, nes jie yra atsakingi už tvarkymo teisėtumą (BDAR 17 str. 1 d.)[22]. BDAR numatomos ir šios teisės išimtys, kuomet duomenų valdytojas gali nesutikti su duomenų subjekto prašymu ištrinti su juo susijusius duomenis.

Daiktu interneto technologijomis tvarkomi asmens duomenys, dažniausiai yra tvarkomi sutikimo ar sutarties su duomenų subjektu pagrindu. Teisė būti pamirštam gali būti įgyvendinama ir kai subjektas atšaukia sutikimą tvarkyti jo duomenis (BDAR 17 str. 1 d. b p.). Reikalavimas, kad duotą sutikimą būtų galima lengvai atšaukti, apibūdinamas kaip būtinas galiojančio sutikimo pagal BDAR aspektas. Tuo atveju, kai teisė atšaukti sutikimą neatitinka BDAR reikalavimų, duomenų valdytojo naudojamas sutikimo mechanizmas neatitinka BDAR (Europos duomenų apsaugos valdyba, 2020, p. 25). Tokiam teisės įgyvendinimui vėl gi yra reikalingas įrenginių gamintojų indėlis kuriant tokius prietaisus, kuriais naudojantis būtų paprasta atšaukti sutikimą. Atšaukus sutikimą tvarkyti asmens duomenis turėtų būti paliekama galimybė toliau vartotojui naudoti įrenginį anonimiškai. Tai yra, vien dėl to, kad duomenų subjektas atšaukė sutikimą tvarkyti duomenis, neturėtų būti prarasta galimybė toliau naudotis įrenginiu.

[22]Tokiu būdu įgyvendinamas ir atskaitomybės principas, kurio vienas iš elementų, kaip aptarta anksčiau, yra bet kada sugebėti įrodyti, kad duomenų tvarkymas yra atliekamas teisėtai (BDAR 5 str. 2 d.).

4.5. Kitos duomenų subjekto teisės

Kitos BDAR numatytos duomenų subjekto teisės yra teisė susipažinti su duomenimis ir gauti informacijos apie jų tvarkymą (BDAR 15 str. 1 d.), teisė reikalauti, kad neišsamūs asmens duomenys būtų papildyti (BDAR 16 str.) (teisė reikalauti ištaisyti duomenis), teisė į duomenų perkeliamumą (BDAR 20 str.).

Duomenų subjekto teisė gauti informacijos apie duomenų tvarkymą yra susijusi su teise būti informuotam apie duomenų tvarkymą. Šiuo atveju informacija gaunama paties duomenų subjekto užklausos pagrindu, ne duomenų valdytojo iniciatyva. BDAR preambulės 63 punkte teisės akto leidėjas numato, kad jeigu tai yra įmanoma, duomenų valdytojas turėtų suteikti nuotolinę prieigą prie saugios sistemos, kurioje duomenų subjektas galėtų naudotis savo asmens duomenimis. Visais atvejais, svarbu užtikrinti, jog vartotojui būtų suteikiama galimybė gauti informaciją suprantamu ir lengvai prieinamu būdu, atsižvelgiant į kiekvieną situaciją atskirai. Pavyzdžiui, vartotojas pateikia prašymą susipažinti su duomenimis ir kartu prašymą dėl duomenų parkėlimo. Duomenų valdytojas, vykdydamas prašymus, informaciją apie duomenis, jų tvarkymą pateikia PDF formatu. Duomenis pateikiant tokiu formatu yra įgyvendinama vartotojo teisė susipažinti su duomenimis, tačiau ribojama galimybė duomenis perkelti ar ištrinti (Europos duomenų apsaugos valdyba, 2021, p. 34). Kaip aptarta anksčiau, daiktų interneto įrenginiai dažniausiai neturi galimybės pateikti visos informacijos vartotojui vienoje vietoje. Todėl ši nuostata galėtų būti įgyvendinama vartotojui pateikiant informaciją interneto svetainėje, į kurią gamintojas pateikia nuorodą ar prie įrenginio prijungtose programėlėse. Žinoma, kyla sunkumų, kai yra prijungti keli ar daugiau įrenginių ir daiktų interneto technologijomis yra tvarkomi asmens duomenys surinkti iš įvairių šaltinių. Tokiu atveju, tikriausiai, tikslingiausia būtų jei kiekvieno įrenginio gamintojas pateiktų tik tuo konkrečiu įrenginiu rinktus bei tvarkomus asmens duomenis. BDAR kartu nustato, jog duomenų valdytojas gali nevykdyti pareigos pateikti užklaustos informacijos duomenų subjektui, jeigu tai prieštarauja kitų asmenų teisėms ir laisvėms (BDAR 15 str. 4 d., preambulės 63 p.). Tokiu būdu užtikrinama pusiausvyra tarp duomenų subjekto, duomenų valdytojo bei trečiųjų asmenų teisių. Duomenų subjektas pasinaudodamas teise susipažinti su tvarkomais duomenimis, o duomenų valdytojas įvykdydamas šią pareigą, įgyvendina skaidrumo principą bei užtikrina pasitikėjimą tarp išmaniųjų įrenginių vartotojų ir gamintojų bei kitų asmenų (kurių interesai galėtų būti pažeisti atskleidžiant tam tikrą informaciją) (Wachter, 2018, p. 18).

Susipažinus su savo asmens duomenimis, duomenų subjektas taip pat turi teisę reikalauti duomenų valdytojo šiuos duomenis ištaisyti (BDAR 16 str.). Vartotojui pastebėjus, jog daiktų interneto technologijomis tvarkomi netikslūs ar pasenę duomenys, gali reikalauti įrenginių gamintojo ar programų kūrėjų ar kitų asmenų, kurie tuo atveju yra duomenų valdytojai, kad šie duomenys būtų ištaisyti. Tokia duomenų subjekto iniciatyva taip pat padeda ir nuoseklesniam daiktų interneto veikimui bei įrenginių funkcijų įgyvendinimui. Duomenų valdytojas turėdamas tikslesnius duomenis apie vartotoją gali užtikrinti, kad įrenginys būtų dar labiau pritaikytas vartotojo poreikiams.

Kita BDAR numatyta teisė, susijusi su aptartomis teisėmis būti informuotam apie duomenų tvarkymą ir susipažinti su duomenimis, yra teisė į duomenų perkeliamumą. BDAR 20 straipsnis numato, kad duomenų subjektas turi teisę gauti su juo susijusius asmens duomenis, kuriuos jis pateikė duomenų valdytojui susistemintu, įprastai naudojamu ir kompiuterio skaitomu formatu, ir turi teisę persiųsti tuos duomenis kitam duomenų valdytojui, kai asmens duomenys yra tvarkomi su duomenų subjekto sutikimu ar sutartimi su juo, kaip teisėto duomenų tvarkymo pagrindu, bei kai yra tvarkomi automatizuotomis priemonėmis. Daiktų internete dažniausiai duomenų tvarkymo pagrindas yra sutikimas arba sutartis su duomenų subjektu, o dėl daiktų interneto specifikos duomenys tvarkomi automatizuotomis priemonėmis. Aptariama BDAR norma taip pat yra keliami reikalavimai patiems įrenginių gamintojams, kad duomenys vartotojui būtų pateikiami susistemintu, įprastai naudojamu ir kompiuterio skaitomu formatu. Vėl gi išmaniųjų įrenginių gamintojui gali kilti problema duomenis pateikti per patį įrenginį, dėl to pats valdytojas turi parinkti tinkamą būdą, kuriuo galėtų įgyvendinti pareigą pateikti duomenis vartotojui. Be to, duomenis gaunantis duomenų valdytojas privalo užtikrinti, kad suteikti perkeliami duomenys būtų aktualūs ir jų nebūtų per daug, palyginti su tuo, kas reikalinga naujam duomenų tvarkymui (ES 29 str. duomenų apsaugos darbo grupė, 2017a, p. 7).

Visos duomenų subjekto teisės gali būti kildinamos iš duomenų apsaugos teisės principų. Kaip ir principų įgyvendinimui, tinkamam šių vartotojo teisių įgyvendinimui reikalingas įrenginių gamintojų ir programų kūrėjų nuoseklus darbas kuriant tokią įrangą, kuri padėtų įgyvendinti vartotojui jo teises, jeigu jis to reikalauja ir tam yra BDAR numatyti pagrindai.

5. KITI BENDROJO DUOMENŲ APSAUGOS REGLAMENTO REIKALAVIMAI, TAIKOMI DAIKTŲ INTERNETUI

BDAR tikslas apsaugoti duomenų subjekto teises įgyvendinamas ne tik principais ir normomis, reguliuojančiomis duomenų subjekto teises, bet ir kitais reikalavimais duomenų valdytojams, o kai kuriais atvejais – duomenų tvarkytojams.

5.1. Pareiga turėti duomenų tvarkymo pagrindą

Siekiant užtikrinti duomenų subjekto teises, BDAR yra įtvirtinta duomenų valdytojo pareiga turėti duomenų tvarkymo pagrindą. Ši pareiga yra susijusi su teisėtumo, sąžiningumo ir skaidrumo principu. Turint teisėtą duomenų tvarkymo pagrindą yra užtikrinamas teisėtumo elementas. Galimi duomenų tvarkymo teisėti pagrindai yra įtvirtinti BDAR 6 straipsnyje ir įvardinti tokie: duomenų subjekto sutikimas, sutartis su duomenų subjektu, teisinė prievolė, gyvybiniai fizinio asmens interesai, užduotis viešojo intereso labui arba viešosios valdžios funkcijos, teisėti duomenų valdytojo ar trečiosios šalies interesai. Visi šie duomenų tvarkymo pagrindai yra galimi tvarkant duomenis, surinktus daiktų interneto technologijomis. Darbo autorė pasirenka darbe aptarti dažniausiai pasitaikančius duomenų tvarkymo pagrindus. Dažniausiai daiktų interneto technologijomis duomenys renkami ir tvarkomi duomenų subjekto sutikimo arba sutarties su duomenų subjektu pagrindu. Daiktų internetui yra būdingas profiliavimas, automatizuotas sprendimų priėmimas, kuriems vykdyti taip pat yra reikalingas, visų pirma, teisėtas pagrindas (vieno iš alternatyvių duomenų tvarkymo pagrindų buvimas).

Pirmasis BDAR įtvirtintas teisėto duomenų tvarkymo pagrindas – sutikimas. Daiktų duomenų subjekto sutikimas rinkti ir tvarkyti duomenis turi būti duotas laisva duomenų subjekto valia, konkretus ir nedviprasmiškas, o pats subjektas, prieš pateikdamas tokį sutikimą, turi būti tinkamai informuotas (Europos Sąjungos pagrindinių teisių agentūra; Europos Taryba, 2019, p. 143; Zaleskis, 2019, p. 144). Daiktų interneto vartotojas dažnu atveju gali nežinoti apie duomenų tvarkymą, atliekamą konkrečių išmaniųjų įrenginių (ES 29 str. duomenų apsaugos darbo grupė, 2014, p. 7) – taip sukeliamas pavojus pačio vartotojo teisėms, o kartu ir tinkamos duomenų apsaugos teisės įgyvendinimui. Be to, duomenų valdytojo siūlymas pateikti sutikimą gali būti per sudėtingas vartotojui suprasti, kokius būtent duomenis įrenginys rinks ir tvarkys. Dėl to išmaniųjų įrenginių gamintojams būtina užtikrinti, kad jų vartotojas būtų tinkamai supažindintas su jam reikalinga informacija – kokie duomenys ir kokiais tikslais bus renkami / tvarkomi, taip užtikrinti, jog

vartotojas priims tinkamą sprendimą. Šios nuostatos įgyvendinimas gali būti apsunkintas, kai įrenginiai yra labai panašūs į neišmaniuosius įrenginius, pavyzdžiui, išmanusis laikrodis. Išmaniajam įrenginiui esant itin panašaus dizaino kaip ir neišmanusis prietaisas (išmanusis laikrodis ir paprastas, prie interneto neprijungiamas laikrodis), asmuo gali būti suklaidinamas dėl būtinybės duoti sutikimą dėl su juo susijusių duomenų tvarkymui. Išmanusis laikrodis gali turėti įrengtą mikrofoną ar kitas funkcijas, kurios gali rinkti duomenis vartotojui ar aplinkiniams asmenims (kurie šiuo atveju irgi tampa duomenų subjektais) nežinant (ES 29 str. duomenų apsaugos darbo grupė, 2014, p. 7). Dėl to išmaniųjų įrenginių gamintojai, turėtų kurti tokį dizainą, kuriuo būtų aplinkiniams aišku, kad įrenginys yra išmanus ir gali sugebėti rinkti duomenis. Žinoma, tai neatitinka pačių įrenginių gamintojų interesų, kurie nori kurti įrenginius kaip tik neišsiskiriančius sudėtingu dizainu ir patrauklius vartotojams. Įrenginių dizainas gali apsunkinti sutikimo vartotojui pateikimą, t. y. įrenginys gali turėti labai mažą ar iš vis jokio ekrano. Pavyzdžiui, išmaniojoje gertuvėje neįmontuotas ekranas, kuriuo gali būti suteikta galimybė vartotojui duoti sutikimą dėl su juo susijusių duomenų tvarkymo. Tokia pati problema kyla ir su kitais išmaniaisiais prietaisais, pavyzdžiui, išmaniąja orkaite, išmanieji elektros ar vandens skaitikliai ir kt. (Peppet, 2014, p. 48). Tokiu atveju sutikimas turėtų būti pateikiamas kitomis priemonėmis (internetiniu tinklapiu ar prie įrenginio prijungta programėle (Eskens, 2016, 37). Taip pat dėl sutikimo, kaip tikrosios vartotojo valios išraiškos kyla problema tuo aspektu, jog vartotojai jaučiasi įpareigoti duoti sutikimą, manydami, kad tik taip galės naudotis visomis išmaniojo įrenginio suteikiamomis funkcijomis. Dar dažniau vartotojas net neskaito jam pateikiamos informacijos apie duomenų tvarkymą. Taip atsitinka dėl to, jog, kaip ir privatumo pranešimų atvejais, informacija, susijusi su sutikimu vartotojui yra pateikiama per daug sudėtingai. Taigi, reikalingas ir pačio vartotojo atidumas.

Daiktų internetui aktuali ir kita su vartotojo sutikimu susijusi BDAR norma, reguliuojanti specialiųjų kategorijų duomenis. BDAR 9 straipsnio 2 dalis pateikia išsamų sąrašą, kuomet įprastai draudžiami tvarkyti specialiųjų kategorijų duomenys, gali būti tvarkomi. Vienas iš alternatyvių reglamento numatytų atvejų yra, kai duomenų subjektas aiškiai sutiko, kad tokie asmens duomenys būtų tvarkomi vienu ar keliais nurodytais tikslais (BDAR 9 str. 2 d.). Taigi, gavęs duomenų subjekto sutikimą, duomenų valdytojas turės teisėtą pagrindą tvarkyti net specialiųjų kategorijų duomenis, kartu ir duomenis gautus profiliavimo būdu.

Kitas dažnas teisėto daiktų interneto technologijomis tvarkomų asmens duomenų tvarkymo pagrindas yra sutartis su duomenų subjektu. Sutartis su duomenų subjektu kaip teisėto duomenų tvarkymo pagrindas turi sąsajų su sutikimu (Zaleskis, 2019, p. 148) – tai

yra sutikimo tvarkyti vartotojo duomenis išraiška. Tam, jog būtų suderintos sąlygos duomenų tvarkymo kontekste dažniausiai duomenų valdytojas pateikia įrenginio vartojimo sąlygas (angl. *Terms of service*). Skirtumas tarp sutarties su duomenų subjektu ir sutikimo tvarkyti duomenis yra tai, kad sutartimi su duomenų subjektu yra nustatomos pareigos ne tik duomenų subjektui, bet ir duomenų valdytojui (Zaleskis, 2019, p. 148). Pateikiant įrenginio vartojimo sąlygas gali kilti tokia pati problema kaip ir su sutikimu, kai duomenų valdytojas turi pateikti informaciją / sąlygas, su kuriomis vartotojas galėtų sutikti / nesutikti, tačiau šios sąlygos dėl specifinio įrenginių dizaino yra pateikiamos pasitelkiant kitus, vartotojui sunkiau prieinamus, šaltinius, pavyzdžiui, sąlygos patalpinamos interneto svetainėje. Taip pat gali kilti problema ir tuo aspektu, jog įrenginio vartojimo sąlygas parengia duomenų valdytojas ir jos suformuluojamos taip, jog vartotojas turi galimybę tik sutikti arba nesutikti su sąlygomis (tačiau negali jų pakeisti ar pan.), todėl vartotojas gali likti silpnąja sutarties šalimi. Tačiau vartotojo ir duomenų valdytojų interesų pusiausvyrai išlaikyti BDAR numatytos duomenų subjekto teisės bei duomenų valdytojų pareigos. Taip pat teisinis reguliavimas yra kuriamas atsižvelgiant į tai, kad vartotojas galimai yra silpnesnė šalis ir orientuotas į vartotojo teisių apsaugojimą (Noto La Diega, Walden, 2016, p. 3, Lindqvist, J., 2018, p. 50) (pavyzdžiui, teisė būti informuotam apie asmens duomenų tvarkymą, teisė nesutikti su duomenų tvarkymu, teisė apriboti duomenų tvarkymą, teisė būti pamirštam, teisė susipažinti su duomenimis ir juos ištaisyti, teisė į duomenų perkeliamumą, duomenų valdytojo pareiga užtikrinti, kad duomenų tvarkymas būtų vykdomas pagal BDAR numatytus principus).

Duomenų subjekto sutikimas ir sutartis su duomenų subjektu yra dažniausiai pasitaikantys duomenų, surinktų daiktų interneto technologijomis, tvarkymo pagrindai. Vartotojo valios dėl sutikimo tvarkyti asmens duomenis išreiškimo sklandžiam įgyvendinimui reikalingas daiktų interneto technologijų kūrėjų indėlis, užtikrinant, jog vartotojui pateikiama sutikimo forma būtų aiški, suprantama ir išsami. Taip pat svarbu užtikrinti, kad vartotojas turėtų galimybę pasirinkti nesutikti su jo duomenų tvarkymu. Nepaisant to, reikalingas ir pačių duomenų subjektų atidumas, atsakingas požiūris į jų pačių asmens duomenų saugumą.

5.2. Pareiga pranešti apie duomenų saugumo pažeidimą

Daiktų interneto technologijomis yra renkami ir tvarkomi įvairaus pobūdžio duomenys, dalis jų gali būti jautrūs (pavyzdžiui, biometriniai duomenys, asmens kodas, kreditinės kortelės duomenys). Dėl to duomenų subjektui yra ypatingai svarbus surinktų duomenų

saugumas. Esant duomenų saugumo pažeidimui, kyla pavojus duomenų subjekto kaip fizinio asmens interesų saugumui. Duomenų subjektui svarbu žinoti ir pasitikėti duomenų valdytoju ir duomenų tvarkytoju, jog esant duomenų saugumo pažeidimui bus imtasi tam tikrų priemonių, kurios padėtų kuo labiau sumažinti galimą žalą. Dėl šios priežasties BDAR numato reikalavimą, taikomą duomenų valdytojui - pareigą pranešti apie duomenų saugumo pažeidimą. Asmens duomenų saugumo pažeidimo atveju duomenų valdytojas per 72 valandas nepagrįstai nedelsdamas nuo tada, kai jis sužino apie asmens duomenų saugumo pažeidimą, apie tai praneša kompetentingai priežiūros institucijai, nebent asmens duomenų saugumo pažeidimas neturėtų kelti pavojaus fizinių asmenų teisėms ir laisvėms. Jeigu yra paskirtas asmens duomenų tvarkytojas, šis apie pažeidimą privalo pranešti duomenų valdytojui (BDAR 33 str. 1, 2 d.). Daiktų internete didelė dalis asmens duomenų yra tvarkoma paskyrus duomenų tvarkytoją (dažnu atveju debesų kompiuterijos paslaugų tiekėją) (Ni Loideain, 2018, p. 32). Dėl šios priežasties svarbu, kad duomenų tvarkytojui taip pat yra paskiriama pareiga stebėti ir, įvykus asmens duomenų pažeidimui, nedelsiant apie tai pranešti duomenų valdytojui.

Svarbu atkreipti dėmesį, kad reglamentas numato, jog apie pažeidimą turi būti pranešta, kai šis kelia pavojų fizinių asmenų teisėms ir laisvėms. Rizika galėtų kilti ir apie pažeidimą turėtų būti pranešta priežiūros institucijai, neapsiribojant tais atvejais, kai pažeidimas kelia pavojų daiktų interneto vartotojų teisėms ir laisvėms (Ni Loideain, 2018, p. 32).

Pareiga pranešti apie duomenų saugumo pažeidimą padeda įgyvendinti skaidrumo principą, tuo pačiu užtikrina daiktų interneto vartotojų pasitikėjimą duomenų valdytojais. Augantis pasitikėjimas skatina vartotojus naudotis išmaniaisiais įrenginiais, o įrenginių gamintojams padeda jų naudojimą pritaikyti būtent pagal konkretaus vartotojo poreikius (Morey *et al*, 2015 cituota Ni Loideain, 2018, p. 33; Wachter, 2017 p. 18-20).

Vis dėlto, net jeigu pažeidimas nekelia pavojaus fizinių asmenų teisėms ir laisvėms, duomenų valdytojas tokį pažeidimą turi užregistruoti (BDAR 33 str. 5 d.). Kiekvieno pažeidimo užregistravimas reikalingas ne tik priežiūros institucijoms, bet ir naudingas patiems daiktų interneto įrenginių ir programų kūrėjams. Buvusių pažeidimų ir jų priežasčių įvertinimas gali padėti kurti saugesnes ir vartotojui saugumo atžvilgiu patrauklesnes technologijas. Ar pažeidimas kelia pavojų fizinių asmenų teisėms ir laisvėms, įvertina pats duomenų valdytojas, kuris pagal atskaitomybės principą turi galėti įrodyti savo sprendimo pagrįstumą. Jeigu duomenų valdytojas, atlikęs vertinimą, nustato, kad yra galimybė, jog dėl pažeidimo kils didelis pavojus fizinių asmenų teisėms ir laisvėms, apie asmens duomenų saugumo pažeidimą praneša duomenų subjektui (BDAR 34 str. 1

d.). BDAR numatytos ir šios pareigos išimtys – duomenų valdytojas neturi pranešti apie asmens duomenų pažeidimą, kai duomenų valdytojas įgyvendino tinkamas technines ir organizacines apsaugos priemones ir tos priemonės taikytos asmens duomenims, kuriems asmens duomenų saugumo pažeidimas turėjo poveikio; duomenų valdytojas vėliau ėmėsi priemonių, kuriomis užtikrinama, kad nebegalėtų kilti didelis pavojus duomenų subjektų teisėms ir laisvėms; tai pareikalautų neproporcingai daug pastangų, o ta pati informacija galėtų būti pateikta viešai (BDAR 34 str. 3 d.) (pavyzdžiui, patalpinus informaciją apie pažeidimą žiniasklaidos tinklalapyje).

Visais atvejais duomenų valdytojas turi atsižvelgti į galimą pavojų fizinių asmenų teisėms ir laisvėms. Tik įvertinęs visas reikšmingas aplinkybes, nuspręsti, ar apie pažeidimą reikia pranešti duomenų subjektui, ar ne. Visais atvejais turi būti vadovaujamasi skaidrumo principu, padedančiu užtikrinti pasitikėjimą tarp daiktų interneto vartotojo ir duomenų valdytojo.

5.3. Poveikio duomenų apsaugai vertinimas

Skaidrumą ir pasitikėjimą tarp vartotojų ir duomenų valdytojų užtikrina reikalavimas duomenų valdytojui, prieš pradedant tvarkyti asmens duomenis, atlikti poveikio asmens duomenų apsaugai vertinimą (BDAR 35 str. 1 d.). Jeigu atlikus vertinimą nustatoma, kad gali kilti pavojus, duomenų valdytojas yra įpareigojamas prieš pradėdamas tvarkyti asmens duomenis konsultuotis su priežiūros institucija (BDAR 36 str. 1 d.).

BDAR numatyti atvejai, kai duomenų valdytojas turi atlikti poveikio duomenų apsaugai vertinimą. Daiktų interneto technologijomis tvarkomų asmens duomenų valdytojai turi laikytis šio reikalavimo, kadangi, vienas iš privalomo vertinimo atvejų yra, kai duomenų valdytojas atlieka sistemingą ir išsamų su fiziniais asmenimis susijusių asmeninių aspektų vertinimą, kuris yra grindžiamas automatizuotu tvarkymu, įskaitant profiliavimą, taip pat, kai tvarkomi jautrūs (specialių kategorijų) duomenys (BDAR 35 str. 3 d. a, b p.) (specialiųjų kategorijų duomenimis laikomi: atskleidžiantys rasinę ar etninę kilmę, politines pažiūras, religinius ar filosofinius įsitikinimus ar narystę profesinėse sąjungose, taip pat genetiniai duomenys, biometriniai duomenys, siekiant konkrečiai nustatyti fizinio asmens tapatybę, sveikatos duomenys arba duomenys apie fizinio asmens lytinį gyvenimą ir lytinę orientaciją (BDAR 9 str. 1 d., BDAR preambulė, 75 p.)). Specialiųjų kategorijų duomenys gali būti lengvai renkami įvairiais išmaniaisiais įrenginiais, pavyzdžiui, išmanioji apyrankė „Fitbit“ sugeba rinkti ir tvarkyti duomenis apie vartotojo širdies ir kraujagyslių veiklą. Atlikus tyrimą buvo nustatyta, kad renkant tokius

duomenis netgi įmanoma nustatyti vartotojo, sergančio bipoliniu sutrikimu, nuotaikų kaitą (Gentili *et al*., 2017 cituota Talboom, Huentelman, 2018, p. R36). Tai parodo, jog išmaniųjų įrenginių renkama informacija yra įvairi ir dažnu atveju gali būti priskiriama BDAR numatytai specialiajai kategorijai. Tokie asmens duomenys tvarkomi automatizuotai ir profiliuojami gali pateikti išvadas apie dar jautresnius asmens duomenis, kurių kartais net pas asmuo, su kuriuo susiję duomenys yra tvarkomi, nežino.

Pareiga atlikti poveikio duomenų apsaugai vertinimą yra numatoma ir kai yra atliekamas sistemingas viešos vietos stebėjimas dideliu mastu (BDAR 35 str. 3 d. c p.). Ši sąlyga galėtų būti taikoma, kai asmens duomenys yra tvarkomi daiktų interneto technologijomis jungiamais išmaniųjų miestų naudojamais įrenginiais, pavyzdžiui viešose erdvėse įrengtomis kameromis, šviesoforais, sugebančiais jutikliais sekti asmenų judėjimą, buvimo vietą.

ES 29 straipsnio darbo grupė, gairėse dėl poveikio duomenų apsaugai vertinimo pabrėžia, kad nors BDAR numato duomenų valdytojo pareigą atlikti vertinimą tik tais atvejais, kai dėl duomenų tvarkymo fizinių asmenų teisėms bei laisvėms gali kilti didelis pavojus, nereiškia, kad neatitikus numatytų sąlygų sumažėja duomenų valdytojo pareiga įgyvendinti priemones, kuriomis būtų tinkamai valdomi duomenų subjektų teisėms ir laisvėms kylanti rizika (ES 29 straipsnio darbo grupė, 2017b, p. 7). Taigi, galima teigti, jog duomenų valdytojai visuomet, nepaisant valdomų duomenų pobūdžio, turėtų nuolatos vertinti valdomų asmens duomenų tvarkymo pavojus išmaniųjų įrenginių vartotojams.

Duomenų valdytojas neturėtų apsiriboti tik BDAR 35 straipsnyje 3 dalyje numatytais atvejais, kada poveikio duomenų apsaugai vertinimas yra privalomas. Priežiūros institucija sudaro ir viešai paskelbia duomenų tvarkymo operacijų rūšių, kurioms taikomas reikalavimas atlikti poveikio duomenų apsaugai vertinimą, sąrašą (BDAR 35 str. 4 d.). Lietuvoje toks sąrašas yra pateikiamas VDAI direktorius įsakymu. Pagal VDAI direktoriaus parengtą sąrašą, poveikio duomenų apsaugai vertinimo procedūra turi būti atlikta šiais alternatyviais atvejais (Valstybinės duomenų apsaugos inspekcijos direktoriaus..., 2019, 1-10 p.):

1) asmens duomenų tvarkymas mokslinių ar istorinių tyrimų tikslais, kai be asmens sutikimo tvarkomi specialių kategorijų asmens duomenys arba asmens duomenų tvarkymas vykdomas susiejant ar derinant duomenų rinkinius; kai tvarkomi nepilnamečių asmenų duomenys; kai tvarkomas asmens kodas.

2) Asmens duomenų tvarkymas vykdomas dideliu mastu, kai asmens duomenys gauti ne iš asmens.

3) Asmens duomenų tvarkymas, kai duomenų gavėjų, kuriems buvo atskleisti asmens duomenys, informavimas apie asmens duomenų ištaisymą, ištrynimą arba tvarkymo apribojimą nėra įmanomas arba pareikalautų neproporcingų pastangų.

4) Biometrinių duomenų, kuriais siekiama konkrečiai nustatyti fizinio asmens tapatybę, tvarkymas asmenų stebėsenos ar kontrolės tikslais arba kai tvarkomi pažeidžiamų asmenų duomenys.

5) Genetinių duomenų tvarkymas vykdant asmens savybių vertinimą arba balų skyrimą, įskaitant profiliavimą ir prognozavimą.

6) Asmens vaizdo duomenų tvarkymas, kai vaizdo stebėjimas vykdomas patalpose ir (ar) teritorijose, kurios nėra duomenų valdytojo valdomos nuosavybės ar kitais teisėtais pagrindais; sveikatos priežiūros, socialinės globos, įkalinimo įstaigose ir kitose įstaigose, kuriose paslaugos yra teikiamos pažeidžiamiems asmenims; kartu su garso įrašymu.

7) Pokalbių telefonu įrašymas.

8) Asmens duomenų tvarkymas naudojant inovatyvias technologijas arba egzistuojančias technologijas panaudojant nauju būdu, kai tvarkomi pažeidžiamų duomenų subjektų asmens duomenys.

9) Vaikų asmens duomenų tvarkymas tiesioginės rinkodaros tikslais, vaikų asmeninių aspektų vertinimas, kuris yra grindžiamas automatizuotu tvarkymu, įskaitant profiliavimą, arba kai vaikams tiesiogiai yra siūlomos informacinės visuomenės paslaugos.

10) Darbuotojų asmens duomenų tvarkymas stebėsenos ar kontrolės tikslais.

Lietuvos nacionalinės teisės numatyti atvejai, kada poveikio duomenų apsaugai vertinimas yra privalomas tik patvirtina, jog daiktų interneto technologijomis renkamų ir tvarkomų duomenų saugiam tvarkymui užtikrinti reikalingas poveikio duomenų apsaugai vertinimas. Ypač svarbu atkreipti dėmesį, jog VDAI direktoriaus įsakymu yra numatytas atvejis, kai asmens duomenų tvarkymas vyksta dideliu mastu[23]. Ši nuostata praplečia BDAR numatytą sąlygą privalomam poveikio duomenų apsaugai vertinimui vykdyti, kai atliekamas sistemingas viešosios vietos stebėjimas dideliu mastu. Daiktų interneto kontekste taip pat svarbi sąlyga, kai yra tvarkomi biometriniai bei genetiniai duomenys. Šie duomenys BDAR yra priskiriami prie specialiųjų duomenų kategorijos ir tokių duomenų tvarkymas BDAR taip pat nurodytas kaip reikalaujantis privalomo poveikio duomenų apsaugai vertinimo. VDAI pateiktame sąraše nurodomas atvejis, kai reikalingas poveikio duomenų apsaugai vertinimas dėl asmens vaizdo duomenų tvarkymas. Toks tvarkymas gali

[23]VDAI nėra pateikusi tikslaus tvarkomų duomenų kiekio ar atitinkamų asmenų skaičiaus, kuriems esant būtų laikytina, kad asmens duomenų tvarkymas atliekamas dideliu mastu (Valstybinė duomenų apsaugos inspekcija, 2019, p. 41).

būti atliekamas išmaniosiomis vaizdo stebėjimo kameromis. Šios vaizdo kameros dažnai yra gebančios ne tik sekti ir įrašyti vaizdą, bet ir stebėti aplinką (per jutiklius gaunamą informaciją gali sudaryti duomenys apie drėgmę, temperatūrą, oro kokybę patalpose) taip pat gali būti naudojamos ir išmaniosios vaizdo kameros prie kurių prijungti išmanieji asistentai (pavyzdžiui, „Google Nest Cam“, kurioje įdiegtas „Googe Assistant“), tokiu būdu kamera renka ne tik asmens vaizdo duomenis, bet ir stebi asmens elgesį, įpročius pagal asmens bendravimą su išmaniuoju asistentu. Asmens (kartu ir pažeidžiamų asmenų) vaizdo duomenys kartu su įrašytu garsu gali būti tvarkomi, kai jie yra gauti iš viešose vietose, tokiose kaip miesto aikštės, gatvės ir pan., įdiegtų vaizdo kamerų. Pasitelkiant išmaniųjų miestų technologijas, be kitų atvejų (pavyzdžiui, išmaniųjų namų technologijomis) gali būti renkami ir tvarkomi ir vaikų asmens duomenys. Įrenginių gamintojai, numatydami galimybę, jog vartotojas gali būti vaikas taip pat turi atlikti poveikio duomenų apsaugai vertinimą.

Taigi, galima teigti, jog VDAI direktoriaus sąraše, nustatančiame poveikio duomenų apsaugai vertinimo reikalaujančias operacijas, yra praplečiamos BDAR normos. Tiek Lietuvos nacionalinės teisės normomis, tiek BDAR normomis numatyti atvejai, kada privalo būti atliktas poveikio duomenų apsaugai vertinimas, aiškiai nurodo, kad daiktų interneto technologijomis atliekamas asmens duomenų tvarkymas (ypač atsižvelgiant į tai, jog yra atliekamas automatizuotomis priemonėmis (įskaitant profiliavimą) bei renkamų duomenų pobūdį) reikalauja poveikio duomenų apsaugai vertinimo.

Reikalavimas atlikti duomenų apsaugos vertinimą ne tik sukuria tvirtesnius pasitikėjimo santykius tarp daiktų interneto vartotojo ir duomenų valdytojo. Tokia pareiga taip pat gali padėti patiems įrenginių ir programų kūrėjams atkreipti dėmesį į probleminius technologijos aspektus ir išvystyti vartotojui saugumo atžvilgiu patrauklesnius įrenginius.

5.4. Pareiga turėti duomenų apsaugos pareigūną

Duomenų valdytojui tinkamai įgyvendinti BDAR nuostatas padeda duomenų apsaugos pareigūnas. Šis reikalavimo įgyvendinimas, kaip ir kiti darbe analizuoti duomenų valdytojui taikomi reikalavimai, didina pasitikėjimą tarp duomenų valdytojo bei subjekto. Pareiga turėti duomenų apsaugos pareigūną siejama su atskaitomybės principu, kadangi vykdydamas nagrinėjamą reikalavimą duomenų valdytojas įpareigojamas prisiimti daugiau atsakomybės už duomenų tvarkymą ir mažina priežiūros institucijos kišimąsi į kasdienę duomenų tvarkymo veiklą (Zaleskis, 2017, p. 162).

Duomenų apsaugos pareigūną gali paskirti tiek duomenų valdytojas, tiek duomenų tvarkytojas. Jeigu duomenų valdytojas yra paskyręs duomenų apsaugos pareigūną, pastarasis turi dalyvauti ir atliekant poveikio duomenų apsaugai vertinimą (BDAR 35 str. 2 d.). Paskirti duomenų apsaugos pareigūną privalo, kai (BDAR 37 str. 1 d.):

1) duomenis tvarko valdžios institucija arba įstaiga;

2) duomenų valdytojo arba duomenų tvarkytojo pagrindinė veikla yra duomenų tvarkymo operacijos, dėl kurių būtina reguliariai ir sistemingai dideliu mastu stebėti duomenų subjektus;

3) arba duomenų valdytojo arba duomenų tvarkytojo pagrindinė veikla yra specialių kategorijų duomenų tvarkymas dideliu mastu arba asmens duomenų apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas tvarkymas dideliu mastu.

Išmanieji įrenginiai ligoninėse, padedantys stebėti pacientų sveikatą, išmanieji keliai, išmanieji skaitikliai (vandens, elektros) – visų šių prietaisų renkamų asmens duomenų valdytoju dažnu atveju yra viešasis juridinis asmuo (savivaldybė, viešoji įstaiga ir kt.). Daiktų interneto technologijomis nuolatos yra renkami ir tvarkomi dideli kiekiai įvairaus pobūdžio asmens duomenų, kurie dažnai gali būti priskiriami specialiosioms kategorijoms, nurodytoms BDAR 9 straipsnyje. Taip pat daiktų interneto įrenginiai pasižymi tuo, kad nuolatos atlieka duomenų subjekto – įrenginio vartotojo stebėseną, tam kad asmens duomenys ir sudaromas asmens profilis būtų kuo tikslesnis ir įrenginio vartojimas galėtų būti orientuotas į konkretų vartotoją. Taigi, darytina išvada, jog beveik visais atvejais daiktų interneto technologijomis tvarkomų asmens duomenų valdytojas ar tvarkytojas bus įpareigotas paskirti duomenų apsaugos pareigūną. Net, jeigu duomenų valdytojas teisiškai neprivalo paskirti duomenų apsaugos pareigūno, ES 29 straipsnio darbo grupė, siekiant užtikrinti atskaitomybės principo įgyvendinimą, siūlo organizacijai savanoriškai paskirti duomenų apsaugos pareigūną (ES 29 straipsnio darbo grupė, 2017b, p. 31).

Taigi, atsižvelgiant į tai, jog daiktų interneto technologijomis tvarkomi duomenys nuolatos naujinami, sisteminami, duomenų apsaugos pareigūnas atlieka itin reikšmingą vaidmenį, nesvarbu kokius duomenis, kokiu mastu renka. Bet koks duomenų valdytojas, tvarkydamas asmens duomenis daiktų interneto technologijomis turėtų (net jeigu tam ir nėra BDAR numatytos teisinės prievolės) paskirti duomenų apsaugos pareigūną, kuris padėtų įgyvendinti visus duomenų apsaugos principus, užtikrinti subjektų teises bei įvykdyti kitus reikalavimus.

IŠVADOS

1) Daiktų internetas yra tinklas, prie kurio gali būti prijungti išmanieji prietaisai. Tokie įrenginiai gali rinkti įvairaus pobūdžio asmens duomenis. Duomenimis prietaisai gali dalintis tarpusavyje, o visa tai padeda prietaisams pritaikyti savo veikimo parametrus pagal vartotojo poreikius. Tai lemia, jog daiktų interneto technologijomis yra renkama ir automatizuotomis priemonėmis (įskaitant profiliavimą) tvarkoma itin dideli kiekiai asmens duomenų. Toks duomenų „maksimizavimas“ kelia grėsmę vartotojų teisės į privatumą ir teisės į duomenų apsaugą užtikrinimui.

2) Tam, jog daiktų internetas būtų naudojamas saugiai, nepažeidžiant asmenų teisės į privatų gyvenimą ir duomenų apsaugos teisės, yra svarbu aiškiai reglamentuoti asmens duomenų objektą, apibrėžti duomenų valdytojo ir tvarkytojo teises ir pareigas, užtikrinti tinkamą duomenų apsaugos reguliavimą bei jo taikymą ne tik ES lygiu, bet ir nacionaliniu mastu. BDAR ES lygiu įtvirtina pamatines bendrąsias asmens duomenų tvarkymo taisykles, taikytinas daiktų internetui.

3) Asmens duomenimis laikomi tokie duomenys, kurie yra susiję su asmeniu, įskaitant duomenis apie asmens įpročius, elgesį. Išmanieji įrenginiai, pasitelkdami juose įmontuotus jutiklius, renka ir tvarko būtent su vartotoju susijusius duomenis, stebi vartotojo elgesį, įpročius, pageidavimus. Asmuo, kurio asmens duomenys tvarkomi, yra laikomas duomenų subjektu. Daiktų interneto kontekste, duomenų subjektas yra išmaniųjų įrenginių vartotojas.

~~4)~~ Duomenų valdytoju pagal BDAR laikomas asmuo, kuris nustato duomenų tvarkymo tikslą bei duomenų tvarkymo priemones. Daiktų interneto kontekste dažniausiai duomenų tvarkymo tikslą ir duomenų tvarkymo priemones nustato daiktų interneto bendrovės (įrenginių, operacinių sistemų gamintojai). Pagal teritorinio BDAR taikymo reguliavimą, BDAR taikomas dviem atvejais: duomenų valdytojui turint buveinę ES arba kai duomenų subjektas yra ES ir duomenų valdytojo duomenų tvarkymo veikla susijusi su prekių ar paslaugų siūlymu arba duomenų subjektų elgesio stebėsena ES. Dažniausiai daiktų interneto bendrovės turi buveinę ES teritorijoje, todėl jos įpareigojamos duomenis tvarkyti vadovaujantis BDAR.

5) BDAR įtvirtinti duomenų apsaugos teisės principai yra pagrindinės nuostatos, BDAR įtvirtinančios duomenų subjektų teises ir pareigas. Pagrindinis duomenų valdytojui keliamas reikalavimas – teisėtas duomenų tvarkymo pagrindas. Daiktų interneto kontekste dažniausiai tai yra vartotojo sutikimas arba sutartis su vartotoju. Vartotojo sutikimo pateikimui esant apsunkintam dėl išmaniųjų įrenginių techninių savybių, siekiant užtikrinti,

kad duomenų subjekto sutikimas tvarkyti jo duomenis būtų duodamas laisva valia ir suteikus jam teisingą informaciją, turi būti pasitelkiamos pagalbinės priemonės. Skaidrumo principu užtikrinamas pasitikėjimas tarp daiktų interneto bendrovių bei jų vartotojų – vartotojas, žinodamas, kokie duomenys ir kokiu tikslu yra tvarkomi nesijaus stebimas ar bejėgis kontroliuoti, kokie su juo susiję duomenys bus tvarkomi.

6) Duomenų valdytojas pagal BDAR įtvirtintą duomenų kiekio mažinimo principą turi užtikrinti, jog būtų tvarkomi nustatytam tikslui įgyvendinti būtini duomenys. Tam, kad būtų užtikrinti duomenų subjekto interesai, bet kartu ir išnaudojamas visas daiktų interneto technologijų potencialas, įrenginių gamintojai turėtų suteikti galimybę duomenų subjektui, kai to reikia, naudotis išmaniaisiais įrenginiais anonimiškai.

7) Duomenų subjektų teisės kildinamos iš BDAR įtvirtintų duomenų apsaugos teisės principų. Duomenų valdytojas turi užtikrinti, jog vartotojui patogiausiu būdu būtų suteikta informacija apie duomenų tvarkymą, suteikta galimybė nesutikti su duomenų tvarkymu, apriboti duomenų tvarkymą, įgyvendinti teisę būti pamirštam, susipažinti su duomenimis, juos ištaisyti bei perkelti duomenis. Šias teises gali būti sunku įgyvendinti dėl daiktų interneto įrenginių dizaino - išmaniuosiuose įrenginiuose ne visada yra įmontuotas ekranas, kuriame duomenų subjektui būtų pateikta visa reikalinga informacija. Tokiais atvejais išmaniųjų įrenginių gamintojai turėtų pasitelkti kitas platformas (prie įrenginių prijungtas programėles, internetinius puslapius ir pan.), kad duomenų subjektas turėtų galimybę lengvai įgyventi savo teises.

8) Atsižvelgiant į tai, jog daiktų interneto technologijomis tvarkomi duomenys nuolatos naujinami, sisteminami, duomenų tvarkymas atliekamas automatizuotomis priemonėmis (įskaitant profiliavimą) bei dažnu atveju yra tvarkomi specialiųjų kategorijų duomenys, duomenų valdytojai yra įpareigojami atlikti poveikio duomenų apsaugai vertinimą bei paskirti duomenų apsaugos pareigūną. Šių reikalavimų įgyvendinimas padeda užtikrinti, jog viso duomenų tvarkymo laikotarpiu būtų laikomąsi asmens duomenų teisės principų bei užtikrinami duomenų subjekto interesai, su juo susijusių duomenų saugumas.

ŠALTINIAI

Specialioji literatūra

1. Ashton, K. (2009). That 'Internet of Things' Thing. *RFID Journal*, [interaktyvus. Žiūrėta 2021 m. balandžio 19 d.]. Prieiga per internetą: http://www.itrco.jp/libraries/RFIDjournal-That%20Internet%20of%20Things%20Thing.pdf.

2. Eskens, S. (2016). Profiling the European Citizen in the Internet of Things: How Will the General Data Protection Regulation Apply to this Form of Personal Data Processing, and How Should It? In *Social Science Research Network*, [interaktyvus. Žiūrėta 2021 m. balandžio 19 d.]. Prieiga per internetą: http://dx.doi.org/10.2139/ssrn.2752010.

3. European Parliamentary Research Service (2015). *The Internet of Things: Opportunities and challenges* [interaktyvus. Žiūrėta 2021 m. balandžio 19 d.]. Prieiga per internetą: https://www.europarl.europa.eu/RegData/etudes/BRIE/2015/557012/EPRS_BRI%282015%29557012_EN.pdf.

4. Europos Sąjungos pagrindinių teisių agentūra; Europos Taryba (2019). *Handbook on European Data protection Law*. Liuksemburgas: Publications Office of the European Union, [interaktyvus. Žiūrėta 2021 m. balandžio 19 d.]. Prieiga per internetą: https://op.europa.eu/en/publication-detail/-/publication/5b0cfa83-63f3-11e8-ab9c-01aa75ed71a1/language-en.

5. Greveler, U., Glösekötter, P., Justus, B. and Loehr, D. (2012). *Multimedia Content Identification Through Smart Meter Power Usage Profiles*. Proc. Int. Conf. Inf. Knowl. Eng. (IKE). [interaktyvus. Žiūrėta 2021 m. balandžio 19 d.]. Prieiga per internetą: https://www.researchgate.net/publication/266461208_Multimedia_Content_Identification_Through_Smart_Meter_Power_Usage_Profiles.

6. Gubbi, J. *et al*. (2013). Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions. *Future Gener. Comput. Syst.*, 29(7), 1645–1660, [interaktyvus. Žiūrėta 2021 m. balandžio 19 d.]. Prieiga per internetą: https://doi.org/10.1016/j.future.2013.01.010.

7. Jusas, N. (2017). Feature Model-Based Development of Internet of Things Applications. Doctoral dissertation, Technological sciences, Informatics Engineering (07T). Kaunas: Kaunas University of Technology.

8. Lindqvist, J. (2018). New challenges to personal data processing agreements: is the GDPR fit to deal with contract, accountability and liability in a world of the Internet of Things? *International Journal of Law and Information Technology*, 26, 1, Spring, 45–

63 [interaktyvus. Žiūrėta 2021 m. balandžio 19 d.]. Prieiga per internetą: https://doi.org/10.1093/ijlit/eax024

9. Maras, M. (2015). Internet of Things: security and privacy implications. *International Data Privacy Law*, 5, 2, 99-104, [interaktyvus. Žiūrėta 2021 m. balandžio 19 d.]. Prieiga per internetą: https://academic.oup.com/idpl/article-abstract/5/2/99/645234.

10. Misra, S., Mukherjee, A. and Roy, A. (2021). *Introduction to IoT*. Cambridge: Cambridge University Press, [interaktyvus. Žiūrėta 2021 m. balandžio 19 d.]. Prieiga per internetą: https://doi.org/10.1017/9781108913560.

11. Ni Loideain, N. (2018). A Port in the Data-Sharing Storm: The GDPR and the Internet of Things. *King's College London Law School Research Paper No. 2018-27,* [interaktyvus. Žiūrėta 2021 m. balandžio 19 d.]. Prieiga per internetą: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3264265.

12. Noto La Diega, G. and Walden, I. (2016). Contracting for the 'Internet of Things': Looking into the Nest. *Queen Mary School of Law Legal Studies Research Paper No. 219/2016* [interaktyvus. Žiūrėta 2021 m. balandžio 19 d.]. Prieiga per internetą: https://ssrn.com/abstract=2725913

13. Peppet, S.R. (2014). Regulating the Internet of Things: First Steps Towards Managing Discrimination, Privacy, Security, and Consent. *Texas Law Review*, (1), p. 85-178.

14. Petraitytė, I. (2013). Asmens duomenų teisinės apsaugos principai. Daktaro disertacija, socialiniai mokslai, teisė (01S). Vilnius: Vilniaus universitetas.

15. Shayegh, P., Ghanavati, S. (2017). Toward an Approach to Privacy Notices in IoT. *IEEE 25th International Requirements Engineering Conference Workshops (REW),* 104-110, [interaktyvus. Žiūrėta 2021 m. balandžio 19 d.]. Prieiga per internetą: https://doi: 10.1109/REW.2017.77.

16. Talboom J. S., Huentelman M. J. (2018). Big data collision: the internet of things, wearable devices and genomics in the study of neurological traits and disease. *Human Molecular Genetics*, 27, R1, R35–R39 [interaktyvus. Žiūrėta 2021 m. balandžio 19 d.]. Prieiga per internetą: https://doi.org/10.1093/hmg/ddy092

17. Vermesan, O. *et al*. (2012). Europe's IoT Strategic Research Agenda 2012. In: Smith, I. (2012). *The Internet of Things 2012: New Horizons.* Technical report, European Research Cluster on the internet of things, 22-118.

18. Wachter, S. (2017). Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR. *Computer Law & Security*

Review, 34 (3), 436-449. [interaktyvus. Žiūrėta 2021 m. balandžio 19 d.]. Prieiga per internetą: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3083554.

19. Wachter, S. (2018). The GDPR and the Internet of Things: A Three-Step Transparency Model. Law*, Innovation and Technology*, 10, 266-294, [interaktyvus. Žiūrėta 2021 m. balandžio 19 d.]. Prieiga per internetą: https://doi.org/10.1080/17579961.2018.1527479.

20. Zaleskis, J. (2017). Duomenų apsaugos pareigūno veiklos pagrindai pagal ES Bendrąjį duomenų apsaugos reglamentą. *Teisė*, 1040, p. 159-170, [interaktyvus. Žiūrėta 2021 m. balandžio 19 d.]. Prieiga per internetą: https://doi: 10.15388/Teise.2017.104.10851.

21. Zaleskis, J. (2019). *Europos Sąjungos Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė*. Monografija. Vilnius: VĮ Registrų centras.

22. Zalieckaitė, L. ir Žilinskas, R. (2016) „Daiktų interneto technologijos taikymo versle nauda ir rizika“, Informacijos mokslai, 720, p. 102-117. 294. [interaktyvus. Žiūrėta 2021 m. balandžio 19 d.]. Prieiga per internetą: https://doi: 10.15388/Im.2015.72.9223.

Teisės norminiai aktai

Tarptautinės sutartys

23. Tarptautinio Teisingumo Teismo statutas (1946). *Valstybės žinios*, 2002, 15-557.

24. Visuotinė žmogaus teisių deklaracija (1948). *Valstybės žinios*, 2006, 68-2497.

Europos Sąjungos teisės norminiai aktai

25. Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). OJ L 119.

Lietuvos teisės norminiai aktai

26. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo Nr. I-1374 pakeitimo įstatymas (2018). TAR, 11733.

27. Valstybinės duomenų apsaugos inspekcijos direktoriaus 2019 m. kovo 14 d. įsakymas Nr. 1T-35 (1.12.E) „Dėl duomenų tvarkymo operacijų, kurioms taikomas reikalavimas atlikti poveikio duomenų apsaugai vertinimą, sąrašo patvirtinimo“. TAR, 4104.

***Soft law* šaltiniai**

28. ES 29 str. duomenų apsaugos darbo grupė (2007). Nuomonė Nr. 4/2007 dėl asmens duomenų sąvokos, birželio 20 d. [interaktyvus. Žiūrėta 2021 m. balandžio 19 d.]. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_lt.pdf.

29. ES 29 str. duomenų apsaugos darbo grupė (2013). Nuomonė Nr. 03/2013 dėl tikslo ribojimo, balandžio 2 d. [interaktyvus. Žiūrėta 2021 m. balandžio 19 d.]. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

30. ES 29 str. duomenų apsaugos darbo grupė (2014). Nuomonė Nr. 8/2014 dėl naujausių daiktų interneto pokyčių, rugsėjo 16 d. [interaktyvus. Žiūrėta 2021 m. balandžio 19 d.]. Prieiga per internetą: https://www.pdpjournals.com/docs/88440.pdf.

31. Europos duomenų apsaugos priežiūros pareigūnas (2015). Nuomonė Nr. 4/2015, rugsėjo 11 d. [interaktyvus. Žiūrėta 2021 m. balandžio 19 d.]. Prieiga per internetą: https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_lt.pdf.

32. ES 29 str. duomenų apsaugos darbo grupė (2016). Skaidrumo užtikrinimo pagal Reglamentą (ES) 2016/679 gairės, lapkričio 29 d. [interaktyvus. Žiūrėta 2021 m. balandžio 19 d.]. Prieiga per internetą: https://www.teismai.lt/data/public/uploads/2020/02/20180411_skaidrumo_uztikrinimo_gaires.pdf.

33. ES 29 str. duomenų apsaugos darbo grupė (2017a). Teisės į duomenų perkeliamumą gairės, balandžio 5 d. [interaktyvus. Žiūrėta 2021 m. balandžio 19 d.]. Prieiga per internetą: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233.

34. ES 29 str. duomenų apsaugos darbo grupė (2017b). Automatizuoto atskirų sprendimų priėmimo ir profiliavimo pagal Reglamentą 2016/679 gairės, spalio 3 d. [interaktyvus. Žiūrėta 2021 m. balandžio 19 d.]. Prieiga per internetą: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.

35. Information Commisioner‘s Office (2017). Big data, artificial intelligence, machine learning and data protection, 4 September [interaktyvus. Žiūrėta 2021 m. balandžio 19 d.]. Prieiga per internetą: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf.

36. Europos duomenų apsaugos valdyba (2019). Gairės Nr. 3/2018 dėl Bendrojo duomenų apsaugos reglamento teritorinės taikymo srities (3 straipsnis), 2.1, lapkričio 12 d. [interaktyvus. Žiūrėta 2021 m. balandžio 19 d.]. Prieiga per internetą: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_consultation_lt.pdf.

37. Valstybinė duomenų apsaugos inspekcija (2019). Asmens duomenų apsaugos gairės smulkiajam ir vidutiniam verslui [interaktyvus. Žiūrėta 2021 m. balandžio 19 d.]. Prieiga per internetą: https://vdai.lrv.lt/uploads/vdai/documents/files/01_%20SolPriPa%20Asmens%20duomenu%20apsaugos%20gaires%20SMULKIAJAM%20IR%20VIDUTINIAM%20VERSLUI%202019-11-08.pdf.
38. Europos duomenų apsaugos valdyba (2020). Gairės 05/2020 dėl sutikimo pagal Reglamentą 2016/679, 1.1 versija, gegužės 4 d. [interaktyvus. Žiūrėta 2021 m. balandžio 19 d.]. Prieiga per internetą: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_lt_0.pdf.
39. Europos duomenų apsaugos valdyba (2021). Gairės 02/2021 dėl virtualių padėjėjų balsu, kovo 9 d. [interaktyvus. Žiūrėta 2021 m. balandžio 19 d.]. Prieiga per internetą: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_022021_virtual_voice_assistants_adopted-public-consultation_en.pdf.

Teismų praktika

40. *Breyer* [ESTT], Nr. C-582/14, [2014. spalio 19 d.]. ECLI:EU:C:2016:779.
41. *Google Spain ir Google* [ESTT], Nr. C-131/12, [2014 m. gegužės 13 d.]. ECLI:EU:C:2014:317.

Kiti šaltiniai

42. „Apple“ internetinis puslapis [interaktyvus. Žiūrėta 2021 m. balandžio 19 d.]. Prieiga per internetą: https://www.apple.com/watchos/feature-availability/.
43. Chokshi, N. (2018). Is Alexa Listening? Amazon Echo Sent Out Recording of Couple’s Conversation. *The New York Times* [interaktyvus. Žiūrėta 2021 m. balandžio 19 d.]. Prieiga per internetą: https://www.nytimes.com/2018/05/25/business/amazon-alexa-conversation-shared-echo.html.
44. Oficialiosios statistikos portalas. Skaitmeninė ekonomika ir visuomenė Lietuvoje (2020 m. leidimas): Daiktų internetas. [interaktyvus. Žiūrėta 2021 m. balandžio 19 d.]. Prieiga per internetą: https://osp.stat.gov.lt/skaitmenine-ekonomika-ir-visuomene-lietuvoje-2020/daiktu-internetas.
45. „Samsung“ internetinis puslapis (2020). How Tizen is Expanding Smart TV Experiences [interaktyvus. Žiūrėta 2021 m. balandžio 19 d.]. Prieiga per internetą: https://news.samsung.com/global/making-tvs-smarter-1-how-tizen-is-expanding-smart-tv-experiences.

SANTRAUKA

Daiktų interneto (IoT) reguliavimas pagal ES Bendrąjį duomenų apsaugos reglamentą

Leila Abi Chaker

Darbo pradžioje yra išanalizuojama, kokia apimti, dėl daiktų interneto savybių, bei juo renkamų duomenų specifikos yra taikomas BDAR. Vėliau darbe yra nagrinėjama atskirų BDAR normų taikymas daiktų internetui. Viso darbo rašymo metu, siekiant išnagrinėti ir identifikuoti probleminius BDAR taikymo daiktų internete aspektus buvo remiamasi *soft law* šaltiniais, ypač ES 29 straipsnio darbo grupės nuomonėmis, gairėmis, bei tarptautine teisės doktrina.

Magistriniame darbe yra analizuojama daiktų interneto savybių keliama problematika siekiant taikyti BDAR normomis įtvirtintus duomenų apsaugos teisės principus: teisėtumo, sąžiningumo ir skaidrumo, tikslo apribojimo, duomenų kiekio mažinimo, duomenų tikslumo, saugojimo trukmės apribojimo, atskaitomybės bei pareiga turėti duomenų tvarkymo pagrindą.

Taip pat darbe yra nagrinėjama, kaip daiktų internete yra užtikrinamos BDAR numatytos duomenų subjektų teisės būti informuotam apie duomenų tvarkymą, nesutikti su duomenų tvarkymu, apriboti duomenų tvarkymą, būti pamirštam, susipažinti su duomenimis ir juos ištaisyti bei teisė į duomenų perkeliamumą. Šios teisės analizuojamos taip pat atsižvelgiant į tai, jog daiktų interneto technologijomis asmens duomenys yra tvarkomi automatizuotomis priemonėmis (įskaitant profiliavimą).

Atsižvelgiant į daiktų interneto ypatybes bei svarbą užtikrinti skaidrumo principą, pasitikėjimą daiktų internete tarp duomenų valdytojo ir duomenų subjekto buvo analizuojami kai kurie BDAR numatyti reikalavimai: pareiga pranešti apie duomenų saugumo pažeidimą, poveikio duomenų apsaugai vertinimas, pareiga turėti duomenų apsaugos pareigūną.

SUMMARY

Regulation of the Internet of Things (IoT) under the EU General Data Protection Regulation

Leila Abi Chaker

First, the thesis analyses to what extent GDPR is applied in the Internet of Things, due to the features of the Internet of Things and the specifics of the data collected by it. Later in the work, the application of separate BDAR norms to the Internet of Things is examined. Throughout the paper, soft law sources, in particular, the opinions and guidelines of the Article 29 EU Working Party also international legal doctrine were used to examine and identify problematic aspects of the application of GDPR in the Internet of Things.

The master's thesis examines the problematic aspects of properly applying data protection principles enshrined in GDPR to the Internet of Things. The studied principles are: legality, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, accountability and the obligation to have a data processing basis.

The thesis also examines how the rights of data subjects to be informed about data processing, to object to data processing, to restrict data processing, to be forgotten, to access and rectify data and the right to data portability are ensured in the Internet of Things. These rights are also analysed in the light of the fact that personal data on the Internet of Things are processed by automated means (including profiling).

Given the nature of the IoT and the importance of ensuring the principle of transparency, the IoT trust between the controller and the data subject the author analyses some of the requirements of the GDPR: the obligation to report a data breach, the data protection impact assessment, the obligation to have a data protection officer.